

CYBER SECURITY INTERNSHIP

Task:01 Cybersecurity Risk Assessment



MARCH 8, 2024

INTERN CAREER

Cybersecurity Risk Assessment:

Cybersecurity risk assessment is the process of identifying, evaluating, and prioritizing potential threats and vulnerabilities that could compromise the confidentiality, integrity, and availability of information systems.

Key Components of Cybersecurity Risk Assessment:

1. **Asset Identification:** Identify and prioritize assets critical to the organization, including hardware, software, data, and personnel.
2. **Threat Identification:** Identify potential threats that could exploit vulnerabilities and impact the security of assets.
3. **Vulnerability Assessment:** Assess weaknesses and vulnerabilities in systems, applications, and processes that could be exploited by threats.
4. **Risk Analysis:** Evaluate the likelihood and impact of identified risks to determine their overall risk level.
5. **Risk Mitigation:** Develop strategies to mitigate or control identified risks, including implementing security controls and best practices.

Threat Identification:

Sample Network/ System Setup:

The provided system is a small business network with a web server, database server, and multiple client workstations. The web server hosts a customer portal and the database server stores sensitive customer information.

Identify Threats and vulnerabilities:

Threats:

1. **Malware:** potential for malware infections due to web server exposure.
2. **Unauthorized Access:** Weaknesses in authentication may lead to unauthorized access.
3. **DDOS Attacks:** The web server is susceptible to Distributed Denial of Service attacks.

Vulnerabilities:

1. **Outdated Software:** The web server software may not be up to date.
2. **Weak Passwords:** Workstations might have weak passwords, increasing the risk of unauthorized access.

Tools for Cybersecurity Risk Assessment:

Nmap:

1. Conducted a network scan to identify active hosts and open ports.
2. Identified the IP addresses of the web server, database server, and workstations.

Ping Scan: The simplest way to check active hosts and open ports is by a ping scan.

```
darknet@5BN2MVC: ~
File Actions Edit View Help
darknet@5BN2MVC: ~ x root@5BN2MVC: /home/darknet x darknet@5BN2MVC: ~ x
(darknet@5BN2MVC)-[~]
$ nmap -sn 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 08:02 CST
Nmap scan report for 192.168.0.1
Host is up (0.0058s latency).
Nmap scan report for 192.168.0.255
Host is up (0.0017s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.34 seconds
(darknet@5BN2MVC)-[~]
```

```
darknet@5BN2MVC: ~
File Actions Edit View Help
darknet@5BN2MVC: ~ x root@5BN2MVC: /home/darknet x darknet@5BN2MVC: ~ x
(darknet@5BN2MVC)-[~]
$ nmap 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 08:17 CST
Nmap scan report for 192.168.0.1
Host is up (0.0069s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
1900/tcp   open  upnp
Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds
(darknet@5BN2MVC)-[~]
```

Service and version detection: To identify services running on open ports and their versions.

```
darknet@5BN2MVC: ~
File Actions Edit View Help
darknet@5BN2MVC: ~ x root@5BN2MVC: /home/darknet x darknet@5BN2MVC: ~ x
(darknet@5BN2MVC)-[~]
$ nmap -sV 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-09 08:19 CST
WARNING: Service 192.168.0.1:1900 had already soft-matched upnp, but now soft-matched rtsp; ignoring second value
WARNING: Service 192.168.0.1:1900 had already soft-matched upnp, but now soft-matched sip; ignoring second value
Nmap scan report for 192.168.0.1
Host is up (0.0081s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain
80/tcp    open  http         BusyBox http 1.19.4
443/tcp   open  ssl/http     BusyBox http 1.19.4
1900/tcp   open  upnp         MiniUPnP 1.8 (UPnP 1.1)
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

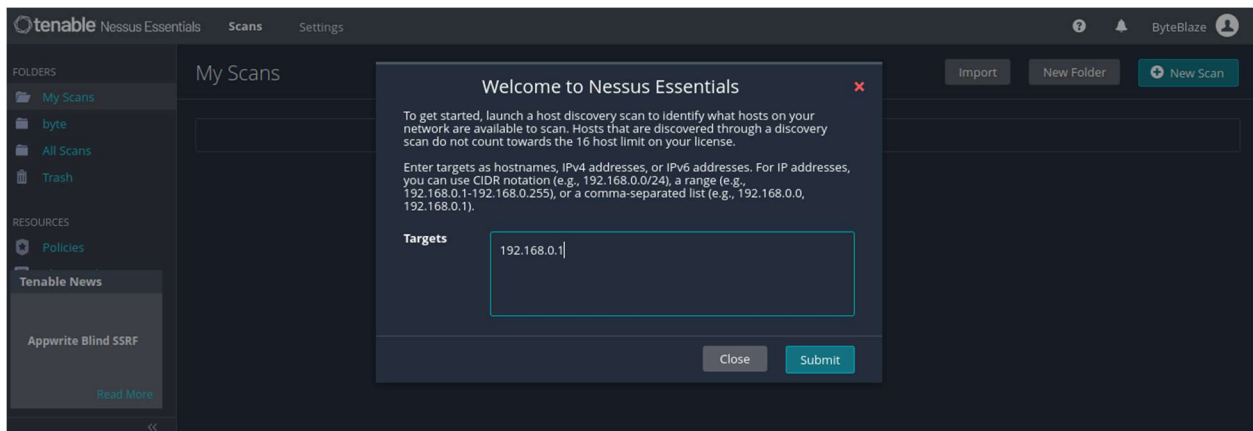
```

Nessus:

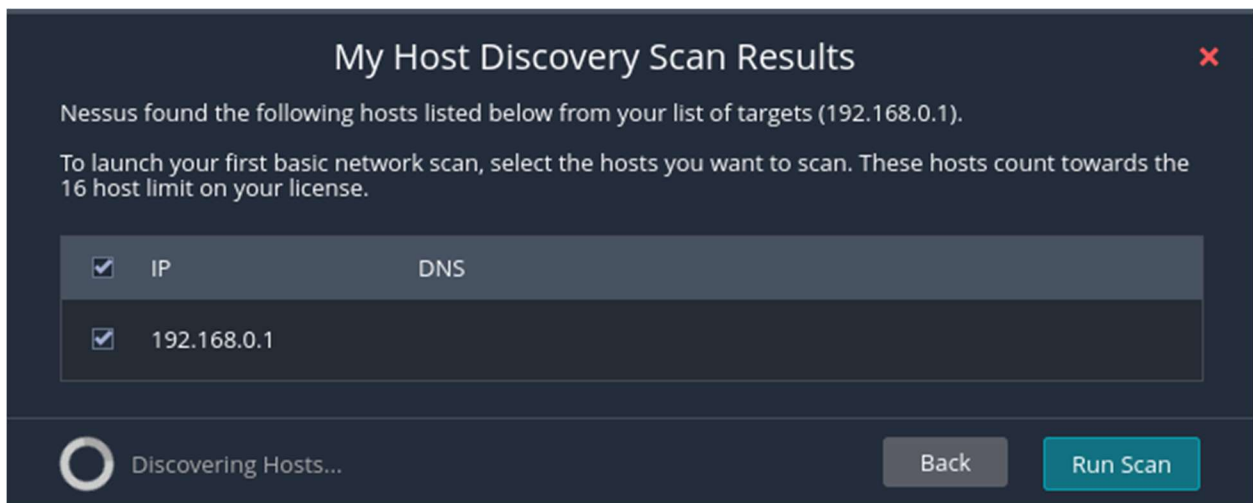
1. Performed a vulnerability scan on each identified host.
2. Discovered vulnerabilities such as outdated software versions and weak configurations.

An effective tool for vulnerability scanning and assessments, Nessus identifies security issues in systems and applications.

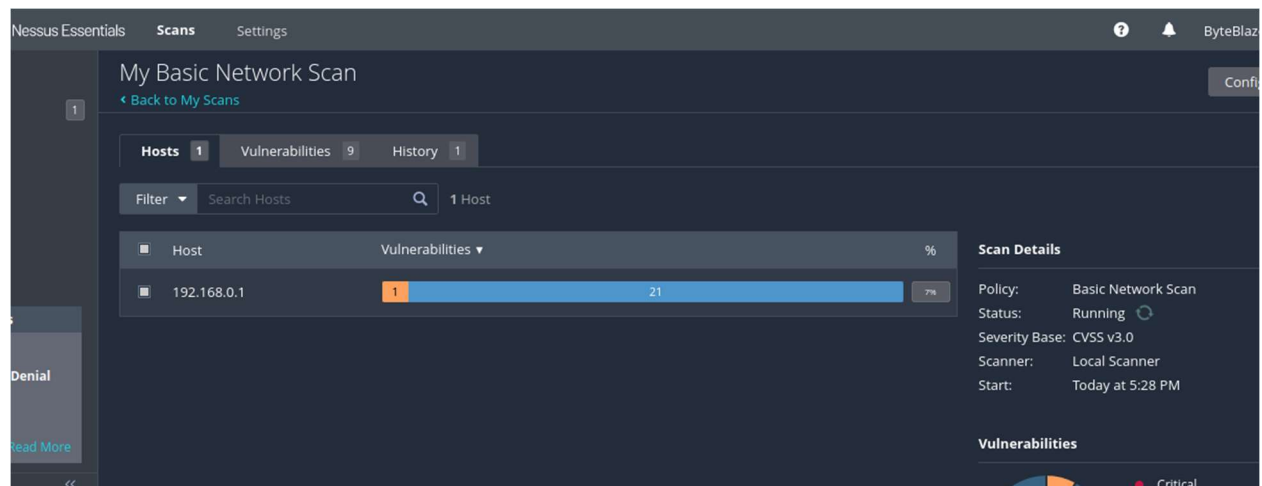
Scan targets IP:



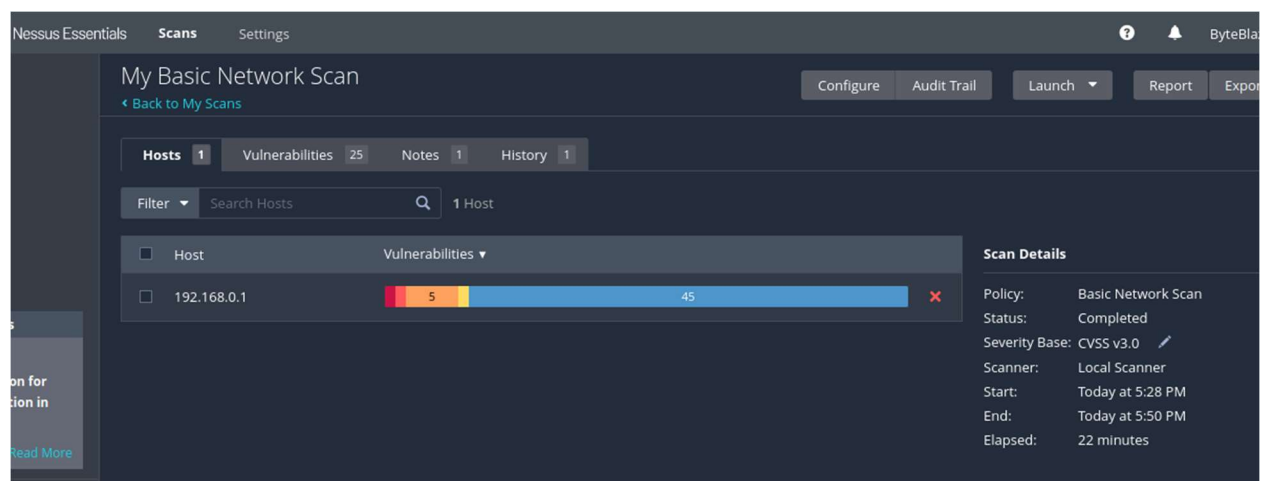
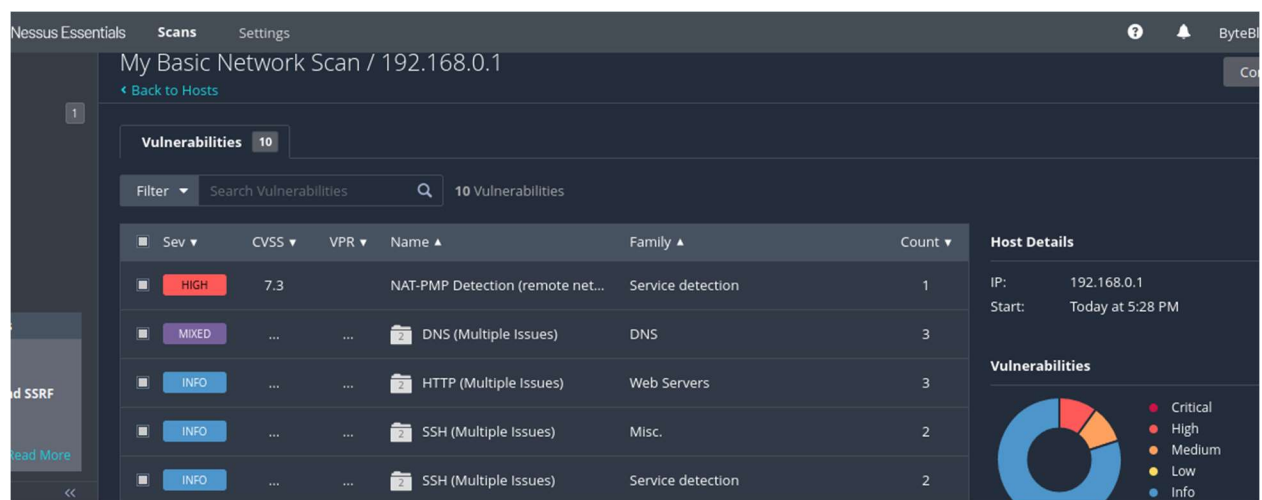
Network scan



Scan Vulnerabilities



Vulnerabilities scan finds high risk



Nessus Essentials Scans Settings

My Basic Network Scan

[Back to My Scans](#) [Configure](#) [Audit Trail](#) [Launch](#) [Report](#)

Hosts 1 Vulnerabilities 25 Notes 1 History 1

Filter Search Vulnerabilities 25 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8		SSL Version 2 a...	Service detection	1
HIGH	7.3		NAT-PMP Detec...	Service detection	1
MIXED	SSL (Multi...	General	10
MIXED	TLS (Multi...	Service detection	4
MIXED	DNS (Multi...	DNS	3

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 5:28 PM

End: Today at 5:50 PM

Elapsed: 22 minutes

Vulnerabilities

Wireshark:

Useful for network protocol analysis and troubleshooting, Wireshark helps examine and analyze network traffic for potential security issues.

1. Analyzed network traffic to identify any abnormal patterns or potential security issues.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
108	16.911430	142.250.182.3	192.168.0.163	QUIC	574	Protected Payload (KP0)
109	16.911575	142.250.182.3	192.168.0.163	QUIC	65	Protected Payload (KP0)
110	16.912177	192.168.0.163	142.250.182.3	QUIC	77	Protected Payload (KP0), DCID=eb89edd42a5deef
111	16.931597	142.250.182.3	192.168.0.163	QUIC	162	Protected Payload (KP0)
112	16.932127	192.168.0.163	142.250.182.3	QUIC	73	Protected Payload (KP0), DCID=eb89edd42a5deef
113	16.968073	142.250.182.3	192.168.0.163	QUIC	67	Protected Payload (KP0)
114	17.309036	192.168.0.163	34.107.199.61	TCP	55	[TCP Keep-Alive] 49659 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1
115	17.339260	34.107.199.61	192.168.0.163	TCP	66	[TCP Keep-Alive ACK] 443 → 49659 [ACK] Seq=1 Ack=2 Win=256 Len=0 SLE=1 SRE=2
116	17.888619	192.168.0.163	204.72.197.222	TCP	54	[TCP Retransmission] 49277 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
117	18.616741	13.107.42.14	192.168.0.163	TLSv1.2	100	Application Data
118	18.860271	192.168.0.163	13.107.42.14	TCP	54	49453 → 443 [ACK] Seq=5889 Ack=276 Win=514 Len=0
119	19.477789	192.168.0.163	191.233.176.51	TCP	54	[TCP Retransmission] 49283 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
120	20.518647	192.168.0.163	142.250.195.174	UDP	71	57966 → 443 Len=29
121	20.557092	142.250.195.174	192.168.0.163	UDP	68	443 → 57966 Len=26
122	20.834950	192.168.0.163	13.89.179.9	TCP	55	49637 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
123	20.837665	13.89.179.9	192.168.0.163	TCP	66	443 → 49637 [ACK] Seq=1 Ack=2 Win=384 Len=0 SLE=1 SRE=2

> Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{...}

> Ethernet II, Src: TP-Link_71:18:84 (34:60:f9:71:18:84), Dst: HonHaiPr_77:b3:f9 (3c:77:e6:77:b3:f9)

> Internet Protocol Version 4, Src: 54.205.102.198, Dst: 192.168.0.163

> Transmission Control Protocol, Src Port: 443, Dst Port: 49638, Seq: 1, Ack: 1, Len: 31

> Transport Layer Security

```

0000  3c 77 e6 77 b3 f9 34 60 f9 71 18 84 08 00 45 00  <w-w-4` q---E-
0010  00 47 07 f6 00 00 ea 06 69 dc 36 cd 66 c6 c0 a8  <G----- i-6-f-
0020  00 a3 01 bb c1 e6 5d 2b 7c f1 31 17 66 3a 50 18  <-----] + | -1-f:P-
0030  01 80 cc b0 00 00 15 03 03 00 1a 00 00 00 00 00  <-----
0040  00 00 03 de 32 5e 32 87 e0 b3 d6 a1 9e 06 1e 00  <-----2^2-
0050  4c 8c a4 de 4e                                     L---N

```


Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

youtube

No.	Time	Source	Destination	Protocol	Length	Info
84	6.804622	192.168.0.163	185.199.111.154	TCP	55	49694 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
85	6.812859	185.199.111.154	192.168.0.163	TCP	66	443 → 49694 [ACK] Seq=1 Ack=2 Win=192 Len=0 SLE=1 SRE=2
86	7.237836	192.168.0.163	204.79.197.239	TCP	55	49706 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
87	7.242585	204.79.197.239	192.168.0.163	TCP	66	443 → 49706 [ACK] Seq=1 Ack=2 Win=384 Len=0 SLE=1 SRE=2
88	8.685533	TP-Link_71:18:84	MonHaiPr_77:b3:f9	ARP	42	Who has 192.168.0.163? Tell 192.168.0.1
89	8.685584	MonHaiPr_77:b3:f9	TP-Link_71:18:84	ARP	42	192.168.0.163 is at 3c:77:e6:77:b3:f9
90	9.280580	192.168.0.163	185.199.111.154	TCP	55	49698 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
91	9.283031	185.199.111.154	192.168.0.163	TCP	66	443 → 49698 [ACK] Seq=1 Ack=2 Win=192 Len=0 SLE=1 SRE=2
92	9.628523	192.168.0.163	142.250.195.174	UDP	71	57966 → 443 Len=29
93	9.668974	142.250.195.174	192.168.0.163	UDP	68	443 → 57966 Len=26
94	11.766091	192.168.0.163	140.82.112.22	TCP	55	49710 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
95	12.047255	140.82.112.22	192.168.0.163	TCP	54	443 → 49710 [RST] Seq=1 Win=0 Len=0
96	13.564750	192.168.0.137	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
97	13.741160	192.168.0.163	54.243.153.181	TCP	54	49677 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
98	13.768795	142.250.193.10	192.168.0.163	UDP	120	443 → 63600 Len=78
99	13.794239	192.168.0.163	142.250.193.10	UDP	75	63600 → 443 Len=33

> Frame 1: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{...}

> Ethernet II, Src: MonHaiPr_77:b3:f9 (3c:77:e6:77:b3:f9), Dst: TP-Link_71:18:84 (34:60:f9:71:18:84)

> Internet Protocol Version 4, Src: 192.168.0.163, Dst: 142.250.195.174

> User Datagram Protocol, Src Port: 57966, Dst Port: 443

> Data (29 bytes)

```

0000  34 60 f9 71 18 84 3c 77 e6 77 b3 f9 08 00 45 00  4 q c w w w E
0010  00 39 c9 6a 40 00 00 11 1d 55 c0 a8 00 a3 8e fa  9 j @ . . . U
0020  c3 ae e2 6e 01 bb 00 25 be c3 43 f1 c2 08 e7 31  . n . . . C . 1
0030  19 68 00 cc 05 5d 7f cd ed 3c 83 d5 33 67 4a a6  . h . . . < 3 g j
0040  6d 84 ac b7 24 db 0e                                . . . $ n

```

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
54	14.300246	192.168.0.163	52.5.28.62	TCP	55	[TCP Keep-Alive] 49748 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1
55	14.608796	52.5.28.62	192.168.0.163	TCP	54	[TCP Keep-Alive ACK] 443 → 49748 [ACK] Seq=2 Ack=2 Win=121 Len=0
56	17.108586	192.168.0.163	140.82.112.25	TCP	55	49713 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
66	17.829850	13.107.42.14	192.168.0.163	TLSv1.2	100	Application Data
67	17.829906	13.107.42.14	192.168.0.163	TCP	100	[TCP Retransmission] 443 → 49453 [PSH, ACK] Seq=47 Ack=1 Win=864 Len=46
68	17.829949	192.168.0.163	13.107.42.14	TCP	66	49453 → 443 [ACK] Seq=1 Ack=93 Win=515 Len=0 SLE=47 SRE=93
69	17.830011	13.107.42.14	192.168.0.163	TCP	100	[TCP Spurious Retransmission] 443 → 49453 [PSH, ACK] Seq=47 Ack=1 Win=864 Len=46
70	17.830036	192.168.0.163	13.107.42.14	TCP	66	[TCP Dup ACK 68#1] 49453 → 443 [ACK] Seq=1 Ack=93 Win=515 Len=0 SLE=47 SRE=93
71	17.830074	13.107.42.14	192.168.0.163	TCP	100	[TCP Spurious Retransmission] 443 → 49453 [PSH, ACK] Seq=47 Ack=1 Win=864 Len=46
72	17.830091	192.168.0.163	13.107.42.14	TCP	66	[TCP Dup ACK 68#2] 49453 → 443 [ACK] Seq=1 Ack=93 Win=515 Len=0 SLE=47 SRE=93
73	17.830118	13.107.42.14	192.168.0.163	TCP	100	[TCP Spurious Retransmission] 443 → 49453 [PSH, ACK] Seq=47 Ack=1 Win=864 Len=46
74	17.830133	192.168.0.163	13.107.42.14	TCP	66	[TCP Dup ACK 68#3] 49453 → 443 [ACK] Seq=1 Ack=93 Win=515 Len=0 SLE=47 SRE=93
75	17.830157	140.82.112.25	192.168.0.163	TCP	66	443 → 49713 [ACK] Seq=1 Ack=2 Win=96 Len=0 SLE=1 SRE=2
98	18.539371	20.198.118.190	192.168.0.163	TCP	54	443 → 49267 [ACK] Seq=1 Ack=1 Win=65535 Len=0
99	18.539438	192.168.0.163	20.198.118.190	TCP	54	[TCP ACKed unseen segment] 49267 → 443 [ACK] Seq=1 Ack=2 Win=515 Len=0
100	18.728791	192.168.0.163	35.186.224.25	TCP	54	49872 → 443 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0

> Frame 10: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF_{...}

> Ethernet II, Src: TP-Link_71:18:84 (34:60:f9:71:18:84), Dst: MonHaiPr_77:b3:f9 (3c:77:e6:77:b3:f9)

> Internet Protocol Version 4, Src: 13.107.42.14, Dst: 192.168.0.163

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 86

Identification: 0x6bfa (27642)

0000 = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 117

Protocol: TCP (6)

Header Checksum: 0xe0e3 [validation disabled]

[Header checksum status: Unverified]

```

0000  3c 77 e6 77 b3 f9 34 60 f9 71 18 84 08 00 45 00  c w w w . q . . . E
0010  00 56 6b fa 00 00 75 06 e0 e3 0d 6b 2a 0e c0 a8  . V k . . . . . k . . .
0020  00 a3 01 bb c1 2d 6a 09 f5 cc a2 9a d5 ea 58 18  . . . . . P . . . . . P
0030  03 60 c4 3c 00 00 17 03 03 00 29 00 00 00 00  . . . . . . . . . . .
0040  00 02 c7 1e 8d 9c 4f af 60 7b c3 6d b1 5c 12 d1  . . . . . O . . . . . m . \
0050  92 63 8f ac c6 d4 73 02 a4 7f f2 d7 40 df 40  . . . . . . . . . . p H @
0060  27 de 19 d1                                           . . . .

```

Conclusion:

The cybersecurity risk assessment conducted as part of this internship has provided valuable insights into the security posture of the organization's digital infrastructure. Through a systematic approach, including threat identification, vulnerability scanning, risk analysis, and mitigation strategies, critical security risks have been identified and addressed.

Overall, this cybersecurity risk assessment internship has provided valuable hands-on experience and insights into the complexities of cybersecurity. As cybersecurity threats continue to evolve, the knowledge and skills gained during this internship will serve as a solid foundation for future endeavors in the field.