Lab 03- ARP Poisoning and DHCP Security

Matthew Belanger

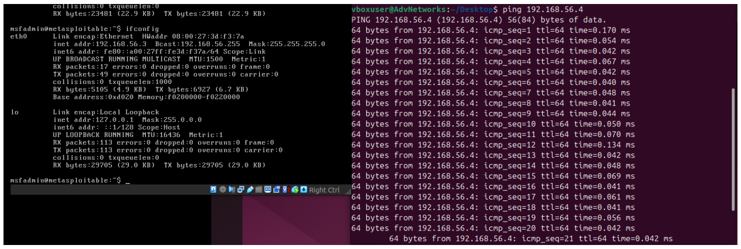
March 4, 2025

1 Task 1: ARP Poisoning Attack

Tasks

1.1 Environment Setup: Create a simple network with two virtual machines (VM1 and VM2) connected through a virtual switch or host-only network. Ensure both VMs can ping each other, confirming network connectivity.

See Figure 1



```
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB)  TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3d:f3:7a
          inet addr:192.168.56.3  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3d:f37a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5105 (4.9 KB)  TX bytes:6927 (6.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29705 (29.0 KB)  TX bytes:29705 (29.0 KB)

msfadmin@metasploitable:~$ _
```

```
vboxuser@AdvNetworks:~/Desktop$ ping 192.168.56.4
PING 192.168.56.4 (192.168.56.4) 56(84) bytes of data.
64 bytes from 192.168.56.4: icmp_seq=1 ttl=64 time=0.170 ms
64 bytes from 192.168.56.4: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 192.168.56.4: icmp_seq=3 ttl=64 time=0.042 ms
64 bytes from 192.168.56.4: icmp_seq=4 ttl=64 time=0.067 ms
64 bytes from 192.168.56.4: icmp_seq=5 ttl=64 time=0.042 ms
64 bytes from 192.168.56.4: icmp_seq=6 ttl=64 time=0.040 ms
64 bytes from 192.168.56.4: icmp_seq=7 ttl=64 time=0.048 ms
64 bytes from 192.168.56.4: icmp_seq=8 ttl=64 time=0.041 ms
64 bytes from 192.168.56.4: icmp_seq=9 ttl=64 time=0.044 ms
64 bytes from 192.168.56.4: icmp_seq=10 ttl=64 time=0.050 ms
64 bytes from 192.168.56.4: icmp_seq=11 ttl=64 time=0.070 ms
64 bytes from 192.168.56.4: icmp_seq=12 ttl=64 time=0.134 ms
64 bytes from 192.168.56.4: icmp_seq=13 ttl=64 time=0.042 ms
64 bytes from 192.168.56.4: icmp_seq=14 ttl=64 time=0.048 ms
64 bytes from 192.168.56.4: icmp_seq=15 ttl=64 time=0.069 ms
64 bytes from 192.168.56.4: icmp_seq=16 ttl=64 time=0.041 ms
64 bytes from 192.168.56.4: icmp_seq=17 ttl=64 time=0.061 ms
64 bytes from 192.168.56.4: icmp_seq=18 ttl=64 time=0.041 ms
64 bytes from 192.168.56.4: icmp_seq=19 ttl=64 time=0.056 ms
64 bytes from 192.168.56.4: icmp_seq=20 ttl=64 time=0.042 ms
        64 bytes from 192.168.56.4: icmp_seq=21 ttl=64 time=0.042 ms
```

Figure 1: VMs Connected

1.2 ARP Security Testing: Write a script using Scapy to perform ARP security testing (pentesting), follow the STRIDE methodology we applied in the class to test and verify the identified vulnerabilities.

See code Repo

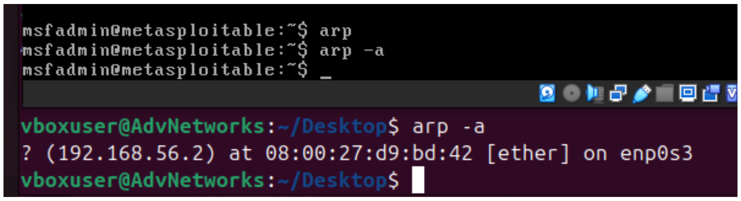
1.3 Mitigation and Report: Discuss and implement basic mitigation strategies against ARP poisoning, such as static ARP entries or using ARP spoofing detection tools.

Report Requirements

Network configurations and ARP tables before and after the attack.

Before

See Figure 2



```
msfadmin@metasploitable:~$ arp
msfadmin@metasploitable:~$ arp -a
msfadmin@metasploitable:~$ _
```

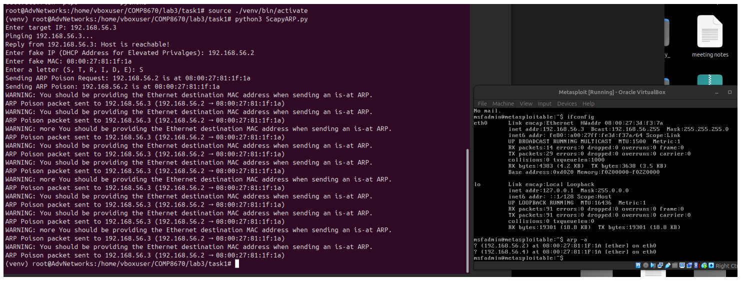
```
vboxuser@AdvNetworks:~/Desktop$ arp -a
? (192.168.56.2) at 08:00:27:d9:bd:42 [ether] on enp0s3
vboxuser@AdvNetworks:~/Desktop$
```

Figure 2: VMs Connected

After

See Figure 3

I am pretending to be the DHCP server here. You can see the ARP table has two IPs with the same MAC.



```
root@AdvNetworks:/home/vboxuser/COMP8670/lab3/task1# source ./venv/bin/activate
(venv) root@AdvNetworks:/home/vboxuser/COMP8670/lab3/task1# python3 ScapyARP.py
Enter target IP: 192.168.56.3
Pinging 192.168.56.3...
Reply from 192.168.56.3: Host is reachable!
Enter fake IP (DHCP Address for Elevated Privalges): 192.168.56.2
Enter fake MAC: 08:00:27:81:1f:1a
Enter a letter (S, T, R, I, D, E): S
Sending ARP Poison Request: 192.168.56.2 is at 08:00:27:81:1f:1a
Sending ARP Poison: 192.168.56.2 is at 08:00:27:81:1f:1a
WARNING: You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: more You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: more You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: more You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
WARNING: You should be providing the Ethernet destination MAC address when sending an is-at ARP.
ARP Poison packet sent to 192.168.56.3 (192.168.56.2 → 08:00:27:81:1f:1a)
(venv) root@AdvNetworks:/home/vboxuser/COMP8670/lab3/task1#
```

meeting notes
Metasploit [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3d:f3:7a
          inet addr:192.168.56.3  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3d:f37a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4383 (4.2 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ arp -a
? (192.168.56.2) at 08:00:27:81:1F:1A [ether] on eth0
? (192.168.56.4) at 08:00:27:81:1F:1A [ether] on eth0
msfadmin@metasploitable:~$
```

Figure 3: Poisoning Screenshot

Scapy scripts used.

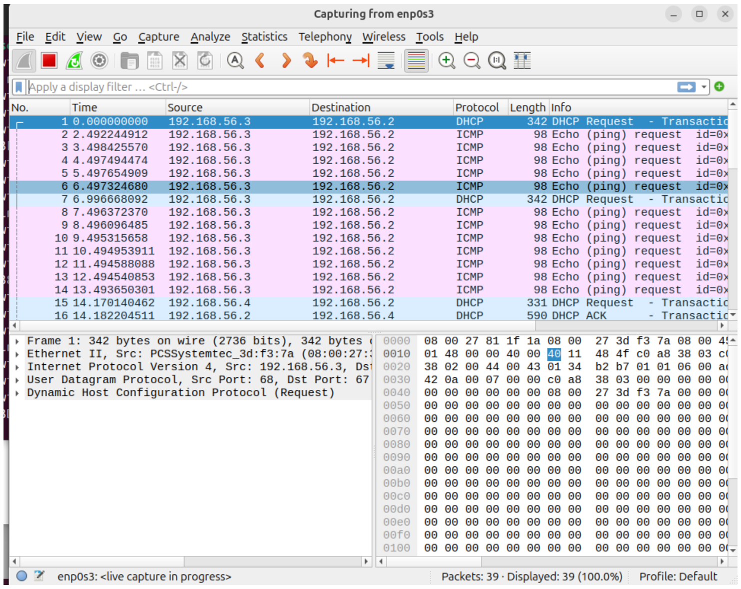
See code Repo

Screenshots demonstrating the success of the attack, including Wireshark captures.

In figure 4 I pretend to be the DHCP server at 192.168.56.2 (actual IP 192.168.56.4). On the victim machine I ping the DHCP server but the packets are recieved on hackers machine.

Discussion on mitigation strategies.

See section 1.3


Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.3	192.168.56.2	DHCP	342	DHCP Request - Transactic
2	2.492244912	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
3	3.498425570	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
4	4.497494474	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
5	5.497654909	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
6	6.497324680	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
7	6.996668092	192.168.56.3	192.168.56.2	DHCP	342	DHCP Request - Transactic
8	7.496372370	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
9	8.496096485	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
10	9.495315658	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
11	10.494953911	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
12	11.494588088	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
13	12.494540853	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
14	13.493650301	192.168.56.3	192.168.56.2	ICMP	98	Echo (ping) request id=0x
15	14.170140462	192.168.56.4	192.168.56.2	DHCP	331	DHCP Request - Transactic
16	14.182204511	192.168.56.2	192.168.56.4	DHCP	590	DHCP ACK - Transactic

```
Frame 1: 342 bytes on wire (2736 bits), 342 bytes (
Ethernet II, Src: PCSSystemtec_3d:f3:7a (08:00:27:3
Internet Protocol Version 4, Src: 192.168.56.3, Dst
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
```

```
0000  08 00 27 81 1f 1a 08 00  27 3d f3 7a 08 00 45
0010  01 48 00 00 40 00 40 11  48 4f c0 a8 38 03 c0
0020  38 02 00 44 00 43 01 34  b2 b7 01 01 06 00 ac
0030  42 0a 00 07 00 00 c0 a8  38 03 00 00 00 00 00
0040  00 00 00 00 00 00 08 00  27 3d f3 7a 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
```

enp0s3: <live capture in progress> Packets: 39 · Displayed: 39 (100.0%) Profile: Default

Figure 4: Wireshark Spoof

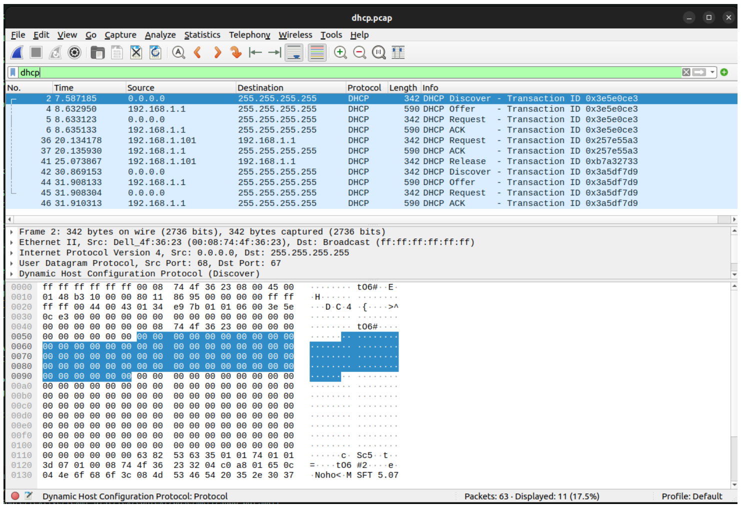
2 Task 2: Security Analysis of The DHCP

2.1 Start Wireshark open the enclosed pcap trace file and list all the DHCP packets in the trace. Use screenshots to support your answer.

See Figure 5

2.2 Create a Finite State Machine model for the DHCP process.

See Figure 6


dhcp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time        Source          Destination      Protocol  Length Info
    2 7.587185    0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0x3e5e0ce3
    4 8.632950    192.168.1.1     255.255.255.255  DHCP       590 DHCP Offer    - Transaction ID 0x3e5e0ce3
    5 8.633123    0.0.0.0         255.255.255.255  DHCP       342 DHCP Request  - Transaction ID 0x3e5e0ce3
    6 8.635133    192.168.1.1     255.255.255.255  DHCP       590 DHCP ACK      - Transaction ID 0x3e5e0ce3
   36 20.134178   192.168.1.101   192.168.1.1      DHCP       342 DHCP Request  - Transaction ID 0x257e55a3
   37 20.135930   192.168.1.1     255.255.255.255  DHCP       590 DHCP ACK      - Transaction ID 0x257e55a3
   41 25.073867   192.168.1.101   192.168.1.1      DHCP       342 DHCP Release  - Transaction ID 0xb7a32733
   42 30.869153   0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0x3a5df7d9
   44 31.908133   192.168.1.1     255.255.255.255  DHCP       590 DHCP Offer    - Transaction ID 0x3a5df7d9
   45 31.908304   0.0.0.0         255.255.255.255  DHCP       342 DHCP Request  - Transaction ID 0x3a5df7d9
   46 31.910313   192.168.1.1     255.255.255.255  DHCP       590 DHCP ACK      - Transaction ID 0x3a5df7d9
```

```
▸ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▸ Dynamic Host Configuration Protocol (Discover)
```

```
0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 00 45 00   ········ tO6#··E·
0010  01 48 b3 10 00 00 80 11  86 95 00 00 00 00 ff ff   ·H······ ········
0020  ff ff 00 44 00 43 01 34  e9 7b 01 01 06 00 3e 5e   ···D·C·4 ·{····>^
0030  0c e3 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 08  74 4f 36 23 00 00 00 00   ········ tO6#····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 74 01 01   ······c· Sc5··t··
0120  3d 07 01 00 08 74 4f 36  23 32 04 c0 a8 01 65 0c   =····tO6 #2····e·
0130  04 4e 6f 68 6f 3c 08 4d  53 46 54 20 35 2e 30 37   ·Noho<·M SFT 5.07
```

Dynamic Host Configuration Protocol: Protocol
Packets: 63 · Displayed: 11 (17.5%)
Profile: Default

Figure 5: DHCP Packet List

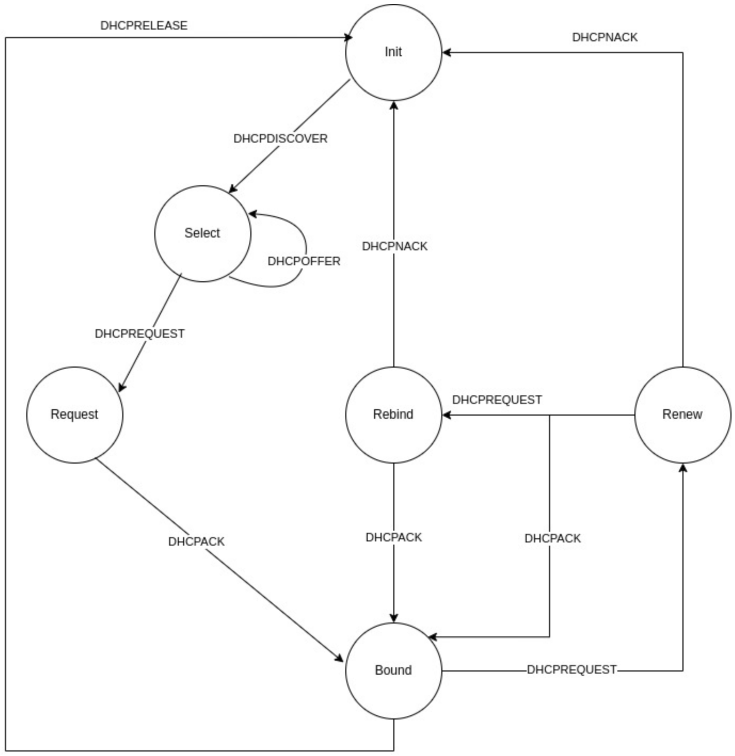


Figure 6: DHCP Finite State Machine

2.3 Apply the STRIDE methodology to the FSM model of DHCP to identify potential security threats. For each STRIDE element, identify possible vulnerabilities in the DHCP process.

2.3.1 Spoofing

2.3.2 Tampering

2.3.3 Repudiation

2.3.4 Information Disclosure

2.3.5 Denial of Service

2.3.6 Elevation of Privilege

2.4 Propose mitigation strategies for each identified vulnerability. This could involve protocol enhance- ments, configuration changes, or additional security mechanisms.

2.4.1 Spoofing

2.4.2 Tampering

2.4.3 Repudiation

2.4.4 Information Disclosure

2.4.5 Denial of Service

2.4.6 Elevation of Privilege