1)

a.

Nmap sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request.

b.

OS detection: nmap -O

Service detection: nmap -sV

Increased verbosity: nmap -v[<level>], --verbose [<level>] (level from -4 to 4)

c)

OS detection: sudo nmap -O scanme.nmap.org

Running (JUST GUESSING): Linux 4.X|3.X|2.6.X (91%), Cisco embedded (87%), Dish embedded (85%)

OS CPE: cpe:/o:linux:linux\_kernel:4.4 cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel cpe:/h:cisco:rv320 cpe:/o:linux:linux\_kernel:2.6.32 cpe:/h:dish:hopper

Aggressive OS guesses: Linux 4.4 (91%), Linux 4.0 (87%), Linux 3.11 - 4.1 (87%), Cisco RV320 router (87%), Linux 2.6.32 (87%), Linux 2.6.32 or 3.10 (87%), Linux 3.10 - 3.12 (86%), Dish Network Hopper media device (85%), Linux 2.6.32 - 3.0 (85%), Linux 2.6.32 - 2.6.35 (85%)

No exact OS matches for host (test conditions non-ideal).

It is likely Linux.

Service detection: sudo nmap -sV scanme.nmap.org

Not shown: 993 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu Linux; protocol 2.0)

25/tcp filtered smtp

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

554/tcp open tcpwrapped

7070/tcp open tcpwrapped

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

Increased verbosity: sudo nmap scanme.nmap.org -v4

Starting Nmap 7.60 ( https://nmap.org ) at 2019-04-03 23:32 CDT

Warning: Hostname scanme.nmap.org resolves to 2 IPs. Using 45.33.32.156.

Initiating Ping Scan at 23:32

Scanning scanme.nmap.org (45.33.32.156) [4 ports]

Completed Ping Scan at 23:32, 0.22s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 23:32

Completed Parallel DNS resolution of 1 host. at 23:32, 0.14s elapsed

DNS resolution of 1 IPs took 0.14s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]

Initiating SYN Stealth Scan at 23:32

Scanning scanme.nmap.org (45.33.32.156) [1000 ports]

Discovered open port 554/tcp on 45.33.32.156

Discovered open port 22/tcp on 45.33.32.156

Discovered open port 80/tcp on 45.33.32.156

Increasing send delay for 45.33.32.156 from 0 to 5 due to 34 out of 112 dropped probes since last increase.

Discovered open port 9929/tcp on 45.33.32.156

Increasing send delay for 45.33.32.156 from 5 to 10 due to 47 out of 155 dropped probes since last increase.

Increasing send delay for 45.33.32.156 from 10 to 20 due to 11 out of 25 dropped probes since last increase.

Increasing send delay for 45.33.32.156 from 20 to 40 due to 11 out of 30 dropped probes since last increase.

Increasing send delay for 45.33.32.156 from 40 to 80 due to max\_successful\_tryno increase to 4

Increasing send delay for 45.33.32.156 from 80 to 160 due to 17 out of 56 dropped probes since last increase.

Increasing send delay for 45.33.32.156 from 160 to 320 due to 11 out of 27 dropped probes since last increase.

SYN Stealth Scan Timing: About 31.60% done; ETC: 23:34 (0:01:07 remaining)

SYN Stealth Scan Timing: About 40.92% done; ETC: 23:34 (0:01:28 remaining)

Discovered open port 31337/tcp on 45.33.32.156

SYN Stealth Scan Timing: About 66.05% done; ETC: 23:35 (0:01:13 remaining)

Discovered open port 7070/tcp on 45.33.32.156

SYN Stealth Scan Timing: About 75.12% done; ETC: 23:36 (0:00:57 remaining)

SYN Stealth Scan Timing: About 84.25% done; ETC: 23:36 (0:00:38 remaining)

Completed SYN Stealth Scan at 23:36, 263.14s elapsed (1000 total ports)

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up, received echo-reply ttl 53 (0.057s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Scanned at 2019-04-03 23:32:24 CDT for 263s

Not shown: 993 closed ports

Reason: 993 resets

PORT STATE SERVICE REASON

22/tcp open ssh syn-ack ttl 53

25/tcp filtered smtp no-response

80/tcp open http syn-ack ttl 53

554/tcp open rtsp syn-ack ttl 64

7070/tcp open realserver syn-ack ttl 64

9929/tcp open nping-echo syn-ack ttl 53

31337/tcp open Elite syn-ack ttl 53

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 263.71 seconds

Raw packets sent: 1193 (52.468KB) | Rcvd: 1179 (47.172KB)

d)

OS detection: sudo nmap -O localhost

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4

OS details: Linux 3.8 – 4.9

Service detection: sudo nmap -sV localhost

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

119/tcp open nntp?

631/tcp open ipp CUPS 2.2

3306/tcp open mysql MySQL 5.7.25-0ubuntu0.18.04.2

5432/tcp open postgresql PostgreSQL DB

Increased verbosity: sudo nmap localhost -v 4

PORT STATE SERVICE REASON

80/tcp open http syn-ack ttl 64

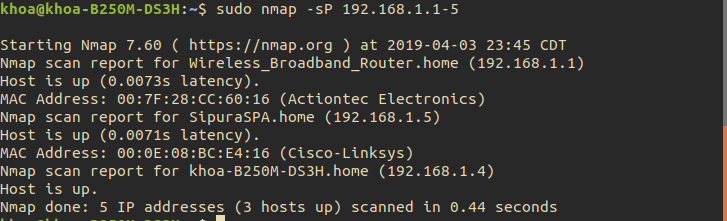
119/tcp open nntp syn-ack ttl 64

631/tcp open ipp syn-ack ttl 64

3306/tcp open mysql syn-ack ttl 64

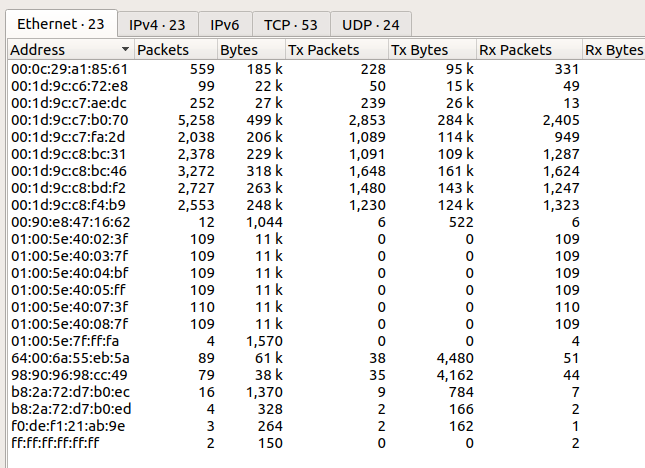
5432/tcp open postgresql syn-ack ttl 64

e)



2)

a.



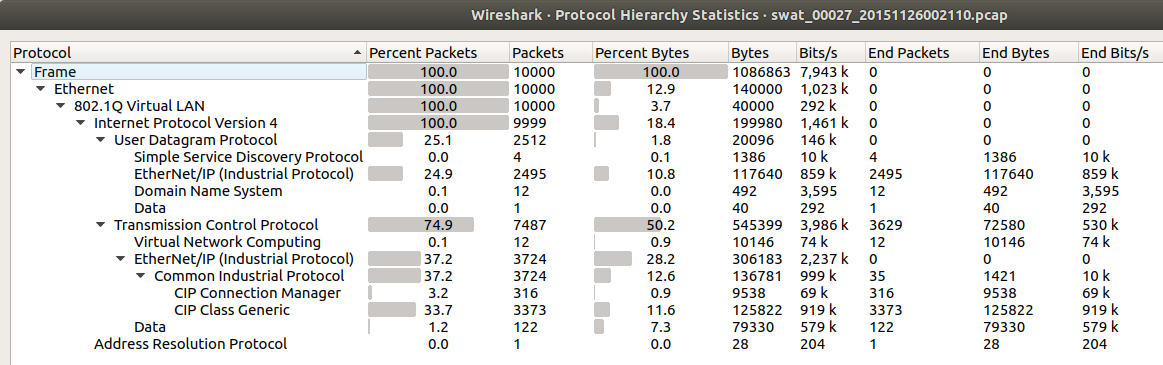
b.

See pdf file.

c.

TCP: 74.9%

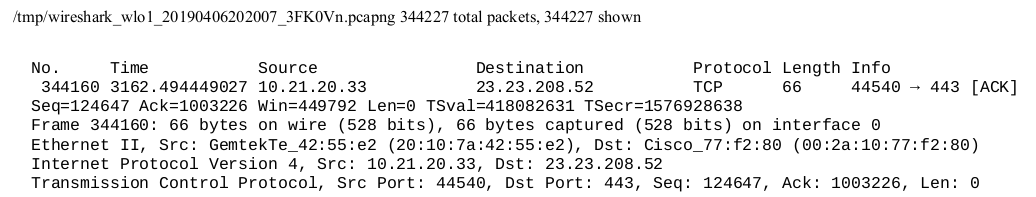
UDP: 25.1%



3)

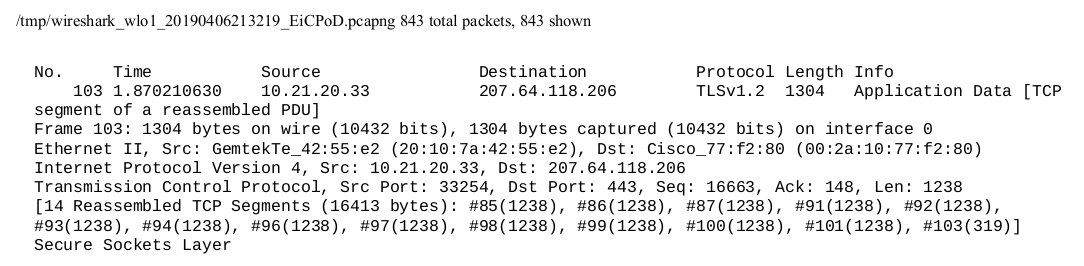
a.





b.

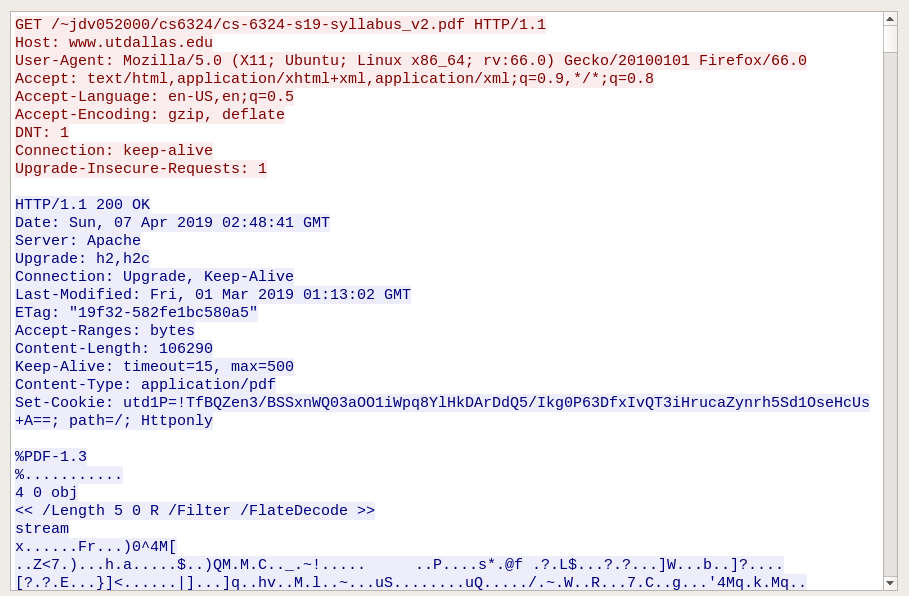
Any package sent to 207.64.118.206



I cannot see my username and password because they have been encrypted. The length of the packets are also padded so all of them look the same.

c.

I see the HTTP header, host, agent, cookie… Then I see the PDF file with the PDF header in text. These are sent in TCP packages after the HTTP request.



Source port: 58696. Destination port: 80.

IP: 10.182.71.70

**HTTPS:**

For https, I don’t see the http request anymore. Everything is encrypted with TLSv1.2 and send over TCP. Source port: 40376, destination port 443.

IP: 10.182.71.70

4)

a.

Six stages:

Reconnaissance: The attacker tries to gain understanding of the target such as physical layout, roles, people, procedures and software used.

Initial Exploitation: the attacker tries to find a way to gain access the system using weak points that take the least effort and highest impact.

Establish Persistence: after the previous phase, the attacker tries to give themselves access, get keys, write scripts to allow them to return to the system.

Install Tools: the attacker install tools that can install heavier tools that do the hacking or fetch data, sending it outside the system.

Move Laterally: move from the place the attacker is to the place that hosts the information the attacker is looking for.

Collect Exfil and Exploit: collect the information the attacker is looking for, sending it outside or do further exploitation.

b.

Email

A link to a malicious website.

A removable media to plug into the system.

c.

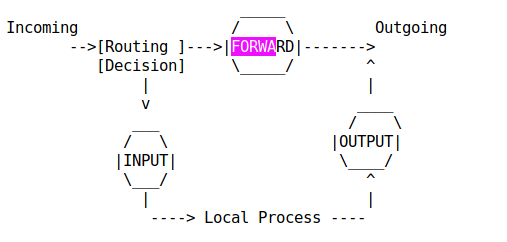
False, unproductive.

d.

Pass the hash is when the attacker already had control over a computer. The attacker obtains the hash of the user’s password, then use it on another machine to gain access to the system. The hash functions just like the clear text password. The attacker can use the same process to get the administrator’s password when they log in remotely, then use the hash on other machines.

5)

a.



The incoming messages’ destination is decided by Routing Decision. The filter looks at the header and decide if the message should be forwarded to another interface (FORWARD). If there are policies specifying how a packet should be treated, then it will be sent down that route to INPUT. The result can be sent to other network interfaces through OUTPUT if they are specified.

If there is no forwarding and no policy specified, the packet will be dropped.

a.

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -A INPUT -s 192.168.0.0/24 -d 10.0.0.10 -p tcp -dport 80.443 -j ACCEPT

iptables -A OUTPUT -s 10.0.0.10 -d 192.168.0.0/24 -p tcp -sport 80,443 -j ACCEPT

b.

iptables -A INPUT -s 192.168.0.21 -p tcp -dport 22 -j ACCEPT

iptables -A OUTPUT -d 192.168.0.21 -p tcp -sport 22 -j ACCEPT

c.

iptables -A INPUT -i eth1 -d 10.0.0.0/24 -j ACCEPT

d.

iptables -A INPUT -s 192.168.0.10,192.168.0.20 -d 10.0.0.50 -p tcp -dport 21 -j ACCEPT

iptables -A output -d 192.168.0.10,192.168.0.20 -s 10.0.0.50 -p tcp -sport 21 -j ACCEPT

e.

iptables -A INPUT -s 192.168.0.11,192.168.0.21 -d 10.0.0.180 -p tcp -dport 993,995 -j ACCEPT

iptables -A INPUT -d 192.168.0.11,192.168.0.21 -s 10.0.0.180 -p tcp -sport 993,995 -j ACCEPT

6)

a.

alert

log

pass

drop

reject

sdrop

activate

dynamic

b.

drop tcp any any → 10.21.20.33 :22

c.

reject tcp any any → any any (content: “|ff 53 4d 42 32 02 00 00 c0|”; msg)