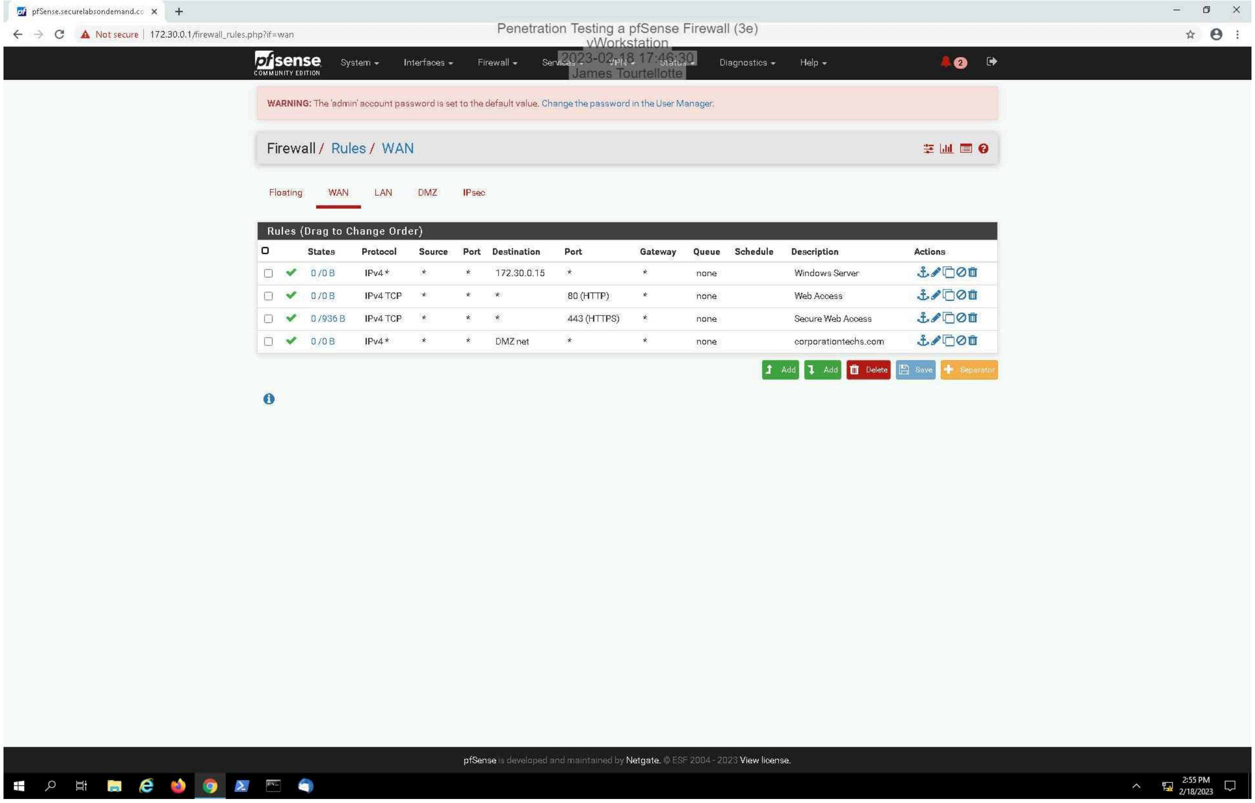
James Everett Tourtellotte IV
ITN 263
2/27/2023

Lab 10: Penetration Testing a Firewall

Lab #10 Screen Captures

Screen Capture 1, Section 1:


pfSense.securelabsondemand.co
Not secure | 172.30.0.1/firewall_rules.php?if=wan
Penetration Testing a pfSense Firewall (3e)
vWorkstation
2023-02-18 17:46:30
James Tourtellotte
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Floating
WAN
LAN
DMZ
IPsec
Add
Add
Delete
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.
2:55 PM
2/18/2023

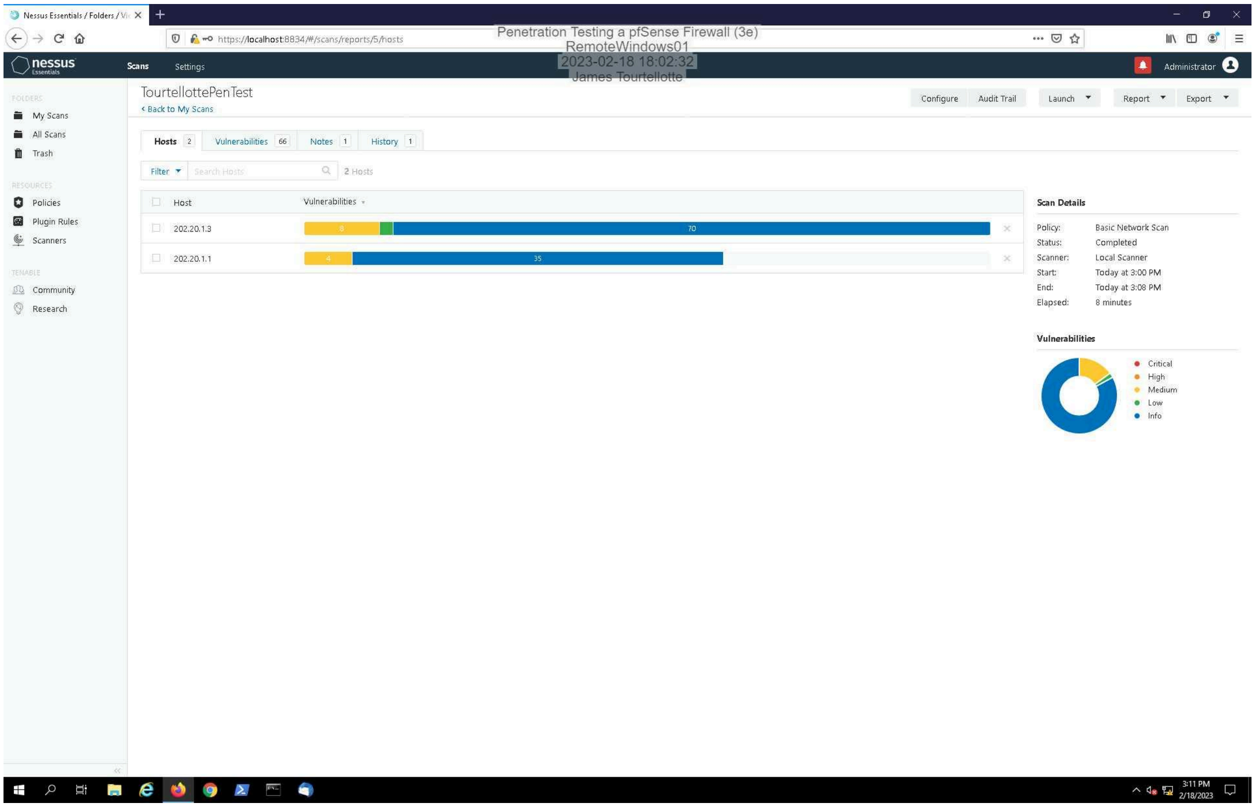
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / WAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 *	*	*	172.30.0.15	*	*	none		Windows Server	
□	✓	0 /0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Web Access	
□	✓	0 /936 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Secure Web Access	
□	✓	0 /0 B	IPv4 *	*	*	DMZ net	*	*	none		corporationtechs.com	

Section 1 Screen Capture 2:



TourtellottePenTest

‹ Back to My Scans

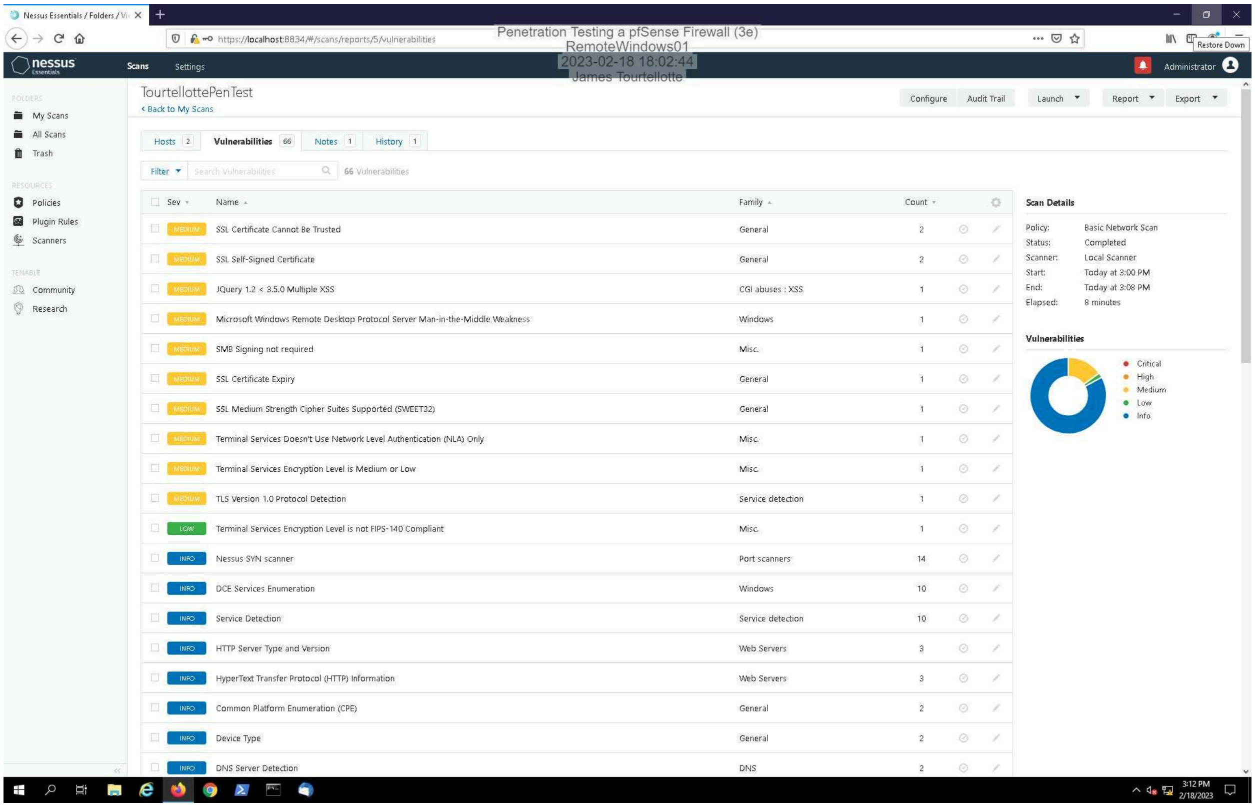
Host	Vulnerabilities
202.20.1.3	8 70
202.20.1.1	4 35

Scan Details

Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 3:00 PM
End: Today at 3:08 PM
Elapsed: 8 minutes

Vulnerabilities

Section 1 Screen Capture 3:



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2023-02-18 18:02:44
James Tourtellotte

TourtellottePenTest
‹ Back to My Scans

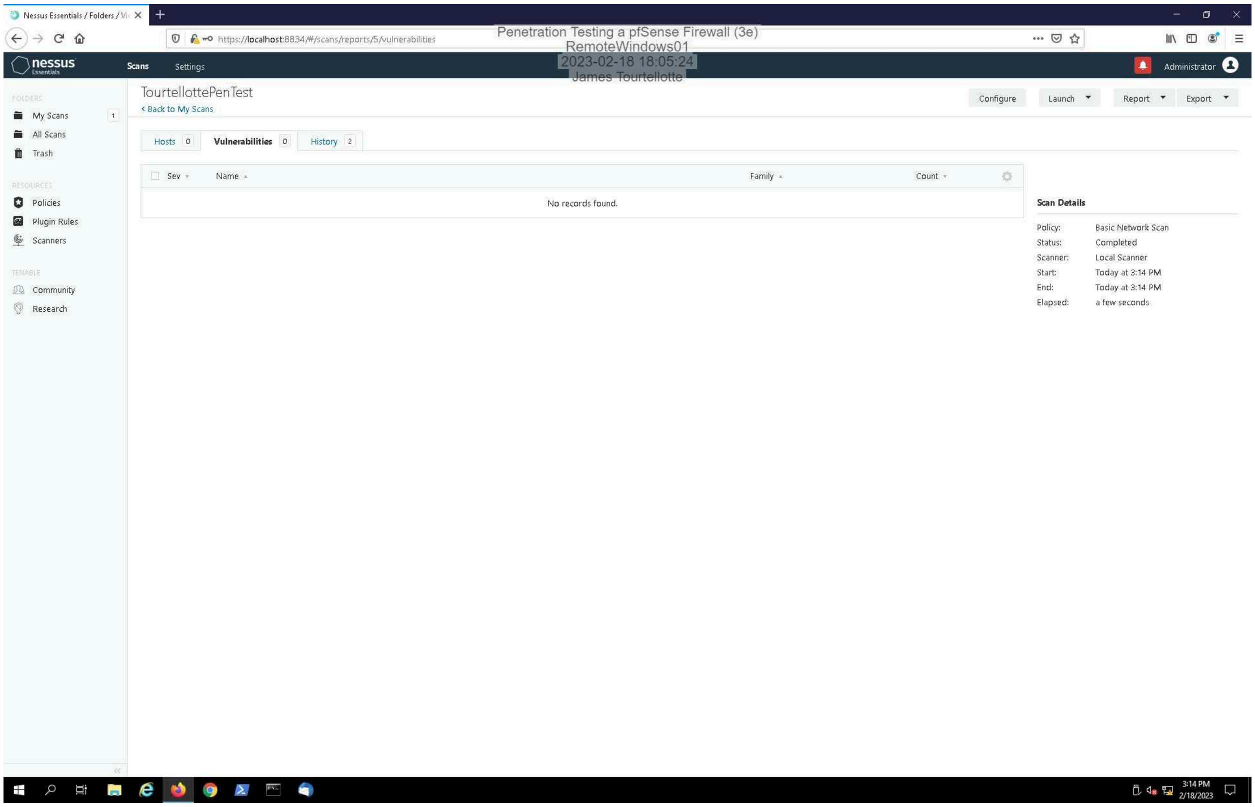
Sev	Name	Family	Count
MEDIUM	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	SSL Self-Signed Certificate	General	2
MEDIUM	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows	1
MEDIUM	SMB Signing not required	Misc.	1
MEDIUM	SSL Certificate Expiry	General	1
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	1
MEDIUM	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Misc.	1
MEDIUM	Terminal Services Encryption Level is Medium or Low	Misc.	1
MEDIUM	TLS Version 1.0 Protocol Detection	Service detection	1
LOW	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1
INFO	Nessus SYN scanner	Port scanners	14
INFO	DCE Services Enumeration	Windows	10
INFO	Service Detection	Service detection	10
INFO	HTTP Server Type and Version	Web Servers	3
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	3
INFO	Common Platform Enumeration (CPE)	General	2
INFO	Device Type	General	2
INFO	DNS Server Detection	DNS	2

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 3:00 PM
End:	Today at 3:08 PM
Elapsed:	8 minutes

Vulnerabilities

Section 1 Screen Capture 4:



Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2023-02-18 18:05:24
James Tourtellotte

TourtellottePenTest

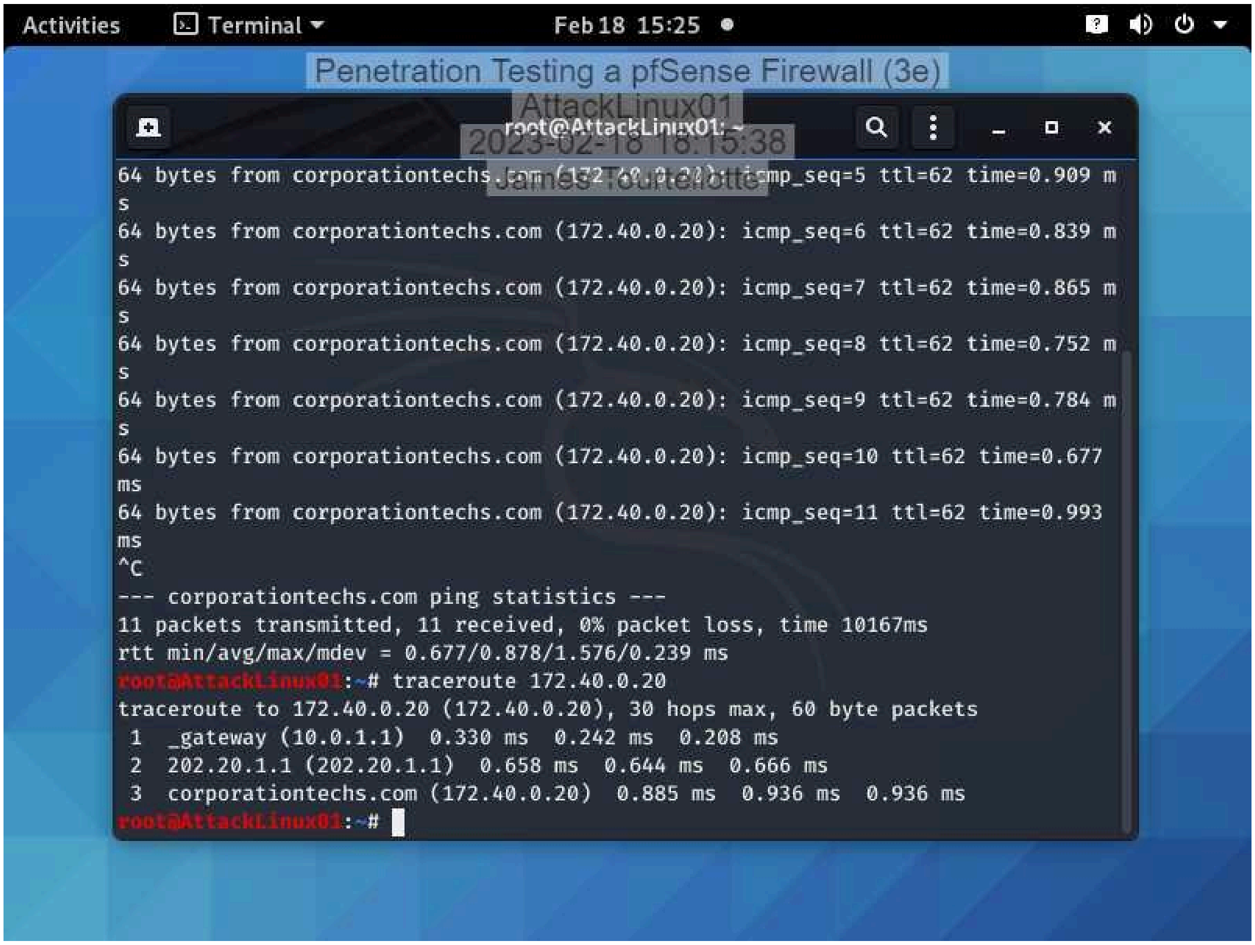
‹ Back to My Scans

Sev	Name	Family	Count
No records found.			

Scan Details

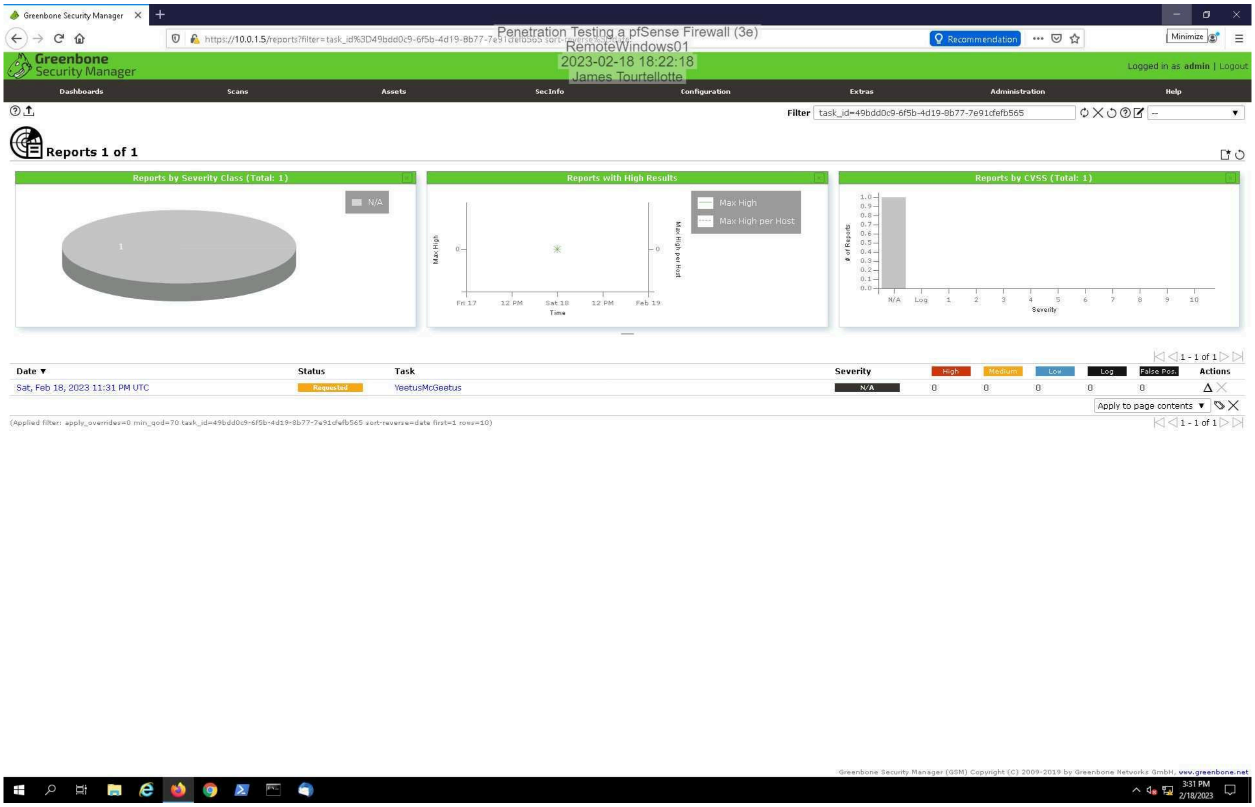
Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 3:14 PM
End:	Today at 3:14 PM
Elapsed:	a few seconds

Screen Capture 1, Section 2:



```
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=5 ttl=62 time=0.909 m
s
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=6 ttl=62 time=0.839 m
s
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=7 ttl=62 time=0.865 m
s
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=8 ttl=62 time=0.752 m
s
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=9 ttl=62 time=0.784 m
s
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=10 ttl=62 time=0.677
ms
64 bytes from corporationtechs.com (172.40.0.20): icmp_seq=11 ttl=62 time=0.993
ms
^C
--- corporationtechs.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10167ms
rtt min/avg/max/mdev = 0.677/0.878/1.576/0.239 ms
root@AttackLinux01:~# traceroute 172.40.0.20
traceroute to 172.40.0.20 (172.40.0.20), 30 hops max, 60 byte packets
 1  _gateway (10.0.1.1)  0.330 ms  0.242 ms  0.208 ms
 2  202.20.1.1 (202.20.1.1)  0.658 ms  0.644 ms  0.666 ms
 3  corporationtechs.com (172.40.0.20)  0.885 ms  0.936 ms  0.936 ms
root@AttackLinux01:~#
```

Screen Capture 2, Section 2:



Greenbone Security Manager
https://10.0.1.5/reports?filter=task_id%3D49bdd0c9-6f5b-4d19-8b77-7e91cfefb565 sort-reverse%3Ddate
Recommendation
Minimize
Greenbone Security Manager
Logged in as admin | Logout
Dashboards
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2023-02-18 18:22:18
James Tourtellotte

Filter task_id=49bdd0c9-6f5b-4d19-8b77-7e91cfefb565

Reports 1 of 1

Reports by Severity Class (Total: 1)
N/A
1
Reports with High Results
Max High
Max High per Host
0
0
Fri 17
12 PM
Sat 18
12 PM
Feb 19
Time
Max High per Host
Reports by CVSS (Total: 1)
# of Reports
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
N/A
Log
1
2
3
4
5
6
7
8
9
10
Severity

1 - 1 of 1

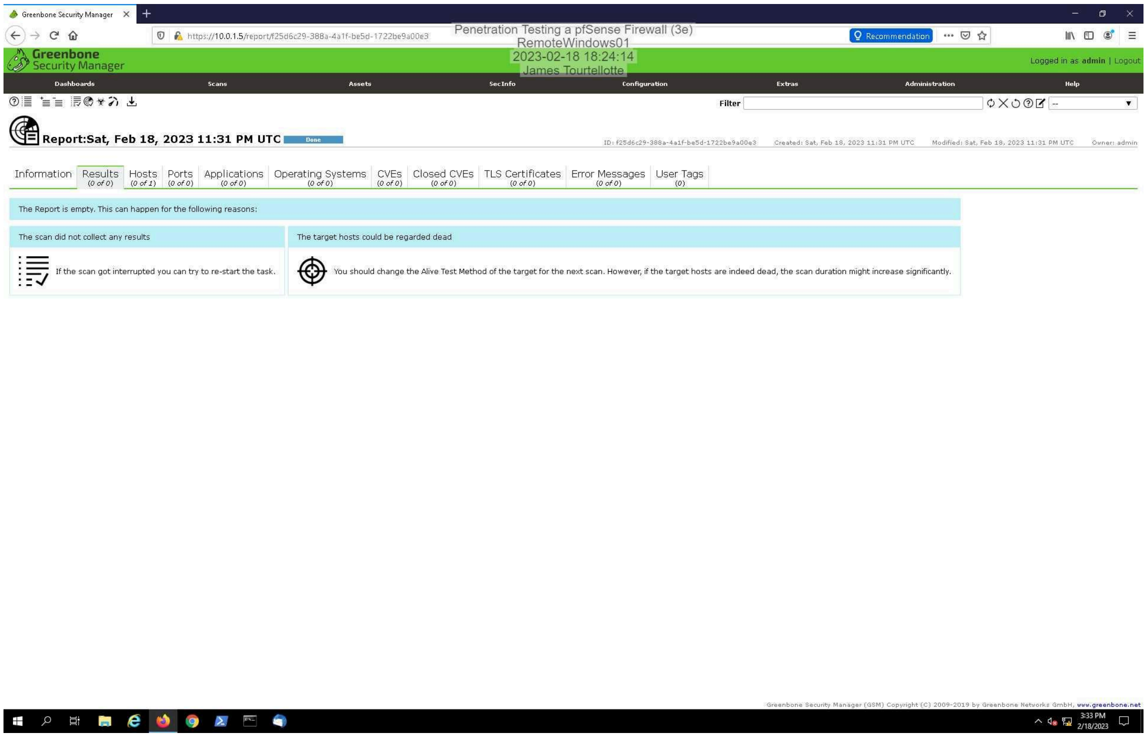
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Sat, Feb 18, 2023 11:31 PM UTC	Requested	YeetusMcGeetus	N/A	0	0	0	0	0	Δ ✕

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 task_id=49bdd0c9-6f5b-4d19-8b77-7e91cfefb565 sort-reverse=date first=1 rows=10)

1 - 1 of 1

Screen Capture 3, Section 2:



Greenbone Security Manager
https://10.0.1.5/report/f25d6c29-388a-4a1f-be5d-1722be9a00e3
Recommendation
Greenbone Security Manager
Logged in as admin | Logout
Dashboards
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

Penetration Testing a pfSense Firewall (3e)
RemoteWindows01
2023-02-18 18:24:14
James Tourtellotte

Filter

Report:Sat, Feb 18, 2023 11:31 PM UTC Done

ID: f25d6c29-388a-4a1f-be5d-1722be9a00e3 Created: Sat, Feb 18, 2023 11:31 PM UTC Modified: Sat, Feb 18, 2023 11:31 PM UTC Owner: admin

Information | Results (0 of 0) | Hosts (0 of 1) | Ports (0 of 0) | Applications (0 of 0) | Operating Systems (0 of 0) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

The Report is empty. This can happen for the following reasons:

The scan did not collect any results

If the scan got interrupted you can try to re-start the task.

The target hosts could be regarded dead

You should change the Alive Test Method of the target for the next scan. However, if the target hosts are indeed dead, the scan duration might increase significantly.