Task 2: Analyze av.pcap

1. What is the source IP making the request?

81.131.131.6

2. What is the destination?

80.239.144.76

3. What protocol is used to download the updates?

FTP

4. Is that protocol secured?

No

5. What username is used to login?

User Anonomyous

6. What does the RETR command do?

RETR stands for retrieve and it is used to download or retrieve a file from a FTP server or client.

7. How many files are retrieved in this PCAP?

8

8. What are the names of the files?

Line 26 - master.xml
Line 62 - avp.klb
Line 111 - avp.set
Line 169 - avp_x.set
Line 199 - black.lst
Line 237 - daily.avc
Line 402 - daily-ex.avc
Line 499 - daily-x.avc

Line 298 - ca.avc (never found directory)

9. How could an attacker use the information from the questions above?

Hackers can intercept ftp data which displays in plaintext. This can involve credential theft.

Hackers can use file paths to try and download sensitive information. In addition to mapping out networks as well.

Task 3: Analyze NetworkProtocol.pcap

1. What protocol is primarily used here?

SNMP (Simple Network Management Protocol)

2. What version is it?

Version #1

3. What is it used for?

SNMP is used for network management, monitoring network devices like routers, switches, printers, and servers. This protocol helps manage network performance and solve any issues

4. What is a community string?

Password-like value used in the SNMP protocol for authentication. This is used as a key that grants access to device configuration settings.

5. What community string is it using?

Public

6. What part of AAA would apply to this protocol?

Authentication

7. What part of CIA would apply to this protocol?

Confidentiality

8. What OID is packet 13 requesting? (Look after the get-request)

a. Use http://www.oid-info.com/search.htm to look up OIDs

NOTE: Drop the "0" from the end of the OID when you search

1.3.6.1.2.1.1.2

9. Why would an attacker want to know this information?

An attacker can learn and map out devices on a network to plan an attack with this information. By reading the oid it states that it is "Fred's router" This can be used as an attack vector in the future.

10. What OID is packet 21 requesting?

NOTE: Drop the "1.5" from the end of the OID when you search

Requesting a prtChanelState

1.3.6.1.2.1.43.14.1.1.6

11. Why would an attacker want to know this information?

If an attacker knows this information they can interfere or manipulate print jobs. For example an attacker can disrupt, capture, or inject malicious data into the print stream.

12. What OID is packet 27 requesting?

NOTE: Drop the "0" from the end of the OID when you search

Sys location

13. Why would an attacker want to know this information?

With this information a attacker can learn the physical location of the network hardware to plan a physical attack.

14. What OID is packet 29 requesting?

NOTE: Drop the "1" from the end of the OID when you search

ifphysaddress

15. Why would an attacker want to know this information?

An attacker has a lot of attack vectors once they have the mac address information. They can spoof devices on the network allowing them to impersonate legitimate devices, and intercept traffic.

16. What is packet 61 telling us?

This packet is a host announcement which is sent by device OKI-15E6BC. The host is announcing that it is available on the network and labels what it can do. In this case it labels "workstation, server, print queue server, and potential browser. In addition to running on windows 95 or above

17. What brand printer is listed in packet 61?

OKI

18. What could an attacker use printer information for?

This information can be used since the attacker knows more about the network. In addition to being able to leverage known OKI exploits. It can also be used for pivoting and denial of service attacks.

19. Is there a more secure version of the main protocol we looked at?

Yes SNMPv3.

Task 4: Analyze Malware.pcap

1. What DNS entry is the infection calling home to?

nofbiatdominicana.com

2. What IP does that translate to?

141.255.167.3

3. What country is the IP associated with? arin.net

Switzerland

4. Based on the answer to question two, do you think that is the actual endpoint? Why or why not?

I think that this is most likely a proxy server or a compromised machine. Attackers usually use these things to conceal themselves.

5. Is this a VM? How can you tell? (Hint: Look for the MAC address)

The prefix of the mac address is a VMware MAC address prefix “00:0c:29:

6. What starts to happen at packet 38 - 43?

A TCP connection is initiated followed by a SSL/TLS handshake. In addition to a Client hello and server Hello, meaning the start of an encrypted session.

7. Why would an attacker want to SSL/TLS encrypt?

An attacker would want to use SSL/TLS encrypt to bypass detection and blend in with encrypted traffic.

8. What URI is the user pointed to for payment? (Hint: Look for HTTP POST)

/w72sh29mlo & /9x358cr5kv2l8g2 & 3ubc5pzotxyp0ui

9. Do a Google search for this URI? What do you find?

“It looks like there aren’t many great matches for your search” If it was a well known malware it should pop let us know by the URI.

Task 5: Shodan.io

1. Search for "default password". What does it find?

Finds a list of devices with the default password on it.

2. What does this likely mean?

This means that no one changed the password for the device so it is the system default

3. What could an attacker do with this?

Access your account just by knowing your username

4. Search for vnc. What does it find?

Shows a bunch of virtual network computing servers which allow remote control of a computer over a network.

5. What is vnc?

A virtual network computing is a graphical desktop-sharing system that uses the remote frame buffer protocol to remotely control another computer.

6. What does this likely mean?

This means that these VNC's are publicly accessible over the internet by anyone who knows the IP.

7. What could an attacker do with this?

Gain remote control of the computer

8. Search for scada. What does it find?

Find a list of SCADA systems

9. What is scada?

A Supervisory Control and Data Acquisition system is used for controlling industrial processes and infrsatructures.

10. What does this likely mean?

This means that SCADA systems are exposed to the internet which is a attack vector for adversaries.

11. What could an attacker do with this?

An attacker could disrupt industrial processes leading to safety hazards, gain control of critical infrastructure, steal sensitive data, and manipulate operational settings.

12. Look at https://www.exploit-db.com/exploits/18187/ How does this relate to Shodan?

This relates to shodan as this is an attack which sends a payload to a SCADA system.

13. Search for rdp. What does it find?

A list of Remote Desktop devices

14. What is rdp?

Remote Desktop which is a protocol developed by microsfot that allows a user to connect to another computer over a network.

15. What does this likely mean?

These devices are able to be publicly remoted into.

16. What could an attacker do with this?

Remote into the device and access any information and upload any files they would like onto the device.

17. What other popular searches are there? (Hint: Look at explore)

Webcam, mongodb, printer, voip, router, nas

18. How could an organization use shodan to protect itself?

An organization would have to have a team that uses shodan and identifies these loose holes to report it to a team or to fix these vulnerabilities in their system. Overall, this tool can help hackers a lot although, if leveraged by a company it will also be able to shut down many hackers.

<u>Lab Write up</u>

1. Why are packet captures so important for troubleshooting connectivity issues?

Packet captures are so important for troubleshooting connectivty issues because it makes it super easy to find the exact point that the issue occurred. As you go down to the root function of connectivity you can see all the processes that are happening which leads to the overall process that you see. By detecting the exact point of failure you can find the exact issue to fix to be back up and running in the fastest time possible.

2. Do you think Shodan.io is good for the security of the Internet? Why or why not?

I think that Shodan.io is great for the internet. This is a easy and simple tool to use by cybersecurity specialist. It could be used by the average person although, with a lot of difficulty and probably not much success. Rather for the average person it could be a good learning tool. This does add another attack vector for companies. Although, if shodan wasn’t doing it someone else on the dark web would. I think that Shodan shows everyone the risk and makes everyone more proactive in mitigating any vulnerabilities.