Laud Mills

Part A: Open your Linux terminal, write down the command by using various options of tcpdump to fulfill the requirements. Also attach the screenshots.

You can refer following URL to understand the functionalities of tcpdump via command prompt: <https://danielmiessler.com/study/tcpdump/#host>

1. Access DVWA application from kali browser and extract HTTP User Agent from HTTP request header through command prompt of kali Linux. What is the name of the User-Agent?

Follow the steps:

1. Open your kali terminal
2. Run the proper tcpdump command that capture HTTP User Agent of DVWA application
3. Open kali browser and connect with Metasploit2 VM
4. Click on DVWA link
5. Click on various links of DVWA
6. Capture the User-Agent on your kali terminal

Answer:

Command : sudo tcpdump -l eth0 -s 0 -A -n port 80

User Agent Name : Mozilla/5.0

Screenshot:

A computer screen with white text

Description automatically generated

1. Access DVWA application from kali browser and extract HTTP User Agent and the Host information from HTTP request header through command prompt of Kali Linux. (Follow the same steps as mentioned above)

Answer:

Command: sudo tcpdump -i eth0 -s 0 -A -n port 80

User-Agent: Mozilla/5.0

Screenshot :

A computer screen with white text

Description automatically generated

1. Capture only HTTP GET packets while accessing Mutillidae service of Metasploit from kali linux. Find out host Ip address, User-Agent, accepted languages by browser, encoding type, session id number

Follow the steps:

1. Open your Kali terminal
2. Run the proper tcpdump command that capture HTTP GET request packets
3. Open Kali browser and connect with Metasploitable2 VM
4. Click on Mutillidae link
5. Click on various links of Mutillidae
6. Capture the GET request packet on your kali terminal

Answer:

Command : sudo tcpdump -i eth0 -s 0 -A -v port 80 | grep -iE "Host:|User-Agent:|Accept-Language:|Content-Encoding:|Cookie:"

Host: www.irongeek.com

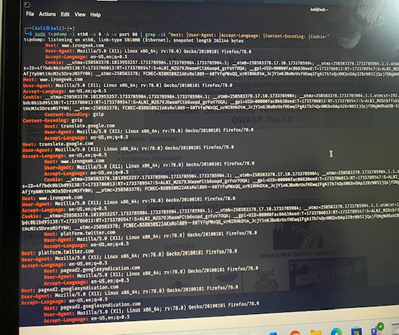
User-Agent: Mozilla/5.0

Accept-Language: en-US, en;q=0.5

Encoding Type: gzip

Session ID: 4f7bdc0b1d95138

Screenshot:



1. Capture username and password (credential) of DVWA login page using POST requests from kali terminal using tcpdump command.

To that do as directed:

1. Open your Kali terminal
2. Run the proper tcpdump command that capture POST request
3. Click on DVWA login link
4. Give the correct credential : Username = admin, password = password
5. Capture the username and password on your Kali terminal

Answer

Command : sudo tcpdump -i eth0 -w credential.pcap -nn -s 0 tcp port 80

Then used sudo tcpdump -nn -r credential.pcap -A ‘tcp[13] ==0x18’

to reveal the content on the captured packets in the credential.pcap

Host: r10.o.lencr.org

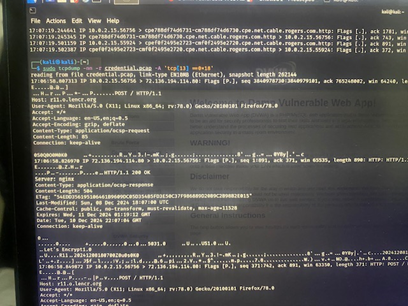
User-Agent: Mozilla/5.0

Accept-Language: en, US, en;q=0.5

Encoding Type: gzip

Session ID: 20241208204700Z

Screenshot:



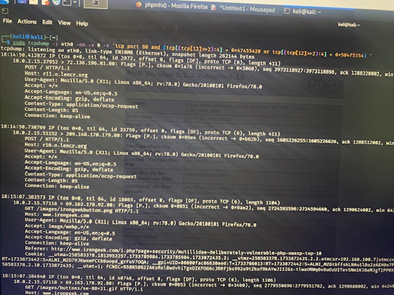
1. Parse Host and HTTP Request location (GET or POST) from the captured traffic of DVWA and Mutillidae at your Kali Linux machine using tcpdump command.

Follow the steps:

1. Open your Kali terminal
2. Run the proper tcpdump command that capture HTTP GET OR POST request packets
3. Open Kali browser and connect with Metasploitable2 VM
4. Click on Mutillidae link
5. Click on various links of Mutillidae
6. Click on DVWA link
7. Click on various links of DVWA
8. Capture the GET request packet on your kali terminal

Command : sudo tcpdump -i eth0 -nn -s 0 -v 'tcp port 80 and (tcp[(tcp[12]>>2):4] = 0x47455420 or tcp[(tcp[12]>>2):4] = 0x504f5354)'

Screenshot:



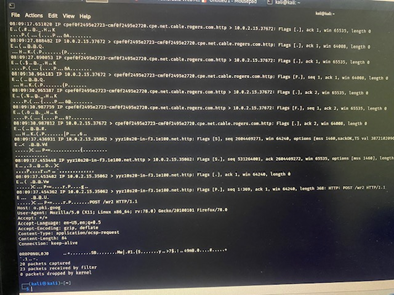
1. Extract HTTP Passwords in POST Requests.

To do as directed:

1. Open your Kali terminal
2. Run the proper tcpdump command that capture POST request
3. Open Kali browser and connect with Metasploitable2 VM
4. Click on DVWA link
5. Give incorrect credentials first time : Username = admin, password = 123456
6. Then Give correct credential : Username = admin, password – password
7. Capture the passwords on your Kali terminal

Command: sudo tcpdump -i eth0 port 80 -A

Screenshot:



1. Capture cookies from the server by searching on Set-Cookie: (from Kali) and Cookie: (from DVWA). Identify host name, session id and security level.
2. Open your Kali terminal
3. Run the proper tcpdump command that capture HTTP set cookie request packets
4. Open Kali browser and connect with Metasploitable2 VM
5. Click on Mutillidae link
6. Click on various links of Mutillidae
7. Click on DVWA link
8. Click on various links of DVWA
9. Capture the cookie of Metasploitable2 server on your Kali terminal

Command : sudo tcpdump -i eth0 -vvAls0 | grep -E 'Set-Cookie|Host:|Cookie:'

Host: r11.o.lencr.org o.pki.goog www.irongeek.com

Cookie: OGPC=19037049-1

Screenshot:

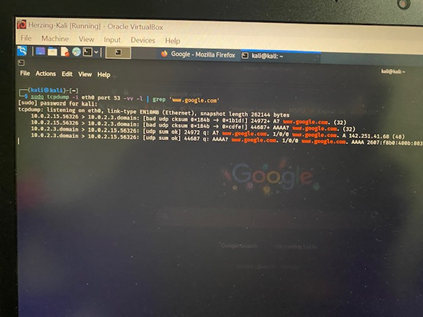
A computer screen with white text

Description automatically generated

1. Use the tcpdump command to retrieve the IP address of the DNS server of www.google.com and its associated links. (Hint: you need to write the tcpdump command specifying the DNS port number and then open the google.com on your Kali browser)

Command : sudo tcpdump -i eth0 port 53 -vv -l | grep 'www.google.com'

Screenshot:



Part B: For the following questions, you should go beyond your textbook and think as a security professional to identify the proper reasons based on real scenario.

1. What is tcpdump, and why is it a good tool for testing the Ubuntu Linux web server and web application security?

It is a command-line tool that helps capture and analyze network traffic, making it useful for testing web application security on Ubuntu Linux. It is good for monitoring traffic like HTTP and DNS, helping to ensure Confidentiality by spotting unencrypted data, Integrity by detecting possible attacks, and Availability by identifying issues like DoS attacks. Its ability to capture real-time data and filter traffic makes it a valuable tool for keeping web applications secure and troubleshooting network problems.

1. What does the Skipfish application do, and why is it a good security tool for web servers and web application testing?

Skipfish is an open-source tool used to scan web applications for security vulnerabilities, helping to improve their overall safety. It detects common issues like SQL injection, XSS, and configuration problems. Security professionals use it to find weaknesses early and fix them, strengthening web applications. Its fast scanning and detailed reports make it a great choice for web security testing.