

Network Sniffing

Introduction



Author Gus Khawaja

Gus.Khawaja@guskhawaja.me

www.ethicalhackingblog.com

Network Monitoring

Process

Collection

```
0000 8e 8d 6e 1c 34 ed e1 58 72 3e 32 12 14 00 3b 01
0010 e8 00 00 00 ec 20 b1 b9 3c 6d 6f 64 75 6c 65 73
0020 3e 3c 6d 6f 64 75 6c 65 3e 3c 76 65 72 73 69 6f
0030 6e 3e 31 31 33 3c 2f 76 65 72 73 69 6f 6e 3e 3c
0040 6e 61 6d 65 3e 69 6d 6d 6f 64 75 6c 65 3c 2f 6e
0050 61 6d 65 3e 3c 6d 6f 64 75 6c 65 69 64 3e 31 31
0060 32 3c 2f 6d 6f 64 75 6c 65 69 64 3e 3c 63 72 63
0070 3e 33 32 35 30 38 36 34 39 35 33 3c 2f 63 72 63
0080 3e 3c 2f 6d 6f 64 75 6c 65 3e 3c 6d 6f 64 75 6c
0090 65 3e 3c 76 65 72 73 69 6f 6e 3e 31 30 33 3c 2f
00a0 76 65 72 73 69 6f 6e 3e 3c 6e 61 6d 65 3e 73 6e
00b0 69 66 6d 6f 64 75 6c 65 3c 2f 6e 61 6d 65 3e
00c0 3c 6d 6f 64 75 6c 65 69 64 3e 31 31 35 3c 2f 6d
```

Conversion

```
⊕ Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
⊕ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊕ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊕ Transmission Control Protocol, Src Port: ncu-2 (3196), Dst Port: http (80), Seq: 0, Len: 0
    Source port: ncu-2 (3196)
    Destination port: http (80)
    [Stream index: 5]
    Sequence number: 0 (relative sequence number)
    Header length: 28 bytes
⊕ Flags: 0x02 (SYN)
    window size value: 64240
```

Analysis



Network Checklist

- ✓ IP ranges
- ✓ Communication equipment
- ✓ Security devices
- ✓ Application/Port numbers
- ✓ Network scan report

Suspicious Traffic

Normal	!!! Suspicious !!!
Known IP address	Unknown IP address
Standard port numbers	Unusual port numbers
Normal TCP patterns	Unusual TCP patterns
Variable bandwidth	Fixed bandwidth
Small amount of broadcasts	Huge amount of broadcasts
Standard DNS query	Massive amount of DNS queries

Attack Types

Malware

DOS/DDOS

MITM

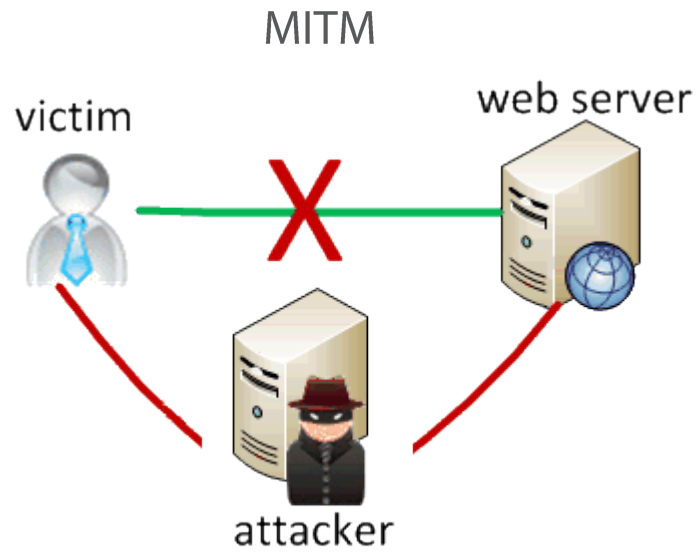
Scanning

Brute-Force

Application

Sniffing with Wireshark

Sniffing Methods



Network tap

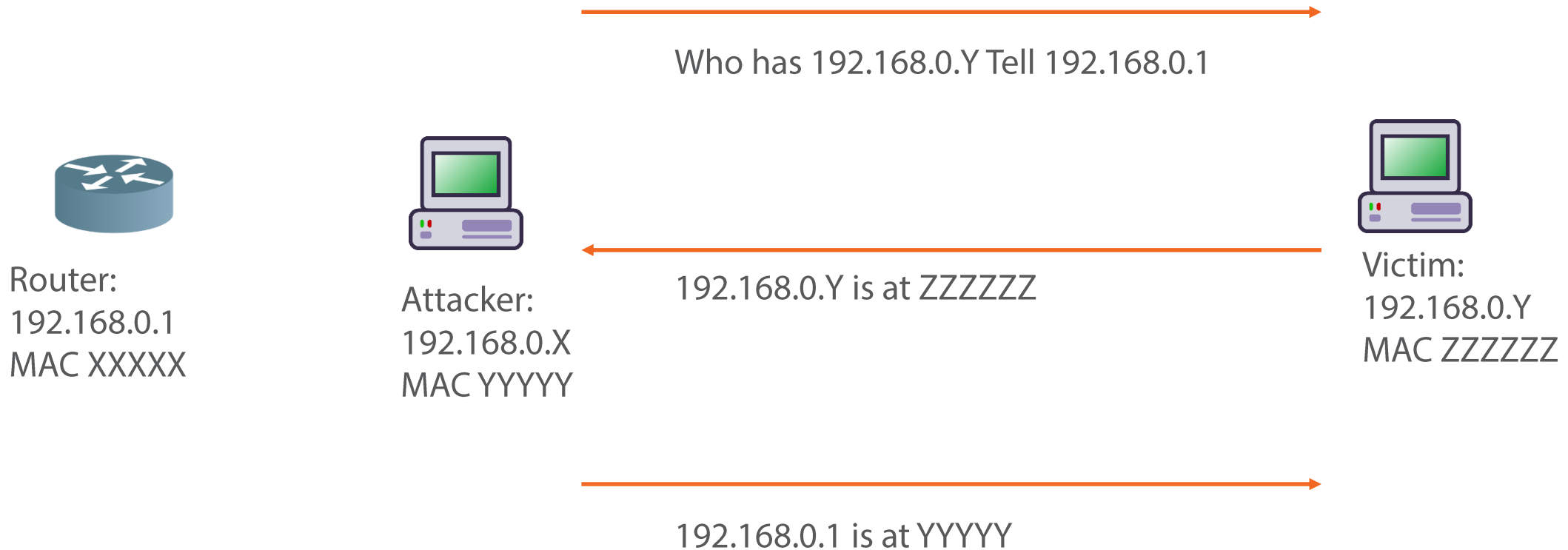


Port mirroring



Detecting MITM

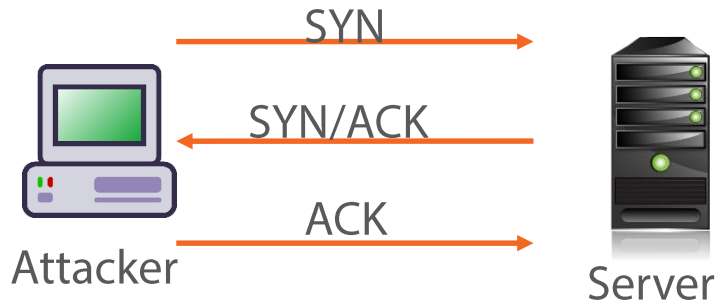
ARP Spoofing Setup



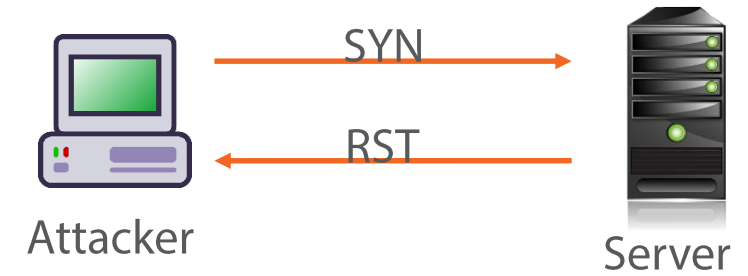
Detecting SYN Scan

TCP SYN Scan

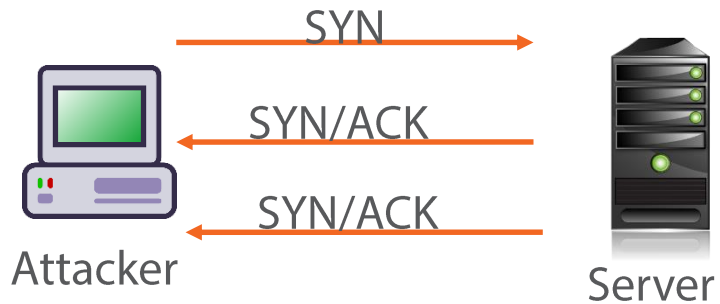
TCP Handshake



Closed Port 80



Open Port 80

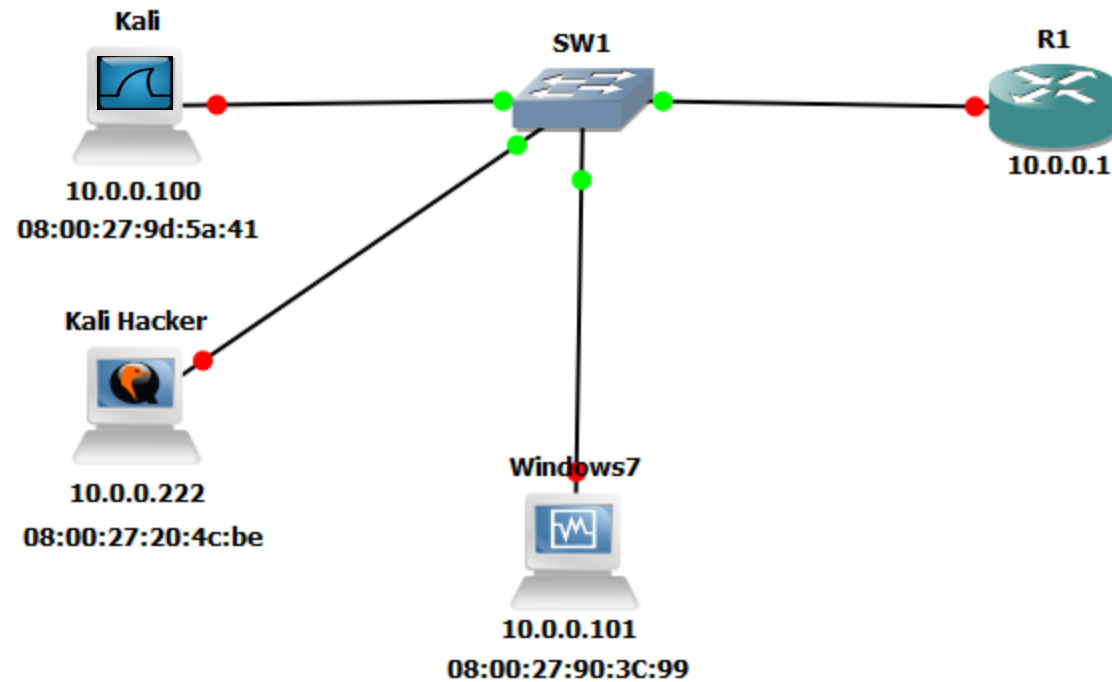


Filtered Port 80



Understanding Brute Force Attack

Our Lab



Clear Text Protocols

- ✓ Internet – HTTP
- ✓ File transfer – FTP / TFTP
- ✓ Email – POP3 / IMAP / SMTP
- ✓ Telnet
- ✓ VoIP

Discovering DOS/DDOS Attacks

Summary

MITM

SYN Scan

Brute-Force

DOS

The image shows a Wireshark packet capture of a network session. The top pane displays a list of 40 packets. Packets 13 through 15 show a SYN scan sequence from 192.168.0.10 to 192.168.0.2. Packet 13 is a SYN packet (Seq: 404510823, Ack: 0, Win: 0). Packet 14 is a SYN-ACK packet (Seq: 366103101, Ack: 404510824, Win: 65535). Packet 15 is an ACK packet (Seq: 366103101, Ack: 404510824, Win: 65535). Packets 17 through 20 show a successful TCP connection establishment. Packet 21 is an HTTP GET request for / HTTP/1.1. The bottom pane shows the details of the selected packet (packet 21), displaying the Ethernet II, Internet Protocol, and Hypertext Transfer Protocol layers. The HTTP layer shows a GET request for / HTTP/1.1 with various headers including User-Agent, Accept, Accept-Language, Accept-Encoding, Accept-Charset, Keep-Alive, and Connection.

No.	Time	Source	Destination	Protocol	Info
13	14.817570	192.168.0.10	192.168.0.2	TCP	1342 → 80 [SYN] Seq=404510823 Ack=0 Win=0
14	14.817999	192.168.0.2	192.168.0.10	TCP	80 → 1342 [SYN, ACK] Seq=366103101 Ack=404510824
15	14.818278	192.168.0.10	192.168.0.2	TCP	1342 → 80 [ACK] Seq=404510824 Ack=366103101
17	14.873815	192.168.0.2	192.168.0.10	TCP	80 → 1342 [ACK] Seq=366103105 Ack=404511203
18	14.873815	192.168.0.10	192.168.0.2	TCP	1342 → 80 [FIN, ACK] Seq=404511210 Ack=366103105
19	14.873815	192.168.0.2	192.168.0.10	TCP	80 → 1342 [ACK] Seq=366103105 Ack=404511203
20	14.873815	192.168.0.10	192.168.0.2	TCP	1342 → 80 [RST] Seq=404511210 Ack=366103105
21	14.873815	192.168.0.10	192.168.0.2	HTTP	GET / HTTP/1.1