

Blue Text - Brad

Green Text - Garrett

8/27/2021

Lab 1

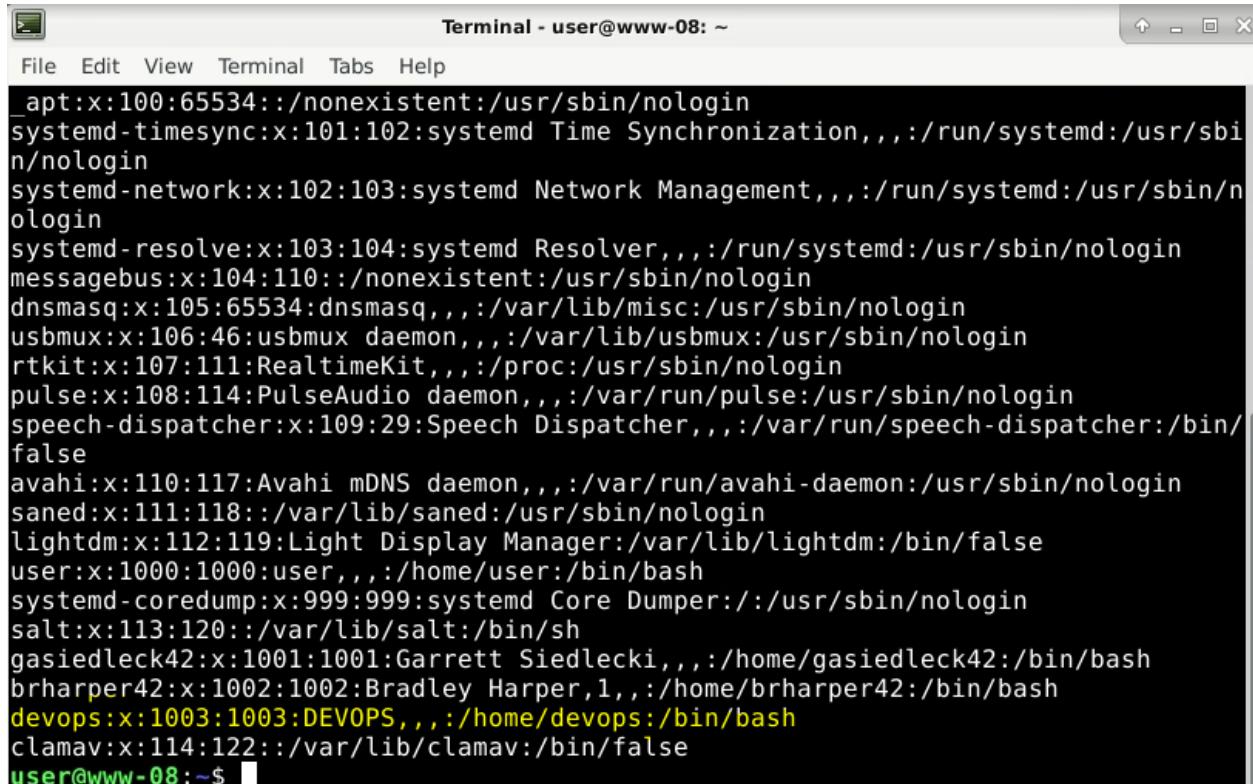
- Workstation
 - Updated Windows 10
 - Updated Local Admin Password
 Password: wiEAF#oXG%pPDNa^
 - Verified Network Settings
 - IP: 192.168.8.3
 - Subnet mask: 255.255.255.128
 - Gateway: 192.168.8.1
 - DNS: 192.168.1.1
- pfSense Router
 - Username and Password verified to provide admin access to system
 - New user created with admin privileges
 - Username: pfsensei
 - Password: CtyJ5BWPJMD4yHJ
 - Router updated
 - Version: 2.4.5-RELEASE-p1
- Windows Server 2016
 - Forced password for admin using 'net user Administrator /passwordreq:yes' in powershell
 - Added "Roles and Features" to begin configuring active directory
 - NEXT Step is clicking yellow triangle and adding domain
 - Clicked triangle to add domain and created new forest
 - Host domain set to pompeii08.net
 - Password is MountVesuvius08
 - AD is configured
 - NEXT step is join windows 10 system to domain
 - Joined windows 10 system to domain
 - Pass: P@ssw0rd!
- Debian Server
 - Updated user password
 - Password: P@\$word
 - New user created for Garrett
 - Username: gasiedleck42
 - Password: P@\$word
 - New user created for Bradley
 - Username: brharper42
 - Password: P@\$word
 - System updated with "apt-get update | apt-get upgrade"

- Installed Apache2
 - Installed PHP7
- Windows 10 Management Laptop
 - Nothing to do here, used in later labs

9/1/2021

Lab2

- Debian Server
 - Added user “devops”
 - Password: Password123!

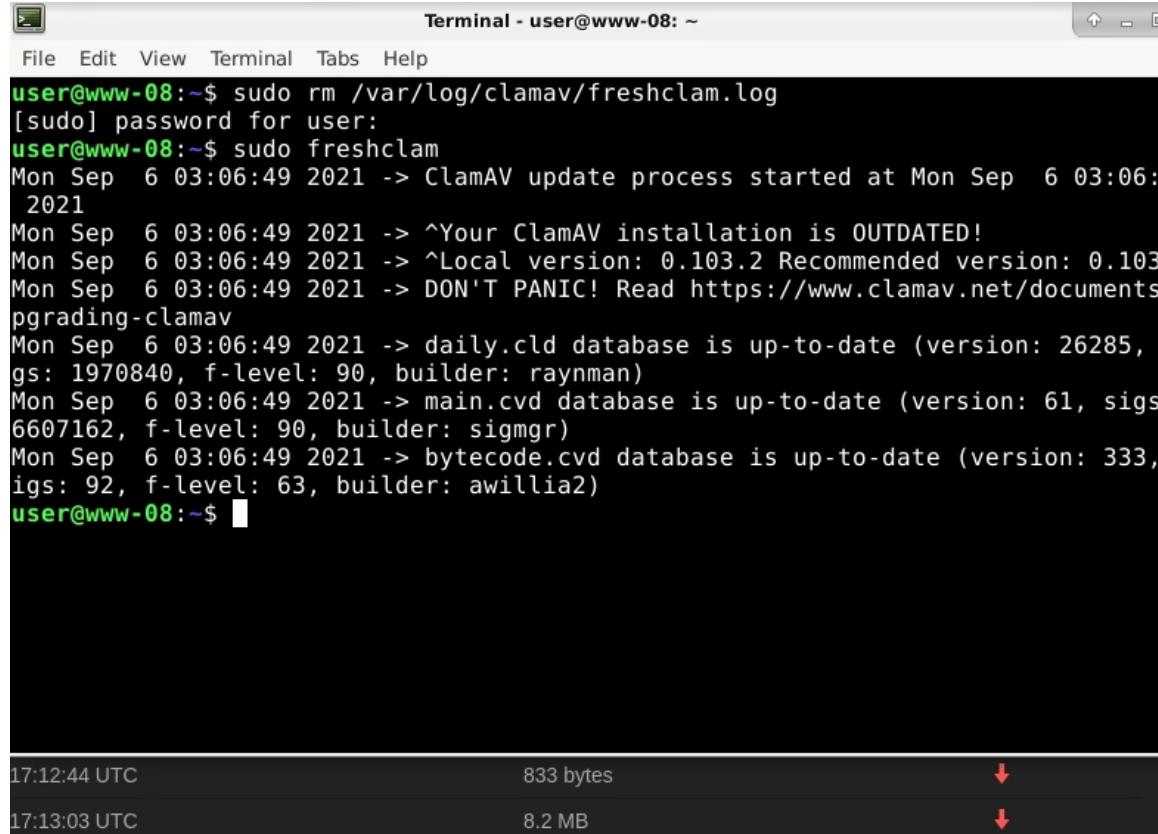


```

Terminal - user@www-08: ~
File Edit View Terminal Tabs Help
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
dnsmasq:x:105:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:107:111:RealtimeKit,,,:/proc:/usr/sbin/nologin
pulse:x:108:114:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:109:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
avahi:x:110:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:111:118::/var/lib/saned:/usr/sbin/nologin
lightdm:x:112:119:Light Display Manager:/var/lib/lightdm:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
salt:x:113:120::/var/lib/salt:/bin/sh
gasiedleck42:x:1001:1001:Garrett Siedlecki,,,:/home/gasiedleck42:/bin/bash
brharper42:x:1002:1002:Bradley Harper,1,,,:/home;brharper42:/bin/bash
devops:x:1003:1003:DEVOPS,,,:/home/devops:/bin/bash
clamav:x:114:122::/var/lib/clamav:/bin/false
user@www-08:~$ 

```

- Added user “devops” to sudo group
- Installed ClamAV (OUTDATED)
- Scanned with sudo freshclam



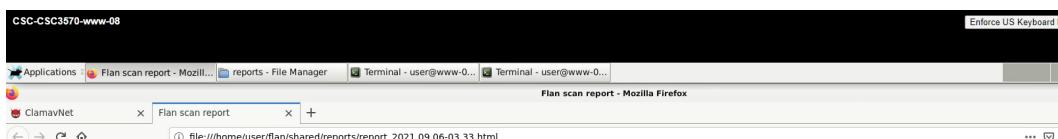
```

Terminal - user@www-08: ~
File Edit View Terminal Tabs Help
user@www-08:~$ sudo rm /var/log/clamav/freshclam.log
[sudo] password for user:
user@www-08:~$ sudo freshclam
Mon Sep  6 03:06:49 2021 -> ClamAV update process started at Mon Sep  6 03:06:49 2021
Mon Sep  6 03:06:49 2021 -> ^Your ClamAV installation is OUTDATED!
Mon Sep  6 03:06:49 2021 -> ^Local version: 0.103.2 Recommended version: 0.103.2
Mon Sep  6 03:06:49 2021 -> DON'T PANIC! Read https://www.clamav.net/documents/upgrading-clamav
Mon Sep  6 03:06:49 2021 -> daily.cld database is up-to-date (version: 26285, gs: 1970840, f-level: 90, builder: raynman)
Mon Sep  6 03:06:49 2021 -> main.cvd database is up-to-date (version: 61, sigs: 6607162, f-level: 90, builder: sigmgr)
Mon Sep  6 03:06:49 2021 -> bytecode.cvd database is up-to-date (version: 333, sigs: 92, f-level: 63, builder: awillia2)
user@www-08:~$ █

```

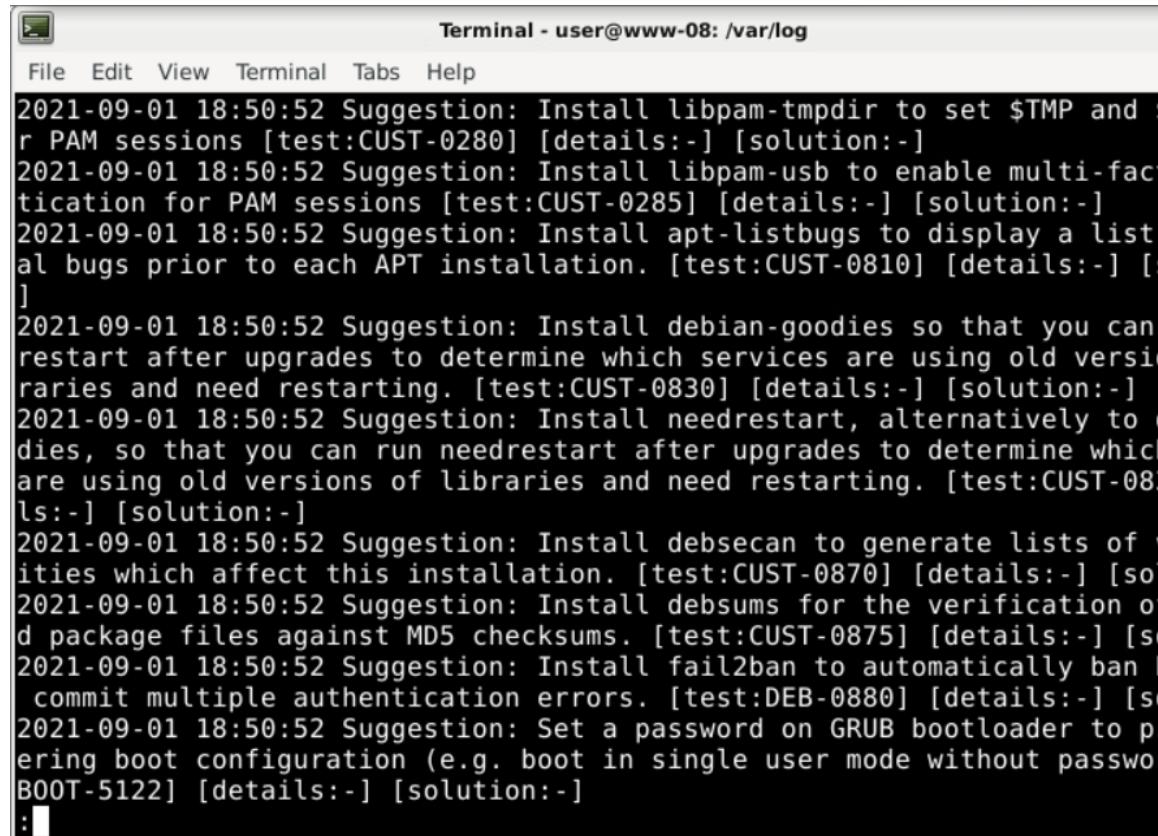
17:12:44 UTC	833 bytes	↓
17:13:03 UTC	8.2 MB	↓

- Installed curl
- Installed git
- Installed make
- Installed docker
- Ran flan scan



- Installed lynis
- Ran a system audit with lynis "sudo lynis system audit -q"

- Analyzed list of suggestions from lynis by issuing command “grep -i Suggestion /var/log/lynis.log | less”



A terminal window titled "Terminal - user@www-08: /var/log". The window displays a list of security suggestions from the lynis log. The suggestions include:

- 2021-09-01 18:50:52 Suggestion: Install libpam-tmpdir to set \$TMP and \$HOME for PAM sessions [test:CUST-0280] [details:-] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Install libpam-usb to enable multi-factor authentication for PAM sessions [test:CUST-0285] [details:-] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Install apt-listbugs to display a list of all bugs prior to each APT installation. [test:CUST-0810] [details:-] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Install debian-goodies so that you can run dpkg --purge --force-reinstreq to determine which services are using old versions of libraries and need restarting. [test:CUST-0830] [details:-] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Install needrestart, alternatively to dpkg --purge --force-reinstreq, so that you can run needrestart after upgrades to determine which services are using old versions of libraries and need restarting. [test:CUST-0830] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Install debsecan to generate lists of dependencies which affect this installation. [test:CUST-0870] [details:-] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Install debsums for the verification of package files against MD5 checksums. [test:CUST-0875] [details:-] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Install fail2ban to automatically ban hosts that commit multiple authentication errors. [test:DEB-0880] [details:-] [solution:-]
- 2021-09-01 18:50:52 Suggestion: Set a password on GRUB bootloader to prevent boot configuration (e.g. boot in single user mode without password). [test:GRUB-5122] [details:-] [solution:-]

- Windows Server 16

- Devops user created with password: Password123!

CSC-CSC3570-DC-08

Server Manager

◀ ▶ Server Manager ▷ Dashboard

User Accounts

Users Advanced



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
Administrator	POMPEII08	Administrators
devops	POMPEII08	Administrators

Add...

Remove

Properties

Password for Administrator



To change your password, press Ctrl-Alt-Del and select Change Password.

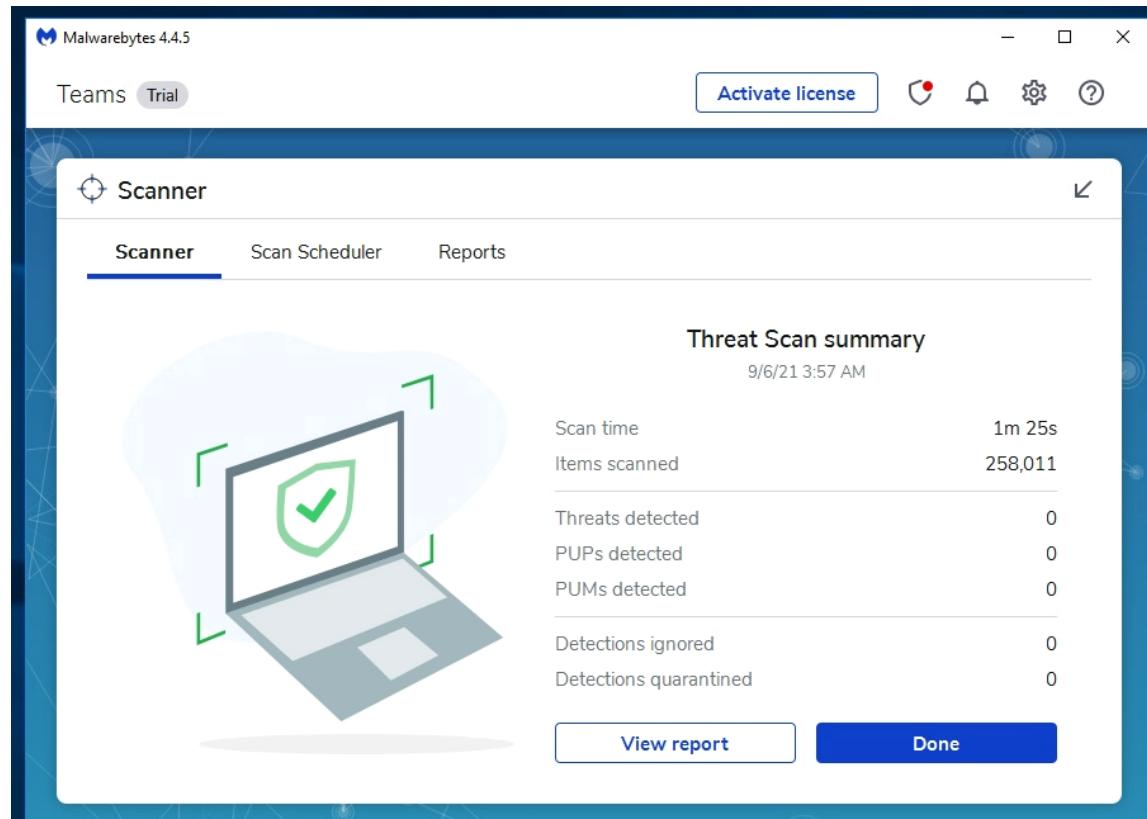
Reset Password...

OK

Cancel

Apply

- Installed malwarebytes and scanned



- Workstation
 - Installed Malwarebytes Free
 - Ran Malwarebytes scan
 - No threats detected

Scanner

Scanner Scan Scheduler Reports

Threat Scan summary
9/6/21 2:46 AM

Scan time	4m 57s
Items scanned	295,832
Threats detected	0
PUPs detected	0
PUMs detected	0
Detections ignored	0
Detections quarantined	0

[View report](#) [Done](#)



Deliverable Part 2:

1. CVE-2017-15710 In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials.
 - a. All httpd users should upgrade to 2.4.30 or later.
2. CVE-2018-1303 A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
 - a. All httpd users should upgrade to 2.4.30 or later.
3. CVE-2019-0217 In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
 - a. All httpd users deploying mod_auth_digest should upgrade to 2.4.39 or later.

Deliverable Part 3:

>Install libpam-tmpdir to set \$TMP and \$TMPDIR for PAM sessions

>>Many programs use \$TMPDIR for storing temporary files. Not all of them are good at securing the permissions of those files. libpam-tmpdir sets \$TMPDIR and \$TMP for PAM sessions and sets the permissions quite tight. This helps system security by having an extra layer of security, making such symlink attacks and other /tmp based attacks harder or impossible

>Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting

>>you want to know which packages occupy the most disk space, or which package might have broken another, or to get a most recent version of a package, or just to get a particular version of a package, then you probably need Debian-goodies.

>Configure minimum password for age

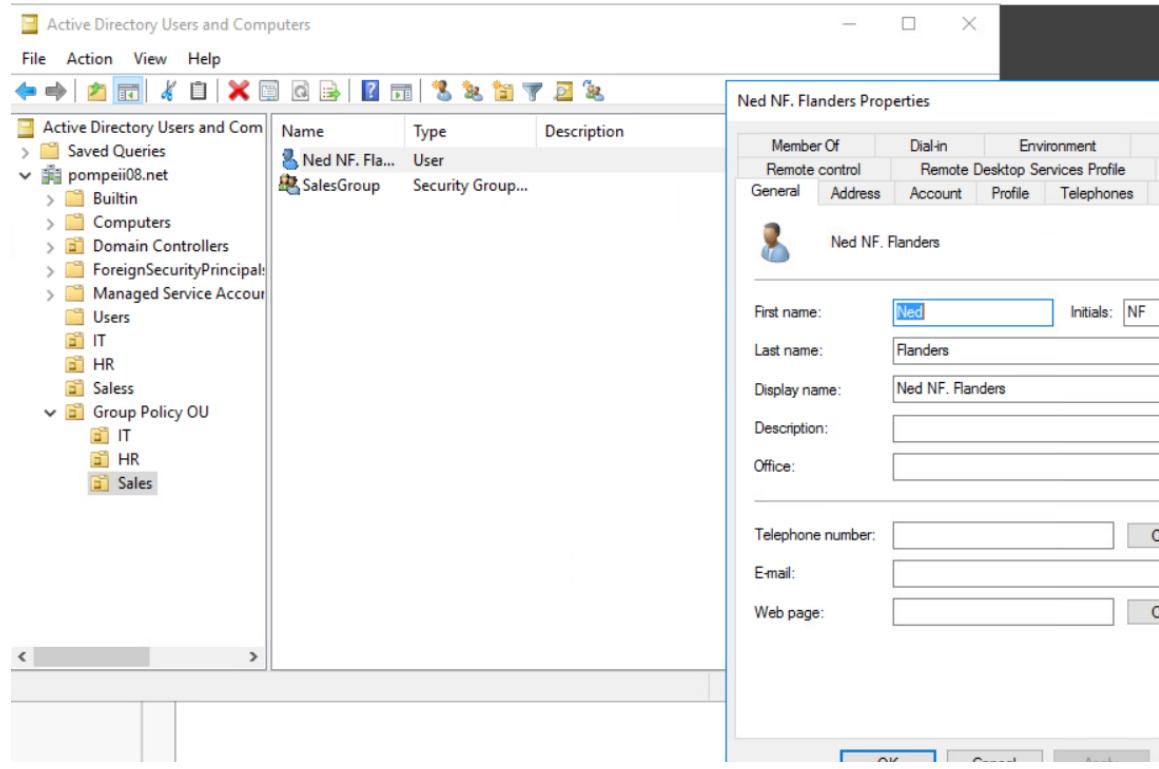
So that passwords are more difficult to guess/crack

Deliverable Part 4:

Weed

Lab 03 P1 09/15/2021

- Windows Server 2016
 - Created Organizational Units for:
 - HR
 - IT
 - Sales
 - Created Security Groups for:
 - HR
 - IT
 - Sales
 - Created user Herbert Garrison in IT using:
 - user: hgarrison
 - Password: pompeii123! (must change at next login)
 - Created user Dwight Schrute in HR using:
 - user: dshrule
 - Password: pompeii123! (must change at next login)
 - Created user Ned Flanders in Sales using:
 - user: nflanders
 - Password: pompeii123! (must change at next login)



- ○ Created a test GPO
- Created GPO for:
 - Set minimum password length (your choice - use best practice)
 - Enable password Complexity
 - Account lockout policy (use best practice)
 - Disable guest account
 - Deny guest account logon as service, or via RDP
 - Display a banner at logon: "Warning: Pompeii employees only.
Logging on to this machine means that you understand and accept
Pompeii's acceptable use policy."
 - Disallow users from creating or logging in with Microsoft accounts
 - Configure machine inactivity limit to lock screen when user is idle
 - Do not allow anonymous enumeration of SAM accounts
 - Do not allow any shared drives to be accessed anonymously
 - Do not store LAN Manager hash values
 - Set LAN Manager authentication to only NTLMv2
 - Configure account logon/logoff audit policy
 - Configure privilege use audit policy
 - Configure log retention policy
 - Set wallpaper on every account to a standard background (your choice)

The screenshot shows the Windows Group Policy Management console. On the left, a navigation pane lists several OUs and GPOs. Under 'Group Policy Objects', the 'SetWallpaperPolicy' GPO is selected. The main pane on the right is titled 'SetWallpaperPolicy' and contains the following sections:

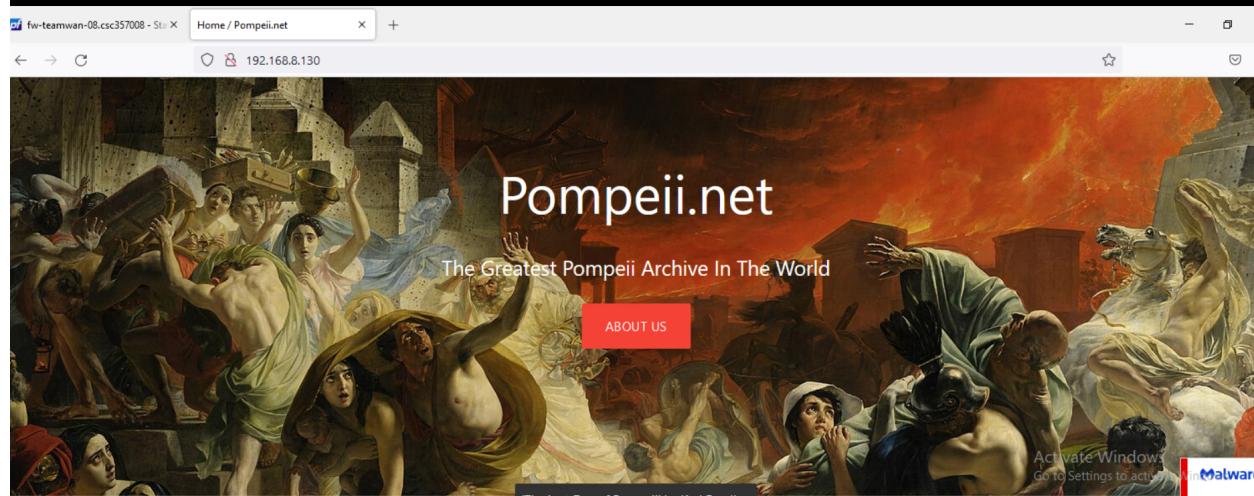
- Links:** Displays a link to 'pompeii08.net'.
- Security Filtering:** Shows that the policy applies to 'Authenticated Users'.
- WMI Filtering:** Indicates that the GPO is linked to a WMI filter named '<none>'.

- **Debian Server**
 - Cloned PompeiiSite to machine through git
 - Changed execute permission to true for
 - Install_webserver.sh
 - Install_mysql.sh
 - Update_webserver.sh
 - Ran ./install_webserver.sh
 - 'dev' group added to system
 - User 'devops' added to the group 'dev'
 - Folder 'devops' added to the root directory
 - Owner of folder 'devops' changed to 'devops' user

```
gasiedleck42@www-08:/devops$ ls -al
total 8
drwxr-xr-x  2 devops  root  4096 Sep 15 18:19 .
drwxr-xr-x 20 root   root  4096 Sep 15 18:19 ..
```

- Workstation

- Verified Website is accessible on local network through Workstation



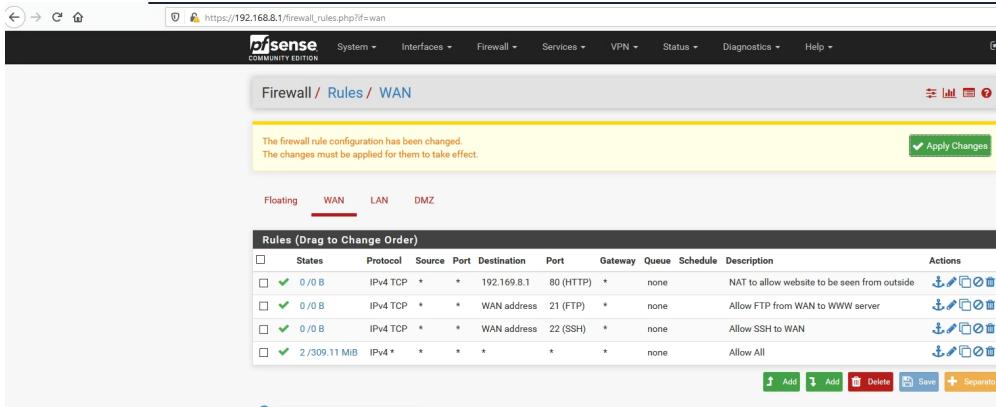
-
- Deliverables
- SCREENSHOTS ADDED WITHIN CHANGELOG
- Group Policies are designed to enable IT admins to centrally manage users and computers across an AD domain. This allows IT admins to easily automate one-to-many management of users and computers, as well as apply policy settings as a whole. It simplifies administrative tasks and reduces IT costs.
- A sticky bit is a permission bit that is set on a file or a directory that lets only the owner of the file/directory or the root user to delete or rename the file. No other user is given privileges to delete the file created by some other user. This ensures that no user can delete (or rename) another user's files by accident.

Lab 03 P2 09/15/2021

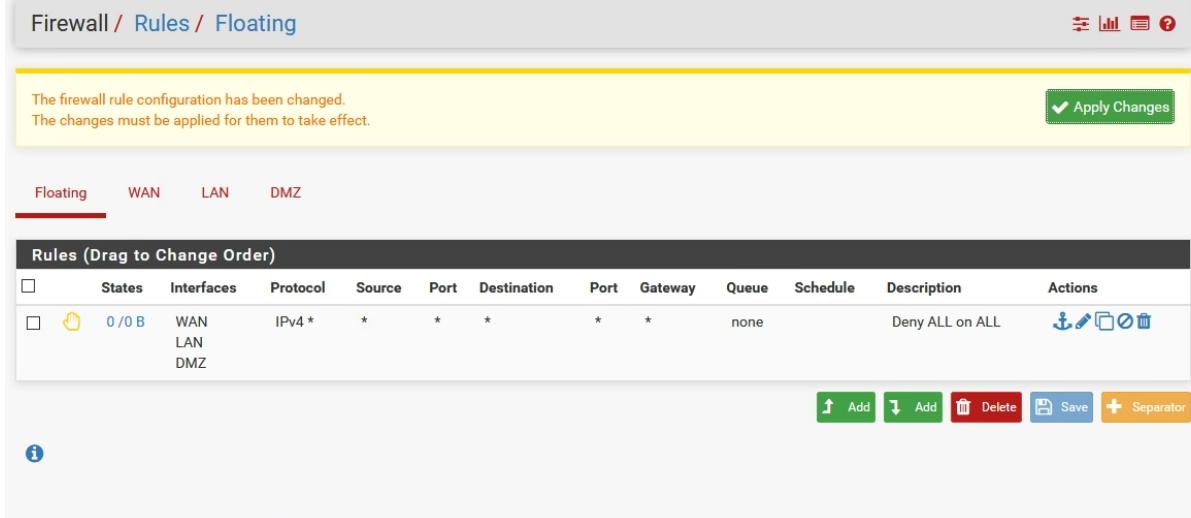
- Windows server 2016
 - Wrote two scripts
 - Add Users from CSV
 - Add gpo one liners
 - Created admin accounts
 - brharper42
 - Password123!
 - Password123? (Updated)
 - Florence123?
 - gasiedleck42
 - Password123! (change on next logon)

Lab 04 10/1/2021

- pfSense
 - Configured rule to make the www server accessible from the internet

○ 

- Changed opt1 to DMZ
- Allow SSH from WAN to WWW server
- Allow SSH from LAN to WWW server
- Allow FTP from WAN to WWW server
- Allow FTP from LAN to WWW server
- Allow the WWW to update (hint what port does Ubuntu use to update? UBUNTU mainly uses ports DNS on UDP 53 and HTTP on TCP 80 for its update services)
- Allow RDP from the MGMT laptop IP address to the DC
- Allow HTTP and HTTPS from LAN to WAN
- Allow DNS from LAN to WAN
- Allow DNS from DMZ to WAN
- Drop ICMP from Internet to WAN interface
- Deny all on all interface

○ 

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Deny Rules Below HERE											<input type="button" value="Delete"/>
<input type="checkbox"/>	X 0 / 0 B	IPv4 ICMP	*	*	WAN address	*	*	none		Drop ICMP from Internet to WAN interface	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
Allow Rules Below HERE											<input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	192.169.8.1	80 (HTTP)	*	none		NAT to allow website to be seen from outside	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	WAN address	21 (FTP)	*	none		Allow FTP from WAN to WWW server	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	WAN address	22 (SSH)	*	none		Allow SSH to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 2 / 309.79 MiB	IPv4 *	*	*	*	*	*	none		Allow All	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

ⓘ

Floating WAN LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0 / 141.82 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	<input type="button" value="Edit"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LAN address	*	WAN address	80 - 443	*	none		Allow HTTP and HTTPS from LAN to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LAN address	*	WAN address	53 (DNS)	*	none		Allow DNS from LAN to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	LAN address	21 (FTP)	*	none		Allow FTP from LAN to WWW server	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	LAN address	22 (SSH)	*	none		Allow SSH to LAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 3 / 2.68 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	*	*	*	*	*	none		Easy Rule: Passed from Firewall Log View	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

ⓘ

Floating WAN LAN DMZ

Firewall / Rules / DMZ

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	DMZ address	*	WAN address	53 (DNS)	*	none		Allow DNS from DMZ to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LAN address	*	WAN address	80 - 443	*	none		Allow HTTP and HTTPS from LAN to WAN	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 3 / 1.02 GiB	IPv4 *	*	*	*	*	*	none		Easy Rule: Passed from Firewall Log View	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	*	*	*	*	*	none		Easy Rule: Passed from Firewall Log View	<input type="button" value="Edit"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

ⓘ

- Disabled Allow * rules
- Left anti-lockout alone
- Only allow access to pfSense web console through HTTPS
- Only allow access to pfSense web console from Domain Controller
- Password protect the serial consolemenu (Hint:Advanced settings)

The screenshot shows the 'Serial Communications' configuration page in pfSense. At the top, there are two 'Add address' buttons: a light blue one and a green one labeled '+ Add address'. Below this is a section titled 'Serial Communications'.

Serial Terminal: A checkbox labeled 'Enables the first serial port with 115200/8/N/1 by default, or another speed selectable below.' Below it is a note: 'Note: This will redirect the console output and messages to the serial port. The console menu can still be used via a card/keyboard. A null modem serial cable or adapter is required to use the **serial** console.'

Serial Speed: A dropdown menu set to '115200' with a note: 'Allows selection of different speeds for the serial console port.'

Primary Console: A dropdown menu set to 'Serial Console' with a note: 'Select the preferred console if multiple consoles are present. The preferred console will show pfSense boot messages, console messages, and the console menu.'

Console Options: A section with a 'Console menu' checkbox checked, labeled 'Password protect the console menu'.

At the bottom is a 'Save' button with a disk icon.

-
- WWW server
 - ADDED RULES FOR:
 - Drop all incoming packets
 - Drop all outgoing packets
 - Allow incoming SSH from Domain Controller IP Address
 - Allow incoming SSH from WAN
 - Allow incoming HTTP and HTTPS from WAN
 - Allow outgoing HTTP and HTTPS
 - Allow outgoing DNS
 - Allow incoming DNS established connection
 - Allow outgoing SSH, HTTP, HTTPS established connections
- Deliverables
 - 1. The main benefit of a DMZ is to provide an internal network with an advanced security layer by restricting access to sensitive data and servers. A DMZ enables website visitors to obtain certain services while providing a buffer between them and the organization's private network.
 - 2. Web servers, Mail servers, FTP servers, and VoIP servers. To limit use from outside to these machines.

- 3. SSH - 22, RDP - 3389, HTTP - 80, HTTPS - 443 , DNS - 53
- 4. Egress network traffic is good so that inside users cannot relay sensitive data to outsiders or out of the internal network
- 5. Fail safe - in the event all else fails, deny all.
- 6. Access, we have denied access to many entrances of our network
- 7. Port 3389 allows for remote desktop, I am unsure if there is a better way, but I believe ssh
- 8. Packet filtering, the most basic kind
- 9. It conserves the number of public addresses used within an organization, and it allows for stricter control of access to resources on both sides of the firewall.

Lab 05 11/10/2021

1. Pfsense

- a. Installed snort
- b. Enabled Snort GPLv2 rules
- c. Enabled ET open
- d. Enable automatic unattended management of logs and 'Enable Directory Size Limit' and set it to 500MB
- e. Updated snort rules

Services / Snort / Updates

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Installed Rule Set MD5 Signature		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	85b7b5741119a5bb34e260057dfcc0f3	Thursday, 11-Nov-21 00:23:57 UTC
Emerging Threats Open Rules	39b4437e10e1b9bdf2c6c394e8a2ba80	Thursday, 11-Nov-21 00:24:02 UTC
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set		
Last Update	Nov-11 2021 00:24	Result: Success
Update Rules	<input checked="" type="button"/> Update Rules	<input type="button"/> Force Update
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.		

Interface to Inspect	WAN (vmx)	<input type="checkbox"/> Auto-refresh view	250	Save					
	Choose interface..		Alert lines to display.						
Alert Log Actions		Download	Clear						
Alert Log View Filter									
3 Entries in Active Log									
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID
2021-11-11 00:29:28		2	TCP	Potentially Bad Traffic	10.45.70.8	33179	10.0.0.250	80	1:
2021-11-11 00:29:28		1	TCP	A Network Trojan was Detected	10.45.70.8	33179	10.0.0.250	80	1:
2021-11-11 00:29:28		2	TCP	Potentially Bad Traffic	10.45.70.8	33179	10.0.0.250	80	1:

f.

Activate Wind

g.

Destination IP	DPort	GID:SID	Description
2.168.8.130	80	1:9000001	HTTP Traffic to WWW Detected
2.168.8.130	80	1:9000001	HTTP Traffic to WWW Detected
2.168.8.130	80	1:9000001	HTTP Traffic to WWW Detected
2.168.8.130	80	1:9000001	HTTP Traffic to WWW Detected
2.168.8.130	80	1:9000001	HTTP Traffic to WWW Detected
2.168.8.130	80	1:9000001	HTTP Traffic to WWW Detected
2.168.8.130	80	1:9000001	HTTP Traffic to WWW Detected

h.

1:9000004 RDP Traffic to Domain Controller
[+] X

1:9000001 HTTP Traffic to WWW Detected
[+] X

i.

1:9000003 SSH Traffic to WWW Detected
[+] X

j.

k.

```

# bantime = 1h

[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 10
bantime = 600

[iptabled-dropped]

enabled = true
filter = iptables-dropped
banaction = iptables-allports
port = all
logpath = /var/log/messages
bantime 600
max retry = 10

```

[Wrote 904 lines]

I. **^G Get Help** **^O Write Out** **^W Where Is** **^K Cut Text** **^L Justify**

Lab 06 10/25/2021

1. Question 1

- a. A Man-In-The-Middle (MITM) attack is achieved when an attacker poisons the ARP cache of two devices with the (48-bit) MAC address of their Ethernet NIC (Network Interface Card). Once the ARP cache has been successfully poisoned, each of the victim devices send all their packets to the attacker when communicating to the other device. This puts the attacker in the middle of the communications path between the two victim devices; hence the name Man-In-The-Middle (MITM) attack.
- b. It allows an attacker to easily monitor all communication between victim devices. The objective of this MITM attack is to take over a session. The intent is to intercept and view the information being passed between the two victim devices.
- c. 192.168.0.133
- d. Employing some sort of encryption so that the attacker cannot decipher the hijacked information.

2. Question 2

- a. SQL injection, SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.
 - b. TCP
 - c. Item=&search=latte%2C+chocolate
 - d. Information not intended for the attacker to see
3. Question 3
- a. Cross-site scripting, Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.
 - b. [http://192.168.0.133/xvwa/vulnerabilities/03/?item=<script>alert\("attack"\)<%2Fscript>](http://192.168.0.133/xvwa/vulnerabilities/03/?item=<script>alert('attack)
 - c. A javascript alert that outputs “attack”
 - d. Sanitize your input
4. Question 4
- a. Brute force attack, A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page.
 - b. Admin
 - c. lock out accounts after a defined number of incorrect password attempts.
5. Question 5
- a. Ping Flood Attack, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings.
 - b. 192.168.0.133
 - c. DoS (Denial of Service), intentionally interrupts services on the defending end
6. Question 6
- a. Network Scanning is taking place, The attacker is scanning the network for open ports by testing every port incrementally.
 - b. The attacker can figure out what open ports are open on a network, so that he can use them maliciously.

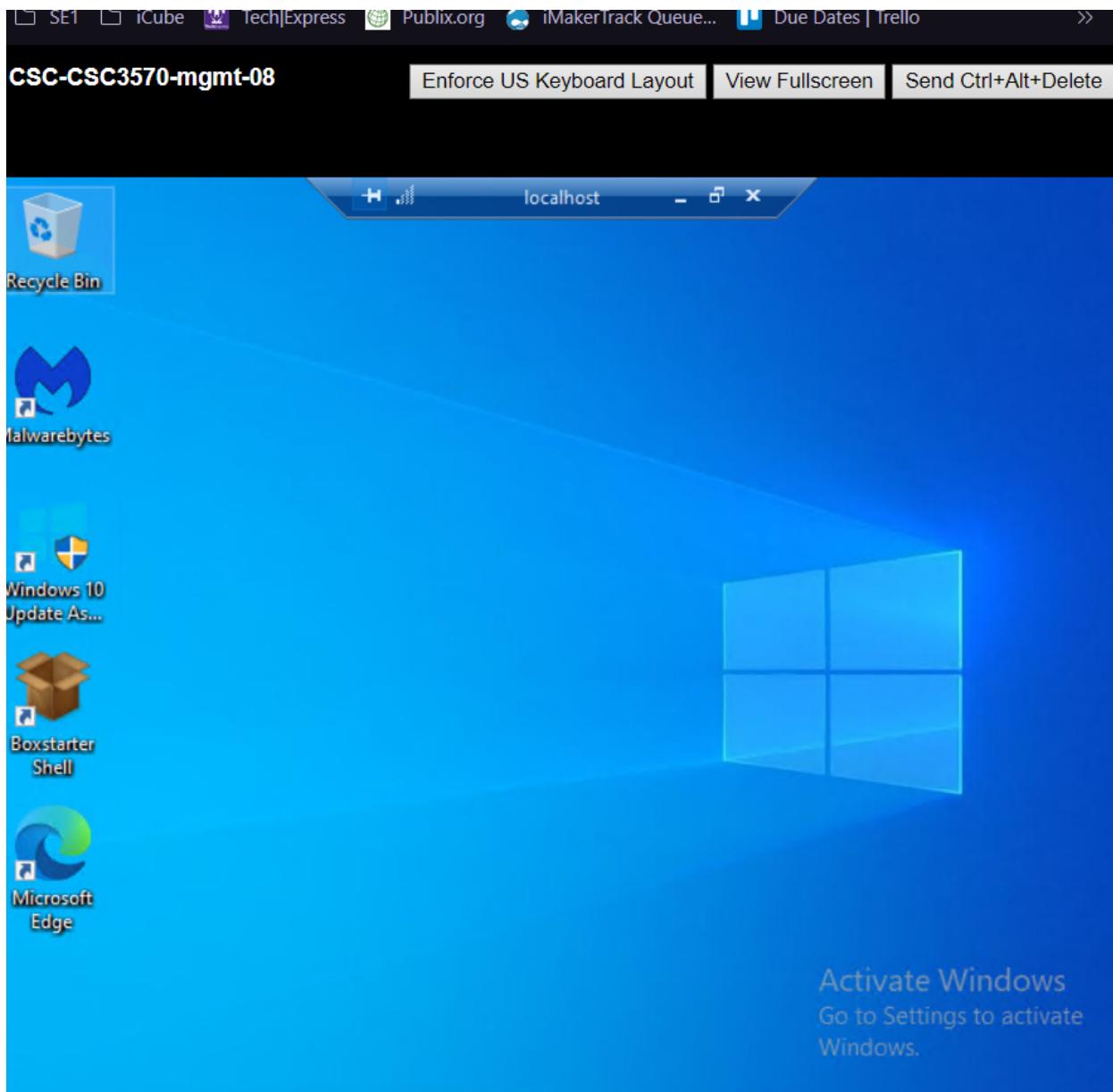
Lab 07 - 11/7/21

1. MGMT machine

- a. Tested ssh with ssh pfsensei@10.45.70.8
- b. Generated rsa private and public keys under
- c. Used type \$env:USERPROFILE\.ssh\id_rsa.pub | ssh {IP-ADDRESS-OR-FQDN}
"cat >> .ssh/authorized_keys" to copy
- d. Used ssh - i id_rsa.pub pfsensei@10.45.70.8 to connect with key
- e. Created a config file

```
Host Fun_Name_For_Me_To_Use
  Hostname 10.45.70.x
  User username_here
  IdentityFile ~/.ssh/keyfilehere
```

f.

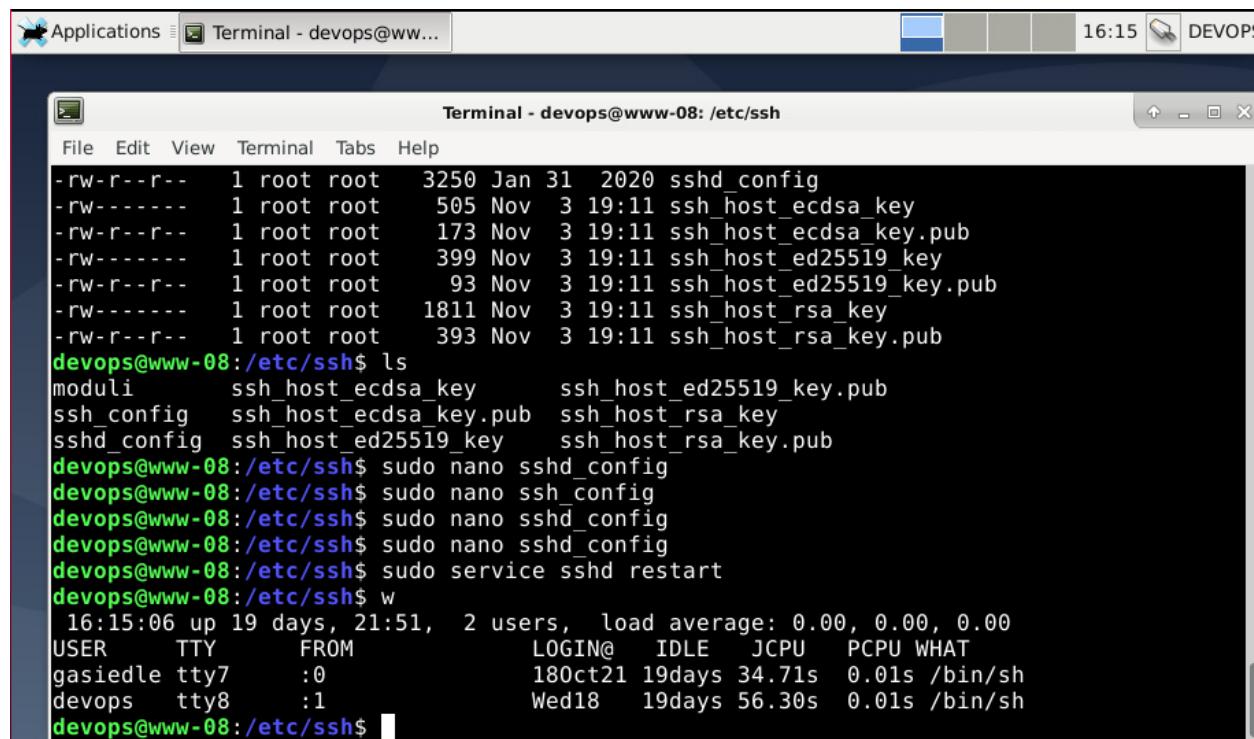


h. Start \Users\user> ssh FunHost -L 8888:192.168.8.3:443 -N

i.

2. WWW

- a. Installed ssh
- b. Changed sshd_config
 - i. Set PasswordAuthentication to no
 - ii. Set PublicKeyAuthentication to yes
 - iii. Set RSAAuthentication to yes
 - iv. Set PermitEmptyPasswords to no
 - v. Set ChallengeResponseAuthentication to no
- c. Restarted ssh service for changes to take effect



```
Applications Terminal - devops@www-08: /etc/ssh
File Edit View Terminal Tabs Help
-rw-r--r-- 1 root root 3250 Jan 31 2020 sshd_config
-rw----- 1 root root 505 Nov 3 19:11 ssh_host_ecdsa_key
-rw-r--r-- 1 root root 173 Nov 3 19:11 ssh_host_ecdsa_key.pub
-rw----- 1 root root 399 Nov 3 19:11 ssh_host_ed25519_key
-rw-r--r-- 1 root root 93 Nov 3 19:11 ssh_host_ed25519_key.pub
-rw----- 1 root root 1811 Nov 3 19:11 ssh_host_rsa_key
-rw-r--r-- 1 root root 393 Nov 3 19:11 ssh_host_rsa_key.pub
devops@www-08:/etc/ssh$ ls
moduli      ssh_host_ecdsa_key      ssh_host_ed25519_key.pub
ssh_config  ssh_host_ecdsa_key.pub  ssh_host_rsa_key
sshd_config ssh_host_ed25519_key  ssh_host_rsa_key.pub
devops@www-08:/etc/ssh$ sudo nano sshd_config
devops@www-08:/etc/ssh$ sudo nano ssh_config
devops@www-08:/etc/ssh$ sudo nano sshd_config
devops@www-08:/etc/ssh$ sudo nano sshd_config
devops@www-08:/etc/ssh$ sudo service sshd restart
devops@www-08:/etc/ssh$ w
16:15:06 up 19 days, 21:51, 2 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
gasiedle  tty7     :0          18Oct21  19days 34.71s  0.01s /bin/sh
devops    tty8     :1          Wed18    19days 56.30s  0.01s /bin/sh
devops@www-08:/etc/ssh$
```

3. Workstation

- a. Enabled rdp on workstation

4. Deliverables

- a. *above*
- b. The main difference between both technologies is that the SSH connects to a particular computer while a VPN connects to a network.
- c. Connecting to one machine
- d. The ip for the management machine 10.45.70.73
- e. Ssh keys allow users to have a way in while keeping unwanted users out by handing the wanted user a key to the door
- f. ssh FunHost -L 8888:192.168.8.3:443 -N

Lab 08 11/10/2021

1. pfSense

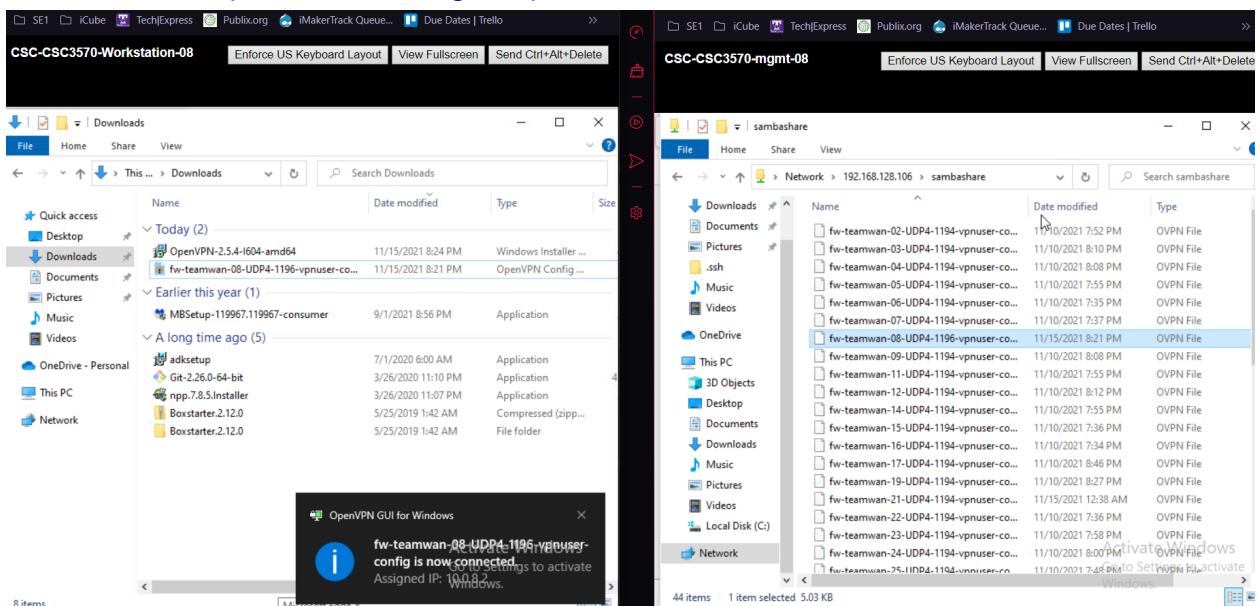
- a. Added allow rule for WAN on port 1194
- b. Created a vpn user + user certificate
 - i. vpnuser
 - ii. password123!
- c. Created an openVPN server
- d. Installed openvpn-client-export
- e. Exported the client config to the sambashare

2. MGMT laptop

- a. Install OpenVPN
- b. Import custom config from

3. Workstation

- a. Installed openVPN
- b. Downloaded the config file
- c. Imported the config to openVPN and connected



Lab 09 11/17/2021

1. WWW Server

- a. Created backups dir in '/'
- b. Created script to archive \$HOME and naming it with current date and time
- c. Added crontab to execute script every day at 3:00 AM local machine time

- d. Added crontab and scripts to stop Apache2 service at 5pm every day, and start apache2 service at 8am every day
2. Workstation

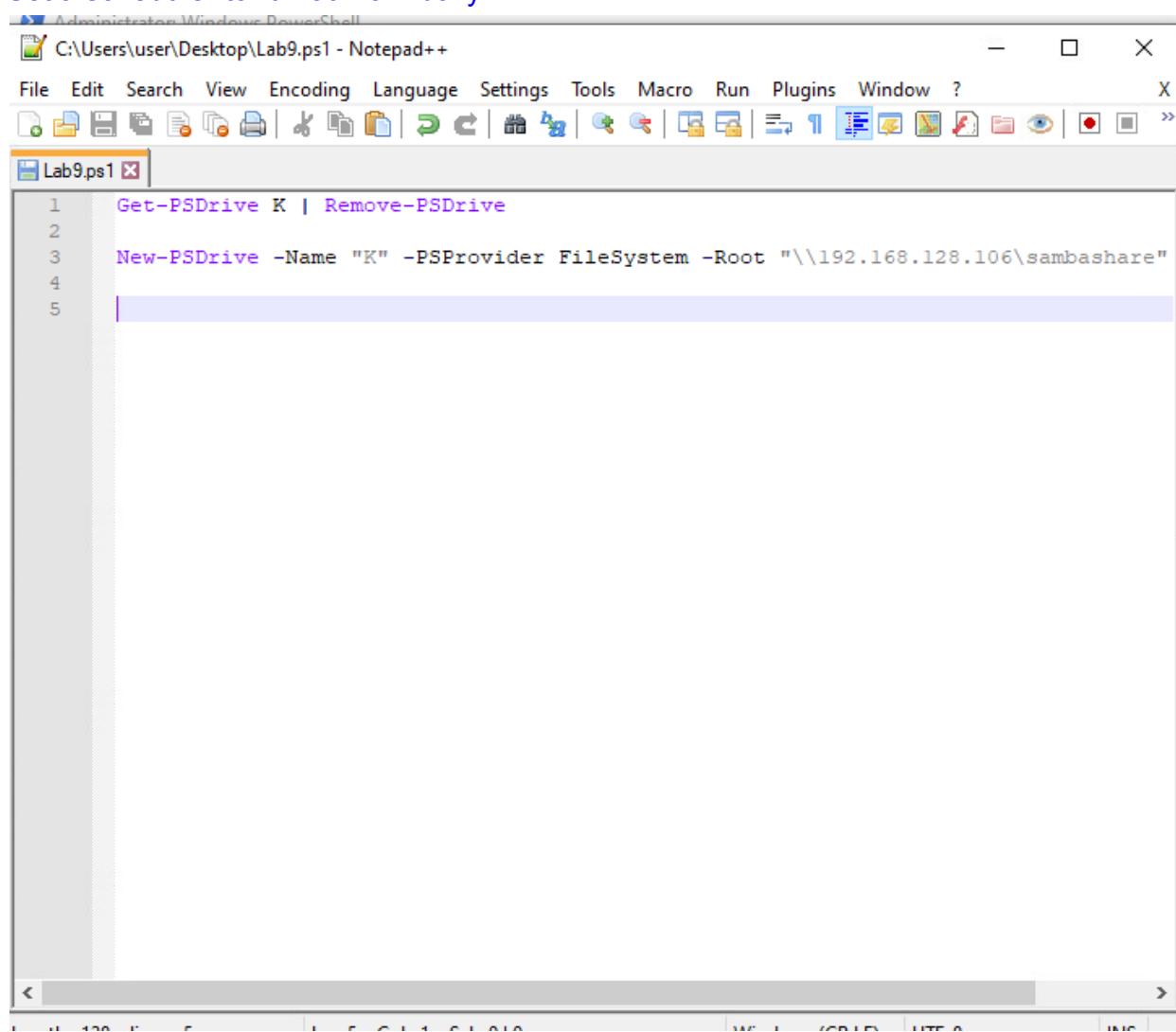
a. Attached sambashare to K

```
PS C:\WINDOWS\system32> Get-PSDrive -PSProvider "FileSystem"

Name      Used (GB)    Free (GB) Provider   Root
----      -----     -----   -----
C           25.81       5.58   FileSystem   C:\
K           4.45        7.29   FileSystem   \\192.168.128.106\sambashare

PS C:\WINDOWS\system32>
```

- b. Deleted k drive
c. Set a scheduler to run at 4 am daily

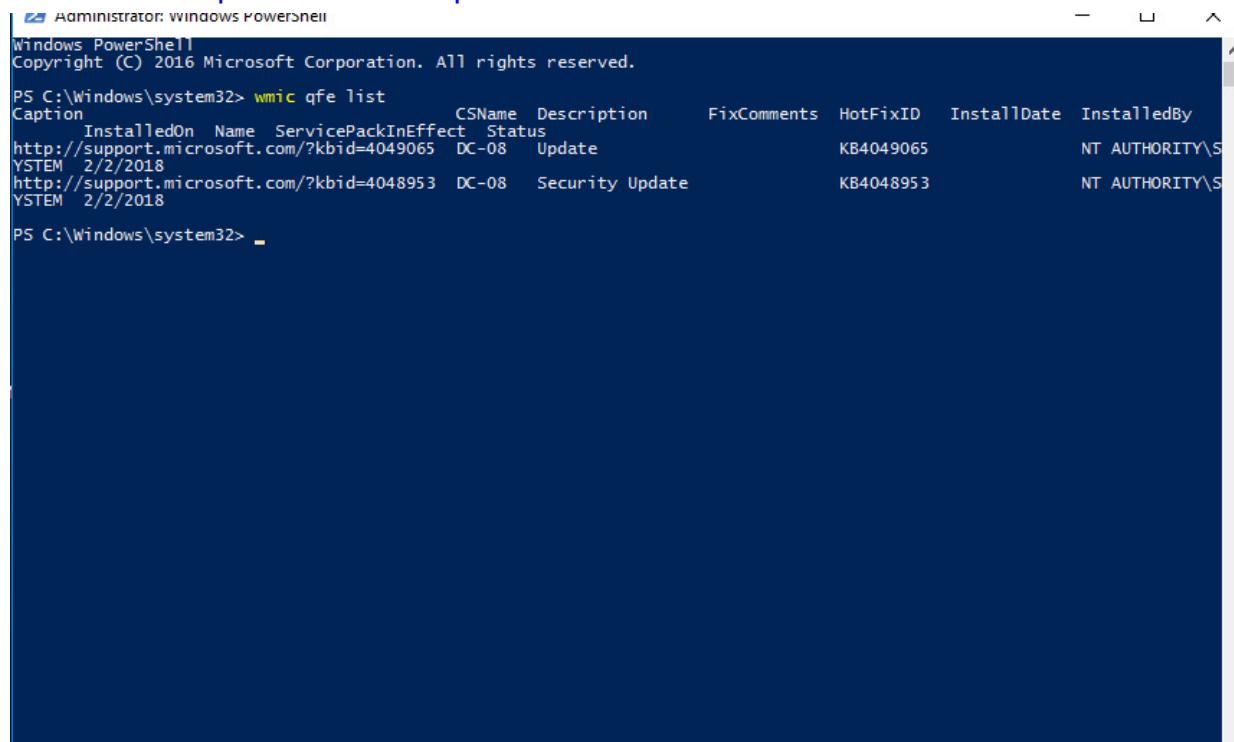


The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell' running in the background. In the foreground, a Notepad++ window is open with a tab labeled 'Lab9.ps1'. The code in the editor is as follows:

```
1 Get-PSDrive K | Remove-PSDrive
2
3 New-PSDrive -Name "K" -PSProvider FileSystem -Root "\\192.168.128.106\sambashare"
4
5
```

- d. Windows server 2016
3. Windows server 2016

- a. Used to wmic qfe list to check updates info

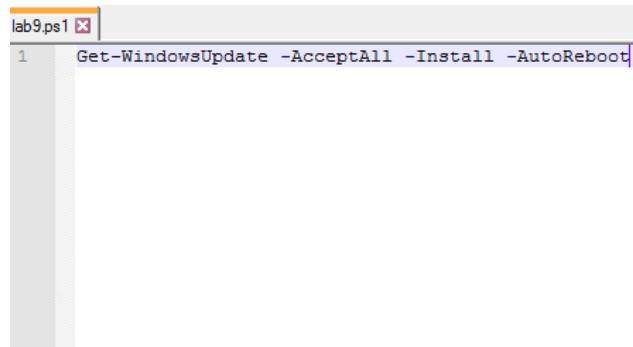


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> wmic qfe list
Caption           CSName   Description      FixComments  HotFixID   InstallDate  InstalledBy
InstalledOn       Name     ServicePackInEffect Status
http://support.microsoft.com/?kbid=4049065  DC-08    Update          KB4049065  2/2/2018    NT AUTHORITY\SYSTEM
http://support.microsoft.com/?kbid=4048953  DC-08    Security Update  KB4048953  2/2/2018    NT AUTHORITY\SYSTEM

PS C:\Windows\system32>
```

- b.



```
lab9.ps1
1 Get-WindowsUpdate -AcceptAll -Install -AutoReboot
```

- c.

4. Deliverables

- a. Changelog
- b. Screenshots
- c. Zip of scripts
- d. Update, Security Update
- e. Control Panel > System and Maintenance > Backup and Restore. Built in
- f. -D file