

Lab 2

2.

iii.

The image shows a Wireshark packet capture of a network traffic. The top pane displays a list of packets. Packet 63 is highlighted, showing a GET request for a ZIP file from www.dchristjan.com. The bottom pane shows the details of this packet, including the HTTP request line and headers.

No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Time	DNS_Time	Info
60	10.9.25.101	49158	23.229.232.193	80	TCP	66		2019-09-25 12:53:40.756429		49158 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
61	23.229.232.193	80	10.9.25.101	49158	TCP	58		2019-09-25 12:53:41.333829		80 → 49158 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
62	10.9.25.101	49158	23.229.232.193	80	TCP	54		2019-09-25 12:53:41.333989		49158 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
63	10.9.25.101	49158	23.229.232.193	80	HTTP	347	www.dchristjan.com	2019-09-25 12:53:41.334373		GET /dd05ce3a-a9c9-4018-8252-d579eed1e670.zip HTTP/1.1
64	23.229.232.193	80	10.9.25.101	49158	TCP	54		2019-09-25 12:53:41.334440		80 → 49158 [ACK] Seq=1 Ack=294 Win=64240 Len=0
66	23.229.232.193	80	10.9.25.101	49158	TCP	1418		2019-09-25 12:53:41.782401		80 → 49158 [PSH, ACK] Seq=1 Ack=294 Win=64240 Len=1364
67	10.9.25.101	49158	23.229.232.193	80	TCP	54		2019-09-25 12:53:41.782574		49158 → 80 [ACK] Seq=294 Ack=1365 Win=62876 Len=0
68	23.229.232.193	80	10.9.25.101	49158	TCP	1418		2019-09-25 12:53:41.785208		80 → 49158 [PSH, ACK] Seq=1365 Ack=294 Win=64240 Len=1
69	23.229.232.193	80	10.9.25.101	49158	HTTP	1256		2019-09-25 12:53:41.785266		HTTP/1.1 200 OK (application/zip)
70	10.9.25.101	49158	23.229.232.193	80	TCP	54		2019-09-25 12:53:41.785356		49158 → 80 [ACK] Seq=294 Ack=3931 Win=64240 Len=0
89	23.229.232.193	80	10.9.25.101	49158	TCP	54		2019-09-25 12:53:46.497108		80 → 49158 [FIN, PSH, ACK] Seq=3931 Ack=294 Win=64240
90	10.9.25.101	49158	23.229.232.193	80	TCP	54		2019-09-25 12:53:46.497370		49158 → 80 [ACK] Seq=294 Ack=3932 Win=64240 Len=0
98	10.9.25.101	49158	23.229.232.193	80	TCP	54		2019-09-25 12:53:56.401836		49158 → 80 [FIN, ACK] Seq=294 Ack=3932 Win=64240 Len=0
99	23.229.232.193	80	10.9.25.101	49158	TCP	54		2019-09-25 12:53:56.401941		80 → 49158 [ACK] Seq=3932 Ack=295 Win=64239 Len=0

Frame 63: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0
Ethernet II, Src: Hewlett-Packard (08:00:00:1c:c7:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.9.25.101, Dst: 23.229.232.193
Transmission Control Protocol, Src Port: 49158, Dst Port: 80, Seq: 1, Ack: 1, Len: 293
Hypertext Transfer Protocol
GET /dd05ce3a-a9c9-4018-8252-d579eed1e670.zip HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.dchristjan.com
Connection: Keep-Alive
[Response in frame: 69]
[Full request URI: http://www.dchristjan.com/dd05ce3a-a9c9-4018-8252-d579eed1e670.zip]

iv. **GET /dd05ce3a-a9c9-4018-8252-d579eed1e670.zip HTTP/1.1**

This line shows the infected host is requesting a ZIP file from www.dchristjan.com that's not a normal website for a user to contact, so it's malicious. It means Trickbot is trying to download an infected ZIP archive from that server.

v. .

```
HTTP/1.1 200 OK
Date: Wed, 25 Sep 2019 17:53:42 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Wed, 25 Sep 2019 08:23:20 GMT
ETag: "9d441d3-dda-5935c5d9faea6-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 3566
Keep-Alive: timeout=5
Content-Type: application/zip
```

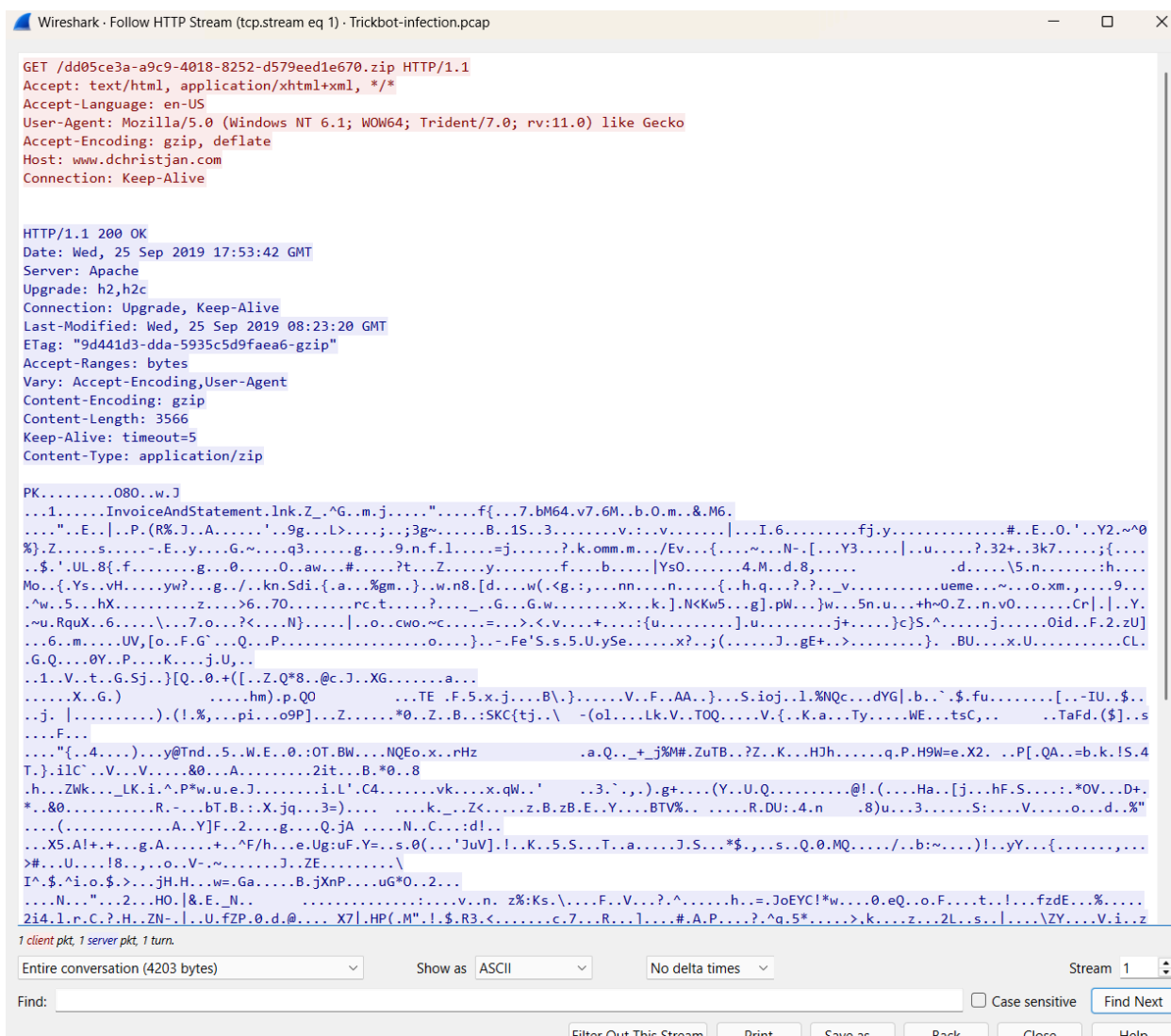
The response is “200 OK”, meaning the file download was successful, and the Content-Type is application/zip, confirming the server sent a ZIP archive file. The response type is ‘application/zip’, indicating that the server sent a ZIP archive back to the infected machine.

vi. InvoiceAndStatement.Ink

```
'{0.....kuy.....0.?s.....x.....e.i.....PK.....  
.....InvoiceAndStatement.InkPK.....E.....
```

The ZIP archive contained a file named ‘InvoiceAndStatement.Ink’, which serves as the Trickbot payload.

vii.



The screenshot shows a Wireshark packet capture of an HTTP transaction. The top pane displays the raw packet data in hexadecimal and ASCII. The middle pane shows the packet details, including the HTTP request and response headers. The bottom pane shows the packet bytes in ASCII.

HTTP Request (GET /dd05ce3a-a9c9-4018-8252-d579eed1e670.zip HTTP/1.1):

- Accept: text/html, application/xhtml+xml, */*
- Accept-Language: en-US
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
- Accept-Encoding: gzip, deflate
- Host: www.dchristjan.com
- Connection: Keep-Alive

HTTP Response (HTTP/1.1 200 OK):

- Date: Wed, 25 Sep 2019 17:53:42 GMT
- Server: Apache
- Upgrade: h2,h2c
- Connection: Upgrade, Keep-Alive
- Last-Modified: Wed, 25 Sep 2019 08:23:20 GMT
- Etag: "9d441d3-dda-5935c5d9faea6-gzip"
- Accept-Ranges: bytes
- Vary: Accept-Encoding,User-Agent
- Content-Encoding: gzip
- Content-Length: 3566
- Keep-Alive: timeout=5
- Content-Type: application/zip

The bottom pane shows the raw data of the response, which is a ZIP archive. The first few bytes of the ZIP file are visible in the ASCII pane.

Observation: The HTTP follow-stream shows the infected host requesting a ZIP file (dd05ec3e-a9c9-4018-8252-d579ed6e167e.zip) from www.dchristjan.com

Evidence: The server response “HTTP/1.1 200 OK” with Content-Type: application/zip and the binary data beginning with “PK” confirm the payload is a ZIP archive.

Comment: This proves the host downloaded a compressed malicious file used to deliver Trickbot.

viii. .

```
GET /solar.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-us
User-Agent: pwttyEKzNtGatwnJjmCcBLbOveCVpc
Host: 144.91.69.195

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 25 Sep 2019 17:54:12 GMT
Content-Type: application/octet-stream
Content-Length: 679008
Connection: keep-alive
Content-Description: File Transfer
Content-Disposition: attachment; filename="phn34ycjtghm.exe"
Expires: 0
Cache-Control: must-revalidate
Pragma: public

MZ.....@.....                .!..L!This program cannot be run in DOS mode.

$......{...{...^...{...g...{X.g...{...b...{...z...{...;...{...g...{...}\...{...f...{...>...{...F...{...Rich...{...
.....PE..L...7..}.....@.....b.....P...@.....                P..
.....,d.....
xt...3.....@.....`..rdata..`j...P...@...P.....@...@.data....`.....0.....@...rsrc...
.....@...@.....
```

Observation: The infected Windows host connected to 144.91.69.195 over HTTP (port 80) and requested /solar.php.

Evidence: The server replied HTTP/1.1 200 OK with Content-Type: application/octet-stream and Content-Disposition: filename="phn34ycjtghm.exe". The payload body begins with the MZ signature, confirming a Windows executable file.

Comment: This packet captures the download of the Trickbot executable, marking the transition from infection setup to full malware installation.

ix. ????

(http.request or tls.handshake.type == 1 or ssl.handshake.type == 1 or tcp.flags.syn == 1) and not ssdp							
No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Host
1061	10.9.25.101	49184	187.58.56.26	449	TCP	66	
1062	187.58.56.26	449	10.9.25.101	49184	TCP	58	
1064	10.9.25.101	49184	187.58.56.26	449	TLSv1	149	
1090	10.9.25.101	49185	176.58.123.25	443	TCP	66	
1091	176.58.123.25	443	10.9.25.101	49185	TCP	58	
1093	10.9.25.101	49185	176.58.123.25	443	TLSv1	166	
1121	10.9.25.101	49186	104.124.58.155	80	TCP	66	
1122	104.124.58.155	80	10.9.25.101	49186	TCP	58	
1124	10.9.25.101	49186	104.124.58.155	80	HTTP	356	www.download.
1200	10.9.25.101	49187	195.123.220.86	447	TCP	66	
1202	195.123.220.86	447	10.9.25.101	49187	TCP	58	
1204	10.9.25.101	49187	195.123.220.86	447	TLSv1	149	
1786	10.9.25.101	49188	187.58.56.26	449	TCP	66	
1802	187.58.56.26	449	10.9.25.101	49188	TCP	58	
1804	10.9.25.101	49188	187.58.56.26	449	TLSv1	181	

???

x. .

```

  issuer: rdnSequence (0)
    rdnSequence: 3 items (id-at-organizationName=Internet Widgits Pty Ltd,id-at-stateOrProvinceName=Some-State,id-at-countryName=AU)
      rdnSequence item: 1 item (id-at-countryName=AU)
        RelativeDistinguishedName item (id-at-countryName=AU)
      rdnSequence item: 1 item (id-at-stateOrProvinceName=Some-State)
        RelativeDistinguishedName item (id-at-stateOrProvinceName=Some-State)
      rdnSequence item: 1 item (id-at-organizationName=Internet Widgits Pty Ltd)
        RelativeDistinguishedName item (id-at-organizationName=Internet Widgits Pty Ltd)

```

xi. .

```

  issuer: rdnSequence (0)
    rdnSequence: 6 items (id-at-commonName=Microsoft IT TLS CA 2,id-at-organizationalUnitName=Microsoft IT,id-at-
      rdnSequence item: 1 item (id-at-countryName=US)
        RelativeDistinguishedName item (id-at-countryName=US)
          Object Id: 2.5.4.6 (id-at-countryName)
          CountryName: US
      rdnSequence item: 1 item (id-at-stateOrProvinceName=Washington)
        RelativeDistinguishedName item (id-at-stateOrProvinceName=Washington)
          Object Id: 2.5.4.8 (id-at-stateOrProvinceName)
          DirectoryString: printableString (1)
            printableString: Washington
      rdnSequence item: 1 item (id-at-localityName=Redmond)
        RelativeDistinguishedName item (id-at-localityName=Redmond)
          Object Id: 2.5.4.7 (id-at-localityName)
          DirectoryString: printableString (1)
            printableString: Redmond
      rdnSequence item: 1 item (id-at-organizationName=Microsoft Corporation)
        RelativeDistinguishedName item (id-at-organizationName=Microsoft Corporation)
          Object Id: 2.5.4.10 (id-at-organizationName)
          DirectoryString: printableString (1)
            printableString: Microsoft Corporation
      rdnSequence item: 1 item (id-at-organizationalUnitName=Microsoft IT)
        RelativeDistinguishedName item (id-at-organizationalUnitName=Microsoft IT)
          Object Id: 2.5.4.11 (id-at-organizationalUnitName)
          DirectoryString: printableString (1)
            printableString: Microsoft IT
      rdnSequence item: 1 item (id-at-commonName=Microsoft IT TLS CA 2)
        RelativeDistinguishedName item (id-at-commonName=Microsoft IT TLS CA 2)
          Object Id: 2.5.4.3 (id-at-commonName)
          DirectoryString: printableString (1)
            printableString: Microsoft IT TLS CA 2

```

3. .

- i. I ran `nmap -sP scanme.nmap.org` to perform host discovery. Nmap resolved `scanme.nmap.org` to `45.33.32.156` and the host responded to discovery probes (reported “Host is up” with ~0.11 s latency). DNS also returned an IPv6 address that was not probed. The Nmap summary shows 1 IP checked and 1 host up. `-sP` (now `-sn`) is useful for quickly identifying live hosts without doing port scans.

```
C:\Windows\System32>nmap -sP scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 13:26 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 3.93 seconds

C:\Windows\System32>
```

- ii. `-sT` performs a TCP connect scan — Nmap completes the full TCP three-way handshake (SYN → SYN/ACK → ACK) on each target port; if the connection succeeds the port is reported open.

```
C:\Windows\System32>nmap -sT -p 80,443 scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 13:41 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.094s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 3.71 seconds

C:\Windows\System32>
```

- iii. `-sS` is a SYN (half-open) scan. Nmap sends a SYN to the target port; if it receives SYN/ACK the port is likely open, and Nmap then sends an RST instead of completing the TCP handshake. Because the full connection is never completed, this can avoid being logged by some application-level services and may bypass simple firewall/IDS rules that only log completed connections.

```
C:\Windows\System32>nmap -sS -p 80,443 scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 13:56 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.074s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds

C:\Windows\System32>
```

- iv. nmap -sT scanme.nmap.org scanned the top 1000 TCP ports; the scan returned 987 closed ports and 4 open ports (22, 80, 9929, 31337).

```
C:\Windows\System32>nmap -sT scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 14:02 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed tcp ports (conn-refused)

PORT      STATE SERVICE
19/tcp    filtered chargen
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
389/tcp   filtered ldap
445/tcp   filtered microsoft-ds
636/tcp   filtered ldapssl
1433/tcp  filtered ms-sql-s
4444/tcp  filtered krb524
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 18.77 seconds

C:\Windows\System32>
```

ipaddr == 45.33.32.156 and tcp.port == 80											
No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Time	DNS_Time	Info	
114	134.124.27.84	34409	45.33.32.156	80	TCP	54		2025-10-13 19:32:50.788036		34409 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0	
123	134.124.27.84	51227	45.33.32.156	80	TCP	66		2025-10-13 19:32:52.491461		51227 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460	
124	45.33.32.156	80	134.124.27.84	51227	TCP	66		2025-10-13 19:32:52.610886		80 → 51227 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0	
125	134.124.27.84	51227	45.33.32.156	80	TCP	54		2025-10-13 19:32:52.611075		51227 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0	
126	134.124.27.84	51227	45.33.32.156	80	TCP	54		2025-10-13 19:32:52.611180		51227 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

ip.addr == 45.33.32.156 and tcp.port == 80										
No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Host	Time	DNS_Time	Info
902	134.124.27.84	45840	45.33.32.156	80	TCP	54		2025-10-13 19:41:00.668485		45840 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
911	134.124.27.84	46096	45.33.32.156	80	TCP	58		2025-10-13 19:41:02.370723		46096 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
912	45.33.32.156	80	134.124.27.84	46096	TCP	58		2025-10-13 19:41:02.476826		80 → 46096 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
913	45.33.32.156	80	134.124.27.84	46096	TCP	58		2025-10-13 19:41:03.486904		[TCP Retransmission] 80 → 46096 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1281	45.33.32.156	80	134.124.27.84	46096	TCP	58		2025-10-13 19:41:05.738369		[TCP Retransmission] 80 → 46096 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Difference between the two handshakes:

- nmap -sT (TCP connect) completes the full three-way handshake: SYN → SYN/ACK → ACK.
- nmap -sS (SYN / half-open) does not complete the handshake: it sends SYN → SYN/ACK → RST (Nmap sends an RST instead of ACK), so the TCP connection is never fully established.

The -sS scan avoids completing connections and therefore can leave fewer logs on the target host or be less obvious to some IDS/firewalls.

- v. -A enabled OS detection, version detection, default NSE scripts, and traceroute. The scan found the host is up and identified several open services and their versions (e.g. 22/tcp open ssh OpenSSH 6.6.1p1, 80/tcp open http Apache httpd 2.4.7), provided SSH host-key fingerprints, gave aggressive OS guesses (various Linux kernels, not a precise match), and produced a traceroute to the host. This output confirms Nmap discovered live services, their versions, and network path ...useful for reconnaissance.

```

C:\Windows\System32>nmap -A scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 14:50 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.100s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
19/tcp    filtered chargen
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
389/tcp   filtered ldap
445/tcp   filtered microsoft-ds
636/tcp   filtered ldapssl
1433/tcp  filtered ms-sql-s
4444/tcp  filtered krb524
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Aggressive OS guesses: Linux 4.19 - 5.15 (92%), IPFire 2.27 (Linux 5.15 - 6.1) (92%), Linux 4.15 (92%), Linux 5.4 (92%), Linux 2.6.39 (91%), Linux 3.10 - 3.16 (91%), Linux 3.10 (89%), Linux 2.6.32 (89%), Linux 2.6.35 (88%), Linux 4.9 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT ADDRESS
1 35.00 ms 134.124.204.242
2 35.00 ms 134.124.98.250
3 86.00 ms kc-core-01-he0-1-0-3-420.mo.more.net (150.199.91.29)
4 106.00 ms fourhundredge-0-0-0-10.1441.core2.kans.net.internet2.edu (198.71.47.161)
5 68.00 ms fourhundredge-0-0-0-1.4079.core2.denv.net.internet2.edu (163.253.1.250)
6 68.00 ms fourhundredge-0-0-0-3.4079.core2.salt.net.internet2.edu (163.253.1.169)
7 68.00 ms fourhundredge-0-0-0-2.4079.core2.sacr.net.internet2.edu (163.253.1.186)
8 69.00 ms fourhundredge-0-0-0-0.4079.core2.sunn.net.internet2.edu (163.253.1.191)
9 69.00 ms fourhundredge-0-0-0-49.4079.aggr1.sanj.net.internet2.edu (163.253.2.42)
10 122.00 ms eqix-sv1.linode.com (206.223.116.196)
11 ... 13
14 69.00 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.84 seconds

```

- vi. I ran `nmap --script vuln scanme.nmap.org`. Nmap reported several open services (SSH, HTTP, nping-echo, and 31337) and executed vulnerability NSE scripts. The `http-slowloris-check` reported State: **LIKELY VULNERABLE** (CVE-2007-6750), indicating the web server may be susceptible to Slowloris DoS. Other HTTP vulnerability scripts found no CSRF/XSS issues, while a few scripts failed to execute (see `_http-vuln-cve2014-3704` and `_http-aspnet-debug`), which typically indicates the script needs debug information or the target did not respond in an expected way.


```

C:\Windows\System32>nmap --script vuln scanme.nmap.org
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 14:58 -0500
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.093s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed tcp ports (reset)
PORT      STATE      SERVICE
19/tcp    filtered  chargen
22/tcp    open      ssh
25/tcp    filtered  smtp
80/tcp    open      http
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|           Slowloris tries to keep many connections to the target web server open and hold
|           them open as long as possible. It accomplishes this by opening connections to
|           the target web server and sending a partial request. By doing so, it starves
|           the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp   filtered  rpcbind
135/tcp   filtered  msrpc
389/tcp   filtered  ldap
445/tcp   filtered  microsoft-ds
636/tcp   filtered  ldapssl
1433/tcp  filtered  ms-sql-s
4444/tcp  filtered  krb524
9929/tcp  open      nping-echo
31337/tcp open      Elite

Nmap done: 1 IP address (1 host up) scanned in 47.15 seconds

C:\Windows\System32>

```

vii. **-sV --version-intensity 5**

- More precise product/version strings — e.g. OpenSSH 6.6.1p1 and Apache httpd 2.4.7 ((Ubuntu)) (shows both product and exact version/build hints).
- Service extra-info / banner-like details — sometimes includes OS distribution hints (here it shows “Ubuntu” in the HTTP/SSH results).

- Service Info / CPE — Nmap reported Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel, which helps map services to known CPE identifiers for vulnerability research.
- Possibly more detected services or protocol details — medium intensity can probe additional ports/protocols and return things simpler probes miss (e.g., SSH host-key info or extended HTTP headers when available).
- Better OS/service fingerprinting accuracy — the extra probes improve Nmap's guesses about OS and service versions (you saw the "Aggressive OS guesses" previously when using -A).

-sV --version-intensity [linux.bz](#)

```
C:\Windows\System32>nslookup linux.bz
Server: ns4.dhcp.ums1.edu
Address: 134.124.2.1

Name: linux.bz

C:\Windows\System32>nslookup linux.bz
Server: middns1.psdr3.org
Address: 10.80.198.30

Name: linux.bz

C:\Windows\System32>nmap -sV --version-intensity 5 10.80.198.30
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 15:36 -0500
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.26 seconds

C:\Windows\System32>nmap -sV --version-intensity 5 linux.bz
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 15:36 -0500
Failed to resolve "linux.bz".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.14 seconds
```

Not sure what's going wrong!

viii. .

```
C:\Windows\System32>nmap -sV -script=banner linux.bz
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-13 15:38 -0500
Failed to resolve "linux.bz".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.18 seconds
```

4.



ii.

