

Computer Security Capstone Project 2 Report - 0816102 陳品戎

Item 1. scenario II

ARP spoofing

| icmp | | | | | | | Expression... | + |
|---|-----------------|---------------|---------------|----------|--------|---------------------|---------------|---|
| No. | Time | Source | Destination | Protocol | Length | Info | | |
| 29708 | 1993.8403384... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request | | |
| 29709 | 1993.8438630... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request | | |
| 29710 | 1993.8498625... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply | | |
| 29711 | 1993.8548402... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply | | |
| ▶ Frame 29708: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0 | | | | | | | | |
| ▶ Ethernet II, Src: Vmware_48:33:a1 (00:0c:29:48:33:a1), Dst: Vmware_27:dd:9a (00:0c:29:27:dd:9a) | | | | | | | | |
| ▶ Internet Protocol Version 4, Src: 192.168.5.131, Dst: 8.8.8.8 | | | | | | | | |
| ▶ Internet Control Message Protocol | | | | | | | | |

victim to attacker

| | | | | | | |
|-------|-----------------|---------------|---------------|------|----|---------------------|
| 29708 | 1993.8403384... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request |
| 29709 | 1993.8438630... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request |
| 29710 | 1993.8498625... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply |
| 29711 | 1993.8548402... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply |

<

attacker to AP

| | | | | | | | |
|---|-------|-----------------|---------------|---------------|------|----|---------------------|
| + | 29708 | 1993.8403384... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request |
| | 29709 | 1993.8438630... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request |
| + | 29710 | 1993.8498625... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply |
| | 29711 | 1993.8548402... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply |

▶ Frame 29710: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

▶ Ethernet II, Src: Vmware_e7:ee:04 (00:50:56:e7:ee:04), Dst: Vmware_27:dd:9a (00:0c:29:27:dd:9a)

▶ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.5.131

▶ Internet Control Message Protocol

AP to attacker

| | | | | | | |
|-------|-----------------|---------------|---------------|------|----|---------------------|
| 29708 | 1993.8403384... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request |
| 29709 | 1993.8438630... | 192.168.5.131 | 8.8.8.8 | ICMP | 98 | Echo (ping) request |
| 29710 | 1993.8498625... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply |
| 29711 | 1993.8548402... | 8.8.8.8 | 192.168.5.131 | ICMP | 98 | Echo (ping) reply |

▶ Frame 29711: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

▶ Ethernet II, Src: Vmware_27:dd:9a (00:0c:29:27:dd:9a), Dst: Vmware_48:33:a1 (00:0c:29:48:33:a1)

▶ Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.5.131

▶ Internet Control Message Protocol

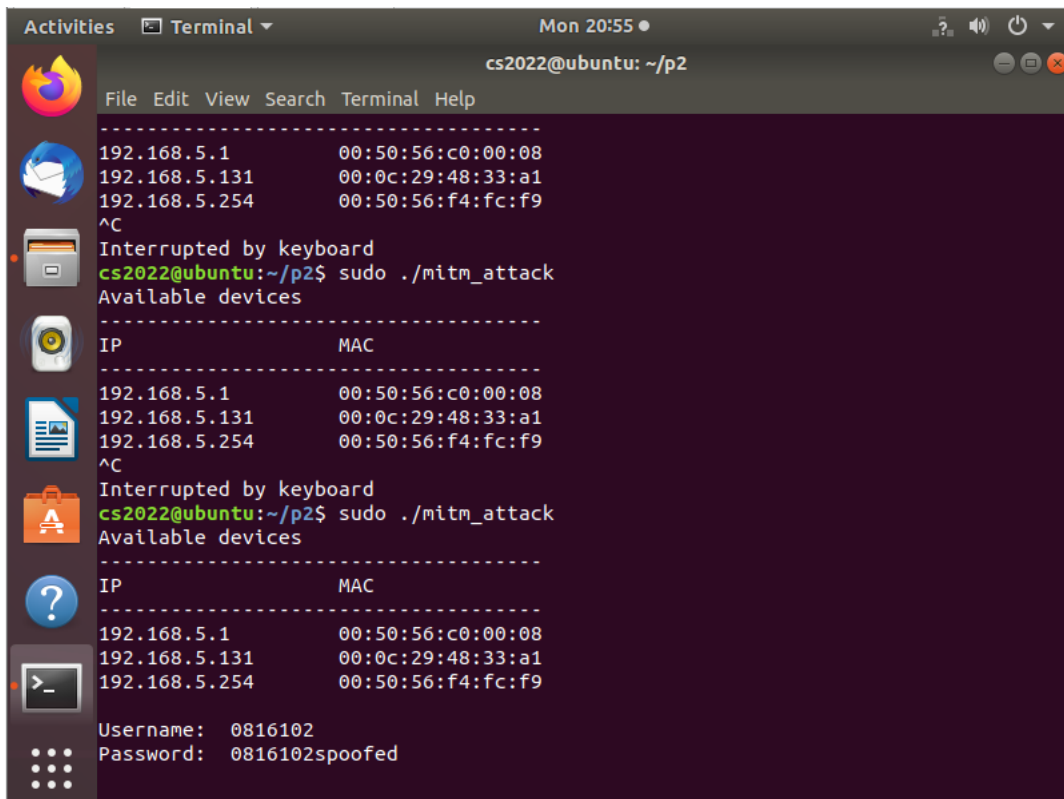
attacker to victim

↑ Ping command from victim

MITM attack



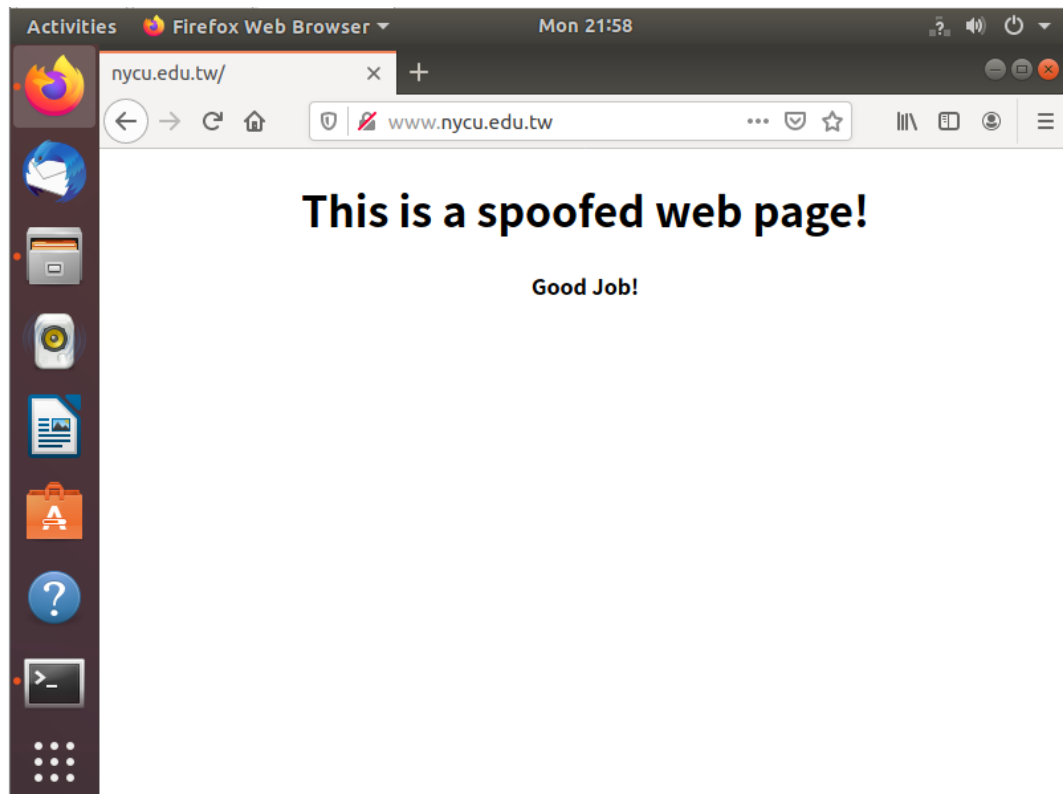
↑ victim



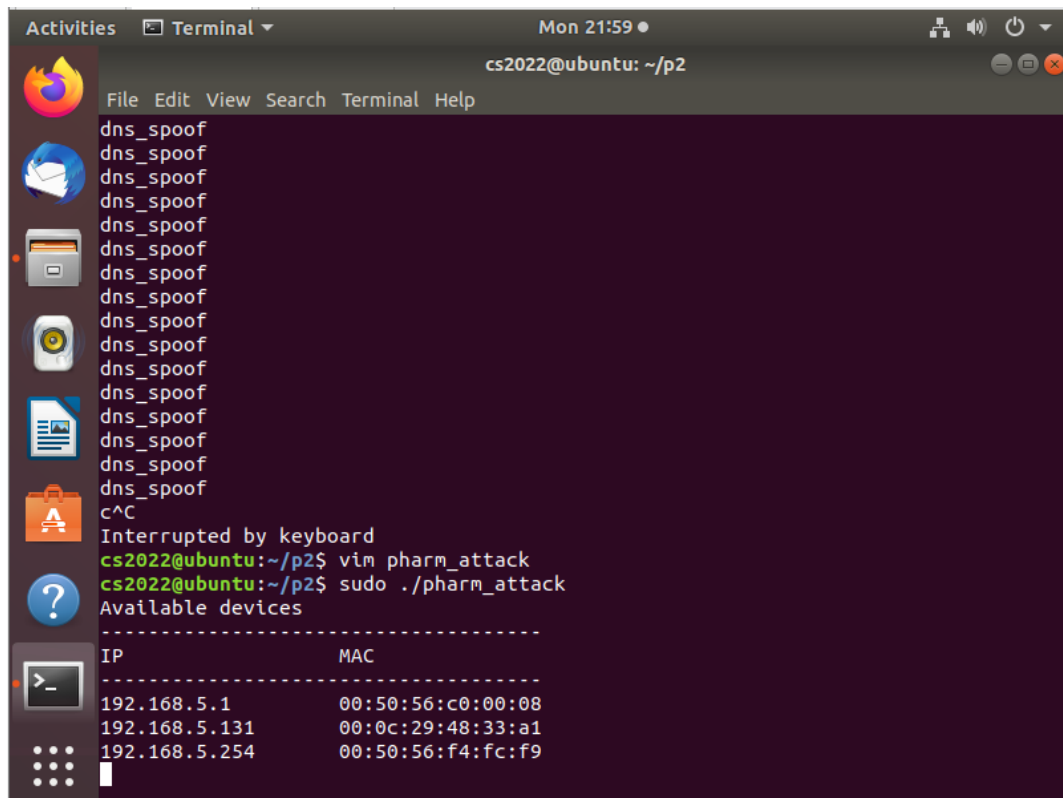
↑ attacker

Item 2: scenario II

DNS spoofing



↑ victim



↑ attacker

Item 3. Defend against the ARP spoofing attack

Ignore ARP responses which do not appear with its request. Every device uses static ARP table in a local network. Keep sending correct ARP response at intervals.