Server Exploits

Section 1

Objectives

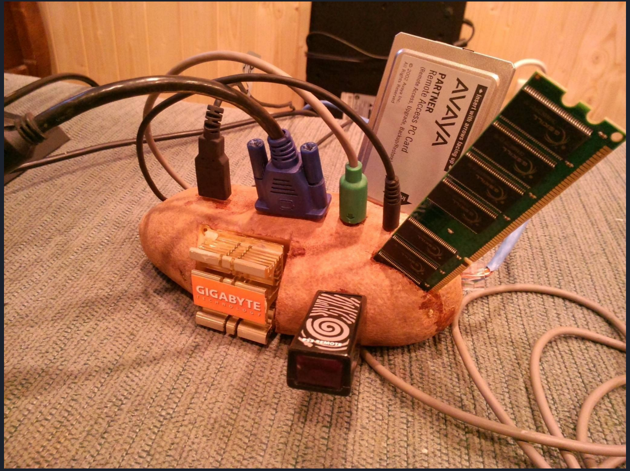
Install and configure server-side technology using industry-accepted practices.

- Install web/application server software in a secure OS.
- Describe the relationship between client-side and server-side tools and protocols
- Describe potential security risks in client-server systems and available mitigation strategies.

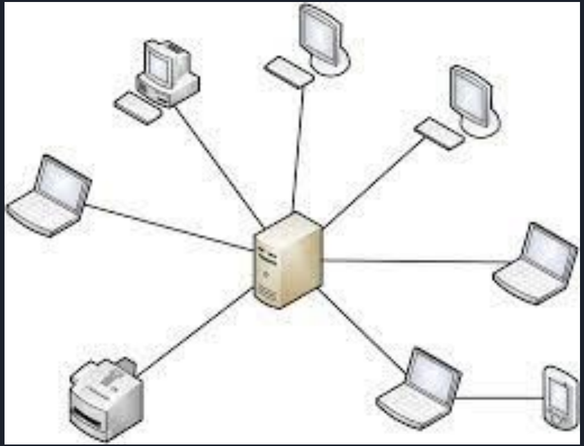
Servers

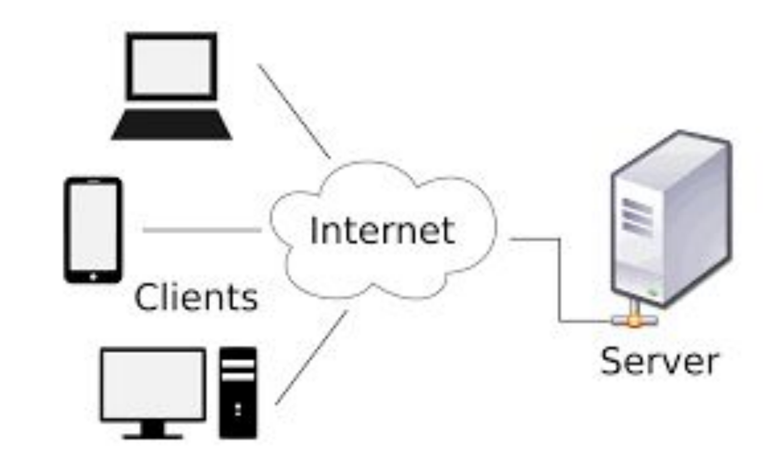
- Provides services to a client
- Usually always on
- Always listening for connections from clients (listener)
- Can accept more than 1 connection for a service

Servers



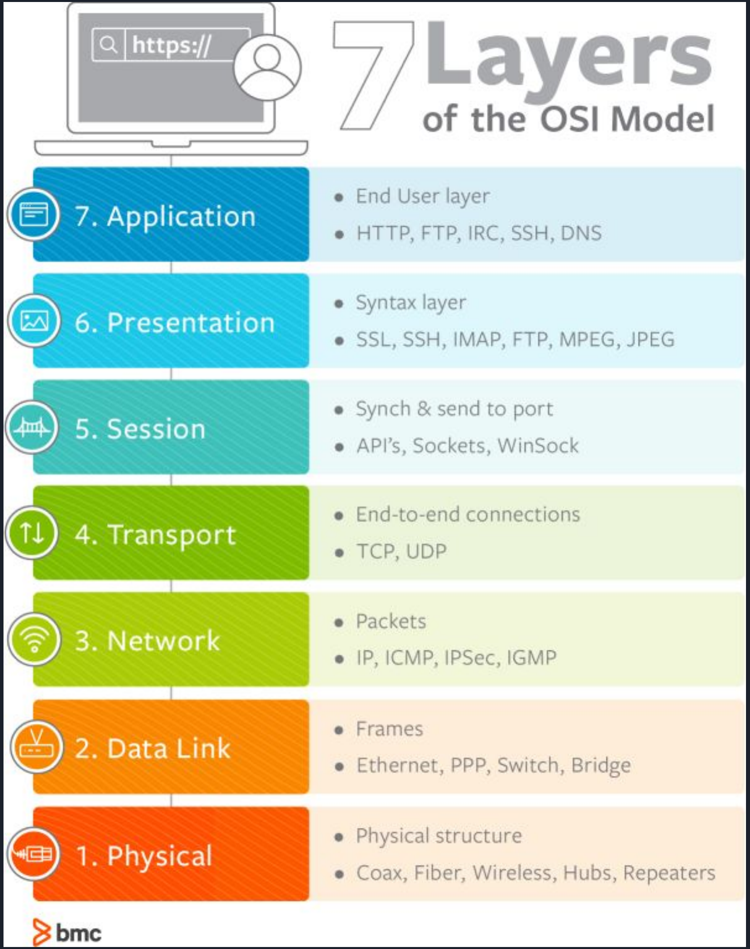
Client - Server Relationship





OSI Layers

- Open Systems Interconnection
- A Standard model for network communications



7 Layers of the OSI Model

7. Application	End User layer HTTP, FTP, IRC, SSH, DNS
6. Presentation	Syntax layer SSL, SSH, IMAP, FTP, MPEG, JPEG
5. Session	Synch & send to port API's, Sockets, WinSock
4. Transport	End-to-end connections TCP, UDP
3. Network	Packets IP, ICMP, IPSec, IGMP
2. Data Link	Frames Ethernet, PPP, Switch, Bridge
1. Physical	Physical structure Coax, Fiber, Wireless, Hubs, Repeaters

bmc

1. Physical Layer

- Server Hardware
- Network Cables
- Transports bits

2. Data Link Layer

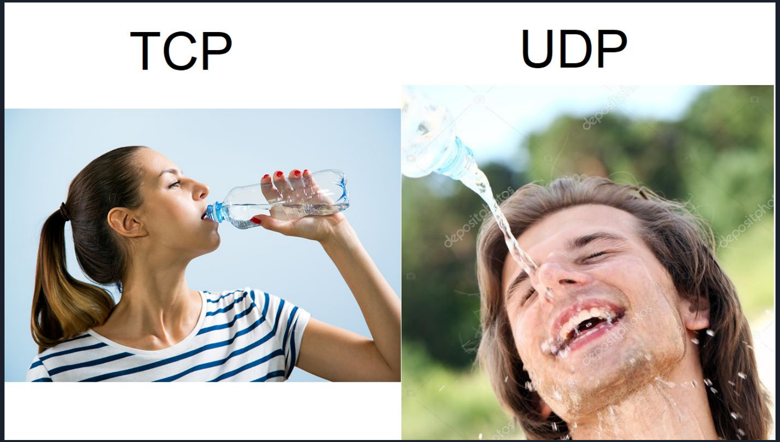
- Node-to-node transfer
- Switches
- MAC

3. Network Layer

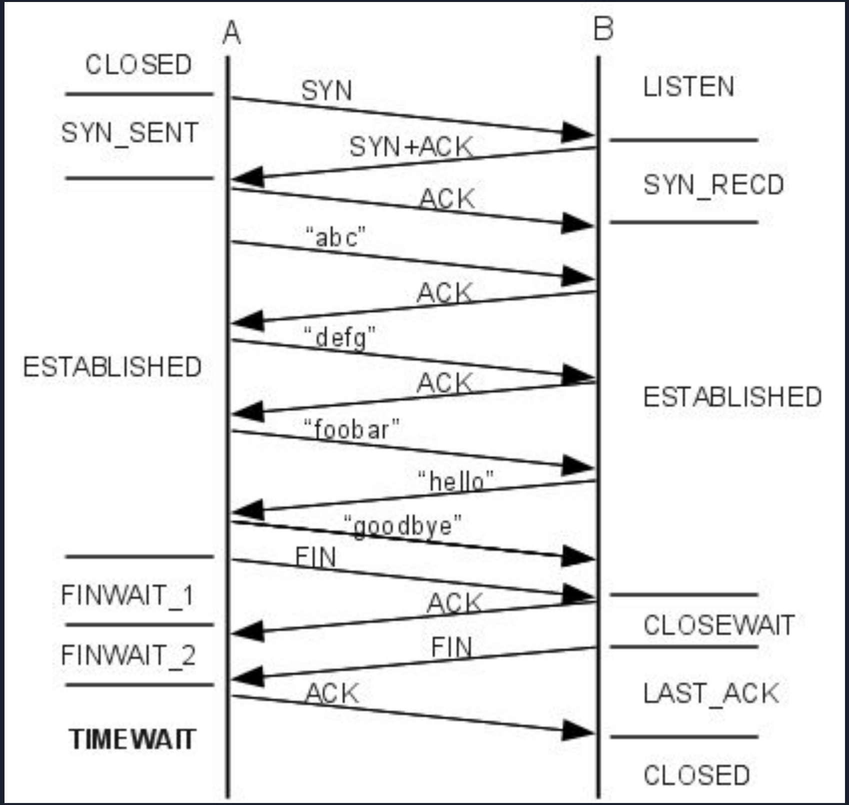
- Router functionality
- IP Addresses
- A good bulk of network configuration

4. Transport

- TCP/UDP
- Manages network traffic between end systems to ensure complete data Transfer
- Controls where and how much data is sent



TCP Connections



5. Session Layer

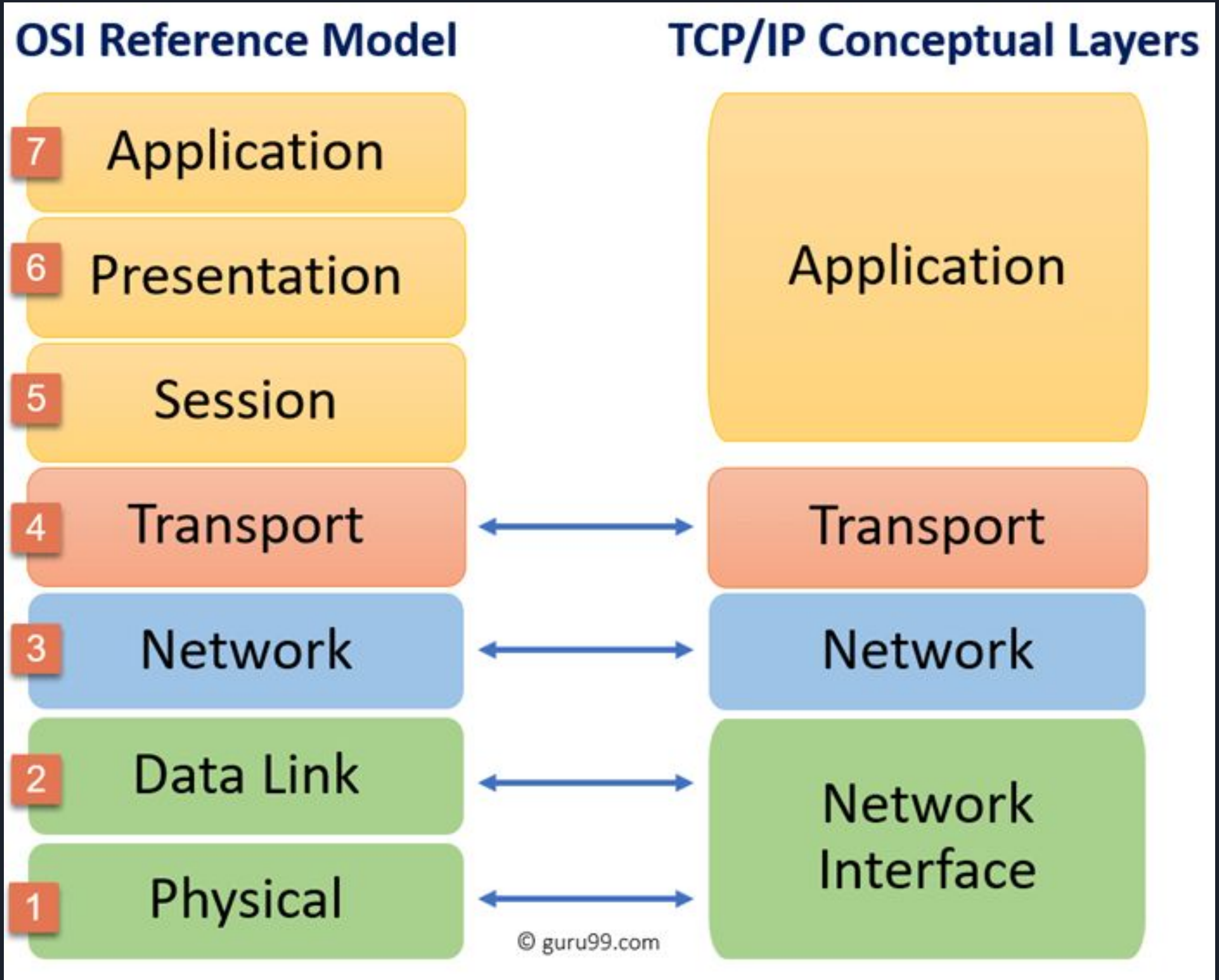
- Application to Application
- Manages sessions
- RPC (Remote Procedure Call) in Windows
  - Supports communications between Windows network Applications
  - Used if File Sharing
- Appletalk

6. Presentation

- Encryption (SSL/TLS)
- Preparation of data for application layer

7. Application

- Closest to end user
- HTTP, SMB, SSH



OSI Reference Model

TCP/IP Conceptual Layers

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

Application

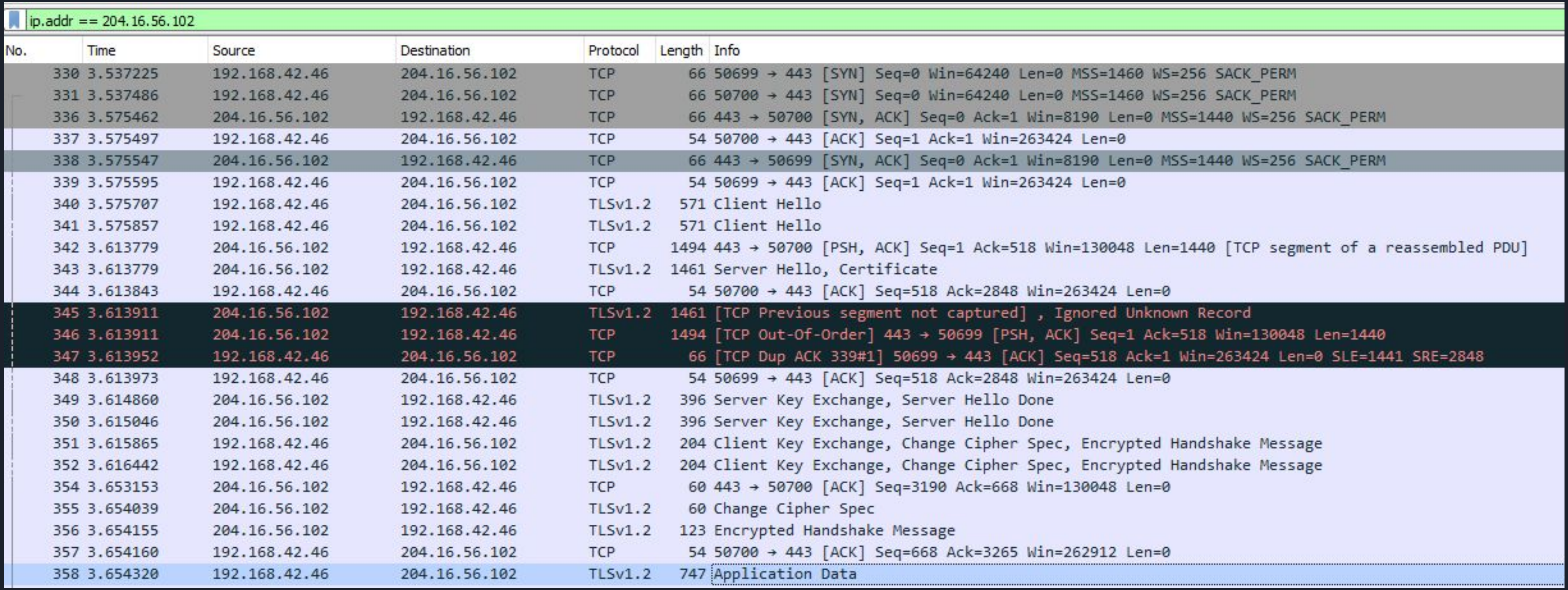
Transport

Network

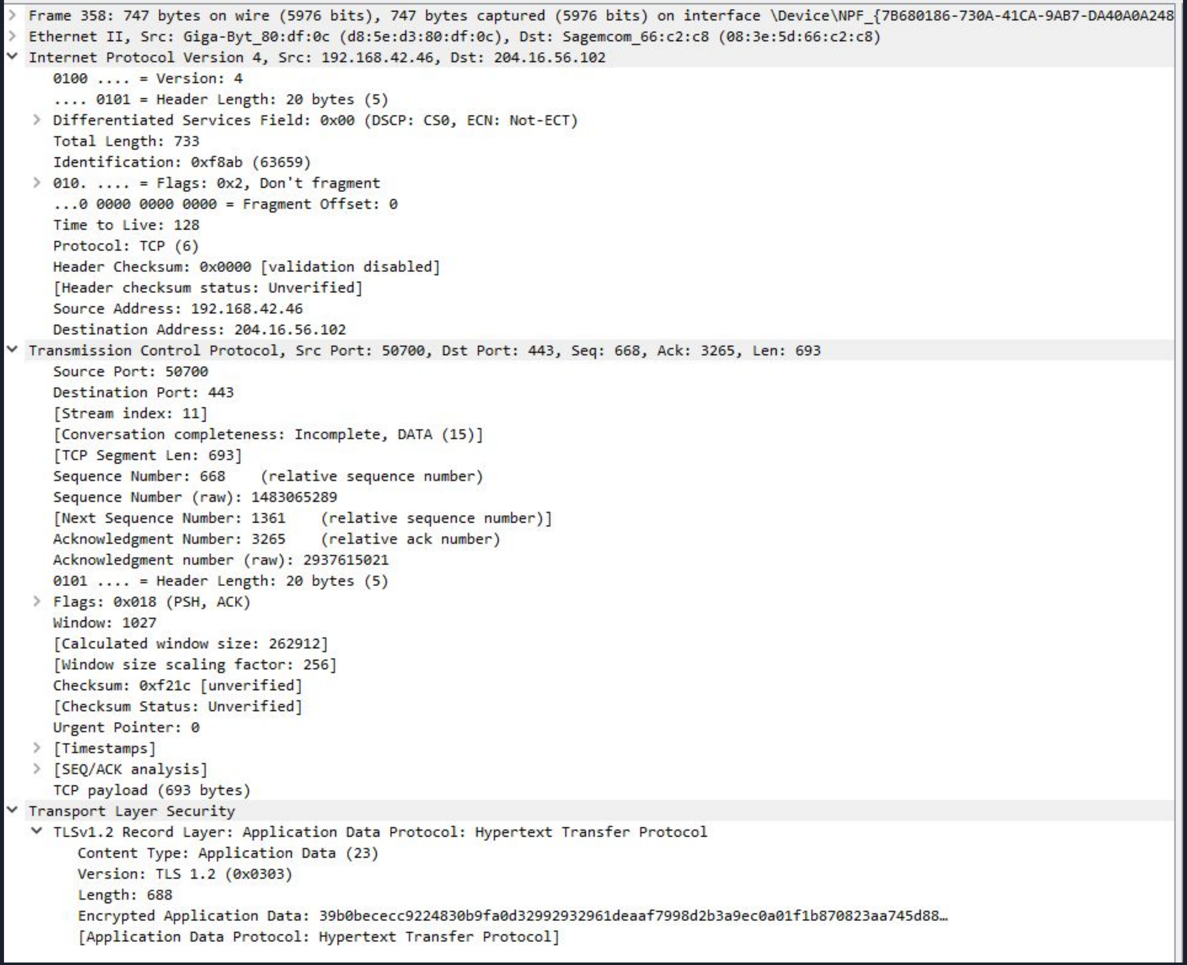
Network Interface

© guru99.com

Wireshark



```
ip.addr == 204.16.56.102

No.   Time      Source          Destination     Protocol  Length Info
  330 3.537225  192.168.42.46   204.16.56.102   TCP         66 50699 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  331 3.537486  192.168.42.46   204.16.56.102   TCP         66 50700 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  336 3.575462  204.16.56.102   192.168.42.46   TCP         66 443 → 50700 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1440 WS=256 SACK_PERM
  337 3.575497  192.168.42.46   204.16.56.102   TCP         54 50700 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
  338 3.575547  204.16.56.102   192.168.42.46   TCP         66 443 → 50699 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1440 WS=256 SACK_PERM
  339 3.575595  192.168.42.46   204.16.56.102   TCP         54 50699 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
  340 3.575707  192.168.42.46   204.16.56.102   TLSv1.2    571 Client Hello
  341 3.575857  192.168.42.46   204.16.56.102   TLSv1.2    571 Client Hello
  342 3.613779  204.16.56.102   192.168.42.46   TCP       1494 443 → 50700 [PSH, ACK] Seq=1 Ack=518 Win=130048 Len=1440 [TCP segment of a reassembled PDU]
  343 3.613779  204.16.56.102   192.168.42.46   TLSv1.2   1461 Server Hello, Certificate
  344 3.613843  192.168.42.46   204.16.56.102   TCP         54 50700 → 443 [ACK] Seq=518 Ack=2848 Win=263424 Len=0
  345 3.613911  204.16.56.102   192.168.42.46   TLSv1.2   1461 [TCP Previous segment not captured] , Ignored Unknown Record
  346 3.613911  204.16.56.102   192.168.42.46   TCP       1494 [TCP Out-Of-Order] 443 → 50699 [PSH, ACK] Seq=1 Ack=518 Win=130048 Len=1440
  347 3.613952  192.168.42.46   204.16.56.102   TCP         66 [TCP Dup ACK 339#1] 50699 → 443 [ACK] Seq=518 Ack=1 Win=263424 Len=0 SLE=1441 SRE=2848
  348 3.613973  192.168.42.46   204.16.56.102   TCP         54 50699 → 443 [ACK] Seq=518 Ack=2848 Win=263424 Len=0
  349 3.614860  204.16.56.102   192.168.42.46   TLSv1.2    396 Server Key Exchange, Server Hello Done
  350 3.615046  204.16.56.102   192.168.42.46   TLSv1.2    396 Server Key Exchange, Server Hello Done
  351 3.615865  192.168.42.46   204.16.56.102   TLSv1.2    204 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  352 3.616442  192.168.42.46   204.16.56.102   TLSv1.2    204 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  354 3.653153  204.16.56.102   192.168.42.46   TCP         60 443 → 50700 [ACK] Seq=3190 Ack=668 Win=130048 Len=0
  355 3.654039  204.16.56.102   192.168.42.46   TLSv1.2     60 Change Cipher Spec
  356 3.654155  204.16.56.102   192.168.42.46   TLSv1.2    123 Encrypted Handshake Message
  357 3.654160  192.168.42.46   204.16.56.102   TCP         54 50700 → 443 [ACK] Seq=668 Ack=3265 Win=262912 Len=0
  358 3.654320  192.168.42.46   204.16.56.102   TLSv1.2    747 Application Data
```



```
> Frame 358: 747 bytes on wire (5976 bits), 747 bytes captured (5976 bits) on interface \Device\NPF_{7B680186-730A-41CA-9AB7-DA40A0A248
> Ethernet II, Src: Giga-Byt_80:df:0c (d8:5e:d3:80:df:0c), Dst: Sagemcom_66:c2:c8 (08:3e:5d:66:c2:c8)
v Internet Protocol Version 4, Src: 192.168.42.46, Dst: 204.16.56.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 733
    Identification: 0xf8ab (63659)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.42.46
    Destination Address: 204.16.56.102
v Transmission Control Protocol, Src Port: 50700, Dst Port: 443, Seq: 668, Ack: 3265, Len: 693
    Source Port: 50700
    Destination Port: 443
    [Stream index: 11]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 693]
    Sequence Number: 668    (relative sequence number)
    Sequence Number (raw): 1483065289
    [Next Sequence Number: 1361    (relative sequence number)]
    Acknowledgment Number: 3265    (relative ack number)
    Acknowledgment number (raw): 2937615021
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1027
    [Calculated window size: 262912]
    [Window size scaling factor: 256]
    Checksum: 0xf21c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (693 bytes)
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 688
      Encrypted Application Data: 39b0bececc9224830b9fa0d32992932961deaaf7998d2b3a9ec0a01f1b870823aa745d88…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

Vulnerabilities

When a server or a service running on a server has a flaw that can be exploited to do some damage

Vulnerabilities

Vulnerability

Exploit

Payload

Causes of a Vulnerability

- Depends on services/server
- Misconfigurations
- Default settings
- Not patching

Types of Servers

Can run any service on any port

File Server

- Remotely Access Files
- SMB, FTP
- Default Ports
  - 445 for SMB
  - 21 for FTP

File Server

Common vulnerabilities and attacks

- Anonymous Access
- Oversharing
- Pass-the-hash
- SMB Relaying
- Kernel Exploits (Eternalblue)
- Malware Distribution
- Privilege Escalation (Windows Services)
- Brute-Forcing
- Weak or no encryption

Remote Server

- Remotely Control PC
- DO NOT FACE EXTERNALLY
  - 0.0.0.0 vs 127.0.0.1
- RDP (Ransomware Deployment Protocol), VNC
- Default Ports
  - 3389 for RDP
  - 5700 for VNC

Remote Server

Common vulnerabilities and attacks

- Brute Force
- Credentials in Program Files (VNC on Windows)
- Weak or no encryption
- Bluekeep (Windows)
- Ridiculous amount of control over machine

Web Server

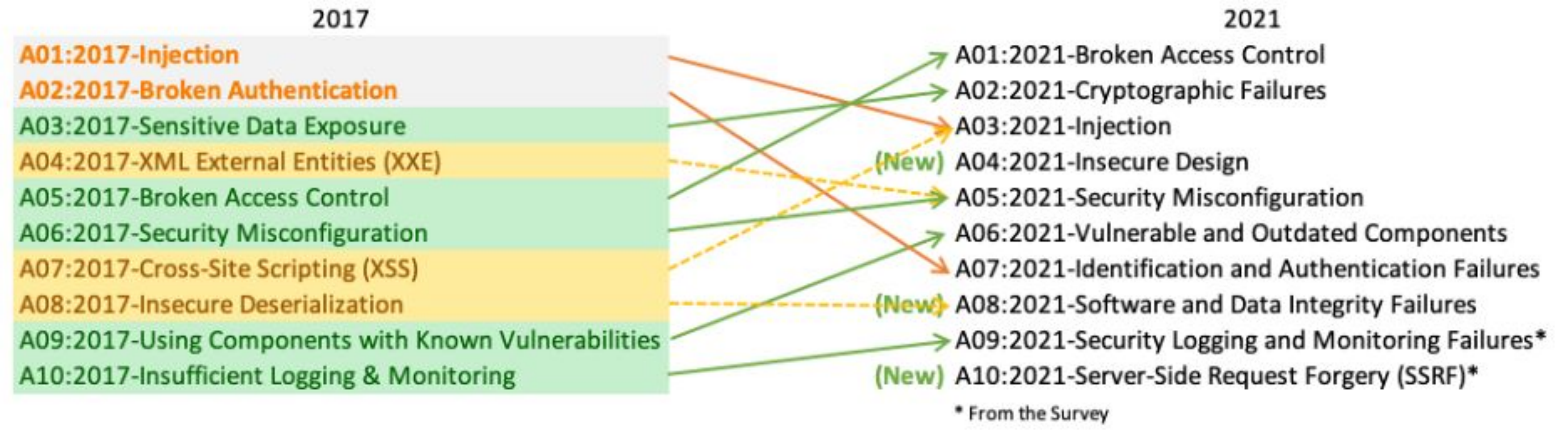
- Web applications
- HTTP (unencrypted)
- HTTPS (encrypted)
  - SSL, TLS version 1.0, 1.1, 1.2, 1.3
- Sometimes connected to Database server
  - Or has database service running on same machine
- Combination of Web Server, database and scripting language (usually)
- Default Ports
  - 443 for HTTPS
  - 80 for HTTP
  - 8080 and 8443 also common

Web Server

Common vulnerabilities and attacks

- OWASP Top 10
- Denial of Service

OWASP Top 10 (2021)



2017	2021
A01:2017-Injection	A01:2021-Broken Access Control
A02:2017-Broken Authentication	A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure	A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New) A04:2021-Insecure Design
A05:2017-Broken Access Control	A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration	A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)	A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New) A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities	A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Broken Access Control

- Getting access to things you shouldn’t
  - Other accounts’ data
  - Administrator pages
  - Violation of POLP
  - API misconfigurations
  - Metadata Manipulation (JWT Hacking)
  - Session misconfigurations

Cryptographic Failures

- Bad certificates
- Bad SSL/TLS
- Bad ciphers
- Authentication with hash
- No encryption

Injection

- SQL injection
- XSS
- HTML Injection
- No validation of client-supplied data

Insecure Design

- Error messages with sensitive information
- Credentials not protected
- Web application design logic is flawed

Security Misconfiguration

- Unnecessary ports or services running
- Default accounts
- Missing security headers
  - X-Frame-Options
  - HSTS
- Errors revealing stack information
- LFI/RFI

Vulnerable and Outdated Components

- Technologies with known vulnerabilities
- Unsupported software

Identification and Authentication Failures

- Brute Forcing
- Weak credentials
- Badly hashes passwords
- Session identifiers in URL
- No MFA

Software and Data Integrity Failures

- Sketchy repositories (NPM) or plugins
- Bad code review process
- Check integrity of serialized data

Security Logging and Monitoring Failures

- Logins, failed logins, transactions are not logged
- Logs are stored locally only
- No detection of attacks in real time

Server-Side Request Forgery

- Forcing the server to make unauthorized requests
  - Can make a request against itself, getting information from pages you shouldn’t see
  - Can make requests to other machines on the network
  - Can make requests to evil server

Database Server

- MySQL, PostgreSQL, MSSQL
- Default Ports
  - 3306 for MySQL
  - 5432 for PostgreSQL
  - 1433 for MSSQL

Database Server

Common vulnerabilities and attacks

- Brute Force
- Bad credentials
- Command execution
- SQL injection
- Bad hashing

NMAP

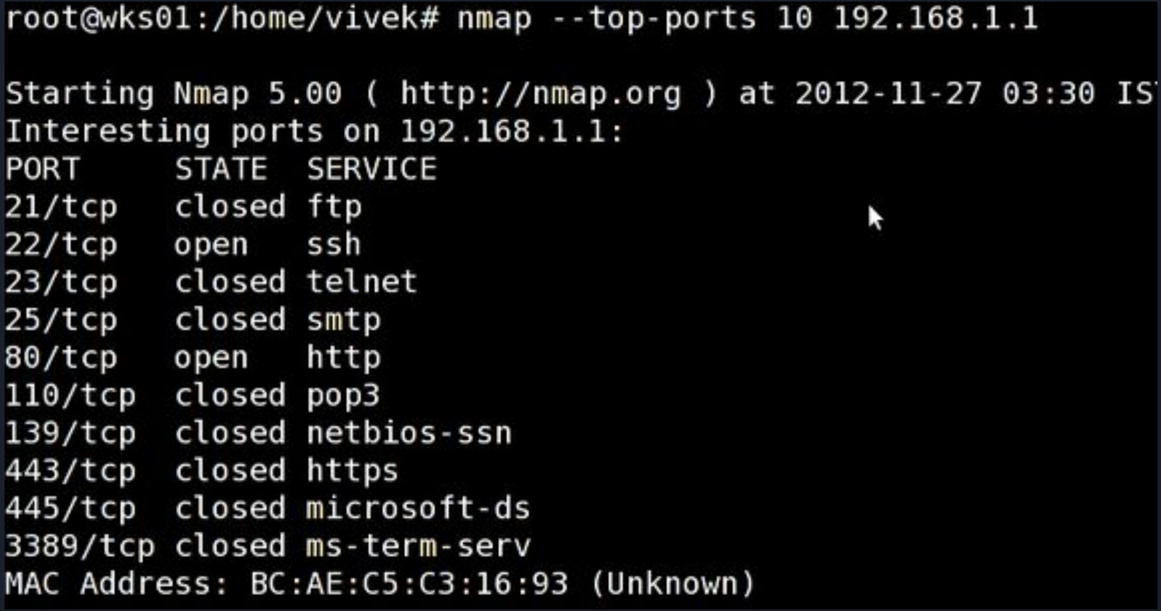
Scan ports

- See what’s externally facing or running

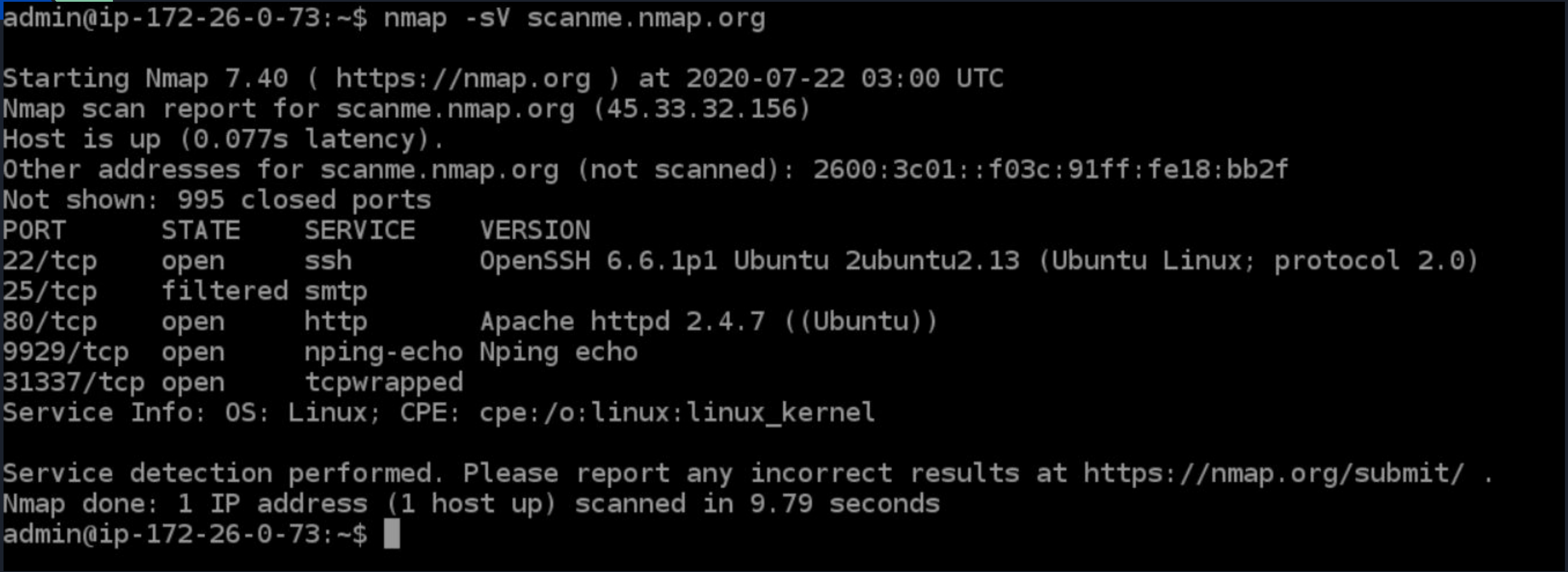
Service Versions

Various nice scripts

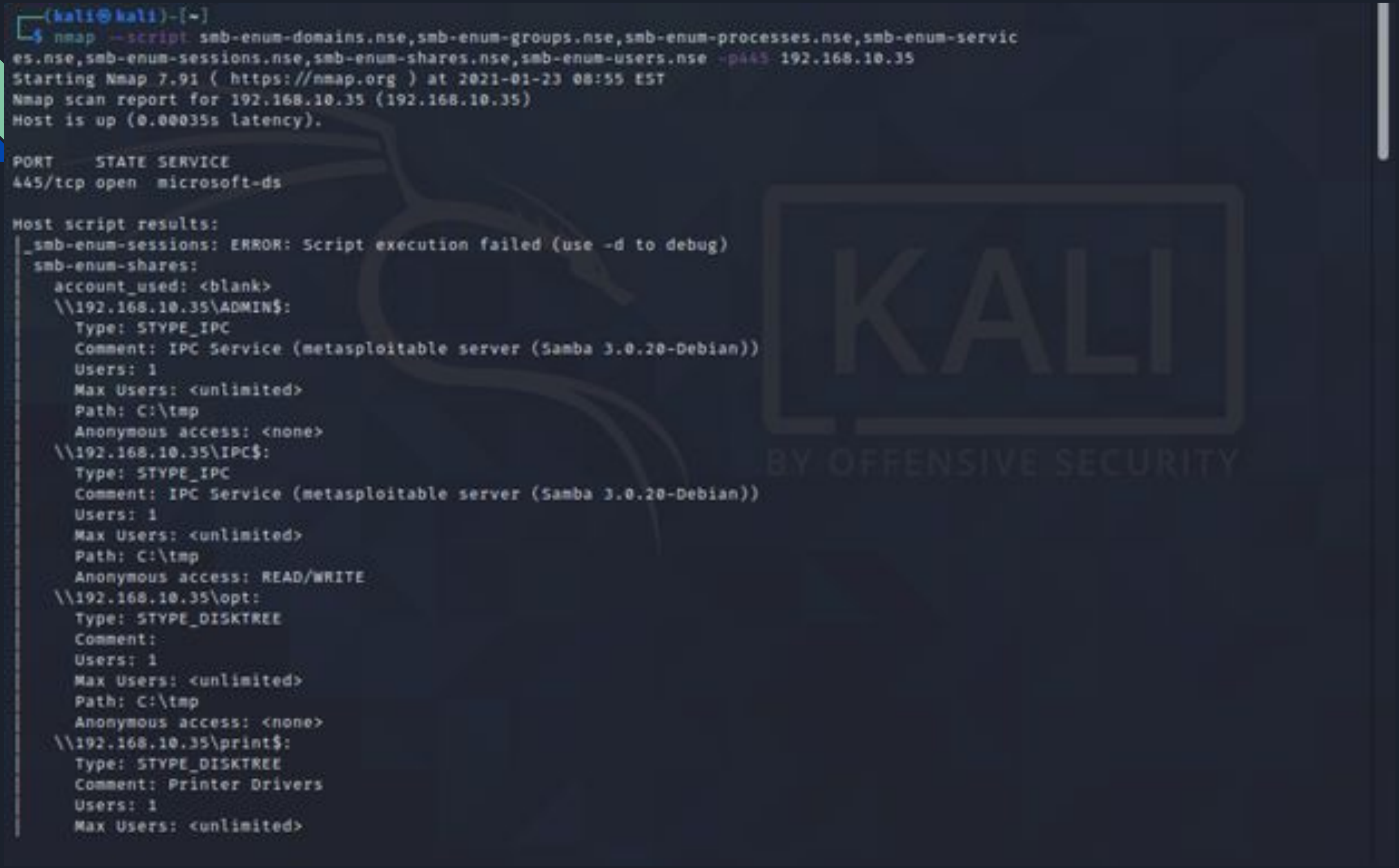
- SMB, FTP, RDP info



```
root@wks01:/home/vivek# nmap --top-ports 10 192.168.1.1

Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 03:30 IS
Interesting ports on 192.168.1.1:
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)
```



```
admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
admin@ip-172-26-0-73:~$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-enum-domains.nse,smb-enum-groups.nse,smb-enum-processes.nse,smb-enum-servic
es.nse,smb-enum-sessions.nse,smb-enum-shares.nse,smb-enum-users.nse -p445 192.168.10.35
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-23 08:55 EST
Nmap scan report for 192.168.10.35 (192.168.10.35)
Host is up (0.00035s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-enum-sessions: ERROR: Script execution failed (use -d to debug)
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.10.35\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.10.35\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.10.35\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.10.35\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
```

Creating a server

1. Platform and OS
    a. Windows or Linux
    b. Images
        i. Unattend.xml

Installing software

Windows

- Some things can do through server management
  - RDP, DHCP, etc
  - Third-Party Software
    - Sage 300, Filezilla

Linux

- Some things come with OS
  - SSH
- Need to install a lot more yourself

Configuration

- Firewalls
- Accounts
- Permissions
- Ports
- Services
  - Encryption
  - Authentication

Windows Server

Admin and User (Local)

RDP

- Remote Users Group
- Strong encryption
- NLA
- No copy/paste
- No restarting

Windows Server (cont.)

Win-RM

- Service to start automatically
- Add trusted hosts (no domain)
- Execute basic command

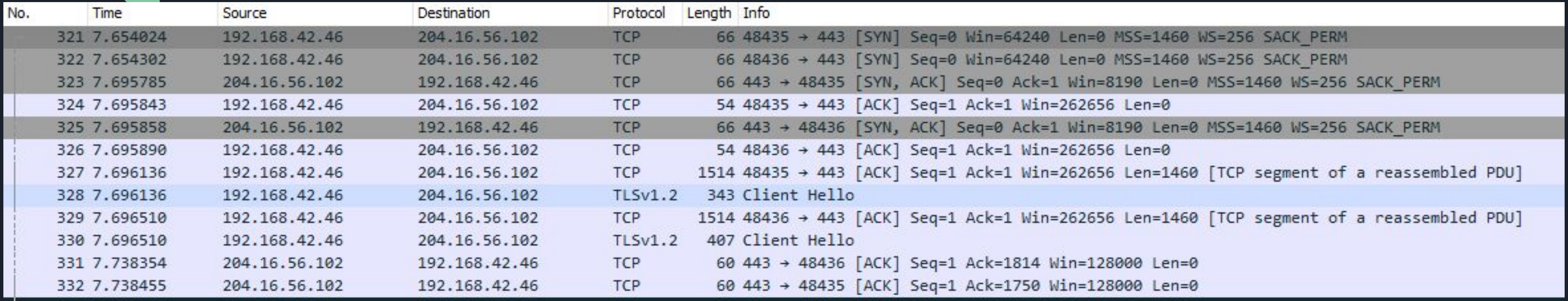
SMB

- Enable signing
- Disable NTLMv1
- Enable SMB 2 and 3

Exercise

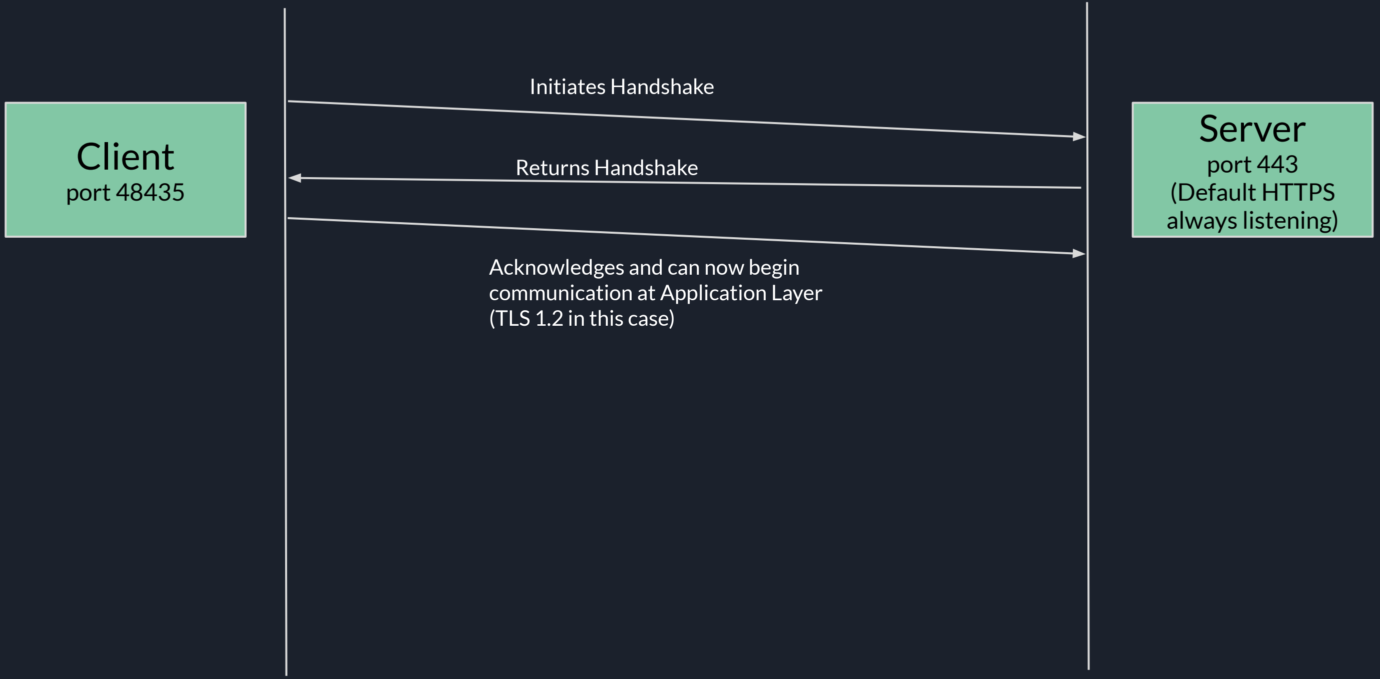
1. Find a web server
2. Open wireshark and select your adapter (likely wifi if laptop or ethernet if desktop)
3. Capture traffic and visit a web server (nscc.ca is a good one)
4. Filter by your web server’s IP address (use ping in cmd.exe nscc.ca to find out)
5. Observer the 3 way handshake
6. Observe TLS 1.2 traffic after
    a. Take a special look at the data part of a packet

Exercise



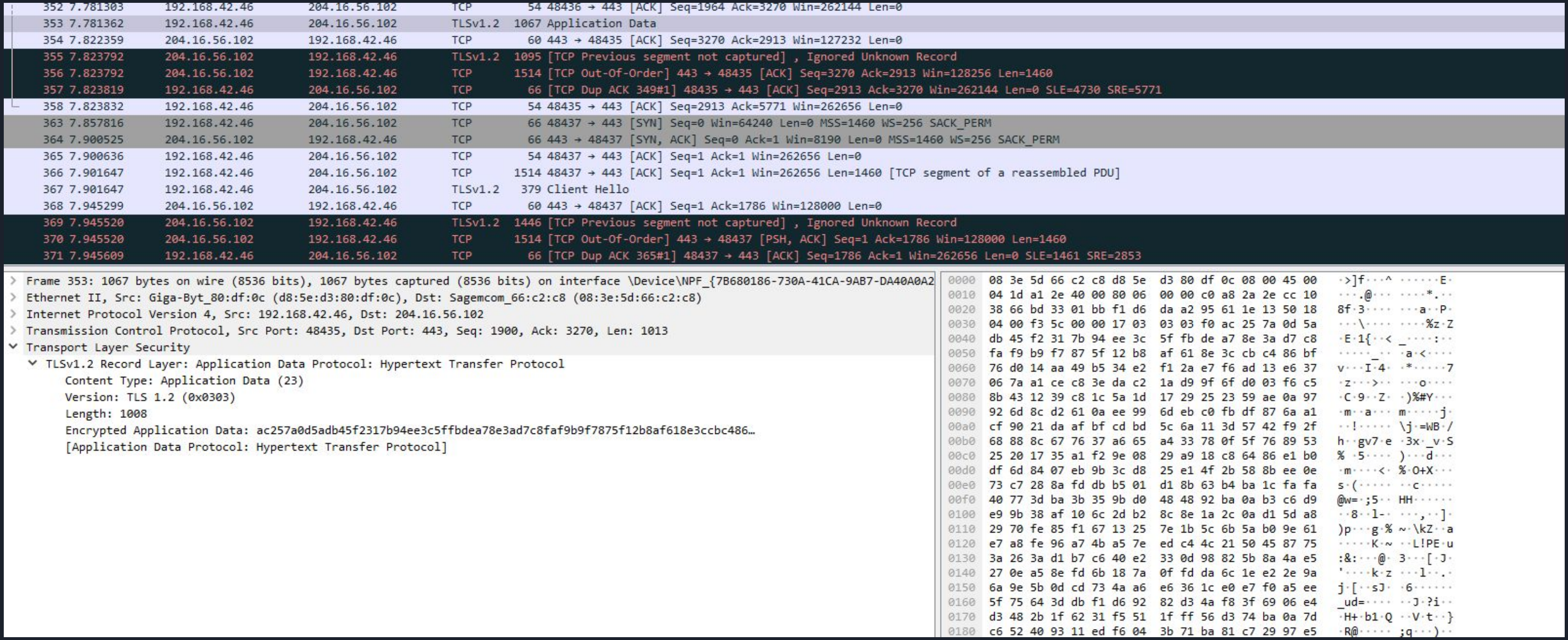
No.	Time	Source	Destination	Protocol	Length	Info
321	7.654024	192.168.42.46	204.16.56.102	TCP	66	48435 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
322	7.654302	192.168.42.46	204.16.56.102	TCP	66	48436 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
323	7.695785	204.16.56.102	192.168.42.46	TCP	66	443 → 48435 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=256 SACK_PERM
324	7.695843	192.168.42.46	204.16.56.102	TCP	54	48435 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
325	7.695858	204.16.56.102	192.168.42.46	TCP	66	443 → 48436 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=256 SACK_PERM
326	7.695890	192.168.42.46	204.16.56.102	TCP	54	48436 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
327	7.696136	192.168.42.46	204.16.56.102	TCP	1514	48435 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
328	7.696136	192.168.42.46	204.16.56.102	TLSv1.2	343	Client Hello
329	7.696510	192.168.42.46	204.16.56.102	TCP	1514	48436 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
330	7.696510	192.168.42.46	204.16.56.102	TLSv1.2	407	Client Hello
331	7.738354	204.16.56.102	192.168.42.46	TCP	60	443 → 48436 [ACK] Seq=1 Ack=1814 Win=128000 Len=0
332	7.738455	204.16.56.102	192.168.42.46	TCP	60	443 → 48435 [ACK] Seq=1 Ack=1750 Win=128000 Len=0

Exercise



Client
port 48435
Server
port 443
(Default HTTPS
always listening)
Initiates Handshake
Returns Handshake
Acknowledges and can now begin
communication at Application Layer
(TLS 1.2 in this case)

Exercise



```
352 7.781303   192.168.42.46   204.16.56.102   TCP        54 48436 → 443 [ACK] Seq=1964 Ack=3270 Win=262144 Len=0
353 7.781362   192.168.42.46   204.16.56.102   TLSv1.2  1067 Application Data
354 7.822359   204.16.56.102   192.168.42.46   TCP        60 443 → 48435 [ACK] Seq=3270 Ack=2913 Win=127232 Len=0
355 7.823792   204.16.56.102   192.168.42.46   TLSv1.2  1095 [TCP Previous segment not captured] , Ignored Unknown Record
356 7.823792   204.16.56.102   192.168.42.46   TCP      1514 [TCP Out-Of-Order] 443 → 48435 [ACK] Seq=3270 Ack=2913 Win=128256 Len=1460
357 7.823819   192.168.42.46   204.16.56.102   TCP        66 [TCP Dup ACK 349#1] 48435 → 443 [ACK] Seq=2913 Ack=3270 Win=262144 Len=0 SLE=4730 SRE=5771
358 7.823832   192.168.42.46   204.16.56.102   TCP        54 48435 → 443 [ACK] Seq=2913 Ack=5771 Win=262656 Len=0
363 7.857816   192.168.42.46   204.16.56.102   TCP        66 48437 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
364 7.900525   204.16.56.102   192.168.42.46   TCP        66 443 → 48437 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=256 SACK_PERM
365 7.900636   192.168.42.46   204.16.56.102   TCP        54 48437 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
366 7.901647   192.168.42.46   204.16.56.102   TCP      1514 48437 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=1460 [TCP segment of a reassembled PDU]
367 7.901647   192.168.42.46   204.16.56.102   TLSv1.2   379 Client Hello
368 7.945299   204.16.56.102   192.168.42.46   TCP        60 443 → 48437 [ACK] Seq=1 Ack=1786 Win=128000 Len=0
369 7.945520   204.16.56.102   192.168.42.46   TLSv1.2  1446 [TCP Previous segment not captured] , Ignored Unknown Record
370 7.945520   204.16.56.102   192.168.42.46   TCP      1514 [TCP Out-Of-Order] 443 → 48437 [PSH, ACK] Seq=1 Ack=1786 Win=128000 Len=1460
371 7.945609   192.168.42.46   204.16.56.102   TCP        66 [TCP Dup ACK 365#1] 48437 → 443 [ACK] Seq=1786 Ack=1 Win=262656 Len=0 SLE=1461 SRE=2853
```

```
> Frame 353: 1067 bytes on wire (8536 bits), 1067 bytes captured (8536 bits) on interface \Device\NPF_{7B680186-730A-41CA-9AB7-DA40A0A2
> Ethernet II, Src: Giga-Byt_80:df:0c (d8:5e:d3:80:df:0c), Dst: Sagemcom_66:c2:c8 (08:3e:5d:66:c2:c8)
> Internet Protocol Version 4, Src: 192.168.42.46, Dst: 204.16.56.102
> Transmission Control Protocol, Src Port: 48435, Dst Port: 443, Seq: 1900, Ack: 3270, Len: 1013
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 1008
      Encrypted Application Data: ac257a0d5adb45f2317b94ee3c5ffbdea78e3ad7c8faf9b9f7875f12b8af618e3ccbc486…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0000  08 3e 5d 66 c2 c8 d8 5e  d3 80 df 0c 08 00 45 00   ·>]f···^ ······E·
0010  04 1d a1 2e 40 00 80 06  00 00 c0 a8 2a 2e cc 10   ···.@··· ····*.··
0020  38 66 bd 33 01 bb f1 d6  da a2 95 61 1e 13 50 18   8f·3···· ···a··P·
0030  04 00 f3 5c 00 00 17 03  03 03 f0 ac 25 7a 0d 5a   ···\···· ····%z·Z
0040  db 45 f2 31 7b 94 ee 3c  5f fb de a7 8e 3a d7 c8   ·E·1{··< _····:··
0050  fa f9 b9 f7 87 5f 12 b8  af 61 8e 3c cb c4 86 bf   ·····_·· ·a·<····
0060  76 d0 14 aa 49 b5 34 e2  f1 2a e7 f6 ad 13 e6 37   v···I·4· ·*·····7
0070  06 7a a1 ce c8 3e da c2  1a d9 9f 6f d0 03 f6 c5   ·z···>·· ···o····
0080  8b 43 12 39 c8 1c 5a 1d  17 29 25 23 59 ae 0a 97   ·C·9··Z· ·)%#Y···
0090  92 6d 8c d2 61 0a ee 99  6d eb c0 fb df 87 6a a1   ·m··a··· m·····j·
00a0  cf 90 21 da af bf cd bd  5c 6a 11 3d 57 42 f9 2f   ··!····· \j·=WB·/
00b0  68 88 8c 67 76 37 a6 65  a4 33 78 0f 5f 76 89 53   h··gv7·e ·3x·_v·S
00c0  25 20 17 35 a1 f2 9e 08  29 a9 18 c8 64 86 e1 b0   % ·5···· )···d···
00d0  df 6d 84 07 eb 9b 3c d8  25 e1 4f 2b 58 8b ee 0e   ·m····<· %·O+X···
00e0  73 c7 28 8a fd db b5 01  d1 8b 63 b4 ba 1c fa fa   s·(····· ··c·····
00f0  40 77 3d ba 3b 35 9b d0  48 48 92 ba 0a b3 c6 d9   @w=·;5·· HH······
0100  e9 9b 38 af 10 6c 2d b2  8c 8e 1a 2c 0a d1 5d a8   ··8··l-· ···,··]·
0110  29 70 fe 85 f1 67 13 25  7e 1b 5c 6b 5a b0 9e 61   )p···g·% ~·\kZ··a
0120  e7 a8 fe 96 a7 4b a5 7e  ed c4 4c 21 50 45 87 75   ·····K·~ ··L!PE·u
0130  3a 26 3a d1 b7 c6 40 e2  33 0d 98 82 5b 8a 4a e5   :&:···@· 3···[·J·
0140  27 0e a5 8e fd 6b 18 7a  0f fd da 6c 1e e2 2e 9a   '····k·z ···l··.·
0150  6a 9e 5b 0d cd 73 4a a6  e6 36 1c e0 e7 f0 a5 ee   j·[··sJ· ·6······
0160  5f 75 64 3d db f1 d6 92  82 d3 4a f8 3f 69 06 e4   _ud=···· ··J·?i··
0170  d3 48 2b 1f 62 31 f5 51  1f ff 56 d3 74 ba 0a 7d   ·H+·b1·Q ··V·t··}
0180  c6 52 40 93 11 ed f6 04  3b 71 ba 81 c7 29 97 e5   ·R@····· ;q···)··
```