Student Name: Andrew Simon

Blue Team Final Achievement

Either: `Make a Copy of this in your personal Google Drive`

Or: `Download this template as .docx locally`

Use it to complete the Practical Challenges and document your work. When you have finished, export your document as a **.pdf** in the following syntax:

`cohortNumber_lastName_firstName.pdf`

Scenario

A fellow analyst believes that an attacker briefly authenticated to your company WiFi network and might have compromised some machines. Your colleague collected network traffic and ran two Splunk queries that might be helpful in your investigation. Attached are resources provided by the analyst for your evaluation.

Use the evidence files to answer the following questions. For each answer, include references to supporting evidence (be detailed!).

Document what steps you took to determine the information (ex. which wireshark searches did you run, which display filters did you use, and which packet numbers contained the information.)

Grading

Questions may be graded on **both** an answer and the supporting evidence. Some questions are subjective and can have more than one answer; include reasoning for full credit.

Answer each question in this file, where directed.

[Example:]

42. `(0 points)` What are the MAC and IP addresses for the host 'DESKTOP-UT31QVI'?

```
Answer:
MAC = '5C:26:0A:5B:C3:7B'
IP = 10.24.0.8

This was found by viewing the 'router_log.png' and
referencing the first entry, whose Device Name
matches the given hostname.
```

Scenario Questions (85 minutes)

Read every question before answering. Some questions may be easier to answer out of order. Each section has a suggested time to answer the questions.

Identify (suggested: 10 minutes)

Use the router logs and the `Statistics > IPv4 Statistics > Destinations and Ports` view in Wireshark to answer the question. The same information is found in `dst-and-ports.txt`.

1. (3.5 points) Who are the actors on this network, and what services might be running?

For each machine, fill out an entry in the table below. You may use fewer rows or add more rows as necessary. The first row is an example.

Listening/open ports are under 10000 (ten thousand).

ID	IPv4	MAC	Open Ports	Running Services
42	10.42.0.8	5c:26:0a:5b:c3:7b	8080, 25	python website, mailserver
1	10.42.0.33	B6:0E:AD:8A:58:36	53, 22	DNS server, ssh
2	10.42.0.41	38:63:9A:6D:5C:00	22	Ssh (victim)
3	10.42.0.91	B6:3F:B5:43:C1:0F	80, 1337	Webserver (attacker), Port 1337 socketed by attacker through Java
4	10.42.0.77	7E:4F:5D:06:17:8B	22, 9997	Splunk server, ssh
5				

Detect (suggested: 60 minutes)

2. (5 points) Which machines are likely the attacker and victim? Why?

[Example]: Machine 1 is the likely attacker and machine 2 is the likely victim. Packets 13100 through 13200 show evidence of a port scan from machine 1 to machine 2.

Answer: 10.42.0.91 seems to be the attacker, while 10.42.0.41 seems to be the victim. The TCP streams from 91 to 41 over port 22 show a shell being setup.(Looks like packets 8003-10,365 show his last activity setting up a shell over 22 before gettinging in) Once in, the TCP streams from 41 to 91 over port 1337 show the user using the “ls” and “cd” command to navigate through the files into root. Topped with signing “Tokyoneon was here”. (This activity on the machine took place between packets 10556 and 11892)

3. (5.5 points) What recon activity does the attacker perform on this network? What port or machine (choose one) is the single target of this recon? Reference a range of packet numbers.

[Example]: The attacker takes pictures of each house in the neighborhood, as seen in the video footage (timestamps 12:34 to 23:45). The target of these pictures is always the door of each house.

Answer:

10.42.0.91	35572	10.42.0.41	22	8
10.42.0.91	37900	10.42.0.77	22	4
10.42.0.91	59134	10.42.0.33	22	4

It looks like he starts by doing some sort of nmap scan on the other systems in the network. Or just seeing who is available to shell in through using port 22 (shown above). He directly follows this with small packet hits over 22 against the 41 system (shown below). This seems to have stared at the 803 packet going to around 5610. With some activity between the 41 machine and the 77 Splunk server in between.

```
10.42.0.91      35578 10.42.0.41      22
10.42.0.91      35580 10.42.0.41      22
10.42.0.91      35582 10.42.0.41      22
10.42.0.91      35584 10.42.0.41      22
10.42.0.91      35586 10.42.0.41      22
10.42.0.91      35588 10.42.0.41      22
10.42.0.91      35590 10.42.0.41      22
10.42.0.91      35592 10.42.0.41      22
```

This is backed up by the info on the dst-and-ports.txt file, where many ports are the destination for the 41 system only once. Indicating a port scan. (shown below)

```
10.42.0.41              5318
 UDP                    450
  65518                 1
  65495                 1
  65493                 1
  65484                 1
  65472                 1
  65443                 1
  65429                 1
  65411                 1
  65343                 1
  65339                 1
```

4. (5.75 points) What attack was carried out following the recon activities? Cite packets that show this attack, as well as evidence from one of the Splunk query logs that support your conclusions.

[Example]: The attacker picked the lock on the victim's front door. We see the attacker hunched over in the 'nestcam-01.png', as well as video footage of them at the door for 2 minutes before going inside.

Answer: This was a brute force attack. The attacker used SSH to shell into the system. Many failed password attempts were made before getting a correct login. All of the data in the splunk-auth file show the list of attempts through the 15 time stamp and around the 43 time stamp. All within seconds or even the same second. This shows this was automated login attempts at an inhuman speed. The time stamp on the splunk-exec file is marked around 41. This tells me with his success during the 15 time stamp he was able to talk with the Splunk server to create processes. He had to go back to attempt passwords again in order to shell in to navigate files and leave his signature “Tokyoneon was here”.

10.42.0.91	35662	10.42.0.41	22	1,628
10.42.0.41	50078	10.42.0.91	80	22
10.42.0.41	50109	10.42.0.77	9997	9
10.42.0.91	35664	10.42.0.41	22	2,306
10.42.0.41	50110	10.42.0.77	9997	9
10.42.0.41	50112	10.42.0.91	1337	1,123

I believe the story of these TCP conversations follows based on the TCP contents:
Line 1- Initial brute force attempt with success
Line 2- Once in, wrote some Java that allowed him access to the Splunk server
Line 3- On the victim machine (41) went to Splunk server to create processes
Line 4- Brute force attack #2 for further access
Line 5- More activity to the Splunk server
Line 6- Access to the system, able to ls directories and leave his signature

5. (5 points) Once the attacker gained access to the victim's machine, what executable did they first use to run commands on the host? Cite evidence from 'splunk-exec.csv'.

[Example]: The attacker used 'zsh', which is a type of shell. We see this command executing at 05:26:93 PM from the host logs.

Answer: The first three executables on the splunk-exec file seem to be centered around monitoring. The first one that has to do with being able to access a remote system is:

C:\Windows\System32\schtasks.exe, at 41.04 time stamp

After doing some research on this executable, it allows the user to create scheduled tasks on a remote computer.

6. (5 points) How did the attacker establish persistence on the machine? Either list the built-in command used or the binary that the attacker supplied (or both). Cite evidence from 'splunk-exec.csv' and/or 'network.pcap'.

[Example]: The attacker sent 'sharknado.exe' to the victim in packet 15203. They used 'cron' on the victim to schedule a reverse shell connection for persistence. We see evidence of 'cron' being launched from 'zsh' shortly after 05:26 PM in the host logs.

Answer:
Looking at the splunk-exec file we see that after the attacker started the schtasks.exe process to begin making changes he started the processes “splunk-powershell.exe” and “backgroundTaskHost.exe” at the 41:05 time stamp allowing him persistence to the machine.

Respond (suggested: 5 minutes)

7. (1.75 points) What containment strategy (segment, isolate, remove) would you use to respond to this attack? Why?

[Example]: Since the HR employee in question should not have access to the database that handles customer's PII, the best containment strategy for this particular is to segment the employee's machine on one network, and the database on to another network. This will reduce the overall possible attack vector for the database, and ensure that the HR employee does not have access to PII they should not have access to.

Answer: I would remove any processes this attacker left on the victim machine and ensure that he/she does not have access again through firewall rules. We have evidence they ran executables, so we must make sure they are removed. We would need to secure passwords of those cracked and make sure the attacker does not back in. Through our firewall rules we need to make sure shelling in through port 22 from that IP is not accessible.

Recover (suggested: 5 minutes)

8. (1.75 points) Why should you fully reinstall Windows on the victim machine?

[Example:] Since Windows XP is EOL, it is completely unsupported regarding new vulnerabilities that are discovered. It is best practice to remove the old version of Windows, and update to a modern version that is being updated as new vulnerabilities are discovered and exploited in the wild.

Answer:
As the attacker was striving to maintain persistence he set up ways to shell in and create a backdoor for himself. The victim's machine and OS is compromised. In order to make sure that the attacker can't use these tools they setup, we should do a full Windows reset.

Protect (suggested: 5 minutes)

9. (1.75 points) What is one defensive tool/measure that could prevent this attack? Explain how that tool/measure would have stopped this attack and specifically where in the attacker's steps it would work (cite packet numbers or evidence if necessary).

[Example]: One defense could be to lock the doors. This would have stopped the attacker from entering the house (exploitation), as we can see them doing in photo 'nestcam-01.png'.

Answer:
The victim system had port 22 available for ssh access. There could easily be a rule to prevent any or specific IPs from doing this through a firewall. This would take place at the attackers initial steps and trying to brute force a password. There could have also been a system in place that limits the amount or frequency of password attempts. Slowing and alerting the security team of a brute force attempt.

Snort Rule

In the previous scenario, the attacker was able to enumerate an open port and attack a discovered service.

Fill in the BLANKs to write a Snort rule that would catch **this one** attack in the future. Do **NOT** use 'any' in your answers.

Challenge:

```
alert {BLANK 1} 10.42.0.0/{BLANK 2} any -> {BLANK 3} {BLANK 4}
(msg:"Potential abuse detected!"; sid:1;)
```

Answer:

Blank 1:	TCP
Blank 2:	24
Blank 3:	10.32.0.41
Blank 4:	22

Scripting Challenges

Use **this log file** to answer the following questions. **You do NOT need to explain how you arrived at your conclusions.** These headers might help you parse the log file:

```
frame.num;frame.time;ip.src;tcp.srcport;ip.dst;tcp.dstport;ip.proto;ip.len;Proto;Info
```

1. Get a count of all the IP addresses in the '`ip.src`' field and the '`ip.dst`' field, and find the IP address which appears the **least**.

   Answer:
   192.168.25.102
   Once as dest. Once as a source. 2 total

2. How many lines in the log file are related to DNS queries to/from one of Google's public DNS servers?

   Answer:
   535 Total
   270 to 8.8.8.8
   265 to 8.8.4.4
