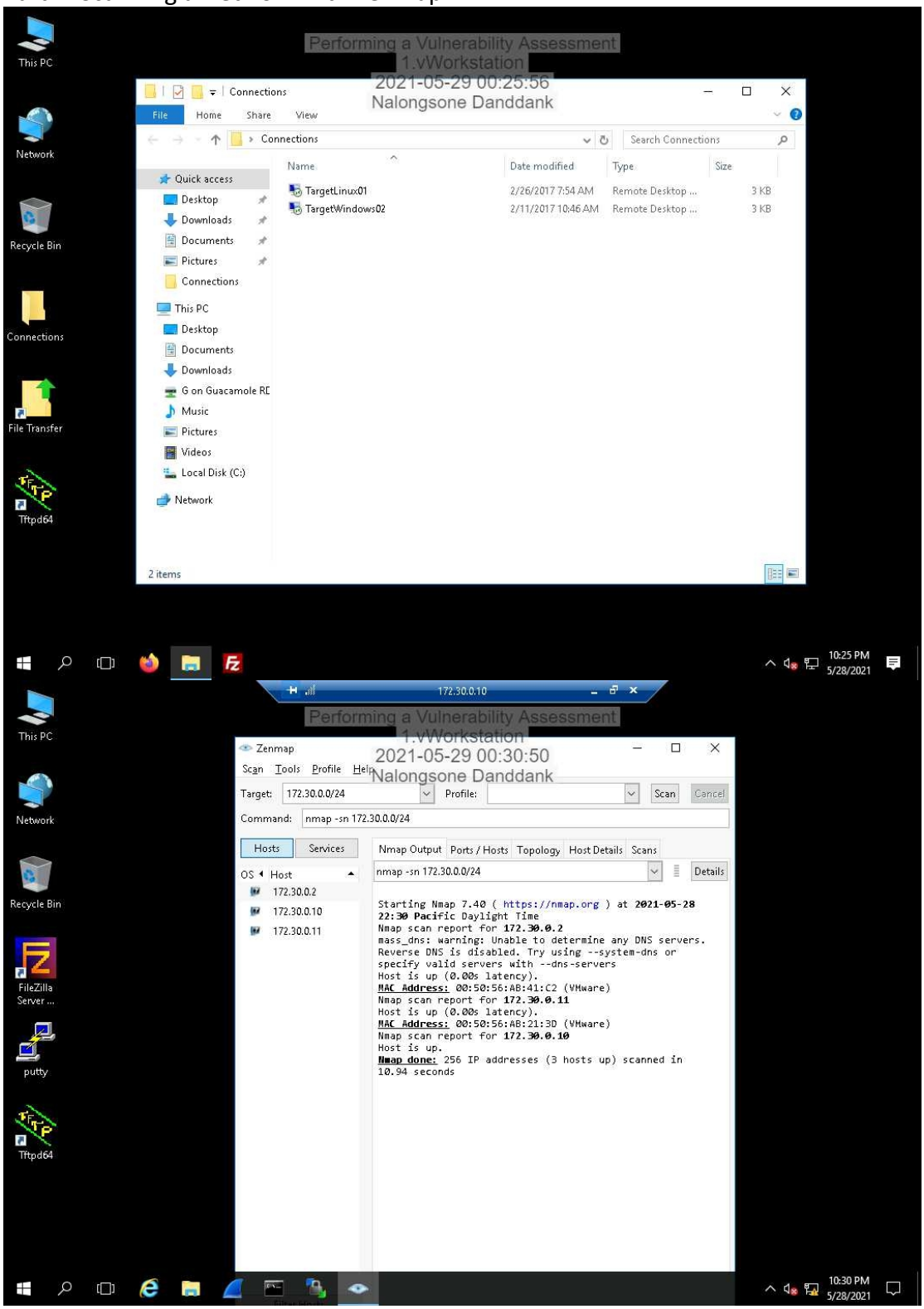
Nalongsone Danddank Student ID : 14958950 StarID: jf3893pd
Email: nalongsone.danddank@my.metrostate.edu\

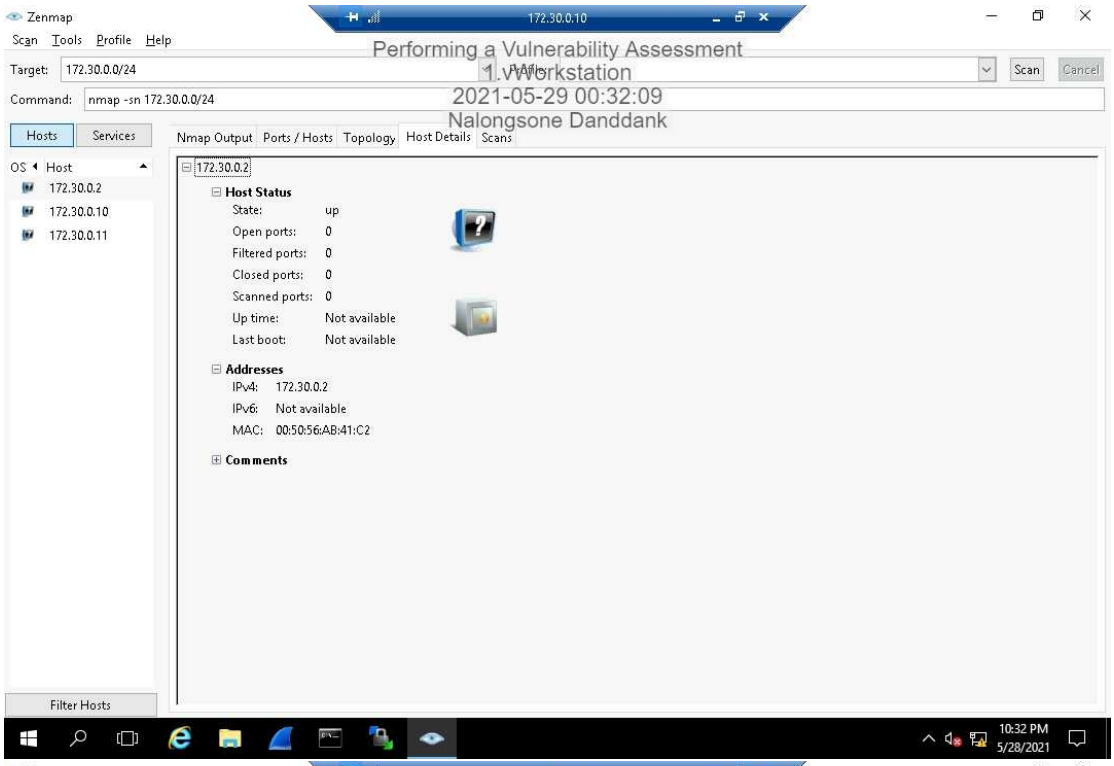
ICS382/CYBR332-51 —Computer Security

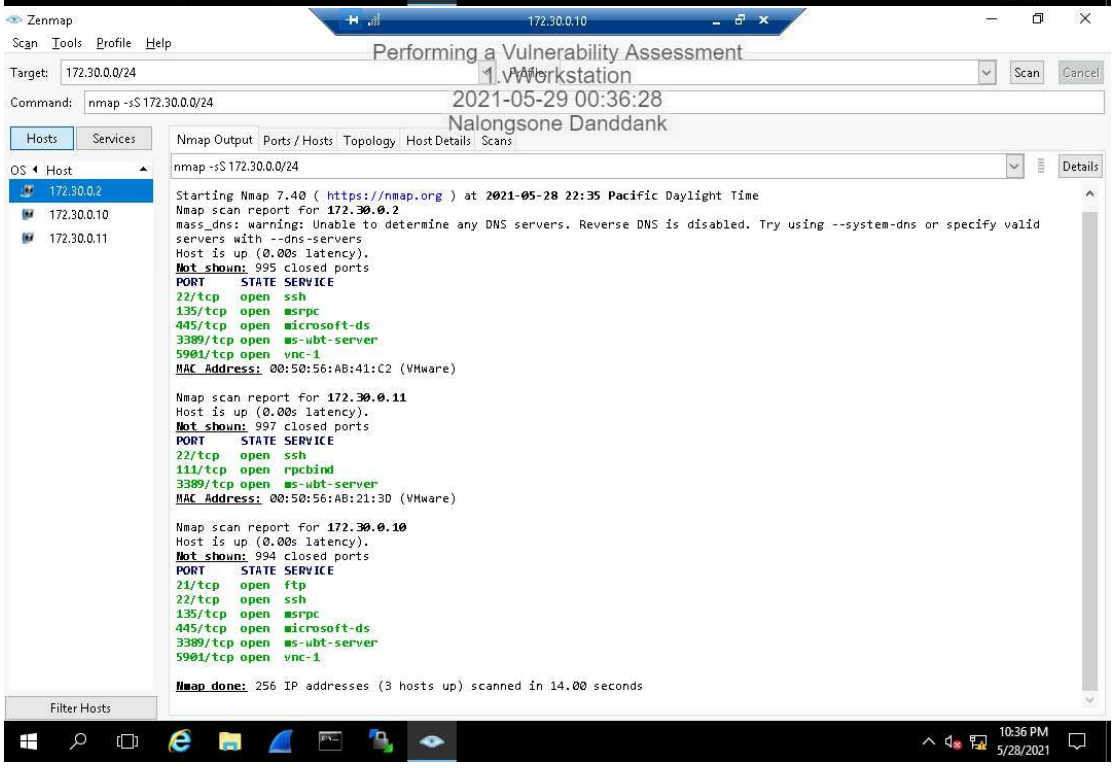
Lab #2 Report

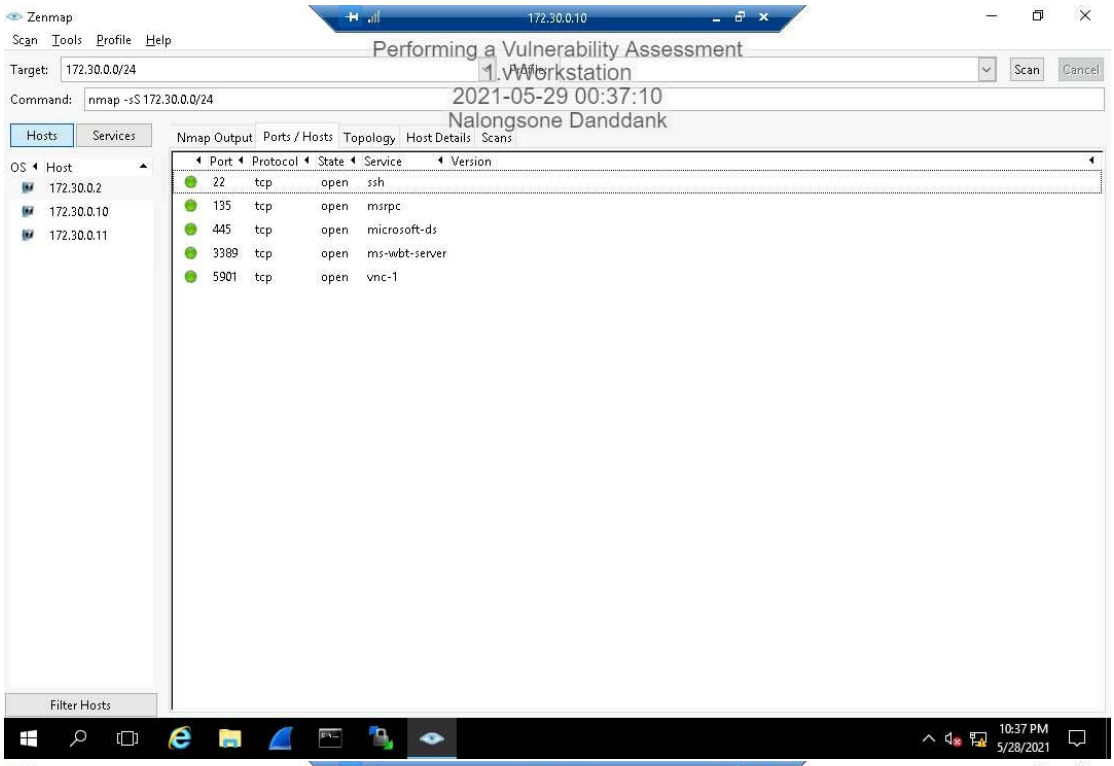
Performing a Vulnerability Assessment

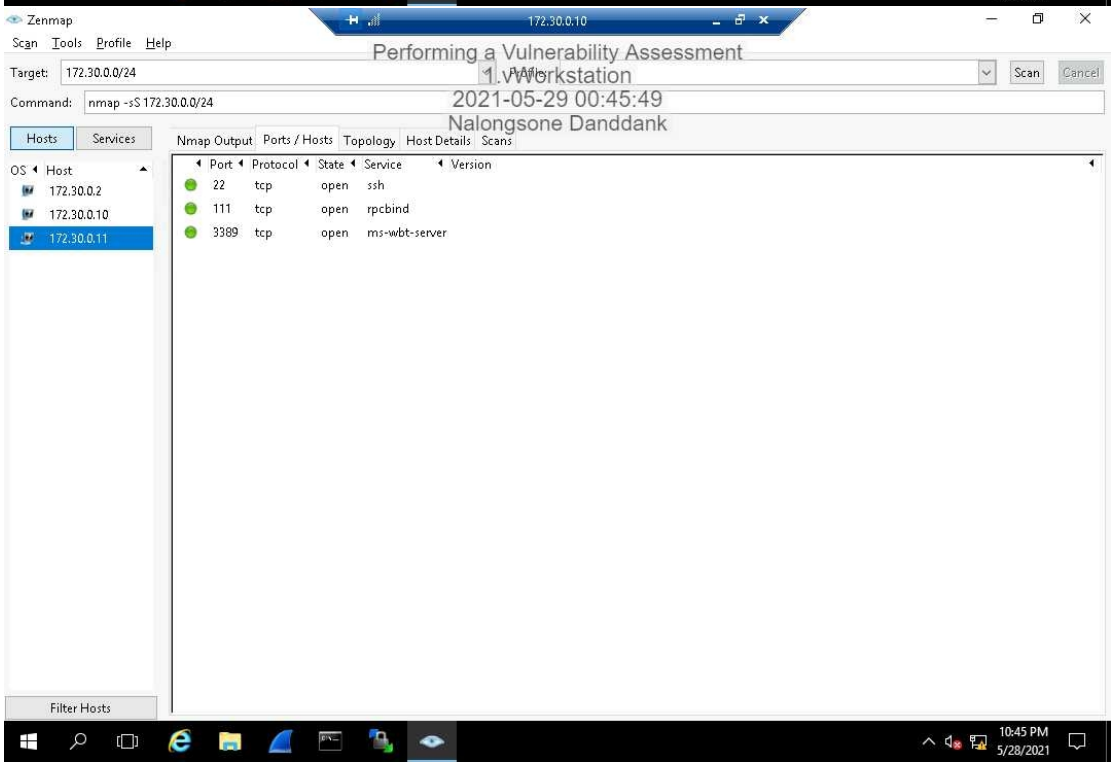
Part 1: Scanning a Network with Zenmap

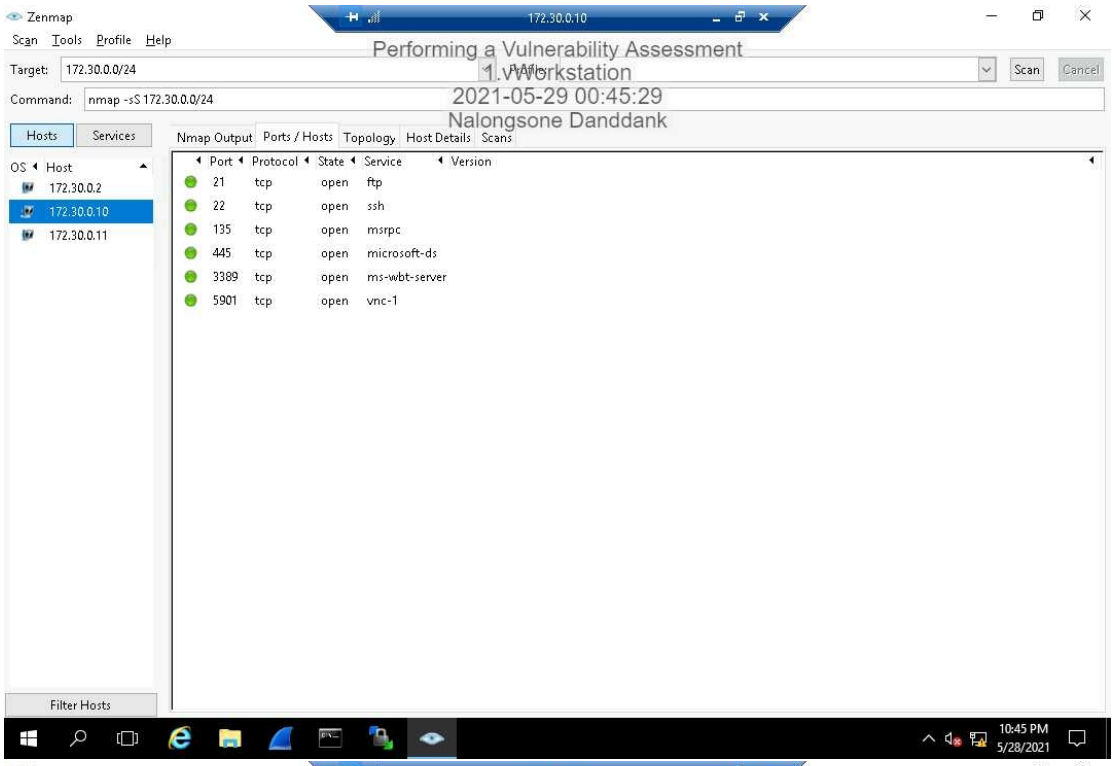


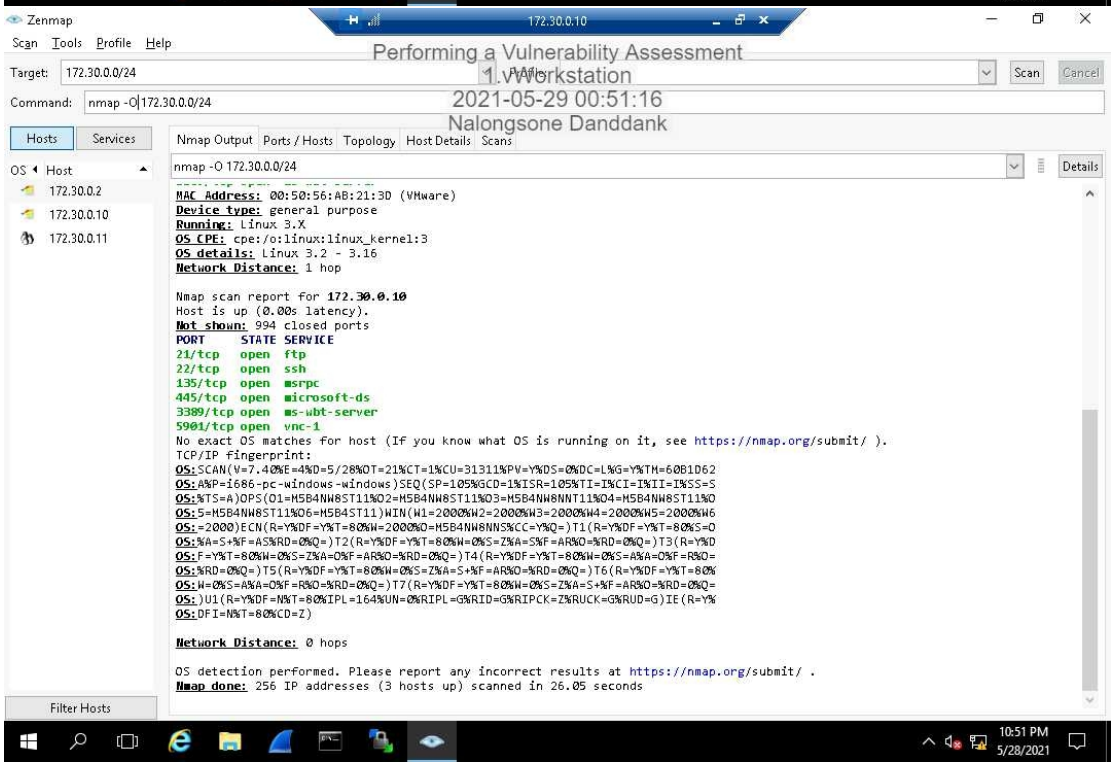

Zenmap
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:32:09
Nalongsone Danddank
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile:
Scan
Cancel
Command: nmap -sn 172.30.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
172.30.0.2
Host Status
State: up
Open ports: 0
Filtered ports: 0
Closed ports: 0
Scanned ports: 0
Up time: Not available
Last boot: Not available
Addresses
IPv4: 172.30.0.2
IPv6: Not available
MAC: 00:50:56:AB:41:C2
Comments
Filter Hosts
10:32 PM
5/28/2021

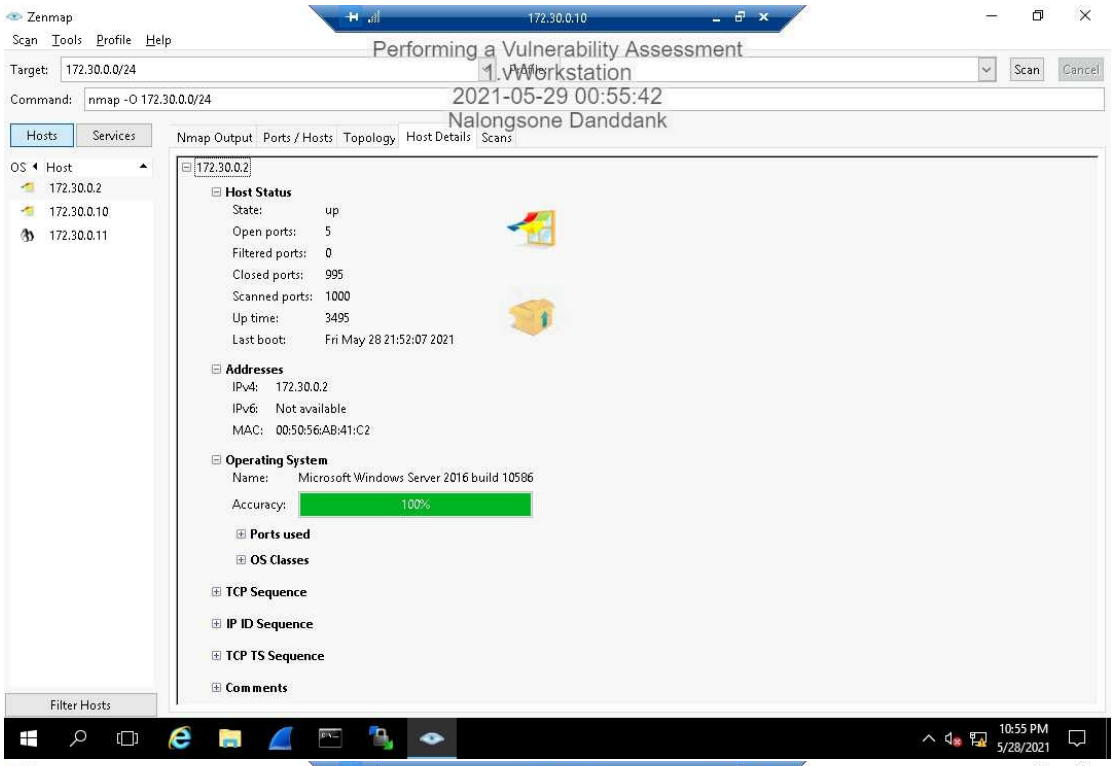

Zenmap
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:36:28
Nalongsone Danddank
Scan Tools Profile Help
Target: 172.30.0.0/24
Profile:
Scan
Cancel
Command: nmap -sS 172.30.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sS 172.30.0.0/24
Details
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
Starting Nmap 7.40 (https://nmap.org) at 2021-05-28 22:35 Pacific Daylight Time
Nmap scan report for 172.30.0.2
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Host is up (0.00s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
135/tcp open msrpc
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
5901/tcp open vnc-1
MAC Address: 00:50:56:AB:41:C2 (VMware)
Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
3389/tcp open ms-wbt-server
MAC Address: 00:50:56:AB:21:3D (VMware)
Nmap scan report for 172.30.0.10
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
135/tcp open msrpc
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
5901/tcp open vnc-1
Nmap done: 256 IP addresses (3 hosts up) scanned in 14.00 seconds
Filter Hosts
10:36 PM
5/28/2021

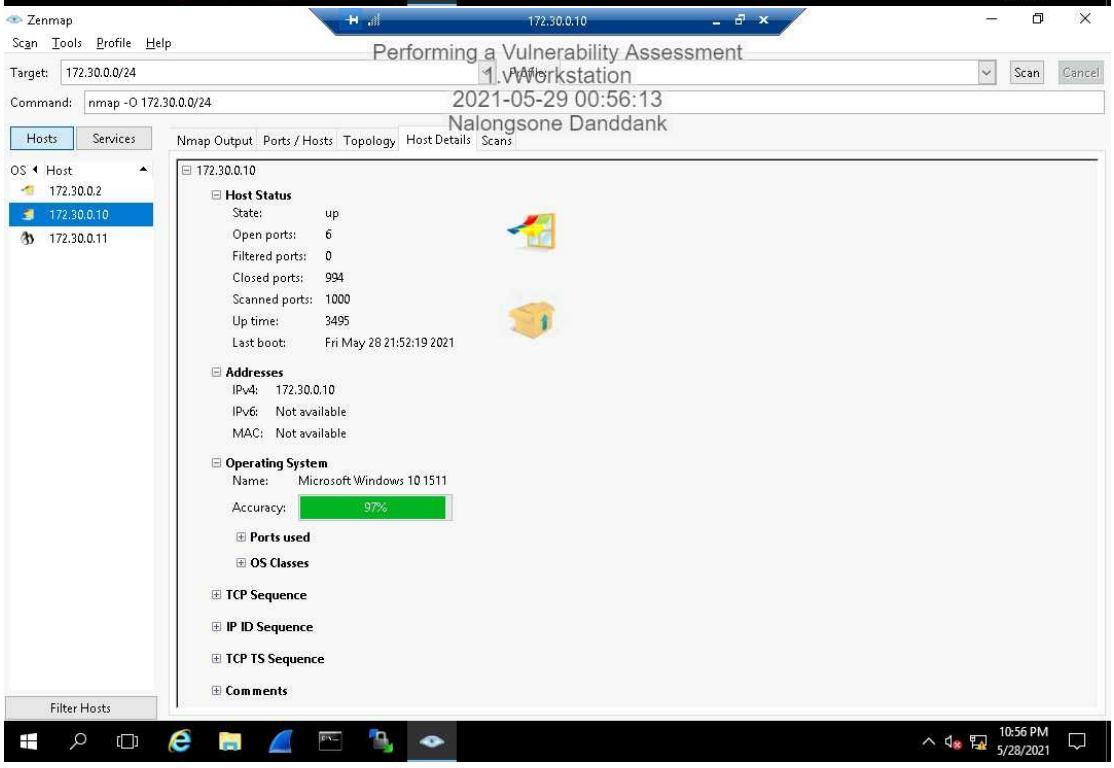

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:37:10
Nalongsone Danddank
Target: 172.30.0.0/24
Profile:
Scan
Cancel
Command: nmap -sS 172.30.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
Port
Protocol
State
Service
Version
22 tcp open ssh
135 tcp open msrpc
445 tcp open microsoft-ds
3389 tcp open ms-wbt-server
5901 tcp open vnc-1
Filter Hosts
10:37 PM
5/28/2021

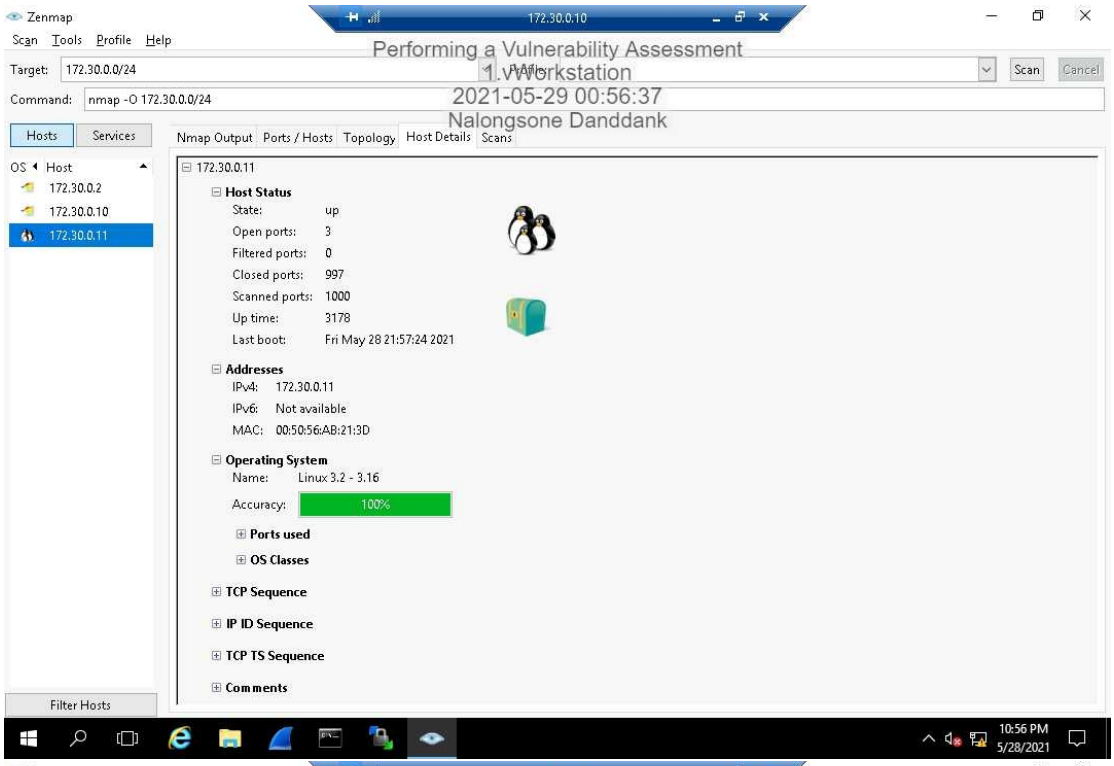

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:45:49
Nalongsone Danddank
Target: 172.30.0.0/24
Profile:
Scan
Cancel
Command: nmap -sS 172.30.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
Port
Protocol
State
Service
Version
22 tcp open ssh
111 tcp open rpcbind
3389 tcp open ms-wbt-server
Filter Hosts
10:45 PM
5/28/2021

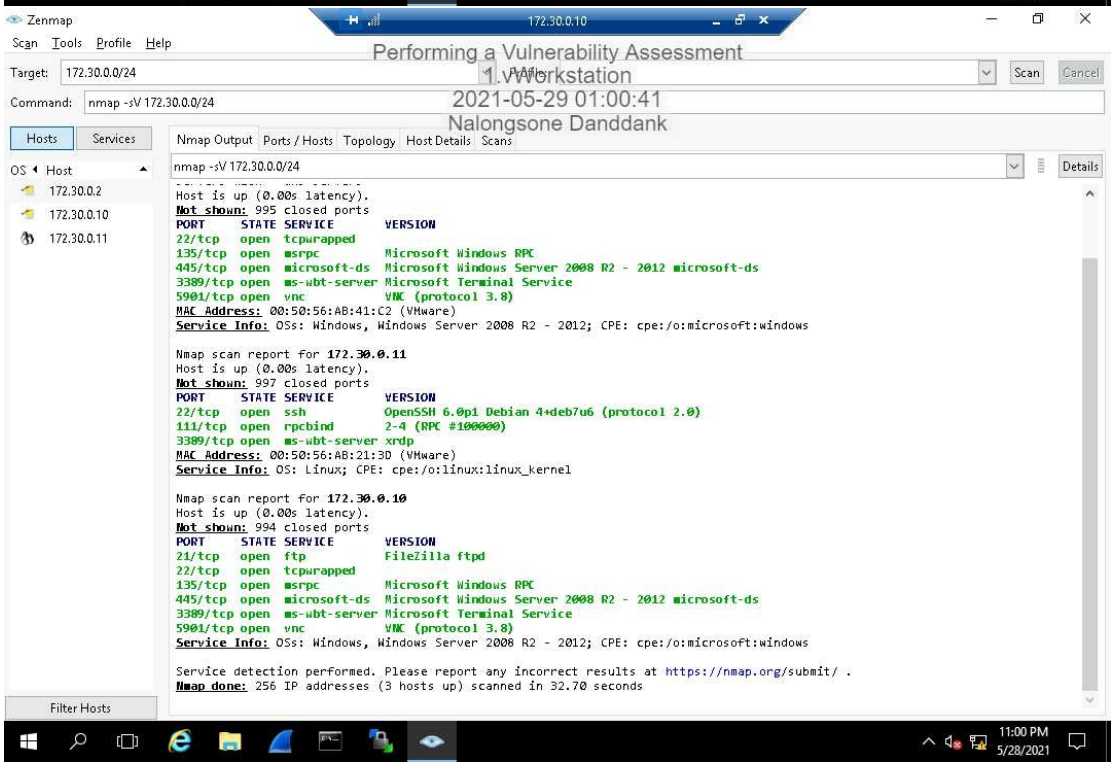

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:45:29
Nalongsone Danddank
Target: 172.30.0.0/24
Profile
Scan
Cancel
Command: nmap -sS 172.30.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
Port
Protocol
State
Service
Version
21 tcp open ftp
22 tcp open ssh
135 tcp open msrpc
445 tcp open microsoft-ds
3389 tcp open ms-wbt-server
5901 tcp open vnc-1
Filter Hosts
10:45 PM
5/28/2021

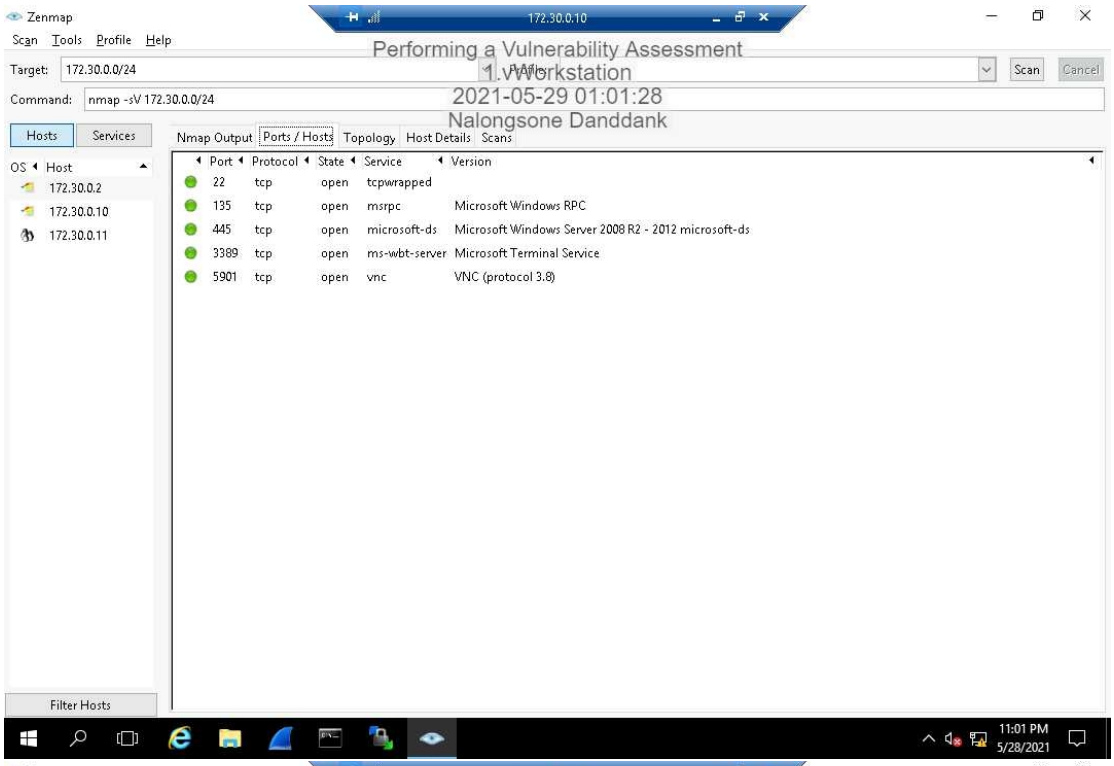

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:51:16
Nalongsone Danddank
Target: 172.30.0.0/24
Profile
Scan
Cancel
Command: nmap -O 172.30.0.0/24
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -O 172.30.0.0/24
Details
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
MAC Address: 00:50:56:AB:21:3D (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Nmap scan report for 172.30.0.10
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
135/tcp open msrpc
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
5901/tcp open vnc-1
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=5/28%OT=21%CT=1%CU=31311%PV=Y%DS=0%DC=L%G=Y%TM=60B1D62
OS:A%P=i686-pc-windows-windows)SEQ(SP=105%GCD=1%ISR=105%TI=I%CI=I%II=I%SS=S
OS:%TS=A)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O
OS:5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6
OS:=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%D
OS:F=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%
OS:W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=80%CD=Z)
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 26.05 seconds
Filter Hosts
10:51 PM
5/28/2021

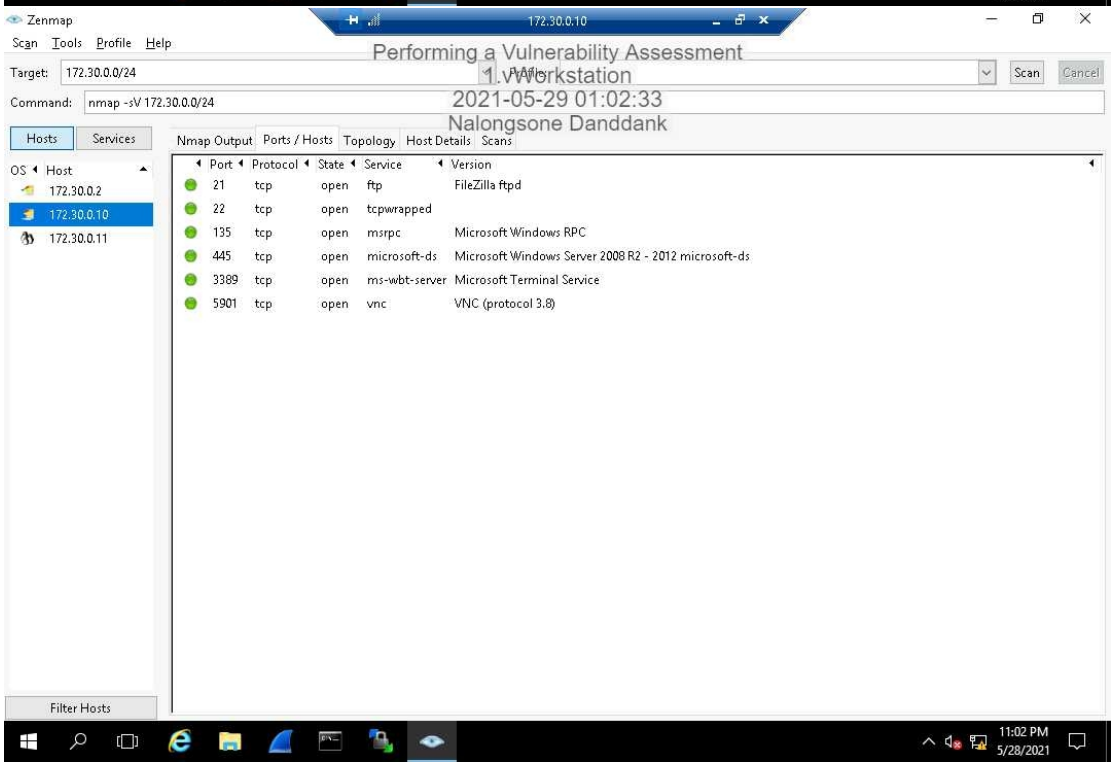

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:55:42
Nalongsone Danddank
Target: 172.30.0.0/24
Command: nmap -O 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
172.30.0.2
Host Status
State: up
Open ports: 5
Filtered ports: 0
Closed ports: 995
Scanned ports: 1000
Up time: 3495
Last boot: Fri May 28 21:52:07 2021
Addresses
IPv4: 172.30.0.2
IPv6: Not available
MAC: 00:50:56:AB:41:C2
Operating System
Name: Microsoft Windows Server 2016 build 10586
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts
10:55 PM
5/28/2021

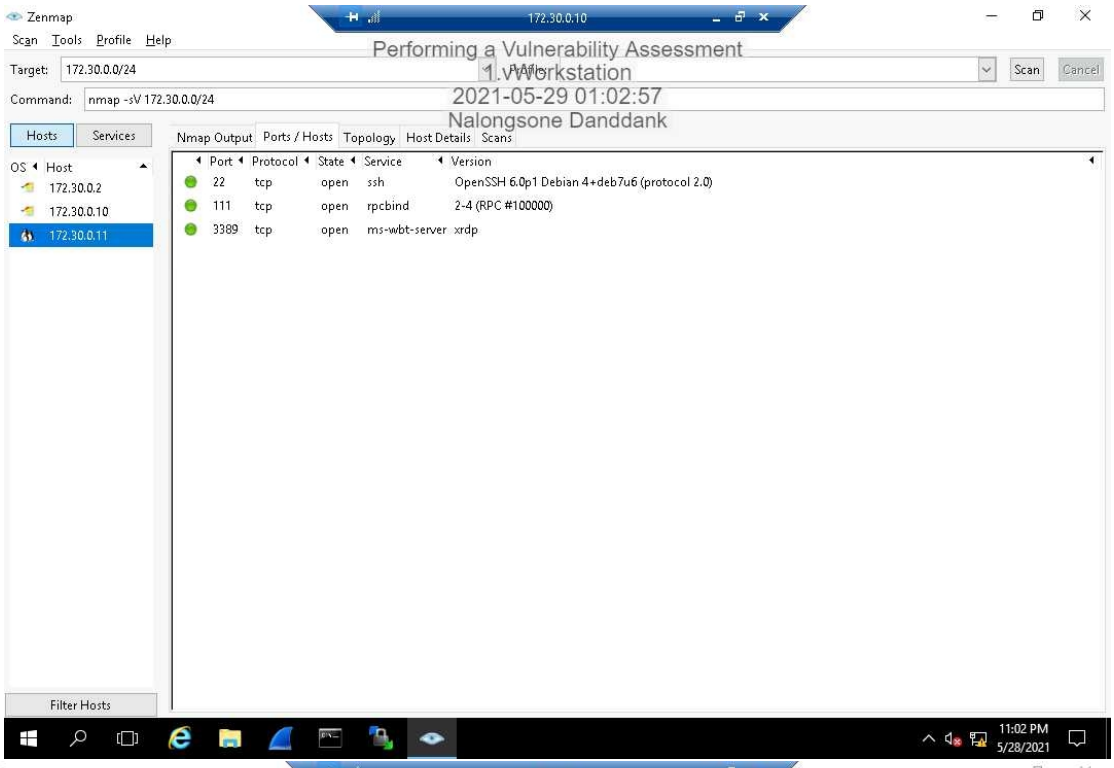

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 00:56:13
Nalongsone Danddank
Target: 172.30.0.0/24
Command: nmap -O 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
172.30.0.10
Host Status
State: up
Open ports: 6
Filtered ports: 0
Closed ports: 994
Scanned ports: 1000
Up time: 3495
Last boot: Fri May 28 21:52:19 2021
Addresses
IPv4: 172.30.0.10
IPv6: Not available
MAC: Not available
Operating System
Name: Microsoft Windows 10 1511
Accuracy: 97%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts
10:56 PM
5/28/2021

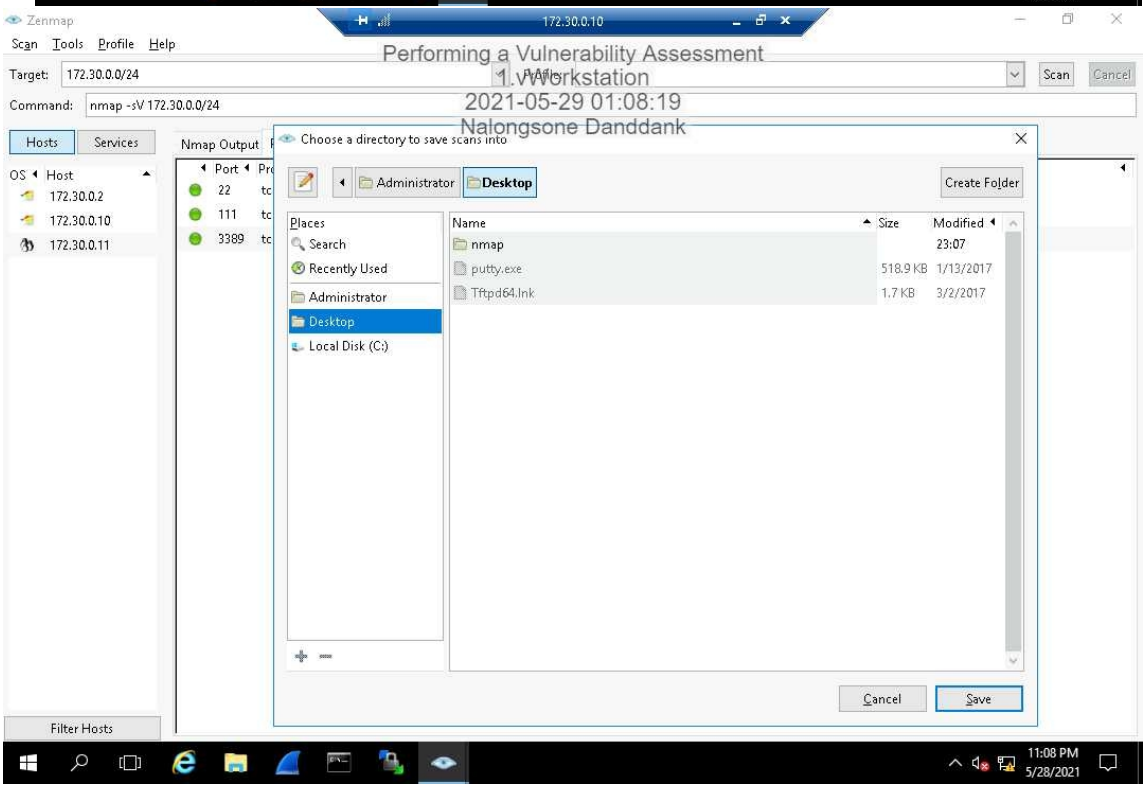

Zenmap
172.30.0.10
Performing a Vulnerability Assessment
1. vWorkstation
2021-05-29 00:56:37
Nalongsone Danddank
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -O 172.30.0.0/24
Scan
Cancel
Hosts
Services
OS Host
172.30.0.2
172.30.0.10
172.30.0.11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
172.30.0.11
Host Status
State: up
Open ports: 3
Filtered ports: 0
Closed ports: 997
Scanned ports: 1000
Up time: 3178
Last boot: Fri May 28 21:57:24 2021
Addresses
IPv4: 172.30.0.11
IPv6: Not available
MAC: 00:50:56:AB:21:3D
Operating System
Name: Linux 3.2 - 3.16
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts
10:56 PM
5/28/2021


Zenmap
172.30.0.10
Performing a Vulnerability Assessment
1. vWorkstation
2021-05-29 01:00:41
Nalongsone Danddank
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -sV 172.30.0.0/24
Scan
Cancel
Hosts
Services
OS Host
172.30.0.2
172.30.0.10
172.30.0.11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sV 172.30.0.0/24
Details
Host is up (0.00s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
22/tcp open tcpwrapped
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open ms-wbt-server Microsoft Terminal Service
5901/tcp open vnc VNC (protocol 3.8)
MAC Address: 00:50:56:AB:41:C2 (VMware)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Nmap scan report for 172.30.0.11
Host is up (0.00s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.0p1 Debian 4+deb7u6 (protocol 2.0)
111/tcp open rpcbind 2-4 (RPC #100000)
3389/tcp open ms-wbt-server xrdp
MAC Address: 00:50:56:AB:21:3D (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap scan report for 172.30.0.10
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp FileZilla ftpd
22/tcp open tcpwrapped
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open ms-wbt-server Microsoft Terminal Service
5901/tcp open vnc VNC (protocol 3.8)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 32.70 seconds
Filter Hosts
11:00 PM
5/28/2021

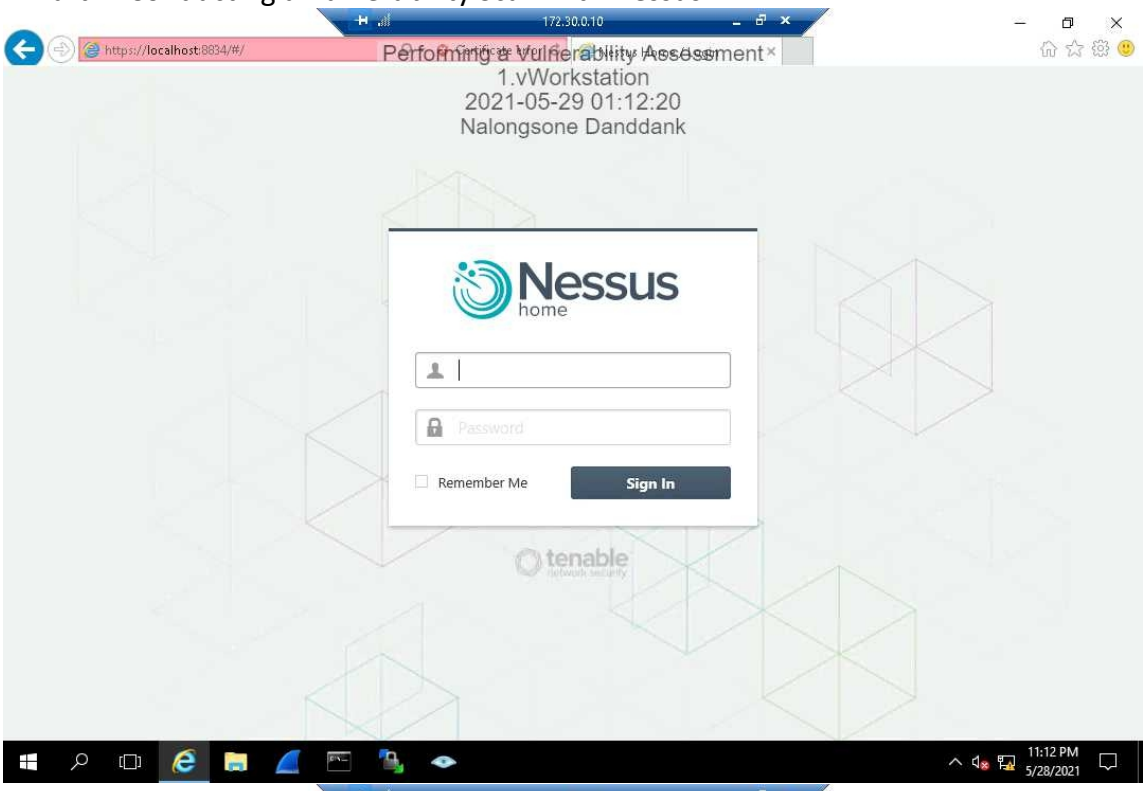

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1. vWorkstation
2021-05-29 01:01:28
Nalongsone Danddank
Target: 172.30.0.0/24
Command: nmap -sV 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
Port Protocol State Service Version
22 tcp open tcpwrapped
135 tcp open msrpc Microsoft Windows RPC
445 tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389 tcp open ms-wbt-server Microsoft Terminal Service
5901 tcp open vnc VNC (protocol 3.8)
Filter Hosts
11:01 PM
5/28/2021

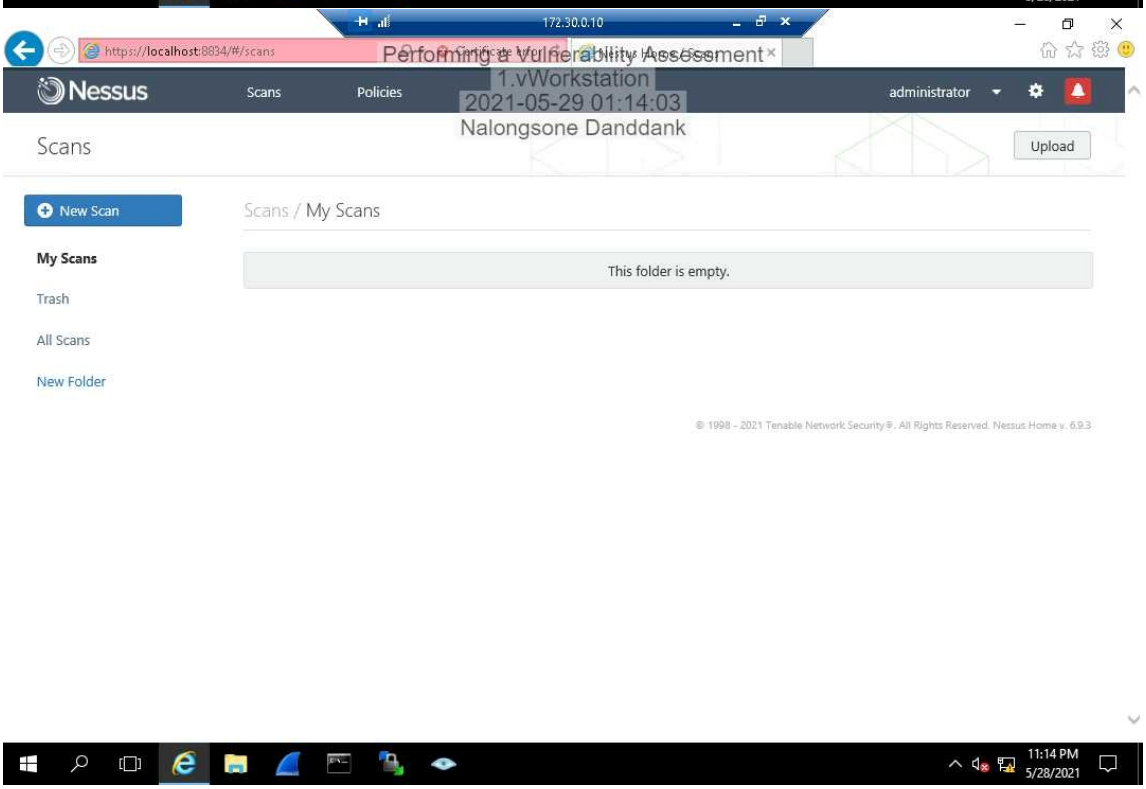

Zenmap
Scan Tools Profile Help
172.30.0.10
Performing a Vulnerability Assessment
1. vWorkstation
2021-05-29 01:02:33
Nalongsone Danddank
Target: 172.30.0.0/24
Command: nmap -sV 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.2
172.30.0.10
172.30.0.11
Port Protocol State Service Version
21 tcp open ftp FileZilla ftpd
22 tcp open tcpwrapped
135 tcp open msrpc Microsoft Windows RPC
445 tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389 tcp open ms-wbt-server Microsoft Terminal Service
5901 tcp open vnc VNC (protocol 3.8)
Filter Hosts
11:02 PM
5/28/2021

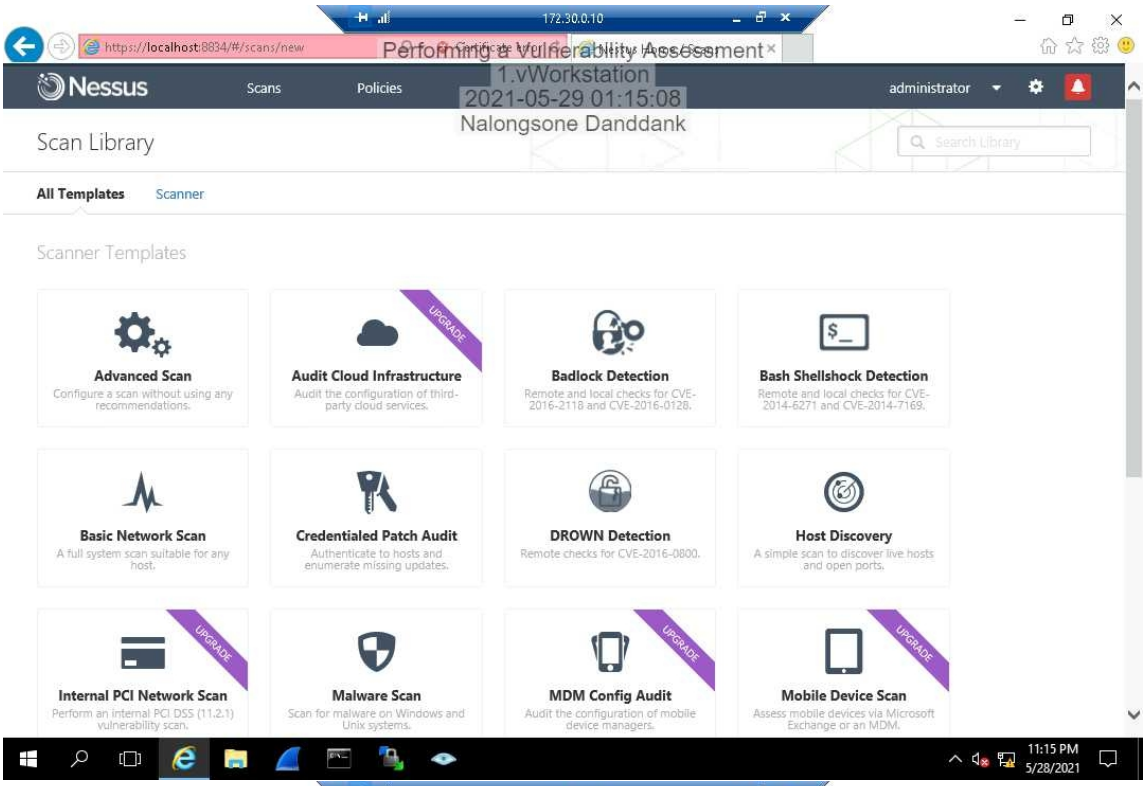

Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -sV 172.30.0.0/24
Scan
Cancel
Hosts
Services
OS Host
172.30.0.2
172.30.0.10
172.30.0.11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port Protocol State Service Version
22 tcp open ssh OpenSSH 6.0p1 Debian 4+deb7u6 (protocol 2.0)
111 tcp open rpcbind 2-4 (RPC #100000)
3389 tcp open ms-wbt-server xrdp
Filter Hosts
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:02:57
Nalongsone Danddank
11:02 PM
5/28/2021

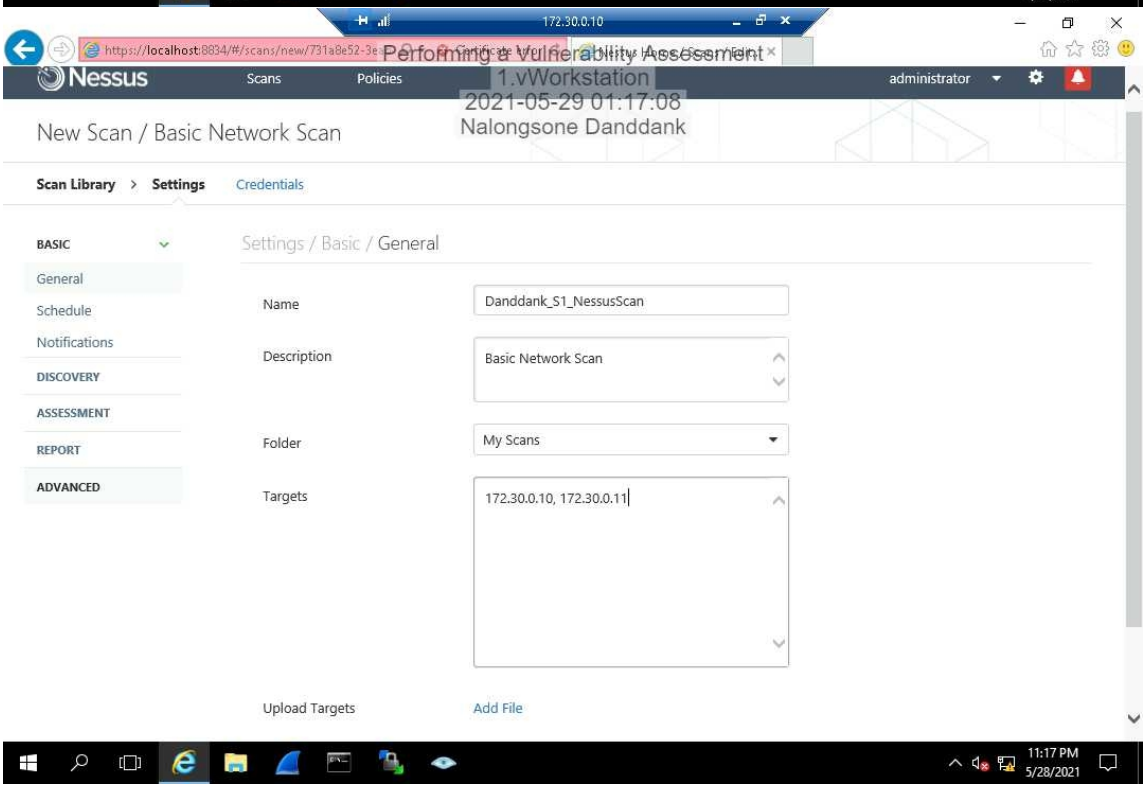

Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -sV 172.30.0.0/24
Scan
Cancel
Hosts
Services
OS Host
172.30.0.2
172.30.0.10
172.30.0.11
Nmap Output
Filter Hosts
Choose a directory to save scans into
Administrator
Desktop
Create Folder
Places
Search
Recently Used
Administrator
Desktop
Local Disk (C:)
Name
Size
Modified
nmap
23:07
putty.exe
518.9 KB
1/13/2017
Tftpd64.lnk
1.7 KB
3/2/2017
Cancel
Save
172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:08:19
Nalongsone Danddank
11:08 PM
5/28/2021

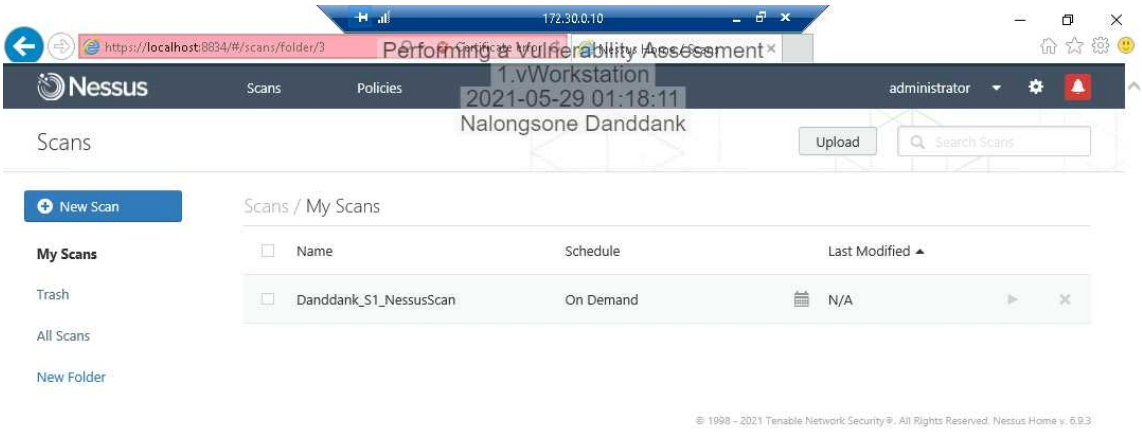
Part 2: Conducting a Vulnerability Scan with Nessus

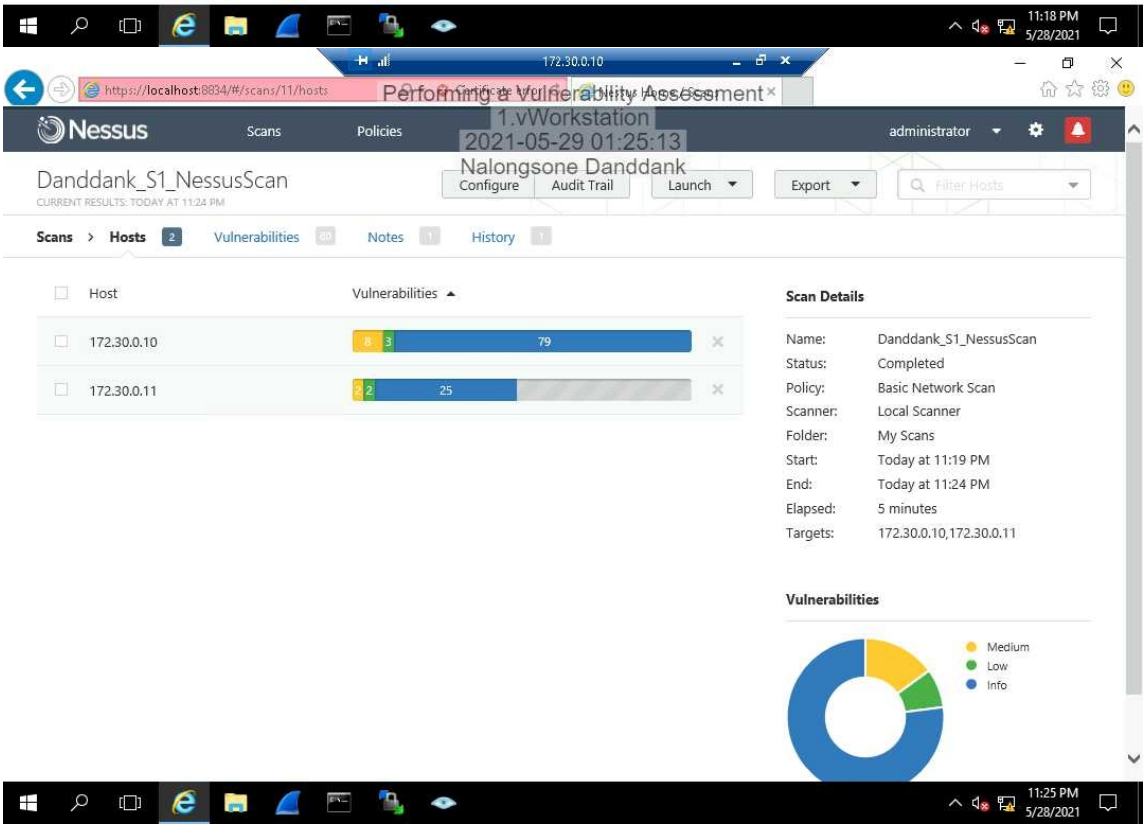


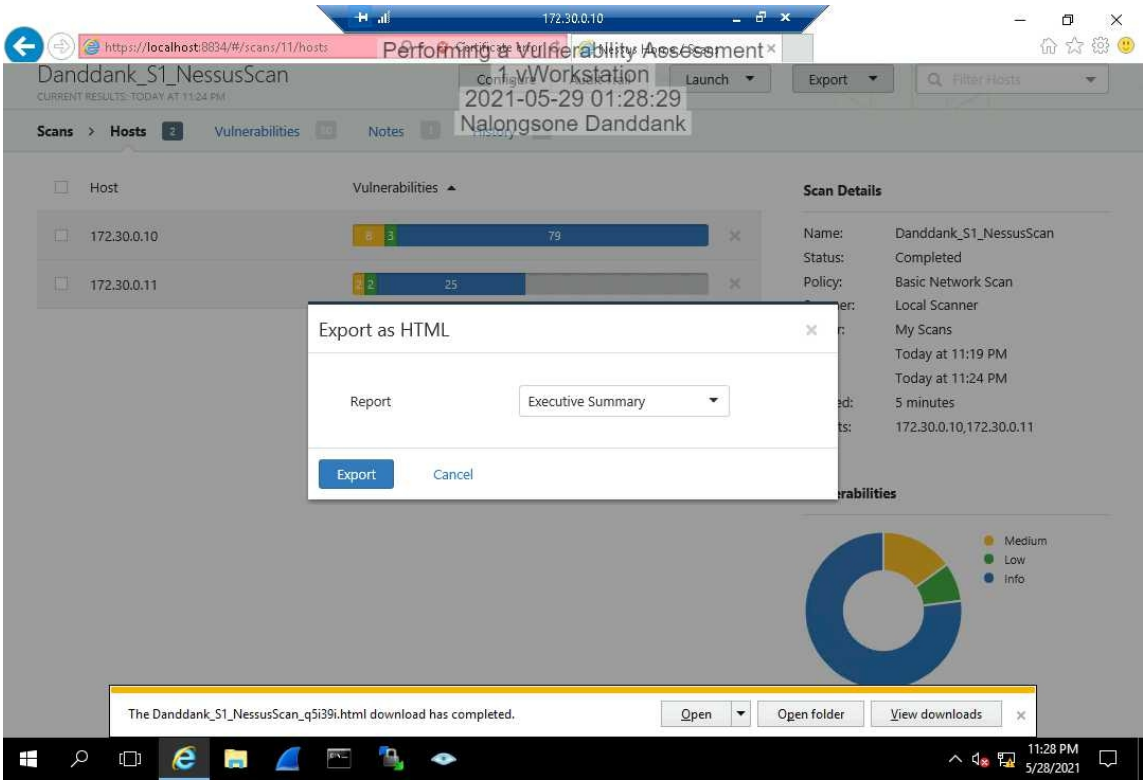



172.30.0.10
https://localhost:8834/#/scans/new
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:15:08
Nalongsone Danddank
Nessus
Scans
Policies
administrator
Scan Library
All Templates
Scanner
Scanner Templates
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
UPGRADE
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
Audit the configuration of mobile device managers.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
11:15 PM
5/28/2021

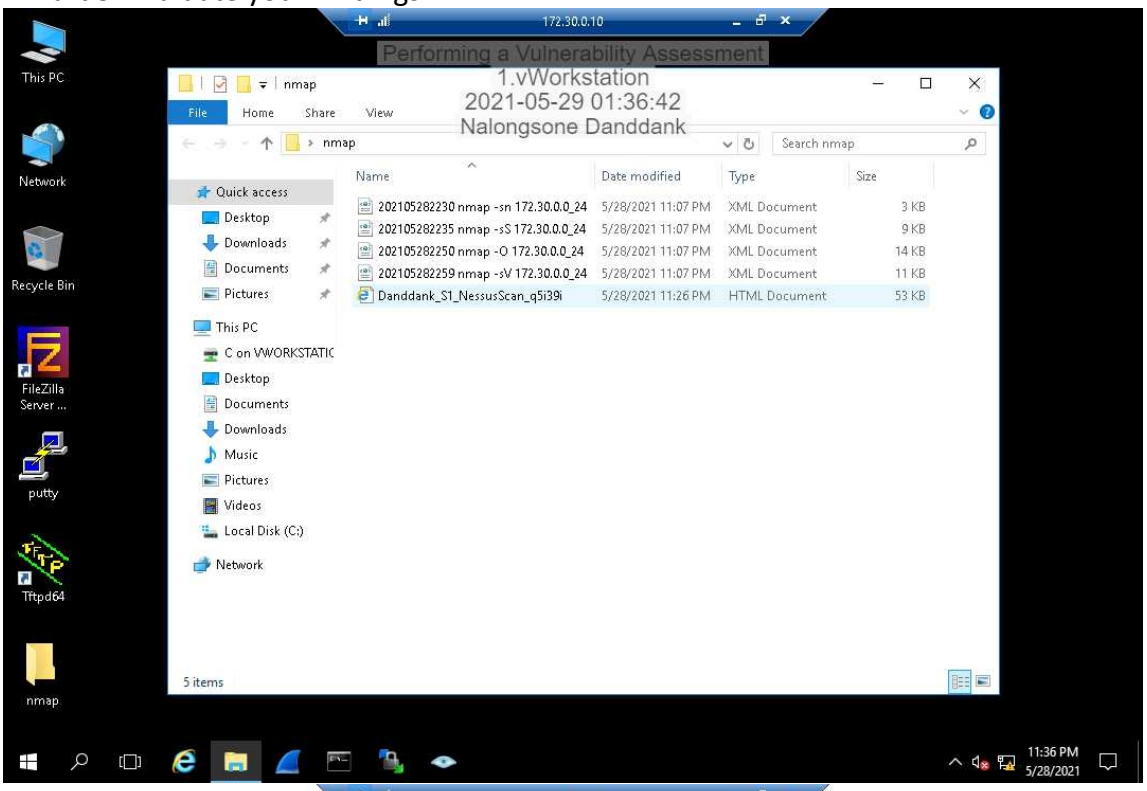

172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:17:08
Nalongsone Danddank
Nessus
Scans
Policies
administrator
New Scan / Basic Network Scan
Scan Library
Settings
Credentials
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Settings / Basic / General
Name
Danddank_S1_NessusScan
Description
Basic Network Scan
Folder
My Scans
Targets
172.30.0.10, 172.30.0.11
Upload Targets
Add File
11:17 PM
5/28/2021

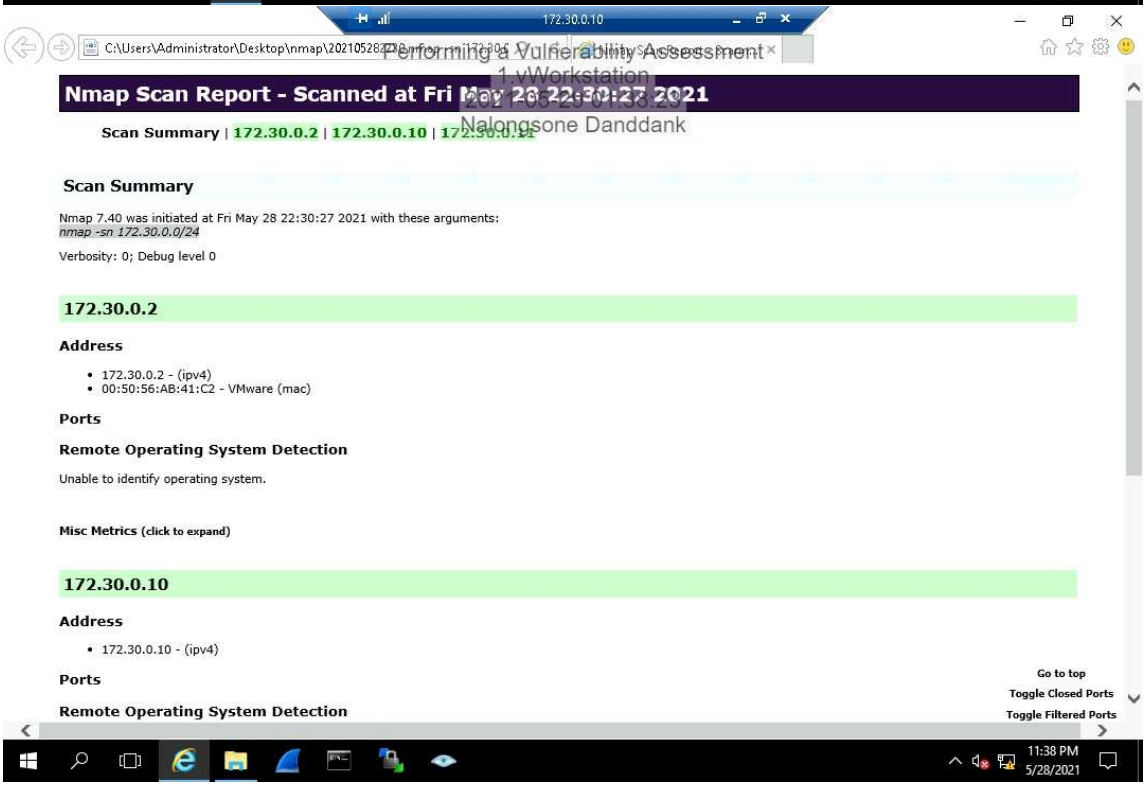

172.30.0.10
https://localhost:8834/#/scans/folder/3
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:18:11
Nalongsone Danddank
Nessus
Scans
Policies
administrator
Scans
Upload
Search Scans
New Scan
Scans / My Scans
My Scans
Trash
All Scans
New Folder
Name
Schedule
Last Modified
Danddank_S1_NessusScan
On Demand
N/A
© 1998 - 2021 Tenable Network Security®. All Rights Reserved. Nessus Home v. 8.9.3

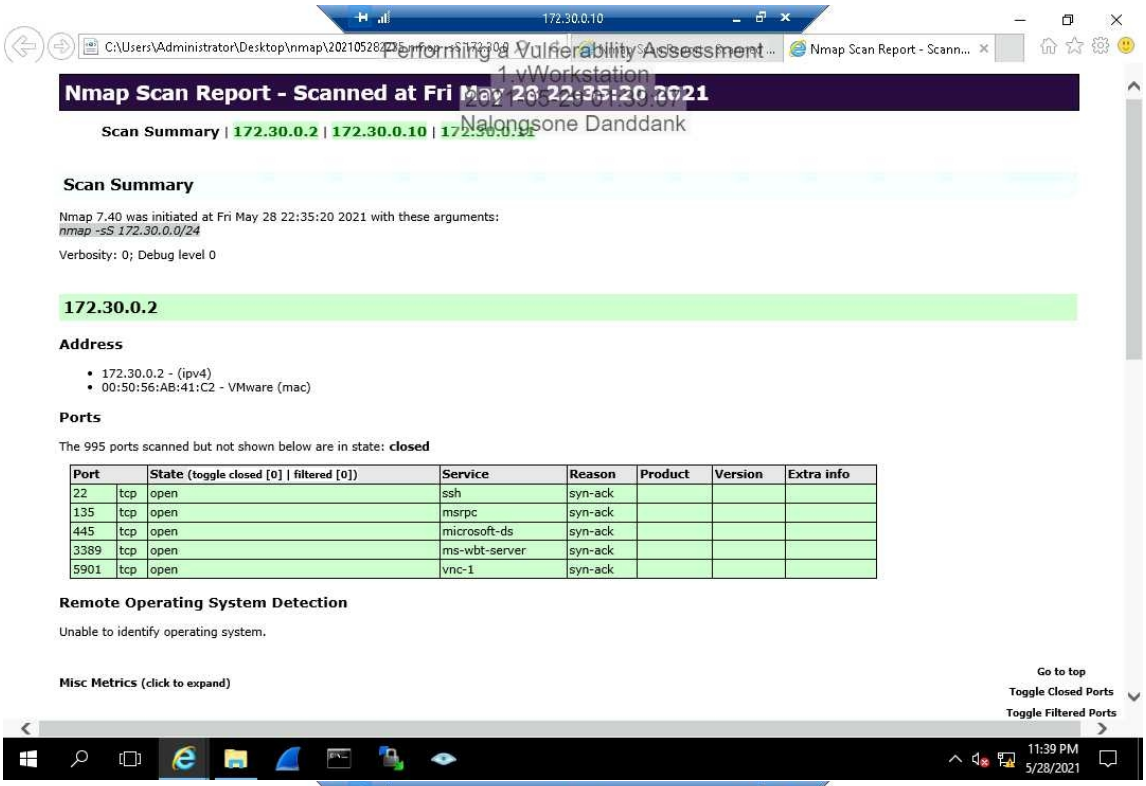

172.30.0.10
https://localhost:8834/#/scans/11/hosts
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:25:13
Nalongsone Danddank
Nessus
Scans
Policies
administrator
Danddank_S1_NessusScan
CURRENT RESULTS: TODAY AT 11:24 PM
Configure
Audit Trail
Launch
Export
Filter Hosts
Scans
Hosts 2
Vulnerabilities 88
Notes 1
History 1
Host
Vulnerabilities
172.30.0.10
8 3 79
172.30.0.11
2 25
Scan Details
Name: Danddank_S1_NessusScan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Folder: My Scans
Start: Today at 11:19 PM
End: Today at 11:24 PM
Elapsed: 5 minutes
Targets: 172.30.0.10,172.30.0.11
Vulnerabilities
Medium
Low
Info

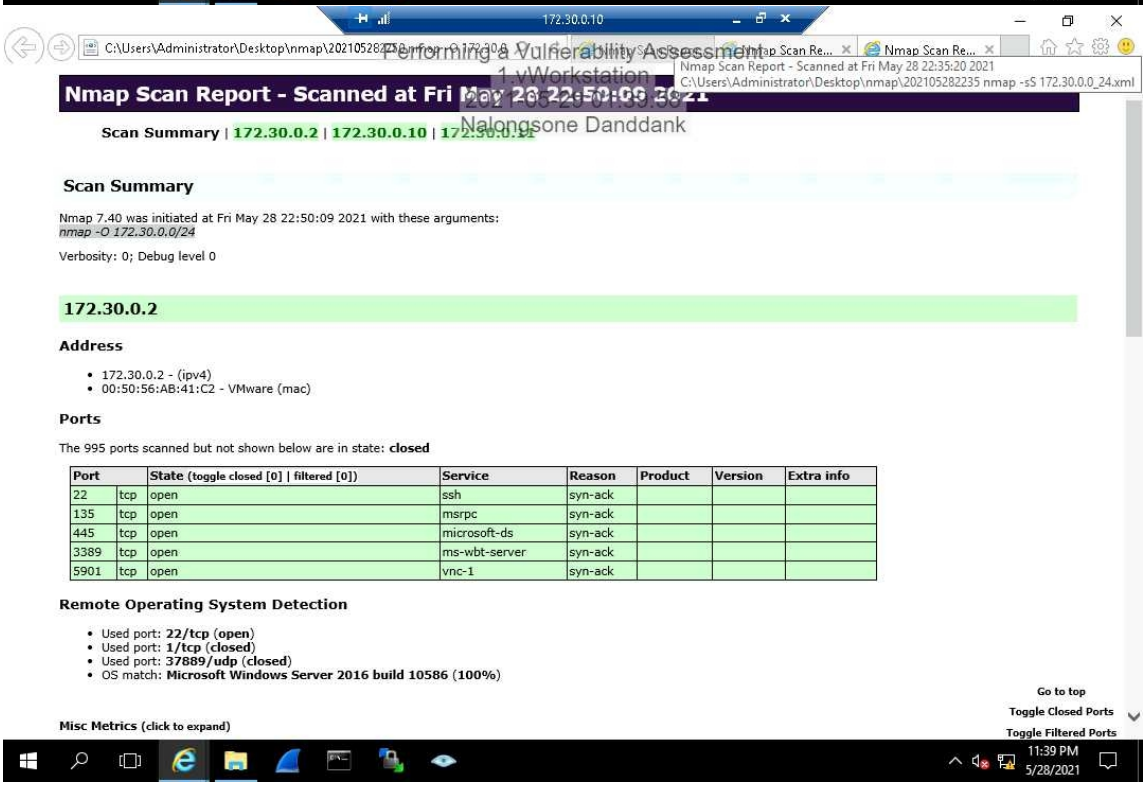

172.30.0.10
https://localhost:8834/#/scans/11/hosts
Performing a Vulnerability Assessment
Danddank_S1_NessusScan
CURRENT RESULTS: TODAY AT 11:24 PM
Launch
Export
2021-05-29 01:28:29
Nalongsone Danddank
Scans > Hosts 2 Vulnerabilities 10 Notes 1
Host
Vulnerabilities
172.30.0.10
172.30.0.11
Scan Details
Name: Danddank_S1_NessusScan
Status: Completed
Policy: Basic Network Scan
Local Scanner
My Scans
Today at 11:19 PM
Today at 11:24 PM
5 minutes
172.30.0.10,172.30.0.11
Export as HTML
Report
Executive Summary
Export
Cancel
Medium
Low
Info
The Danddank_S1_NessusScan_q5i39i.html download has completed.
Open
Open folder
View downloads
11:28 PM
5/28/2021

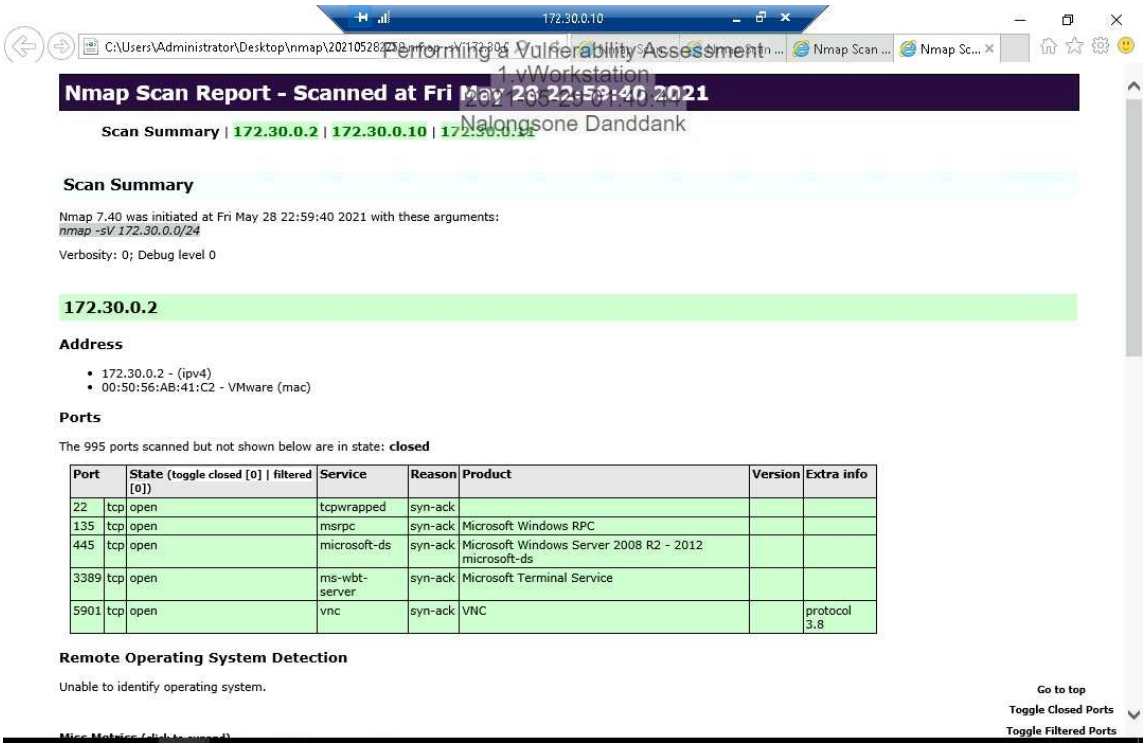
Part 3: Evaluate your Findings.



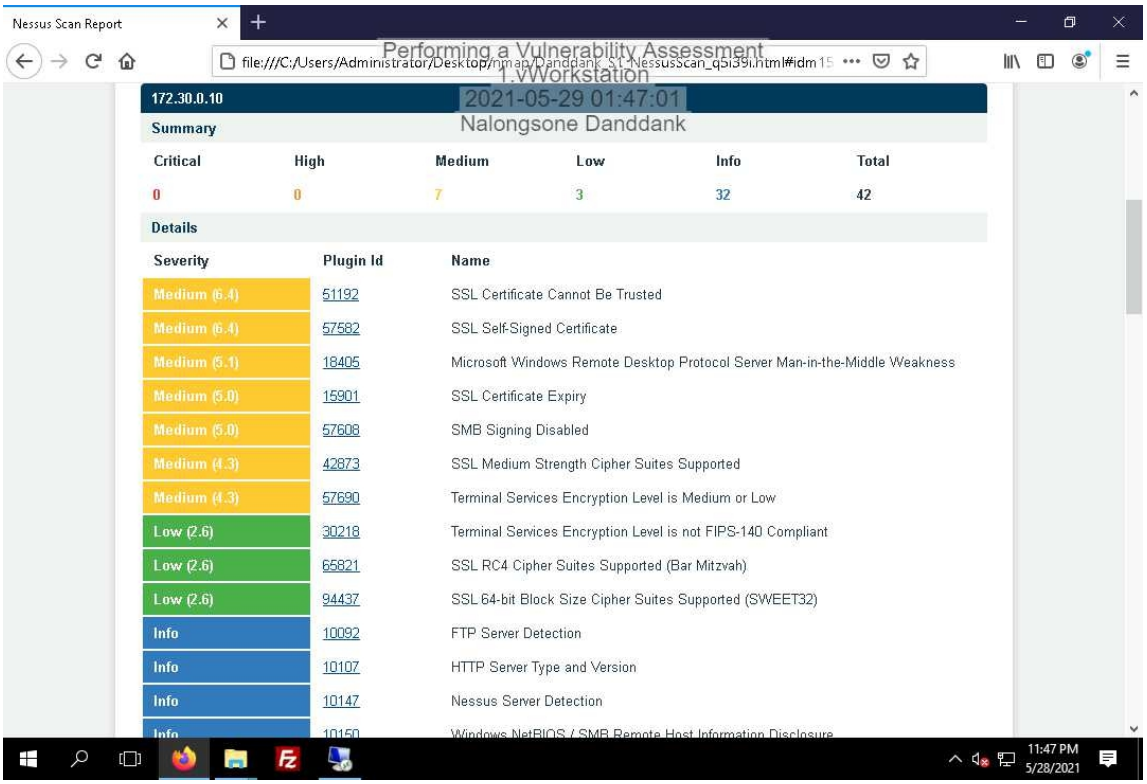


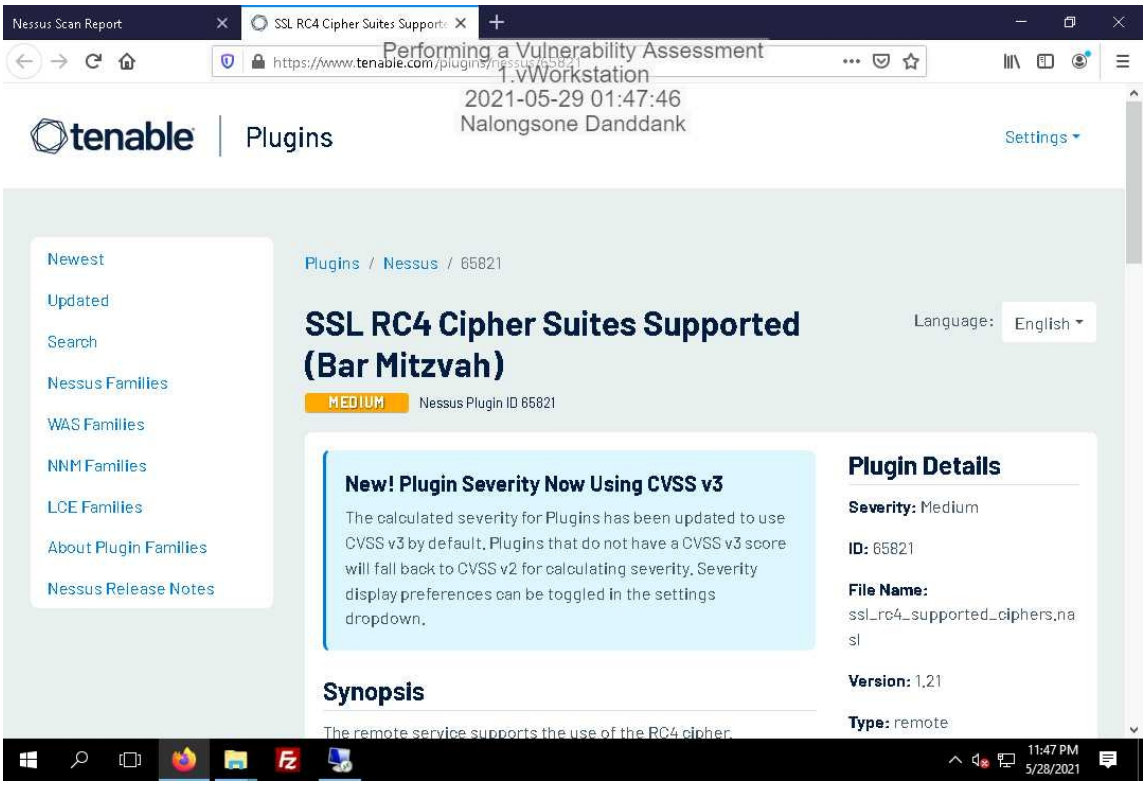

172.30.0.10
Performing a Vulnerability Assessment
1 vWorkstation
Nalongsone Danddank
Nmap Scan Report - Scann...
Nmap Scan Report - Scanned at Fri May 28 22:35:20 2021
Scan Summary | 172.30.0.2 | 172.30.0.10 |
Scan Summary
Nmap 7.40 was initiated at Fri May 28 22:35:20 2021 with these arguments:
nmap -sS 172.30.0.0/24
Verbosity: 0; Debug level 0
172.30.0.2
Address
172.30.0.2 - (ipv4)
00:50:56:AB:41:C2 - VMware (mac)
Ports
The 995 ports scanned but not shown below are in state: closed
Port | State (toggle closed [0] | filtered [0]) | Service | Reason | Product | Version | Extra info
22 tcp open ssh syn-ack
135 tcp open msrpc syn-ack
445 tcp open microsoft-ds syn-ack
3389 tcp open ms-wbt-server syn-ack
5901 tcp open vnc-1 syn-ack
Remote Operating System Detection
Unable to identify operating system.
Misc Metrics (click to expand)
Go to top
Toggle Closed Ports
Toggle Filtered Ports
11:39 PM
5/28/2021

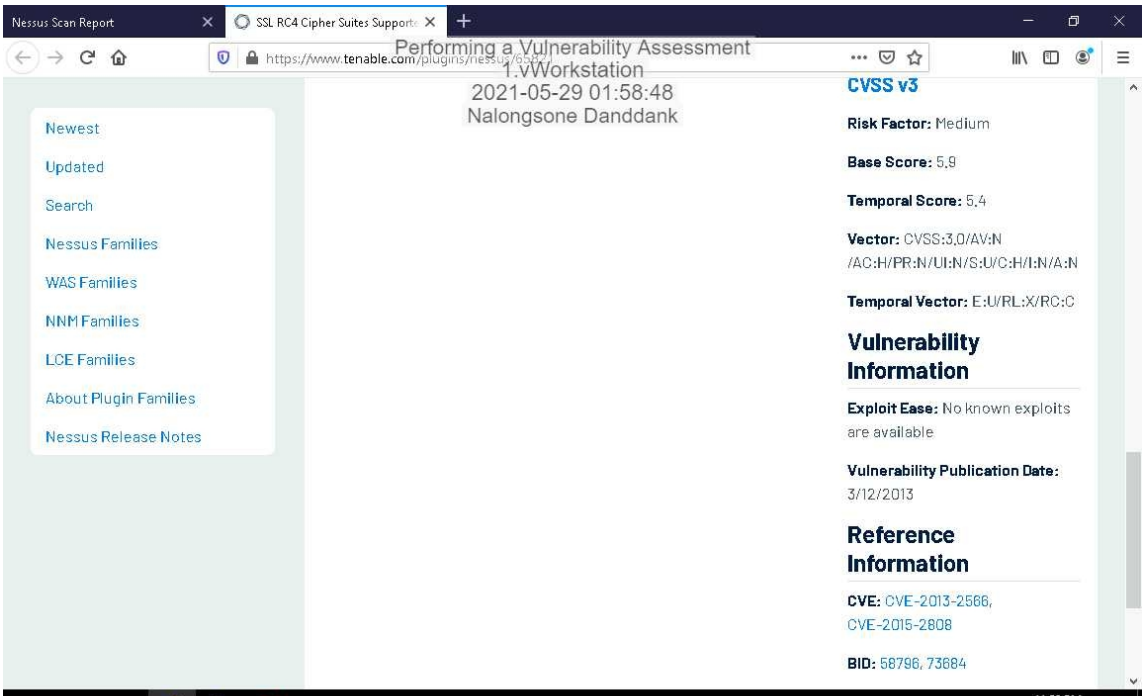

172.30.0.10
Performing a Vulnerability Assessment
1 vWorkstation
Nalongsone Danddank
Nmap Scan Re...
Nmap Scan Report - Scanned at Fri May 28 22:35:20 2021
C:\Users\Administrator\Desktop\nmap\202105282235 nmap -sS 172.30.0.0_24.xml
Nmap Scan Report - Scanned at Fri May 28 22:50:09 2021
Scan Summary | 172.30.0.2 | 172.30.0.10 |
Scan Summary
Nmap 7.40 was initiated at Fri May 28 22:50:09 2021 with these arguments:
nmap -O 172.30.0.0/24
Verbosity: 0; Debug level 0
172.30.0.2
Address
172.30.0.2 - (ipv4)
00:50:56:AB:41:C2 - VMware (mac)
Ports
The 995 ports scanned but not shown below are in state: closed
Port | State (toggle closed [0] | filtered [0]) | Service | Reason | Product | Version | Extra info
22 tcp open ssh syn-ack
135 tcp open msrpc syn-ack
445 tcp open microsoft-ds syn-ack
3389 tcp open ms-wbt-server syn-ack
5901 tcp open vnc-1 syn-ack
Remote Operating System Detection
Used port: 22/tcp (open)
Used port: 1/tcp (closed)
Used port: 37889/udp (closed)
OS match: Microsoft Windows Server 2016 build 10586 (100%)
Misc Metrics (click to expand)
Go to top
Toggle Closed Ports
Toggle Filtered Ports
11:39 PM
5/28/2021

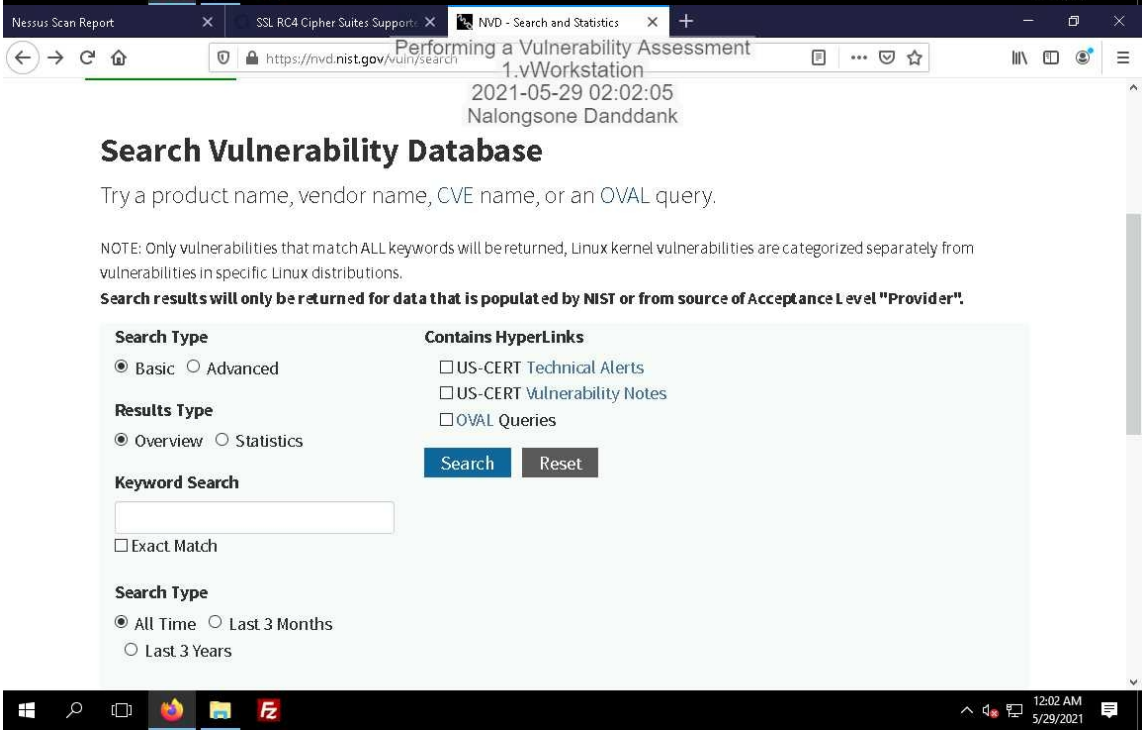

172.30.0.10
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:40:44
Nalongsone Danddank
Nmap Scan Report - Scanned at Fri May 28 22:59:40 2021
Scan Summary | 172.30.0.2 | 172.30.0.10 | 172.30.0.11
Scan Summary
Nmap 7.40 was initiated at Fri May 28 22:59:40 2021 with these arguments:
nmap -sV 172.30.0.0/24
Verbosity: 0; Debug level 0
172.30.0.2
Address
172.30.0.2 - (ipv4)
00:50:56:AB:41:C2 - VMware (mac)
Ports
The 995 ports scanned but not shown below are in state: closed
Port | State (toggle closed [0] | filtered [0]) | Service | Reason | Product | Version | Extra info
22 tcp open tcpwrapped syn-ack
135 tcp open msrpc syn-ack Microsoft Windows RPC
445 tcp open microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389 tcp open ms-wbt-server syn-ack Microsoft Terminal Service
5901 tcp open vnc syn-ack VNC protocol 3.8
Remote Operating System Detection
Unable to identify operating system.
Go to top
Toggle Closed Ports
Toggle Filtered Ports
11:40 PM
5/28/2021

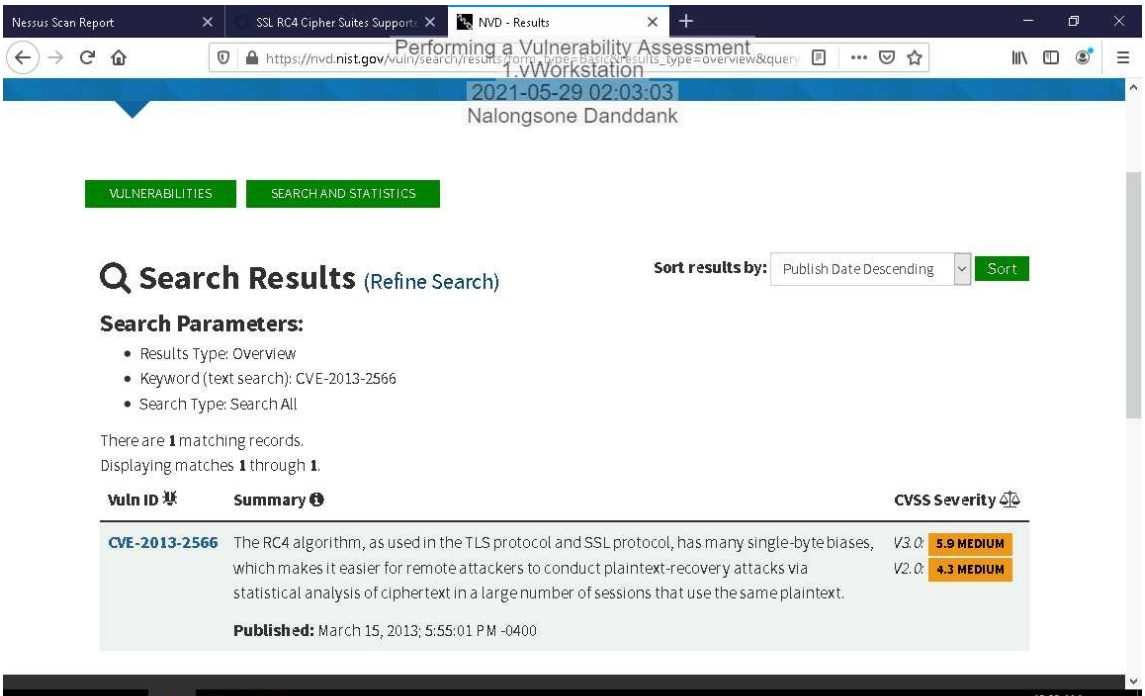

Nessus Scan Report
file:///C:/Users/Administrator/Desktop/nmap/Danddank_CT-Nessusscan_q5i39i.html
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:45:52
Nalongsone Danddank
Nessus
vulnerability scanner
Nessus Scan Report
Fri, 28 May 2021 23:19:11 Pacific Standard Time
Table Of Contents
Hosts Summary (Executive)
172.30.0.10
172.30.0.11
Hosts Summary (Executive)
[-] Collapse All
[+] Expand All
172.30.0.10
Summary
Critical High Medium Low Info Total
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share
11:45 PM
5/28/2021

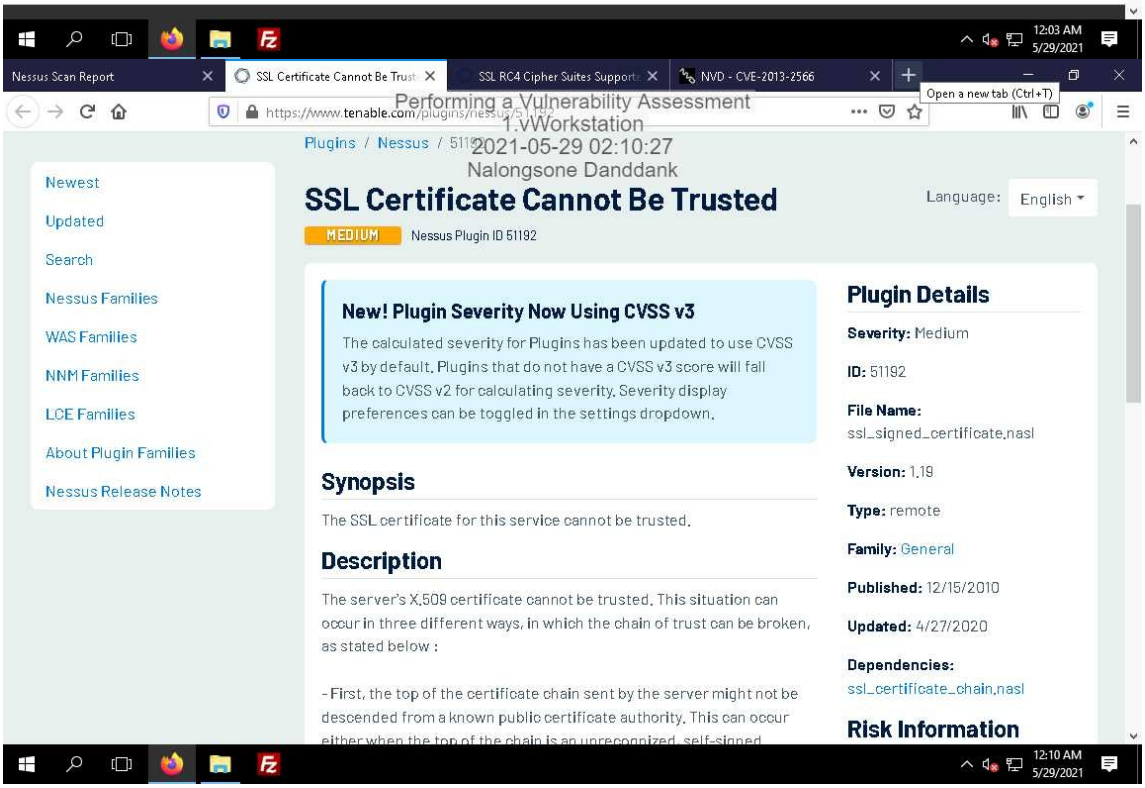

Nessus Scan Report
file:///C:/Users/Administrator/Desktop/nmap/Danddank_S1_NessusScan_q5i39i.html#idm15
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:47:01
Nalongsone Danddank
172.30.0.10
Summary
Critical High Medium Low Info Total
0 0 7 3 32 42
Details
Severity Plugin Id Name
Medium (6.4) 51192 SSL Certificate Cannot Be Trusted
Medium (6.4) 57582 SSL Self-Signed Certificate
Medium (5.1) 18405 Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0) 15901 SSL Certificate Expiry
Medium (5.0) 57608 SMB Signing Disabled
Medium (4.3) 42873 SSL Medium Strength Cipher Suites Supported
Medium (4.3) 57690 Terminal Services Encryption Level is Medium or Low
Low (2.6) 30218 Terminal Services Encryption Level is not FIPS-140 Compliant
Low (2.6) 65821 SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6) 94437 SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Info 10092 FTP Server Detection
Info 10107 HTTP Server Type and Version
Info 10147 Nessus Server Detection
Info 10150 Windows NetBIOS / SMB Remote Host Information Disclosure
11:47 PM
5/28/2021

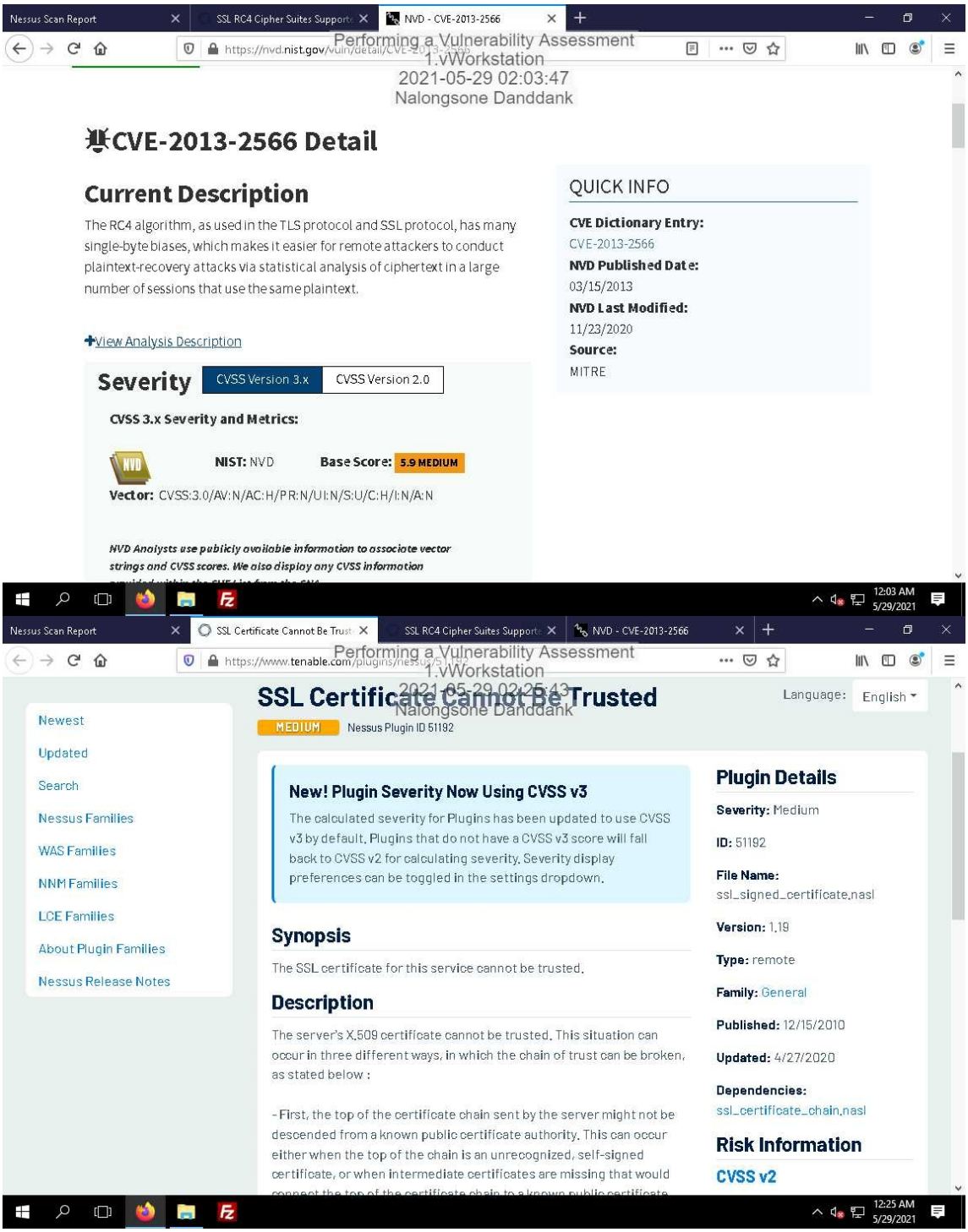

Nessus Scan Report
SSL RC4 Cipher Suites Support
https://www.tenable.com/plugins/nessus/65821
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:47:46
Nalongsone Danddank
tenable | Plugins
Settings
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
Plugins / Nessus / 65821
SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Language: English
MEDIUM
Nessus Plugin ID 65821
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Plugin Details
Severity: Medium
ID: 65821
File Name: ssl_rc4_supported_ciphers.nasl
Version: 1.21
Type: remote
Synopsis
The remote service supports the use of the RC4 cipher
11:47 PM
5/28/2021


Nessus Scan Report
SSL RC4 Cipher Suites Support
https://www.tenable.com/plugins/nessus/65821
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 01:58:48
Nalongsone Danddank
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
CVSS v3
Risk Factor: Medium
Base Score: 5.9
Temporal Score: 5.4
Vector: CVSS:3.0/AV:N /AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
Temporal Vector: E:U/RL:X/RC:C
Vulnerability Information
Exploit Ease: No known exploits are available
Vulnerability Publication Date: 3/12/2013
Reference Information
CVE: CVE-2013-2566, CVE-2015-2808
BID: 58796, 73684
11:58 PM
5/28/2021

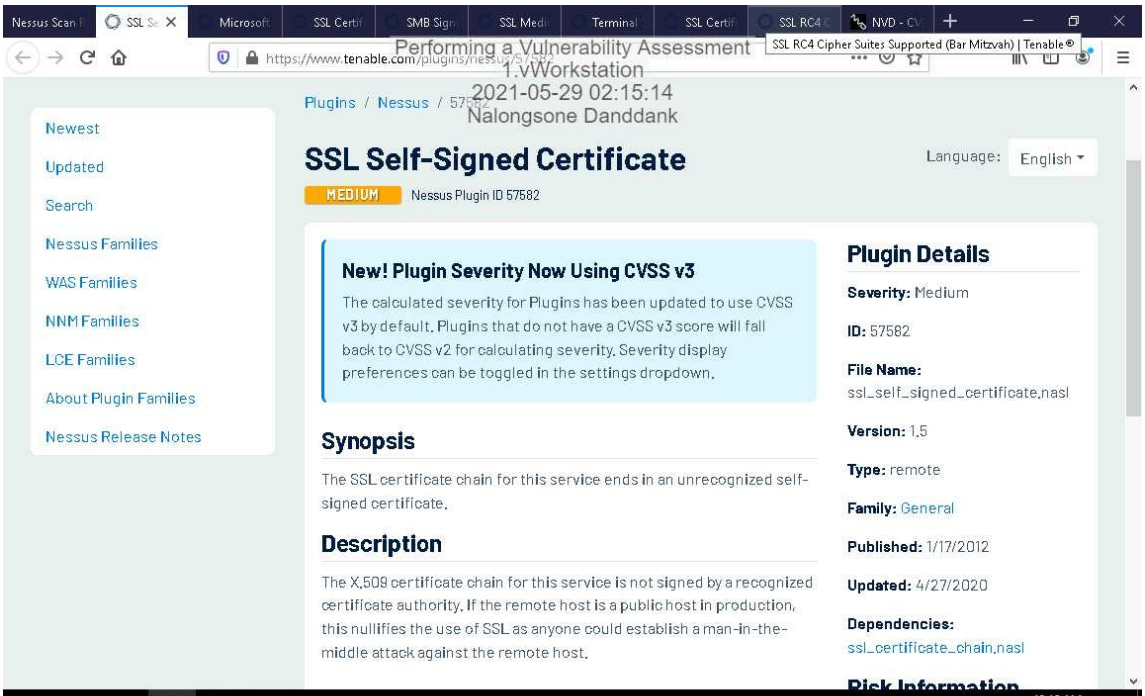

Nessus Scan Report
SSL RC4 Cipher Suites Support
NVD - Search and Statistics
https://nvd.nist.gov/vuln/search
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:02:05
Nalongsone Danddank
Search Vulnerability Database
Try a product name, vendor name, CVE name, or an OVAL query.
NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.
Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".
Search Type
Basic Advanced
Results Type
Overview Statistics
Keyword Search
Exact Match
Search Type
All Time Last 3 Months
Last 3 Years
Contains HyperLinks
US-CERT Technical Alerts
US-CERT Vulnerability Notes
OVAL Queries
Search
Reset
12:02 AM
5/29/2021

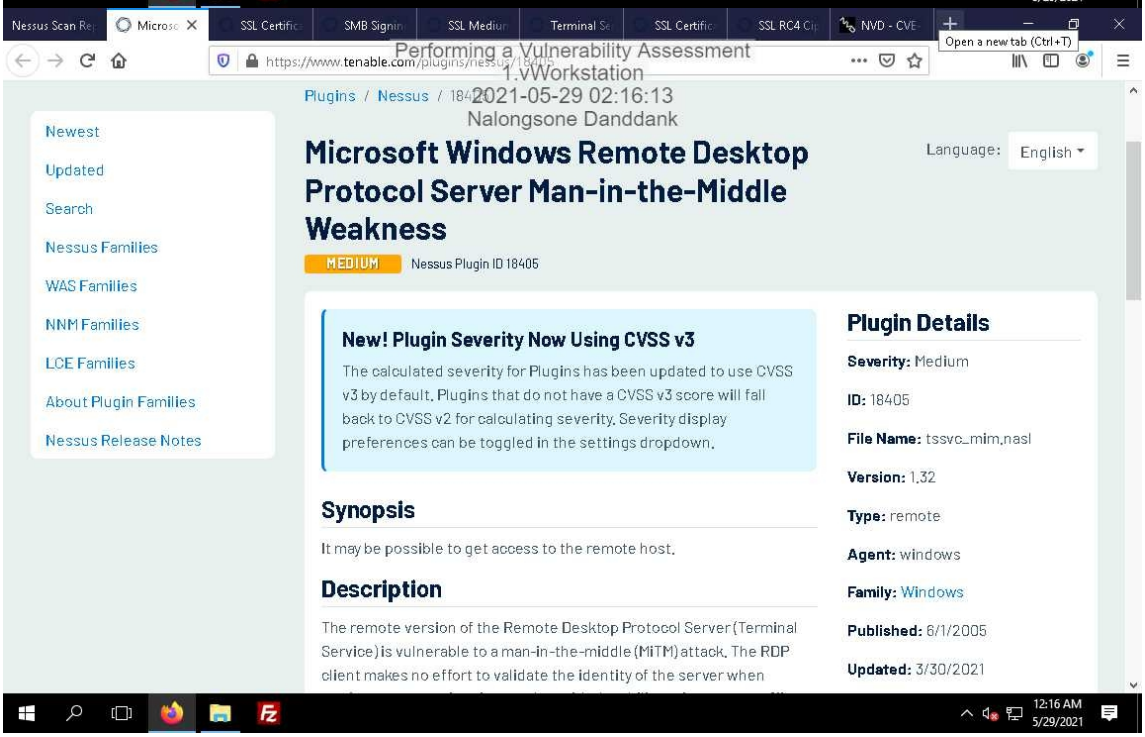

Nessus Scan Report
SSL RC4 Cipher Suites Support
NVD - Results
https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:03:03
Nalongsone Danddank
VULNERABILITIES
SEARCH AND STATISTICS
Search Results (Refine Search)
Sort results by: Publish Date Descending
Sort
Search Parameters:
Results Type: Overview
Keyword (text search): CVE-2013-2566
Search Type: Search All
There are 1 matching records.
Displaying matches 1 through 1.
Vuln ID
Summary
CVSS Severity
CVE-2013-2566
The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.
V3.0: 5.9 MEDIUM
V2.0: 4.3 MEDIUM
Published: March 15, 2013; 5:55:01 PM -0400

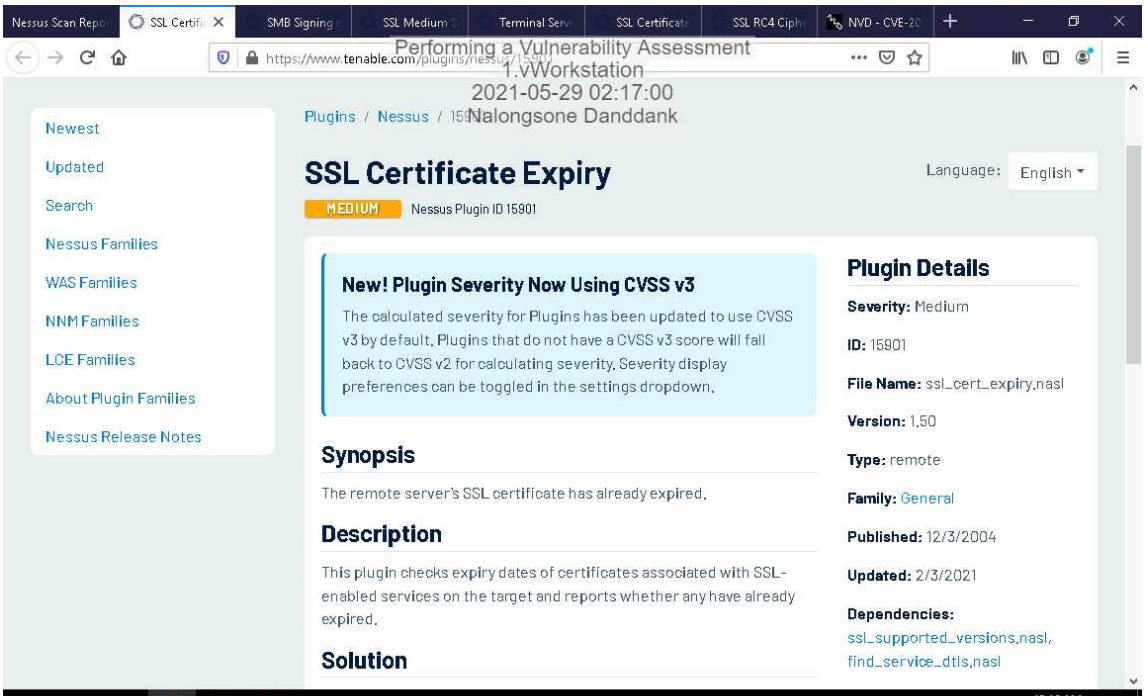

12:03 AM
5/29/2021
Nessus Scan Report
SSL Certificate Cannot Be Trust
SSL RC4 Cipher Suites Support
NVD - CVE-2013-2566
Open a new tab (Ctrl+T)
https://www.tenable.com/plugins/nessus/51192
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:10:27
Nalongsone Danddank
Plugins / Nessus / 51192
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
SSL Certificate Cannot Be Trusted
Language: English
MEDIUM
Nessus Plugin ID 51192
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
The SSL certificate for this service cannot be trusted.
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed
Plugin Details
Severity: Medium
ID: 51192
File Name: ssl_signed_certificate.nasl
Version: 1.19
Type: remote
Family: General
Published: 12/15/2010
Updated: 4/27/2020
Dependencies: ssl_certificate_chain.nasl
Risk Information
12:10 AM
5/29/2021

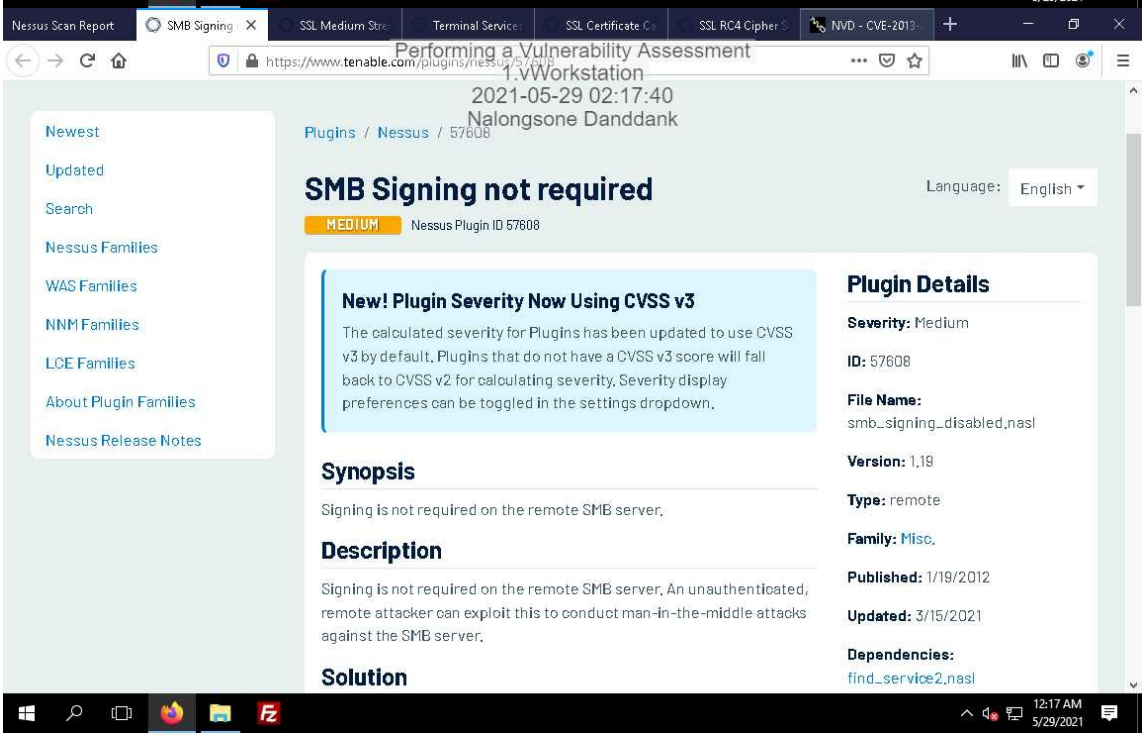

Nessus Scan Report
SSL RC4 Cipher Suites Support
NVD - CVE-2013-2566
https://nvd.nist.gov/vuln/detail/CVE-2013-2566
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:03:47
Nalongsone Danddank
CVE-2013-2566 Detail
Current Description
The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.
View Analysis Description
QUICK INFO
CVE Dictionary Entry:
CVE-2013-2566
NVD Published Date:
03/15/2013
NVD Last Modified:
11/23/2020
Source:
MITRE
Severity
CVSS Version 3.x
CVSS Version 2.0
CVSS 3.x Severity and Metrics:
NIST: NVD
Base Score: 5.9 MEDIUM
Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information
12:03 AM
5/29/2021

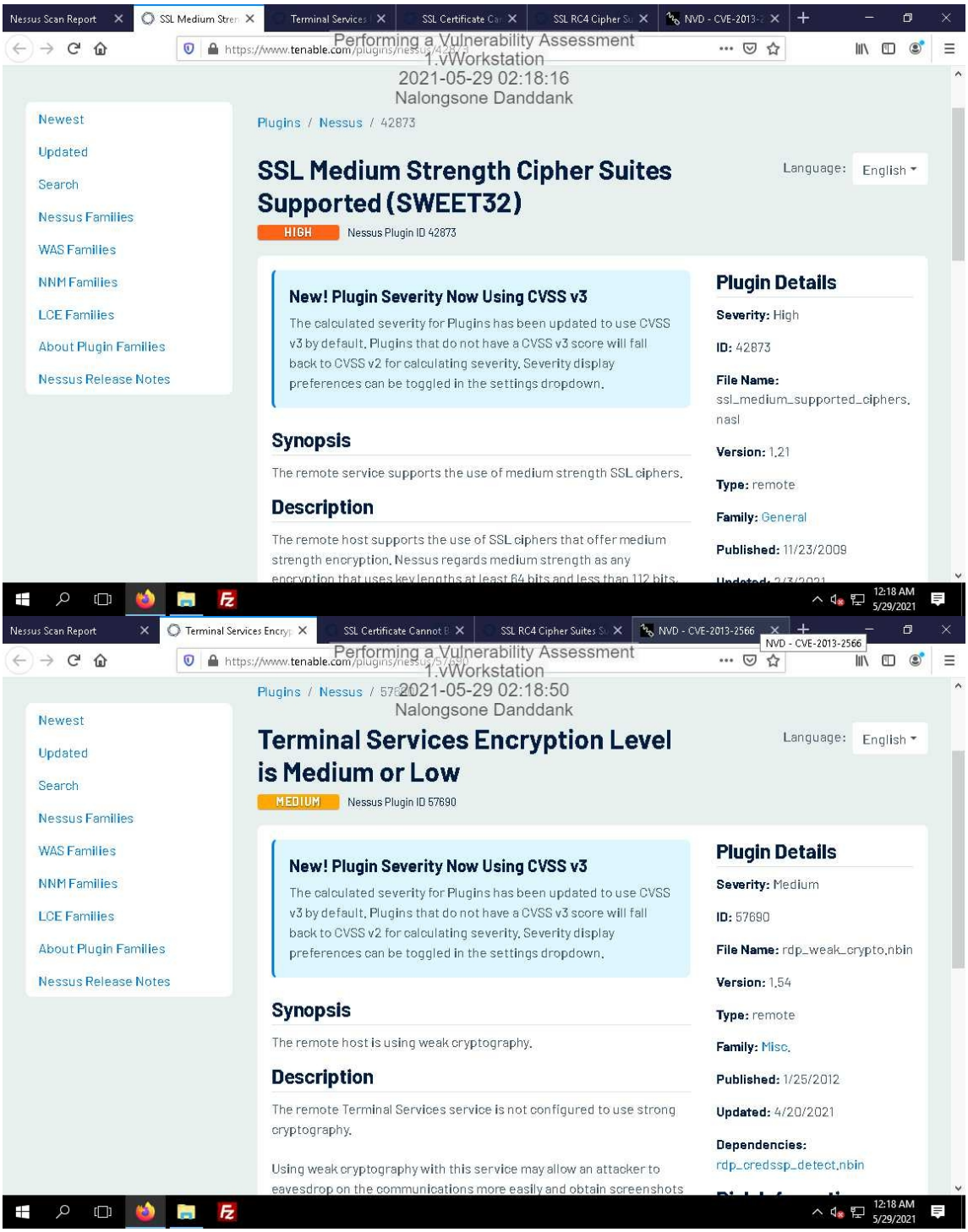
Nessus Scan Report
SSL Certificate Cannot Be Trust
SSL RC4 Cipher Suites Support
NVD - CVE-2013-2566
https://www.tenable.com/plugins/nessus/51192
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:25:43
Nalongsone Danddank
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
SSL Certificate Cannot Be Trusted
Language: English
MEDIUM
Nessus Plugin ID 51192
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
The SSL certificate for this service cannot be trusted.
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would
Plugin Details
Severity: Medium
ID: 51192
File Name: ssl_signed_certificate.nasl
Version: 1.19
Type: remote
Family: General
Published: 12/15/2010
Updated: 4/27/2020
Dependencies: ssl_certificate_chain.nasl
Risk Information
CVSS v2
12:25 AM
5/29/2021


Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:15:14
Nalongsone Danddank
SSL RC4 Cipher Suites Supported (Bar Mitzvah) | Tenable®
https://www.tenable.com/plugins/nessus/57582
Plugins / Nessus / 57582
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
SSL Self-Signed Certificate
Language: English
MEDIUM
Nessus Plugin ID 57582
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
Description
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Plugin Details
Severity: Medium
ID: 57582
File Name: ssl_self_signed_certificate.nasl
Version: 1.5
Type: remote
Family: General
Published: 1/17/2012
Updated: 4/27/2020
Dependencies: ssl_certificate_chain.nasl
12:15 AM
5/29/2021


Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:16:13
Nalongsone Danddank
Open a new tab (Ctrl+T)
Plugins / Nessus / 18405
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Language: English
MEDIUM
Nessus Plugin ID 18405
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
It may be possible to get access to the remote host.
Description
The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when
Plugin Details
Severity: Medium
ID: 18405
File Name: tssvc_mim.nasl
Version: 1.32
Type: remote
Agent: windows
Family: Windows
Published: 6/1/2005
Updated: 3/30/2021
12:16 AM
5/29/2021


Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:17:00
Nalongsone Danddank
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
Plugins / Nessus / 15901
SSL Certificate Expiry
Language: English
MEDIUM Nessus Plugin ID 15901
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
The remote server's SSL certificate has already expired.
Description
This plugin checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.
Solution
Plugin Details
Severity: Medium
ID: 15901
File Name: ssl_cert_expiry.nasl
Version: 1.50
Type: remote
Family: General
Published: 12/3/2004
Updated: 2/3/2021
Dependencies:
ssl_supported_versions.nasl,
find_service_dtls.nasl
12:16 AM
5/29/2021


Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:17:40
Nalongsone Danddank
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
Plugins / Nessus / 57608
SMB Signing not required
Language: English
MEDIUM Nessus Plugin ID 57608
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
Signing is not required on the remote SMB server.
Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
Solution
Plugin Details
Severity: Medium
ID: 57608
File Name:
smb_signing_disabled.nasl
Version: 1.19
Type: remote
Family: Misc.
Published: 1/19/2012
Updated: 3/15/2021
Dependencies:
find_service2.nasl
12:17 AM
5/29/2021


Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:18:16
Nalongsone Danddank
Newest
Updated
Search
Nessus Families
WAS Families
NNM Families
LCE Families
About Plugin Families
Nessus Release Notes
Plugins / Nessus / 42873
SSL Medium Strength Cipher Suites Supported (SWEET32)
Language: English
HIGH
Nessus Plugin ID 42873
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
The remote service supports the use of medium strength SSL ciphers.
Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any
Plugin Details
Severity: High
ID: 42873
File Name: ssl_medium_supported_ciphers.nasl
Version: 1.21
Type: remote
Family: General
Published: 11/23/2009
12:18 AM
5/29/2021
Performing a Vulnerability Assessment
1.vWorkstation
2021-05-29 02:18:50
Nalongsone Danddank
NVD - CVE-2013-2566
Plugins / Nessus / 57690
Terminal Services Encryption Level is Medium or Low
Language: English
MEDIUM
Nessus Plugin ID 57690
New! Plugin Severity Now Using CVSS v3
The calculated severity for Plugins has been updated to use CVSS v3 by default. Plugins that do not have a CVSS v3 score will fall back to CVSS v2 for calculating severity. Severity display preferences can be toggled in the settings dropdown.
Synopsis
The remote host is using weak cryptography.
Description
The remote Terminal Services service is not configured to use strong cryptography.
Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots
Plugin Details
Severity: Medium
ID: 57690
File Name: rdp_weak_crypto.nbin
Version: 1.54
Type: remote
Family: Misc.
Published: 1/25/2012
Updated: 4/20/2021
Dependencies: rdp_credssp_detect.nbin
12:18 AM
5/29/2021

End.