OLD DOMINION UNIVERSITY

CYSE 301 Cybersecurity Techniques and Operations

Assignment 1: Traffic Tracing and Sniffing

Stuart N. Howard 01241576 Task B: Sniff LAN traffic

- 1. Sniff ICMP traffic (10 + 10 = 20 points)
- a. Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic.

b. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from <u>External Kali VM</u> and goes to <u>Ubuntu 64-bit VM</u>.



- 2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)
 - a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of

ubuntu VM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.

Ran FTP with ubuntu IP address and applied FTP filter on internal Kali wireshark



b. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.

Analyze the internal Kali captured packets in to find the FTP communication between External Kali and the FTP server. Look for packets with information related to FTP. View the packet details in Wireshark to locate the password. Found a field that said "PASS" in the FTP protocol section.

| | Mon 03:17 | | 1 till (1) - | |
|---|--|---|--------------------------------------|--|
| | Mon US:17 | • | | |
| File Edit V | Wireshark · Packet 18270 · eth0 | 000 | | |
| Frame 18270: 81 bytes on Ethernet II, Src: Micros Internet Protocol Version Transmission Control Protocol (- File Transfer Protocol (- PASS password\r\n | n wire (648 bits), 81 bytes captured (648 bit of_40:57:1e (00:15:5d:40:57:1e), Dst: Micro: nn 4, Src: 192.168.217.3, Dst: 192.168.10.10 toccol, Src Port: 32804, Dst Port: 21, Seq: : FTP) | ts) on interface 0 sof_40:57:0c (00:15:5d:40 15, Ack: 55, Len: 15 | Expression + | |
| 1/908 /1 17910 71 18270 72 18271 73 18271 73 18274 72 25424 10 25425 16 | ss rd ry:] | | he password. | |
| Image: Prame 18; 0000 00 15 5d 40 57 0c 0f Bello 00 15 3d 11 14 0f 03 Ethernet Internet 000 06 04 11 14 06 3 Transmiss 000 06 06 10 00 00 15 33 06 06 10 00 00 10 10 00 10 00 00 00 00 10 00 00 10 00 | 0 15 5d 40 57 1e 08 00 45 10]@W]@W]@ f 06 e5 64 c0 a8 d9 03 c0 a8C.@.?.d. 9 9c 22 66 ee 2f 7b 4c 80 18\$.9 "f. 101 08 08 e2 68 f5 ed 07 fe 9 70 61 73 73 77 6f 72 64 0d s. <mark>?ASS</mark> p ass | /(L·· h··· word· | | |
| 0000 00 1 0010 00 4 0020 0a 6 0030 00 e 0040 73 118270 · Time: 719.343920300 · Source: 10050 0a 1 | 192.168.217.3 - Destination: 192.168.10.10 - Protocol: FTP - Length: 81 - Inf | o: Request: PASS password Close | | |
| | | Activ Go to | vate Windows Settings to activate | |
| wireshark_eth0_20230710024933_ytVxC | p.pcapng Packets | : 42514 · Displayed: 9 (0.0%) | Profile: Default | |

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these "secrets" from the attacker VM, which is Internal Kali.

Analyze the internal Kali captured packets in to find the FTP communication between External Kali and the FTP server. Look for packets with information related to FTP. View the packet details in Wireshark to locate the password. Found a fields that captured used new and password the FTP protocol section.



Task C – Extra credit: Steal files with Wireshark (15 points)

Login to Ubuntu VM, and create a file in your home directory, named "YOUR_MIDAS.txt". Put the current timestamp and your name in the file. You can use the following command in the example below to do the job.



Once you have the file ready in Ubuntu, switch back to **External Kali**. Get the file you just created with FTP protocol remotely. Below is an example.

To retrieve the from the Ubuntu VM using the FTP protocol

- Use the ftp command to connect to the FTP server running on Ubuntu.
- enter the FTP username (cyse301) and password (password) to authenticate and establish the FTP connection.
- Once connected, use the 'get' command to download the file from the FTP server. Enter the

As an attacker, you need to complete the following tasks in Internal Kali:

1. Apply a proper display filter to display the FTP-DATA packets between External Kali and Ubuntu VM.

Open the capture file containing the FTP traffic between External Kali and the Ubuntu VM. Enter display filter to show only FTP-DATA packets

| 👻 Attacke Cali - External Workstation on SHOWADDE - Ketaal Machine Connections - 🗆 X Refer Chabered View H | Help |
|---|---|
| File Action Media Clipboard View Help | - D X |
| Bi 🖉 🖲 🞯 🕼 🕪 🧕 D 🔮 💼 | 10 12-57 AM (C) |
| Applications - Places - 🖸 Terminal - Mon 03:57 🔢 🖊 🖌 🗐 🕑 😔 😌 🕫 🛤 | |
| root@CS2APenTest: Applications * Places * 🗐 Wireshark * | Man 03:57 🔢 🗸 🗸 🕫 🗸 🖓 |
| File Edit View Search Terminal Help | *eth0 0 0 0 |
| File Edit View Go Sapture Analyze Statisti | tics Telephony Wireless Tools Help |
| 220 (vsFTPd 3.9.3) | • |
| Name (192.106.10.10:root): showa006 331 Please socity the password. | |
| Password: | Will * Expression. * |
| 330 Login incorrect. Login failed. | 192,168,217,3 FTP-DA 102 FTP Data; 43 bytes (PORT) (RFTR showa606.tx |
| ftp» exit | |
| 4/1 Takeout. rootK632APemText: # ftp 192.168.10.10 | |
| Connected to 192.168.10.10. | |
| 220 (sylro 3.0.2) Name (192.168.16.19:root): cyse381 | |
| Balance specify the password, | the second s |
| 230 Login successful. | |
| Remote system type is UNIX. Using binary mode to transfer files. | hite) 400 hites entrued (017 hite) as interfere 0 |
| ftp> get showa086.txt | (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e) |
| Local: showad00.txt remote: showad00.txt remote: showad00.txt internet Protocol Version 4, 5rc: 192 200 PORT command successful, Consider using PASV. | 2.168.10.10, Dst: 192.168.217.3 |
| 150 Opening BINARY mode data connection for showa006.txt (43 bytes). | 011. 20, 051 P011. 37421, 369. 1, AGR. 1, LEN. 43 |
| 220 Transfer Complete. 43 Dytes received in 8-09 secs (1.3228 MB/s) | |
| ftps ftps ftps ftps | Per se |
| Command frame: 98419 | |
| 🚰 • Line-based text data (2 lines) | 10 Mar |
| | |
| | 77 OC 08 00 45 08] [OV] [IV E 9 8 8 8 9 c 0 c 0 8 500 0 |
| | e 28 4a aa 89 18 |
| | 19 al 0/ 1/ 5C 01 11 30 20 30 30 3a A Mon Ju l 10 00: |
| 0059 34 35 3a 33 35 28 56 44 54 29 33 | 12 38 32 33 29 8a 45:35 PD T 2023 |
| | |
| | Activate Windo |
| | Control Sectiones to an anti- |
| | 200 8 0 |
| Istean Revening 🔤 🖉 📀 😤 FTP Data: Protocol | Packets: 102724 - Displayed: 1 (0.0%) Profile: Default |
| 1 🔎 😫 🥘 🚺 Hyper V Manager 👷 Manaker Kall - Eder 🤰 Ubardes 64 kild en S 🧶 phanes - Frenzel E 🎘 Kall - Internal Wink 🗠 Advenishator C.a. | ^ 152 40 7/10/28 |
| J 22 (a) ≤ 10 (b) = 0 (c) | ∧ 🗢 ♥ d0 🐱 1137.99 76/002 |