Nicolas Huber: 2506144

Question 1:

Task 1- How can you discover any network, and which tool is used to identify the host? Which command is used to collect the information? (5%)

We can use a port scanner tool like Nmap to discover any network. Other tools are hping3 or fping, which we also used in the lab. The picture shows the usage of Nmap (Version 7.60) to identify the host.

The following command was used to collect the information: **nmap 203.0.113.0/24**

Task 2- From the figure, which port is open on the Raspberry Pi? (5%)

The Port 80 is open; we can see that in the line: 80/tcp open http.

Question 2

Task 1- What's the purpose of using the Nmap command with the -sU option in the Kali VM terminal? (5%)

The purpose is to perfom a UDP scan: We check which UDP ports are open. (In the UDP header, there are no flags like SYN like in TCP).

Task 2- In the figure (red box), why does the information say “Destination port is unreachable”? (5%)

If we receive “Destination port is unreachable” message, that means the port is closed, e.g., the UDP packets we have sent let us detect closed (and open) ports.

Task 3- Check out the packets in Wireshark. Which protocols were utilised to discern the operating system? (10%)

ICMP and TCP.

Although there is one UPD entry, UDP isn't commonly employed in OS detection because it doesn't establish a connection and thus provides less reliable response data for the kind of detailed analysis required in OS fingerprinting. The command that was used is nmap -O 203.0.113.20; typically used for OS detection.

Question 3

Task 1- What command is used to host the DoS attack using hping3? (5%)

We can use (assuming the IP address we want to target is 203.0.11.20, as it is in the image) for DoS SYN flooding, which is also shown in the picture: hping3 -S 203.0.11.20 -p 88 --flood

Or we can use ICMP Flood attack (THIS IS NOT shown in the picture, just for completeness): hping3 --flood –icmp -p 203.0.11.20

Task 2- What type of TCP messages were observed in Wireshark during this DoS attack? And what was the destination TCP port targeted by the attack? (5%)

We send TCP SYN messages. We target port 88. (DoS SYN flood against port 88)

Question 4

Task 1- Define a Denial of Service (DoS) attack and discuss its potential impact on IoT devices and networks. (5%)  
  
  
A Denial of Service (DoS) attack is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. This is typically accomplished by overwhelming the target with a flood of internet traffic.

The potential impact of a DoS attack on IoT devices and networks includes the cripppling of device functionality, which can disrupt essential services and compromise the security of networked systems. For IoT networks, which often lack robust security measures, DoS attacks can lead to broader network disruptions, rendering critical systems like healthcare, home security, and industrial automation inoperative.

Task 2- Look at the picture below and explain the meaning of the command. Why are the source and destination IP addresses the same? (5%)  
  
hping3: This is the command to run the hping3 tool, which is used for crafting network packets.

-S: This flag sets the SYN flag in the TCP packet. SYN is typically used to initiate a TCP connection.

203.0.113.20: This is the IP address specified for both the source and destination, indicating a Land Attack.

-a 203.0.113.20: This option "spoofs" the source IP address to be the same as the destination IP address, a hallmark of the Land Attack, where the packet appears to originate from the target itself.

-k: This option keeps the socket open after sending packets, allowing for continuous packet flow.

-s 89 -p 89: These options set both the source and destination ports to 89. In a traditional Land Attack, the source and destination ports are identical.

--flood: This flag sends packets as quickly as possible, not waiting for any replies, to flood the target with overwhelming amounts of traffic.

This attack / command sends a packet with the same source IP/port combination as the destination IP/port. This means, we "spoof" the source IP address by replacing the Kali VM address another value in the packets

Question 5

Task 1- Based on the Bluetooth Sniffing Lab, describe how the attacker can steal your information via Bluetooth sniffing (describe in detail which command is used in each step) (10%)

The commands; assuming the Pi has a IP address and we connectetd via SSH

rfkill list (if Bluetooth blocked: rfkill unblock bluetooth)

systemctl status bluetooth.service (if not active: systemctl start bluetooth.service)

hciconfig hci0 (if not up: hciconfig hci0 up) -> display status of Bluetooth interface hci0

we can now enter the bluetooth cli:

blueoothcli -> we are now in a Bluetooth terminal

scan on -> take notes of the various MAC addresses

scan off -> turn off scan

decide which Bluetooth device to attack

info [MAC-ADDRESS]

(trust the device; this was a bit buggy in the lab)

paired-device -> list device that are paired with the Pi

pair [MAC-ADDRESS] -> accept on blueooth device e..g, iPHone (the iphone MUST be in bluetooth settings)

connect [MAC-ADDRESS] -> accept onbluetooth device

(do some stuff)

quit -> leave bluethoothcli

systemctl stop bluetooth.service

Task 2 -Can an attacker connect to your smartphone via Bluetooth without your permission? Explain why? (5%)

No! Smartphones (like iPhones) have very good protection mechanism that would recognize such an unwanted parining / connection.

Question 6

Task 1- Based on the Web Application Vulnerability lab, which tool is used to exploit the vulnerability of web applications? Give a brief explanation about the tool. (5%)

This is a screenshot of the sqlmap tool. sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It offers a powerful detection engine, capable of retrieving database server details, accessing the underlying file system, and executing commands on the operating system via out-of-band connections. The tool supports a wide range of database systems, making it a essential tool for security professionals assessing the security of web applications.

Task 2 -What does the term “vulnSensors” mean? Provide the command used to obtain the result (shown in figure) and explain the flags of the command in detail. (10%)

vulnSensors is the database that we discovered.

It was discovered by using the following command (assuming the application is running on 203.0.113.21 and port 8080): sqlmap -u http://203.0.113.21:8080/add/test?temperature=26 --dbs --threads=10 --current-db

-u (--url): Specifies the URL to be tested. In this case, http://203.0.113.21:8080/add/test?temperature=26 is the target.

--dbs: Tells sqlmap to enumerate the database management system (DBMS) databases available on the server. This is useful for understanding what databases can be accessed or compromised.

--threads=10: Sets the number of threads that sqlmap will use to perform the testing. Increasing the number of threads can speed up the testing process by performing multiple operations in parallel.

--current-db: Requests sqlmap to retrieve the name of the current database. This is useful to quickly identify which database the application is primarily interacting with.

This command is designed to efficiently discover and list databases from the server, specifically targeting the service running on port 8080 with a query parameter temperature=26, and it uses multiple threads to expedite the process.

Question 7

Task 1- Which cyberattack does this command aims to host? What will happen after the attack occurs? Explain why? (10%)

The URL in the command includes an SQL injection payload: 1'); drop table sensors;-- . This payload aims to:

Terminate any previous SQL commands (1' which closes the query parameter value started by another single quote).

Start a new SQL command to drop table sensors; which aims to delete the table named 'sensors' from the database.

The -- is a comment marker in SQL which effectively makes the database ignore the rest of the query, preventing it from causing errors or revealing the attack.

Therefore, this wget command sendig a malicous payload / query, it will delete (i.e., drop) the table sensors from the database vulnSensors. This will result in data loss.

Explanation: This attack exploits poor input sanitization in the web application handling database queries. By failing to properly sanitize user inputs (like those in the URL parameters), the application allows the execution of malicious and bad SQL statements. This can cause unauthorized modification, deletion, or retrieval of data within the database. The use of wget simply facilitates sending the malicious query to the server, illustrating how easily such an attack can be executed remotely. We have seen in the lab that we can use e.g., the .decode(“UTF-8”) function to make it secure against SQL injection.

Task 2- Describe the defence method to prevent this attack. (describe in detail the process, which command is used to enable the defence mechanism) (10%)

See line 67 in code (app.py)

db.escape\_string(sensor\_name).decode("UTF-8"): This method call is crucial.

db.escape\_string() is a function that escapes special characters in the sensor\_name variable that are part of SQL syntax. This escaping neutralizes potentially malicious code within the input, thereby preventing the input from altering the SQL command's structure.

The .decode("UTF-8") part ensures that the result is correctly formatted as a UTF-8 string, which is necessary for correctly handling characters in databases that expect UTF-8 encoding.

To do that we:  
We stop the server and change the server code: (sudo nano -l app.py)

Comment Line 67 and “activate” by decommenting line 68

Save the file and exit nano (CTRL + X and y)

Rerun the applcaiton (i.e., the server)