Paola N. Baez Hernandez

Lab 5 - Wireshark / Shodan

Task 1: Download and Install Wireshark

Deliverable: No deliverable for this task.

Task 2: Analyze av.pcap

1. Download the pcap.zip from FSO under Lab 5

   Done

2. Open av.pcap

   Done

3. What is the source IP making the request?

   IPV 81.131.131.6

4. What is the destination?

   Destination 64.246.6.133

5. What protocol is used to download the updates?

   Protocol FTP

6. Is that protocol secured?

   That protocol is not secure as it is easy to be interpret by an attacker.

7. What username is used to log in?

   Username is Anonymous Guest

8. What does the RETR command do?

   This is a request for the server to send the file's content through the connection already established by the client.

9. How many files are retrieved in this PCAP?

   There's 9

10. What are the names of the files?

    Their called Updates50

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

    They would be able to copy all the information from previous and current updates to see logins and other details from the server they downloaded from.

Deliverable: Include your answers in the deliverables document.

Task 3: Analyze NetworkProtocol.pcap

1. Open NetworkProtocol.pcap in Wireshark from the pcap.zip file you downloaded
   in Task 2.

   DONE

2. What protocol is primarily used here?

   SNMP Protocol

3. What version is it?

It's Version 1

4. What is it used for?

   SNMP is used to monitor and manage network devices such as routers, switches, servers, printers, and IoT devices.

5. What is a community string?

   A community string acts as a password to group data into either read-only or read-write areas.

6. What community string is it using?

   It's using Public (read-only)

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

   It would apply to Authentication and Accounting

8. What part of the CIA would apply to this protocol?

   It would apply to integrity and confidentiality.

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

   It's requesting 1.3.6.1.2.1.1.2 - MIB object for network management

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

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

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

It gives attackers a snapshot of the device's characteristics itself, including its type, the operating system version, and how long it's been running for. This information can be used to tailor specific exploits that target known vulnerabilities in that particular setup.

11. What OID is packet 21 requesting?

    OID 1.3.6.1.2.1.43.14.1.1.6 its requesting whether print data and control commands can pass through.

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

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

    This could help an attacker understand how data flows and potentially manipulate or disrupt printing operations.

13. What OID is packet 27 requesting?

    1.3.6.1.2.1.1.5 - An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. If the name is unknown, the value is the zero-length string. Max-access to read-write.

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

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

    This may provide device configuration settings or firmware details to attackers, which can be useful for exploiting vulnerabilities.

15. What OID is packet 29 requesting?

    29 is requesting 1.3.6.1.2.1.2.2.1.6. - The interface's address at its protocol sub-layer.

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

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

    An attacker would want to know this information because it provides print jobs information, which attacker could intercept and manipulate print jobs.

17. What is packet 61 telling us?

    It is making an announcement that the server types and OS installed on them. Server Workstation, Print Queue Server, WfW host, in Potential Browser, Windows 95 or above.

18. What brand printer is listed in packet 61?

    Printer Fujifilm

19. What could an attacker use printer information for?

    Attackers could use printer information to manipulate jobs.

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

    Yes, There is.

Deliverable: Include your answers in the deliverables document.

Task 4: Analyze Malware.pcap

1. Open Malware.pcap in Wireshark from the pcap.zip file you downloaded in Task 2.

   DONE

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

   The infection is called home nofbiatdominicana.com

3. What IP does that translate to?

   It translates to 141.255.167.3

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

   Uncertain country

5. Based on the answer to question two, do you think that is the actual endpoint?

a. Why or why not?

   Somewhat Not, Attackers mostly use proxy servers VPNs or compromised hosts as part of their command and control infrastructure.

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

   Yes, because it is using a virtual private server service.

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

   Between packets 38-43, the infected machine starts talking to 95.215.45.172; this is probably another command-and-control server or the next step in the attack. It’s noticeable the SSL/TLS handshake in here, meaning the malware is setting up an encrypted connection, likely to hide whatever data it's about to send or receive.

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

   Because it could protect the attacker’s infrastructure from reverse engineering by the defenders.

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

POST /w72sh29mlo HTTP/1.1 (application/x-www-form-urlencoded)
POST /9×358c5kv218g2 HTTP/1.1 (application/x-www-form-urlencoded)
POST /3ubc5pzotxypOui HTTP/1.1 (application/x-www-form-urlencoded)

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

    Yes, it does and it reveals how successful the connection was. For example, (a client's request was successfully received, understood, and accepted).

Deliverable: Include your answers in the deliverables document.

Task 5: Shodan.io

1. Create a Shodan account. (You will need to validate an email before you can login)

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

   Shodan reveals 51,548 devices that are publicly accessible and still using factory-default login credentials.

3. What does this likely mean?

   This means many organizations and users have the same default passwords, leaving them exposed.

4. What could an attacker do with this?

   Attackers could gain access, misconfigured devices, they could also pivot to other systems, steal data, and even take control.

5. Search for vnc. What does it find?

   VNC reveals publicly accessible VNC servers, with a significant number in China.

6. What is vnc?

VNC is a remote desktop sharing protocol that allows the users to have control over another computer remotely.

7. What does this likely mean?

   This means millions are exposed to the internet without having the proper authentications and using weak credentials.

8. What could an attacker do with this?

   The attacker could have full control over these vulnerable remote desktops. Allowing then to steal data and install malware.

9. Search for scada. What does it find?

   SCADA finds systems that are exposed via Remote Desktop with higer exposure in Indonesia, USA, Brazil, India and Japan

10. What is scada?

    SCADA is an industrial control system that is used to monitor and control the infrastructure.

11. What does this likely mean?

    SCADA is being exposed due to plenty of misconfigurations, weak authentications, and outdated security practices.

12. What could an attacker do with this?

    An attacker could take control of the industrial processes, potentially shutting down the power grids. They could cause physical damage by Altering the system settings.

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

    Shodan helps find internet-exposed CoDeSys SCADA v2.3 systems, while the Exploit-DB entry (CVE-2011-5007) provides a remote buffer overflow exploit to take control of them. Attackers can use Shodan to locate vulnerable targets and then deploy the exploit to gain remote access.

14. Search for rdp. What does it find?

    It finds 6,535 exposed RDP instances worldwide, with a higher number in the USA.

15. What is rdp?

    RDP is a Microsoft protocol that allows users to remotely connect to and control Windows-based computers over the network.

16. What does this likely mean?

    It means thousands of computers are publicly accessible over the internet via RDP. Which is a significant security risk if they are not properly configured.

17. What could an attacker do with this?

    An attacker could brute force weak RDP credentials to gain access. Also, exploit RDP vulnerabilities.

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

    Searches include ICS, databases, network infrastructure, and video games.

19. How could an organization use Shodan to protect itself?

    Companies could use Shodan to check what parts of their network are exposed online, find security risks, detect outdated software, and identify unauthorized devices before hackers do.

Deliverable: Include your answers in the deliverables document.

Lab Write Up

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

   Packet captures are essential for diagnosing network issues because they will provide a real-time view of data traffic. By analyzing these captures, network administrators can get to identify problems such as dropped packets, latency,

misconfigurations, or unauthorized access attempts. This level of detail allows for precise troubleshooting, helping to resolve connectivity issues efficiently and improve overall network performance.

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

Shodan.io is a great powerful tool with both positive and some negative implications for the security of the internet. On one hand, security professionals use it to identify exposed systems, detect misconfigurations, and strengthen defenses before vulnerabilities can or could be exploited. On the other hand, cybercriminals can use the same data to locate unsecured devices and launch attacks. Ultimately, its impact on internet security depends on how it is used by their ethical researchers to enhance security or by malicious actors for exploitation.