**System Hacking**

To perform this attack, Kali and Mr. Robot were installed on VirtualBox. Kali is the attacking machine, and Mr. Robot is the target system. The scope of the attack covers only the target machine, Mr. Robot.

**Stage 1: Reconnaissance and Foot-Printing**

This stage involves finding information about the target system, infrastructure, and networks to spot possibilities to breach them. The type of reconnaissance deployed in this attack is both active and passive.

**Step 1: Using Netdiscover**

This is an active address reconnaissance tool designed for wireless networks without DHCP servers. To perform reconnaissance on the target machine, Netdiscover sends out ARP probes and listens for responses, which allows it to determine the IP and MAC addresses of active network devices. Mr. Robot. Figure 2 shows the use of Netdiscover to discover the active network or live.

Command: $sudo netdiscover.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 2: Target Network Discover

**Stage 2: Enumeration**

Enumeration is the process of gathering information about the target, such as the workgroup, server name, and others.

Step 1: Using Nmap To Find Open Ports

Nmap provides a lot of features, including OS detection, host discovery, service detection, etc. To further discover the host and OS service detection about the target, a scan was carried out on the discovered IP address on the network, and its shows that only one IP address is live and has open port functioning. Figure 3 shows the usage of Nmap to carry out further scanning. Nmap on the Fourth IP address.

Command: $ **nmap -T4 -p- -sS -sV -A 192.168.20.14**

A screenshot of a computer

Description automatically generated

Figure 3:Nmap Scan

After performing a Nmap scan in Figure 3, a browser was launched to test the opening port running on HTTP as seen in Fig 4 to verify which target the address. The discovered target running on 192.168.20.14 is Mr. Robot, which was earlier stated that is the target machine.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4: Target Verification

Step 2: Using Nikto to find a vulnerability

Nikto is an open-source web server scanner that scans web servers for various vulnerabilities, such as login pages and loopholes. It also investigates HTTP server options, locates installed web servers and applications, and looks for multiple index files. Plugins and scan components can automatically update and receive frequent updates. Figure 5 shows the Nikto scan on the target machine (Mr Robot with IP address 192.168.20.14). Nikto v2.5.0 was used, and it’s preinstalled on Kali. The use of Nikto in Figure 5 results in the finding of a login page, which makes the pen test exercise easier for the attacker.

Command: $ Nikto - -host 192.168.20.14

The Nikto scan has discovered a login page that indicates potential vulnerabilities in the system, providing the attacker with valuable insights for possible exploitation. Figure 5 illustrates the utilisation of Nikto, which successfully identifies the presence of a login page, thereby simplifying the penetration testing exercise and facilitating the exploitation process.

A computer screen with white text

AI-generated content may be incorrect.

Figure 5:Nikto Scan

Step 3: Using DIRB For Vulnerability

Content scanning tools like DIRB v2.22 by Dark Raver were used to check the content of the target machine. The application is preinstalled in Kali. The content scanning using the dirb command in Figure 6 resulted in the discovery of the robots.txt folder. The folder will be used to find hidden directories inside the folder.

Command: dirb [http://192.168.20.14](http://192.168.20.14/)

A computer screen with white text

AI-generated content may be incorrect.

Figure 6: Content Scanning

Step 4: Finding the Hidden Directory

To find the hidden directory, a web browser launches with the use of this URL/path name. The image in Fig 7 contains the fsocity.dic and key-1-of-3.txt which is the dictionary file and hash value keys respectively.

url: <http://192.168.20.14/robots.txt>

A screenshot of a computer

AI-generated content may be incorrect.

Figure 7: Directory

Step 5: Download the Directory

Figure 8 shows the use of the wget command in downloading files or folders. The following command was used to download the directory.

Command: wget <http://192.168.20.14/fsocity.dic>to download the dictionary files, which contain global usernames.

Command: wget <http://192.168.20.14/key-1-of-3.txt> to download the hash files

A screenshot of a computer

AI-generated content may be incorrect.

Figure 8:Fsocity.dic and key-1.txt

Step 6: Sort the Fsocity.dic and copy it to a new folder

This step will sort the dictionary directory and also copy the content to the new folder, as shown in Figure 9.

Command: sort fsocity.dic | uniq >fsocity\_filtered.dic whereas the fsocity\_filered.dic is the new folder

A black background with red text

AI-generated content may be incorrect.

Figure 9: Sorting

**Stage 3: Gaining Access**

This section involves gaining by using the brute force method to get the password of the login page attached to the system. This stage will exploit the vulnerabilities discovered in the system like a login page, dictionary files containing passwords and usernames, and a secret key.

Step 1: Brute Forcing

To find the username and password of the login page, tools like Burp suite, and hydra would be used to brute-force the dictionary file to find possible usernames and passwords.

Burp Suite is a vulnerability scanning, penetration testing, and application security platform. While Hydra, on the other hand, is a brute force tool that helps ethical hackers to crack passwords from network services.

To find the parameters to use for a brute force attack, a Burp Suite v2023.1.12 was launched to intercept proxy communication. A WordPress login was attempted with the username “sani” and password “pass123” to log in. Why try to log in with a proxy foxy on the browser, which enables Burp Suite to capture the login details of the attempt? The Burp Suite interception examines that the login request is a “Post” and shows the type of log information. See Figures 10,11, 12 and 13 for details.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 10:Burp Suite

Figure 11 shows the functionality of foxyproxy in conjunction with burp suite in intercepting login attempt for password cracking. The service allow to identify weakness in the system or the login mechanism. The Intercept login is shown in figure 12.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 11:FoxyProxy

The screenshot reveals that both the username "sani" and the password "password123" are invalid credentials for the system, as indicated by the "invalid username" error code. However, this information assists an attacker in identifying the relevant parameters, directories, or tactics to employ while attempting a brute-force attack on the target machine

A screenshot of a login screen

AI-generated content may be incorrect.

Figure 12:Login Page

A screenshot of a computer

AI-generated content may be incorrect.

Figure 13:Interception

Using Hydra to brute force the dictionary files linked to the target machine, random usernames and passwords were discovered. A user with the name “elliot” and password “pass123” was tested on the login page of WordPress attached to the target machine and it shows that the username is a valid one but with an incorrect password. See Figures 14,15,16 and 17 for details.

Command: hydra -V -L fsocity\_filtered.dic -p 123 192.168.20.4 http-post-form ‘/wp- form.login:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username’.

A screenshot of a computer screen

AI-generated content may be incorrect.

Figure 14:Password cracking using hydra-2

A screen shot of a computer code

AI-generated content may be incorrect.

Figure 15:Password cracking using hydra-2

Figure 16 demonstrates that the username "elliot" is valid; however, an incorrect password was provided. This discovery provides the attacker with an opportunity to attempt different passwords and potentially gain unauthorized access to the database.

A login screen with a logo and a blue circle

AI-generated content may be incorrect.

Figure 16:Valid Username But Incorrect Password

A screenshot of a computer

AI-generated content may be incorrect.

Figure 17:Intercept-2 For correct Password

Hydra was able to detect the correct username for the page. To find the correct password and gain access to the login page, the service of Hydra is also required with different parament given to Hydra to unravel the correct password. Figure 18 shows the correct password for the username “elliot”. Figure 18 shows a successful login and access to the WordPress page with the correct credentials.

Command:hydra -l elliot -p fsocity\_filtered.dic 192.168.20.4 http-post-form ‘/wp- form.login:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=is incorrect’

Explanation: Hydra is a tool used for password cracking. The "-l" flag instructs Hydra to target a single username, in this case, "elliot". The "-p" flag tells Hydra to search for a password for the username "elliot". The file "fsocity\_filtered.dic" contains a list of possible passwords that Hydra will use in its search. The target IP is "192.168.20.4". Using the option "http-pot-form" informs Hydra that this is a POST request. The path "/wp-form.login" indicates the specific location to target. The field labelled "USER" is the username field, while "PASS" represents the password field. The field "wp" is the submit field. The text "Log+In:F" directs Hydra to look for a failed login message, indicating an incorrect password, and determine if it matches any user.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 18:Password Hacked

Figure 19 shows a login to the web page was successful after obtained valid credentials of the target device.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 19:Login Successful

**Step 2: Creating a Payload**

A payload refers to a piece of code or software that is designed to be executed on a target system to exploit a vulnerability or perform a specific action. Payloads are typically used in conjunction with exploit frameworks, such as Metasploit, to gain illegal access to a target device or to perform various actions on the system, such as stealing sensitive data, installing malware, or taking control of the system.

To create a payload for this attack, the Metasploit frame v6.3.4 work will be used. Metasploit is a vulnerability exploitation platform used by ethical hackers or pen testers to find loopholes and exploit them to gain access to the system. Figure 20 shows the use of Metasploit.

Command: msfconsole

A computer screen with white text

AI-generated content may be incorrect.

Figure 20:Metasploit

Figure 21 shows the result of the modules to be used in the exploitation of the target device. This could be searching a WordPress shell since the enumeration said the target is running on WordPress.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 21:Wordpress Shell

Figure 22 shows the setting up of payloads to launch an attack against the target device. The figure also shows that the target is vulnerable to attack. With this type of information, it gives an attacker a hit to penetrate the system. It also shows the result of the exploitation of the system by opening the Meterpreter to allow the attacker to communicate with the target.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 22:Payload Setup and Exploit

**Stage 4: Maintaining Access**

One of the stages in Penetration testing or ethical hacking is maintaining access once exploitation has been successful.

Step 1: Privilege Escalation

Figure 23 shows the hidden files which contain the password of Mr. Robot. An md5 key was discovered with a hash function and was cracked to see the password of Mr. Robot using a crack station to reveal the password. The figure also shows meterpreter session created after running exploit on the target.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 23: Meterpreter Session

**Using John the Ripper**

John the ripper is used to cracked hash functions of any hash type. After discovered the hash value and its identifier in figure 23, john the ripper was used crack the hash value. figure 24 shows the cracked hash value and reveal the password.

Command: john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt

Explanation: john is the tool, --format=raw-md5 (md5 hash type), -- wordlist=/usr/share/wordlists/rockyou.txt is the path to wordlists file that john will used for words combination and password.txt is the hash value found which john will used to cracked into plaintext.

A computer screen with white text

AI-generated content may be incorrect.

Figure 24:Hash Crack

Step 2: Login Using Shell

The shell will enable login into the Mr. Robot system as shown in figure 25. The figure shows successful login as a robot with a discovered password.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 25: Privilege Escalation

Step 3: Nmap Interactive session

Figure 26 shows other keys discovered in the system and the use of the Nmap interactive section to interact with the system. To use the Nmap interactive session, the use of! will be used before any command.

A screenshot of a computer program

AI-generated content may be incorrect.

Figure 26:Nmap Interactive Session

**Step 4: Change of Robot Password**

Figure 27 shows that the attacker was able to change the password because of access to the system. The change of the password was to deny access to the legitimate owner of the account. The password was changed from abcdefghijklmnopqrstuvwxyz to brad2023

A screenshot of a computer

AI-generated content may be incorrect.

Figure 27:Robot Password Changed by Attacker

Figure 28 shows further modification by the attacker, by deleting the key-3-of-3.txt from the system because of the access it has to the system as the root user.

A black background with white spots

AI-generated content may be incorrect.

Figure 28:Modification

**Stage 5: Clear Tracks**

Every attacker aims is to hide their identity, so every trace of their activities on the system would be deleted. Figure 29 shows the logs and detail of the activities related to the attack carried out on the system.

A screen shot of a computer

AI-generated content may be incorrect.

Figure 29:Log Files

Figure 30 shows the content of auth.log and the activities of the attacker. The figure shows how the attacker change the password of the users and take control of the system.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 30:auth.log

Figure 31 shows the attacker has deleted the auth.log, and syslog from the logs. These files deleted show the details activities of penetration into the system. The necessary for the attacker to delete the history.

A screen shot of a computer

AI-generated content may be incorrect.

Figure 31:Deleted Logs Files

Figure 32 shows that the attacker was able to gain access to the main Mr.Robot Application after a successful attack on the device. The login details used are:username: robot, password:brad2023

A computer screen shot of a computer

AI-generated content may be incorrect.

Figure 32:Mr Robot Terminal