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 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

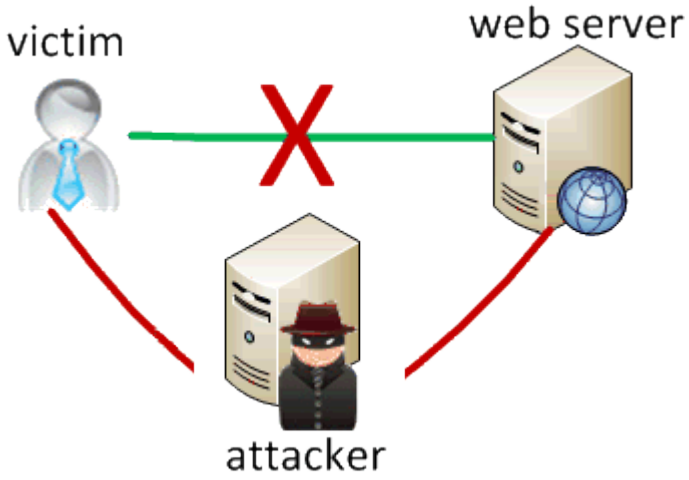
Brute-Force

Application

Sniffing with Wireshark

Sniffing Methods

MITM



Network tap

Port mirroring

Detecting MITM

ARP Spoofing Setup

Router:
192.168.0.1
MAC XXXXX

Attacker:
192.168.0.X
MAC YYYYY

Who has 192.168.0.Y Tell 192.168.0.1

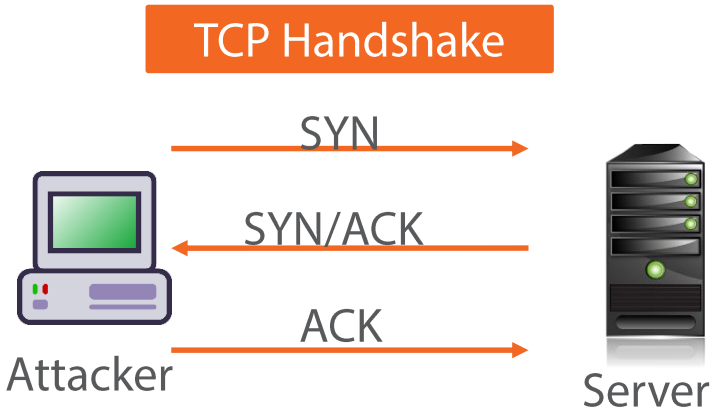
192.168.0.Y is at ZZZZZZ

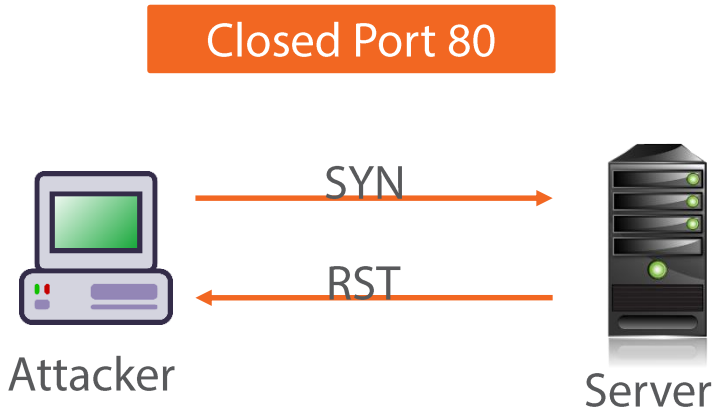
192.168.0.1 is at YYYYY

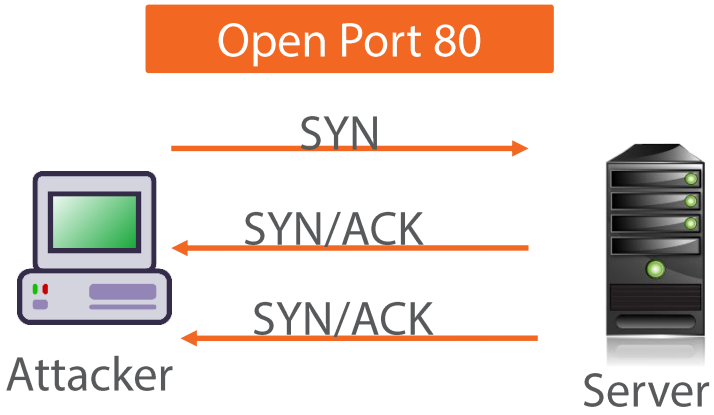
Victim:
192.168.0.Y
MAC ZZZZZZ

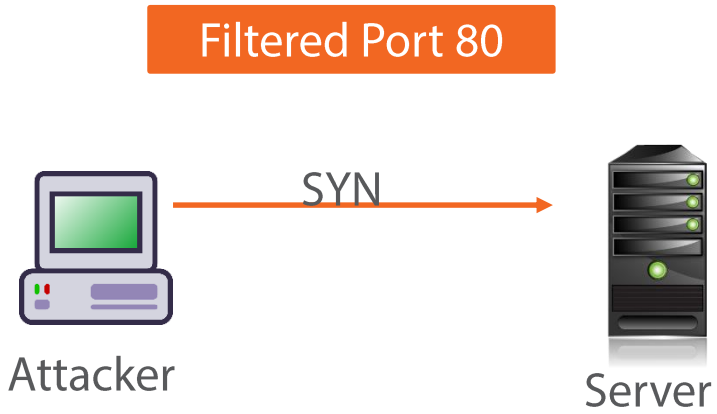
Detecting SYN Scan

TCP SYN Scan



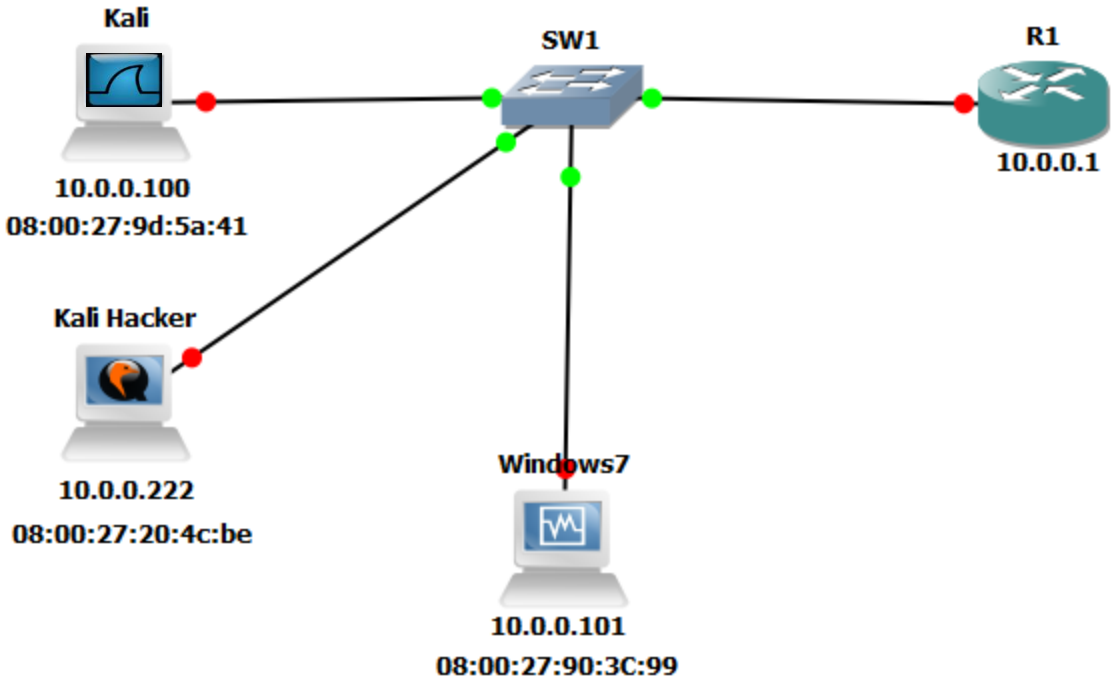






Understanding Brute Force Attack

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