CYBER FORENSICS (CYFO) VT 24
Lab Assignment

Fernando M. Sanfeliz
Dept. of Computer and Systems Sci.
Stockholm University
Stockholm, Sweden
fesa6676@student.su.se

Gustav Mönefors
Dept. of Computer and Systems Sci.
Stockholm University
Stockholm, Sweden
gumo9296@student.su.se

Silas Pohl
Dept. of Computer and Systems Sci.
Stockholm University
Stockholm, Sweden
sipo6151@student.su.se

April 24, 2024

Assignment 1: Introduction to Network Forensics

A virtual machine running Kali 2024.1 and Wireshark (wireshark:amd64/kali-rolling 4.2.2-1) was used to analyse the .pcap files of assignment 1.

Evidence file:	`1.pcap`
MD5 Hash:	`47451679a42fc2a5a637886e97fd7283`
SHA-1 Hash:	`4623636b88b6293888a3ebcb75cffb767bd11094`

Verifying the hashes

```
$ md5sum 1.pcap
47451679a42fc2a5a637886e97fd7283  1.pcap
$ sha1sum 1.pcap
4623636b88b6293888a3ebcb75cffb767bd11094  1.pcap
```

1. What is/are the source(s) (IP address) of the suspicious traffic?

`192.0.2.245, 192.0.2.196, 192.0.2.207, 192.0.2.6, 192.0.2.25, 192.0.2.120, 192.0.2.83, 192.0.2.154, 192.0.2.253, 192.0.2.236`

2. What is the destination (IP address) of the suspicious traffic?

`192.0.2.2`

3. What is the transport layer protocol used?

Transmission Control Protocol (TCP)

4. What is/are the source port(s)?

`35356, 44463, 23784, 51136, 57003, 20920, 36927, 52048, 62151, 46528`

5. What is/are the destination port(s)?

`64354, 58034, 25895, 62694, 48897, 46680, 35104, 43120, 17166, 19043`

6. What conclusions can you draw from the type of the "attack"/activity illustrated by this pcap?

The network activity observed appears to involve attempts to establish connections with various ports on the destination address 192.0.2.2. This behavior could indicate a port scan, where the scanning party seeks to identify open ports on the target system. While not inherently malicious, port scanning can be a precursor to unauthorized access attempts or reconnaissance activities. Alternatively, the repeated connection attempts to the same destination address could suggest a potential Distributed Denial of Service (DDoS) attack. However, the number of connections initiated (10 in this case) is unlikely to overwhelm a server and cause a significant disruption in service.

Evidence file:	`2.pcap`
MD5 Hash:	`19633e3a2a3d4c315994fddc3ce7090f`
SHA-1 Hash:	`f9d5be156ca124b46450910d2b7b1e79f2f6825c`

Verifying the hashes

```
$ md5sum 2.pcap
19633e3a2a3d4c315994fddc3ce7090f  2.pcap
$ sha1sum 2.pcap
f9d5be156ca124b46450910d2b7b1e79f2f6825c  2.pcap
```

1. What is the source(s) (MAC address) of the suspicious traffic?

`CIMSYS_33:44:55 (00:11:22:33:44:55)`

2. What is/are the destination (MAC address[es]) of where the suspicious traffic is mostly directed towards?

- `Intel_83:13:e8 (00:0e:0c:83:13:e8)` received 3279 packets
- `Broadcast (ff:ff:ff:ff:ff:ff)` received 541 packets
- all other destinations received ≤ 20 packets

3. What is the link layer protocol used?

Address Resolution Protocol (ARP)

4. What is the purpose of this protocol?

The purpose of ARP is to map an IP address to a MAC address on a local network. This mapping is necessary because devices communicate using MAC addresses at the data link layer (Layer 2) of the OSI model, while IP addresses are used at the network layer (Layer 3). When a device on a LAN wants to communicate with another device, it needs to know the MAC address of the target device. ARP helps in this process by broadcasting an ARP request message to all devices on the network, asking for the MAC address corresponding to a specific IP address. The device with the matching IP address responds with its MAC address, allowing the requesting device to establish a direct communication link.[1]

5. What conclusions can you draw from the type of the attack illustrated by this pcap? How can this attack be used for launching other kinds of attacks?

The source MAC address (`CIMSYS_33:44:55`) is consistently sending the suspicious traffic. This suggests that the traffic is likely originating from a single device or attacker. The suspicious traffic is directed towards various MAC addresses, including broadcasting and `Intel_83:13:e8`, as well as other less frequent destinations, such as `ASUSTekCOMPU_1b:32:11`, `AniCommunica_91:12:a8`, etc. This pattern is indicative of ARP poisoning attacks. 516 packets are configured with "Duplicate IP addresses." ARP spoofing involves sending falsified ARP messages over a local area network. Attackers may send ARP replies with their own MAC address in response to ARP requests, causing

network devices to update their ARP caches with incorrect mappings. This allows attackers to intercept, modify, or redirect network traffic. ARP spoofing can be used as a stepping stone for launching other types of attacks, including:

- Man-in-the-Middle (MITM) Attacks: By intercepting and redirecting network traffic, attackers can eavesdrop on communications, steal sensitive information, or modify data packets.
- Denial of Service (DoS) Attacks: ARP spoofing can be used to flood a network with falsified ARP messages, leading to network congestion or disruption of communication between legitimate devices.
- Session Hijacking: By intercepting and manipulating ARP traffic, attackers can hijack established network sessions, gaining unauthorized access to sensitive systems or services.[2]

Evidence file:	`3.pcap`
MD5 Hash:	`0944977919541d4ee176450b7ce36f9d`
SHA-1 Hash:	`7349e1fea8e6ed6b4dce3f89898b1c6492f3a610`

Verifying the hashes

```
$ md5sum 3.pcap
0944977919541d4ee176450b7ce36f9d  3.pcap
$ sha1sum 3.pcap
7349e1fea8e6ed6b4dce3f89898b1c6492f3a610  3.pcap
```

1. What is the source (IP address) of the suspicious traffic?

`10.0.23.109`

2. What is the destination (IP address) of the suspicious traffic?

`80.237.98.132`

3. What is the transport layer protocol used?

Transmission Control Protocol (TCP)

4. This may be considered as not a direct attack but as a preparation step before an attack. Name the technique used and its purpose.

Mostly SYN connections (the first part of the TCP three-way handshake) are observed. TCP Retransmissions occur when the sender fails to receive an acknowledgment (ACK) from the receiver within a certain time period. This behavior indicates a SYN port scanning activity (stealth scan). The purpose of port scanning is to find out which of the ports of the target machine are open to investigate/attack them further in the next step.

Assignment 2: Suspicious Wireless Traffic

1 Introduction

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

2 Methods

3 Results

4 Discussion

Assignment 3: Intrusion Analysis

1 Introduction

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

2 Methods

3 Results

4 Discussion

References

[1] "An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware." RFC 826, 1982.

[2] V. Ramachandran and S. Nandi, "Detecting ARP Spoofing: An Active Technique," in *Information Systems Security* (S. Jajodia and C. Mazumdar, eds.), (Berlin, Heidelberg), pp. 239–250, Springer Berlin Heidelberg, 2005.