Intercepting and Interpreting Network Traffic with Packet Sniffing Tools

(CompTIA Security + SY – 601)

Objectives:

- To use TcpDump in intercepting SSH network traffic
- To use Wireshark in capturing packets packet

Resources:

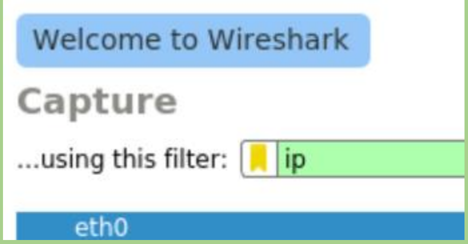
- Wireshark Application
- Kali Virtual Machine
- Windows Virtual Machine
- Packet Sniffing Tools (TcpDump, Wireshark)

Instructions:

<u>Wireshark</u>

1. From the desktop, select the Wireshark application

2. Under capture select eth0 adapter
3. In the capture filter type ip



Welcome to Wireshark

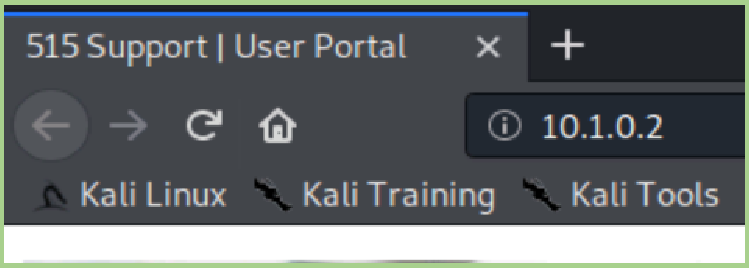
Capture

...using this filter: ip

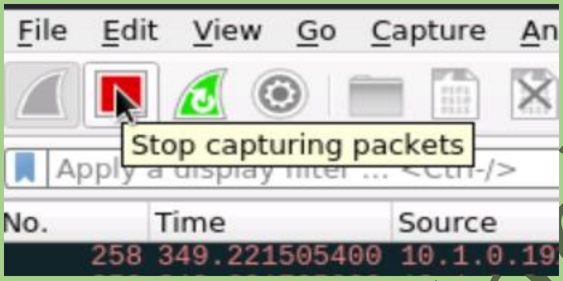
eth0

4. Start capturing by selecting the ‘blue start capturing packets’ button in the top left corner of the Wireshark interface

5. On the Kali VM desktop launch firefox and connect to http://10.1.0.2

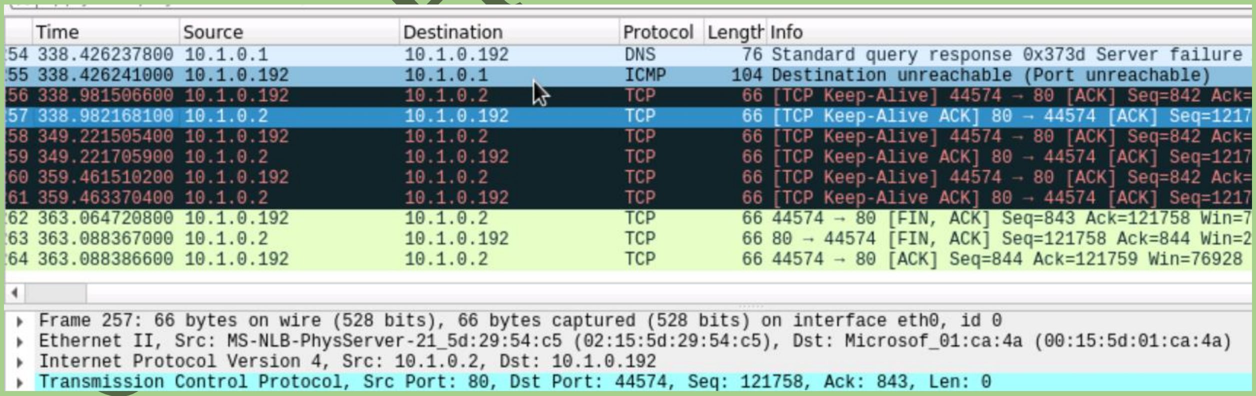


6. Navigate back to stop the packet capturing



```
258 349.221505400 10.1.0.19
```

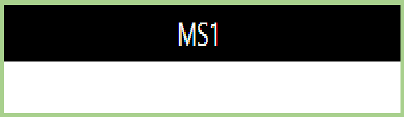
7. Select any DNS frame (color-coded as Light-blue)



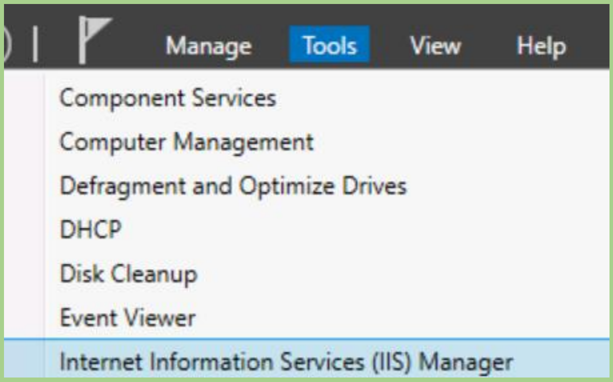
```
   Time          Source       Destination  Protocol Length Info
:54 338.426237800 10.1.0.1     10.1.0.192   DNS       76 Standard query response 0x373d Server failure
:55 338.426241000 10.1.0.192   10.1.0.1     ICMP     104 Destination unreachable (Port unreachable)
:56 338.981506600 10.1.0.192   10.1.0.2     TCP       66 [TCP Keep-Alive] 44574 → 80 [ACK] Seq=842 Ack=
:57 338.982168100 10.1.0.2     10.1.0.192   TCP       66 [TCP Keep-Alive ACK] 80 → 44574 [ACK] Seq=1217
:58 349.221505400 10.1.0.192   10.1.0.2     TCP       66 [TCP Keep-Alive] 44574 → 80 [ACK] Seq=842 Ack=
:59 349.221705900 10.1.0.2     10.1.0.192   TCP       66 [TCP Keep-Alive ACK] 80 → 44574 [ACK] Seq=1217
:60 359.461510200 10.1.0.192   10.1.0.2     TCP       66 [TCP Keep-Alive] 44574 → 80 [ACK] Seq=842 Ack=
:61 359.463370400 10.1.0.2     10.1.0.192   TCP       66 [TCP Keep-Alive ACK] 80 → 44574 [ACK] Seq=1217
:62 363.064720800 10.1.0.192   10.1.0.2     TCP       66 44574 → 80 [FIN, ACK] Seq=843 Ack=121758 Win=7
:63 363.088367000 10.1.0.2     10.1.0.192   TCP       66 80 → 44574 [FIN, ACK] Seq=121758 Ack=844 Win=2
:64 363.088386600 10.1.0.192   10.1.0.2     TCP       66 44574 → 80 [ACK] Seq=844 Ack=121759 Win=76928

▸ Frame 257: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
▸ Ethernet II, Src: MS-NLB-PhysServer-21_5d:29:54:c5 (02:15:5d:29:54:c5), Dst: Microsof_01:ca:4a (00:15:5d:01:ca:4a)
▸ Internet Protocol Version 4, Src: 10.1.0.2, Dst: 10.1.0.192
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 44574, Seq: 121758, Ack: 843, Len: 0
```

TcpDump

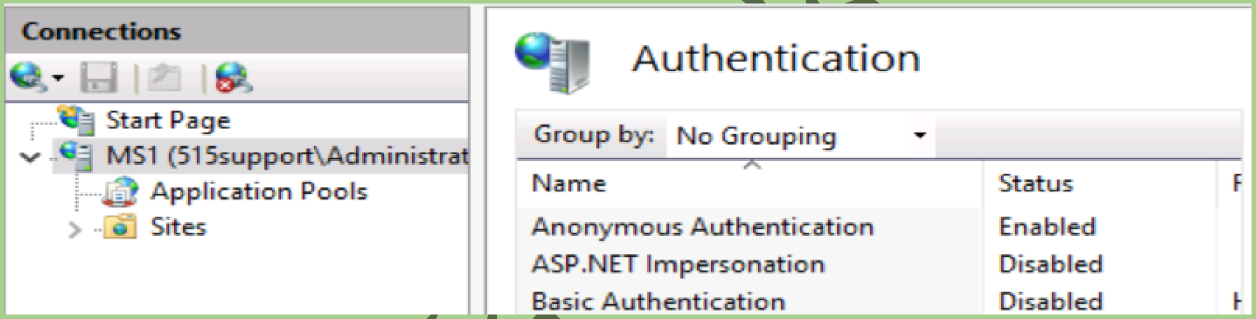
1. Switch to the MS1 server and sign in



2. From the server manager select Tools >>> Internet Information Services (IIS) Manager



3. Expand the MS1 and sites nodes to display the Default Web sites
4. Double-click the authentication Applet in the Default Web Site Home page
5. Select Anonymous authentication and disable it
6. Select Basic Authentication and enable it



Group by: No Grouping

Name	Status
Anonymous Authentication	Enabled
ASP.NET Impersonation	Disabled
Basic Authentication	Disabled

7. On the Kali VM terminal run the command: tcpdump -vv dst 10.1.0.10 and port ssh -w ssh.pcap
8. Open a second terminal window and run the following command: ssh root@10.1.0.10
9. Switch or launch the Wireshark application
10. Select the File menu then open the ssh.pcap file from the root user's home directory

Observations:

Wireshark

1. The Wireshark application was accessed via the Kali VM desktop
2. The network connection was configured using the eth0 adapter
3. The packet capturing was filtered for ip only
4. Capturing was started by clicking the 'blue start capturing packets' button in the top left corner of the Wireshark interface
5. A web interface was accessed via http://10.1.0.2
6. A bunch of packets were displayed after stopping the packet capturing (Time >>> Source >>> Destination >>> Protocol >>> Length Information)

7. Detailed and organized information about the packets captured were displayed in the DNS frame
8. The Wireshark command displayed captured packets upon opening of the ssh.pcap file

Tcp Dump

1. The MS1 server was logged in using a specific username and a password
2. Through Navigating in the Tools section, the Internet Information Service (IIS) Manager was accessed
3. Different Web Sites were observed in MS1 sites nodes
4. Authentication was properly configured
5. A terminal was opened in the Kali VM
6. On the Kali VM terminal the following command was successfully run: tcpdump -vv dst 10.1.0.10 and port ssh -w ssh.pcap
7. A second terminal on the Kali VM was opened and the following command was successfully run: ssh root@10.1.0.10

Results:

TcpDump

- TcpDump allowed packet capturing via the Kali VM terminal
- It allowed analysis of the ssh network traffic

Wireshark

- Wireshark allowed packet capturing customized for ip
- It allowed detailed analysis of the network traffic

Conclusion:

In this lab, we successfully utilized TcpDump and Wireshark to intercept and analyze network traffic. The exercises involved configuring network settings, capturing packets, and interpreting traffic data, providing essential hands-on experience with packet sniffing tools for the CompTIA Security+ certification.

Future Work:

Future work should focus on advanced packet analysis techniques, exploring additional network protocols, and enhancing the lab environment to include more complex network configurations and security scenarios.