Deployment Of Web Application Scanner - N-Stalker

By Michael Emil Santos

Introduction:

Web Application Vulnerability Scanners are automated tools that scan web applications. It is designed to help security professionals identify security vulnerabilities in web applications and websites, such as Cross-site scripting, SQL Injection, Command Injection, Path/directory traversal and insecure server configuration. **N-Stalker** Web Application Scanner is applied to check the Badstore website vulnerability in this lab and we will practice how to use it and address benefits of such a tool.

The website BadStore.net was created to demonstrate the widespread security vulnerabilities that are present in many programmes that are accessible via internal networks, extranets, and the Internet. Many people tasked with designing operating, and securing Web Applications have never seen the variety of attacks available to compromise these applications – or what they can do to protect these applications. To run the BadStore.net application, it can be used under a virtual environment, such as VirtualBox or VMWare.

This project demonstrates the use of N-Stalker, a web application vulnerability scanner, to identify security gaps in a web application (BadStore.net). The scan aimed to detect common vulnerabilities like Cross-Site Scripting (XSS), SQL Injection, and insecure configurations, providing actionable recommendations to improve the application's security.

Project Objectives and Steps

1. **Setting Up the Target Web Application**

- **Objective**: Deploy BadStore.net in a virtual environment to simulate a vulnerable web application.
- **Steps**: Installed and configured BadStore.net as the target for testing, representing a realistic security assessment scenario.

2. **Running the N-Stalker Vulnerability Scan**

- **Objective**: Identify web application vulnerabilities by performing a comprehensive scan.
- **Steps**: Configured N-Stalker with the OWASP Policy and ran a full scan. N-Stalker detected common web security issues, including XSS, HTTP Parameter Pollution, and insecure cookie configurations.

3. **Analyzing the Report and Findings**

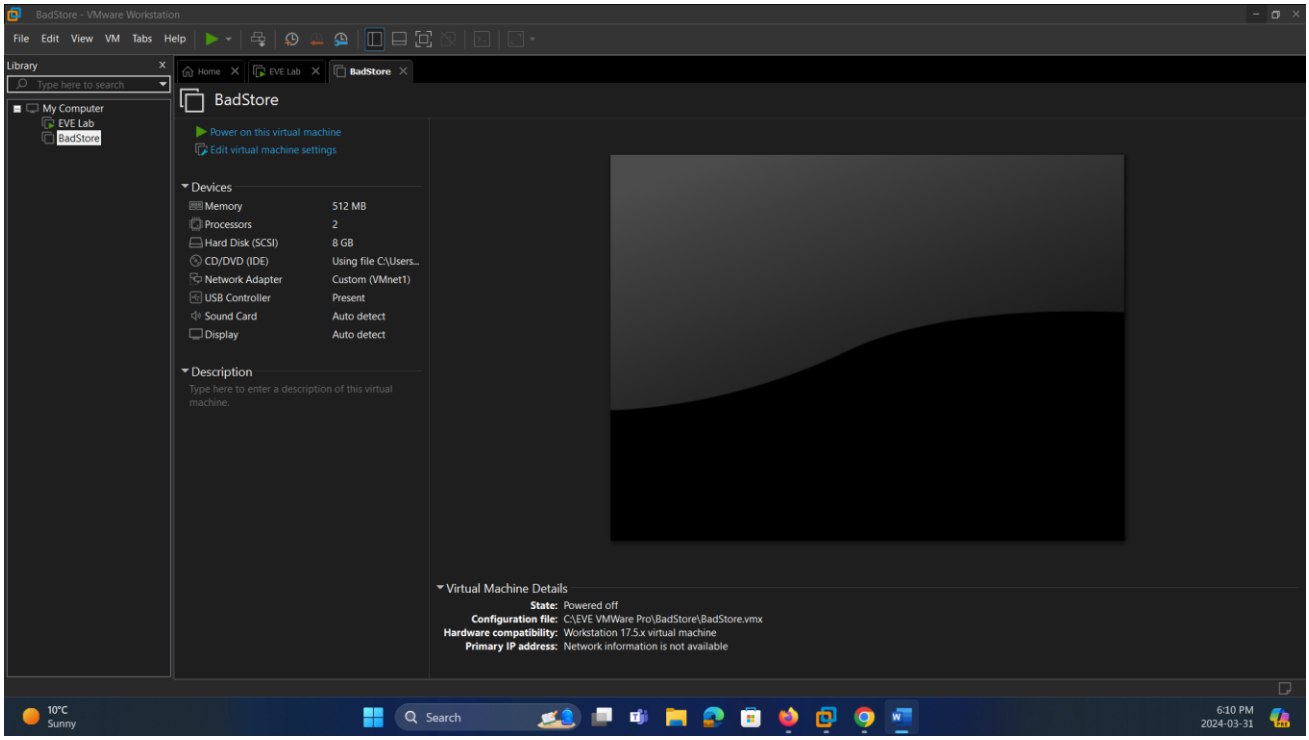
- **Objective**: Review scan results and prioritize vulnerabilities for remediation.
- **Steps**: Examined the report to understand detected issues, severity levels, and detailed insights into vulnerabilities like Cross-Site Request Forgery (CSRF) and insecure authentication methods.

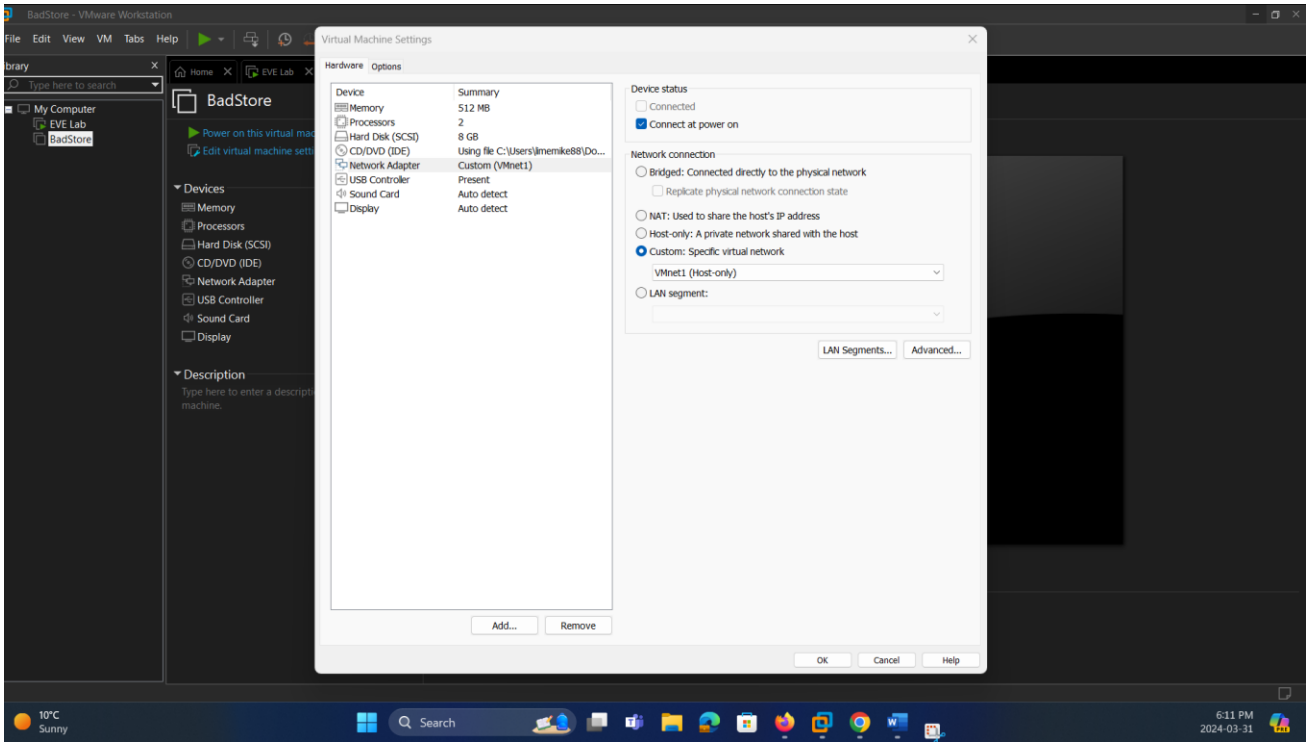
4. **Recommendations for Security Enhancement**

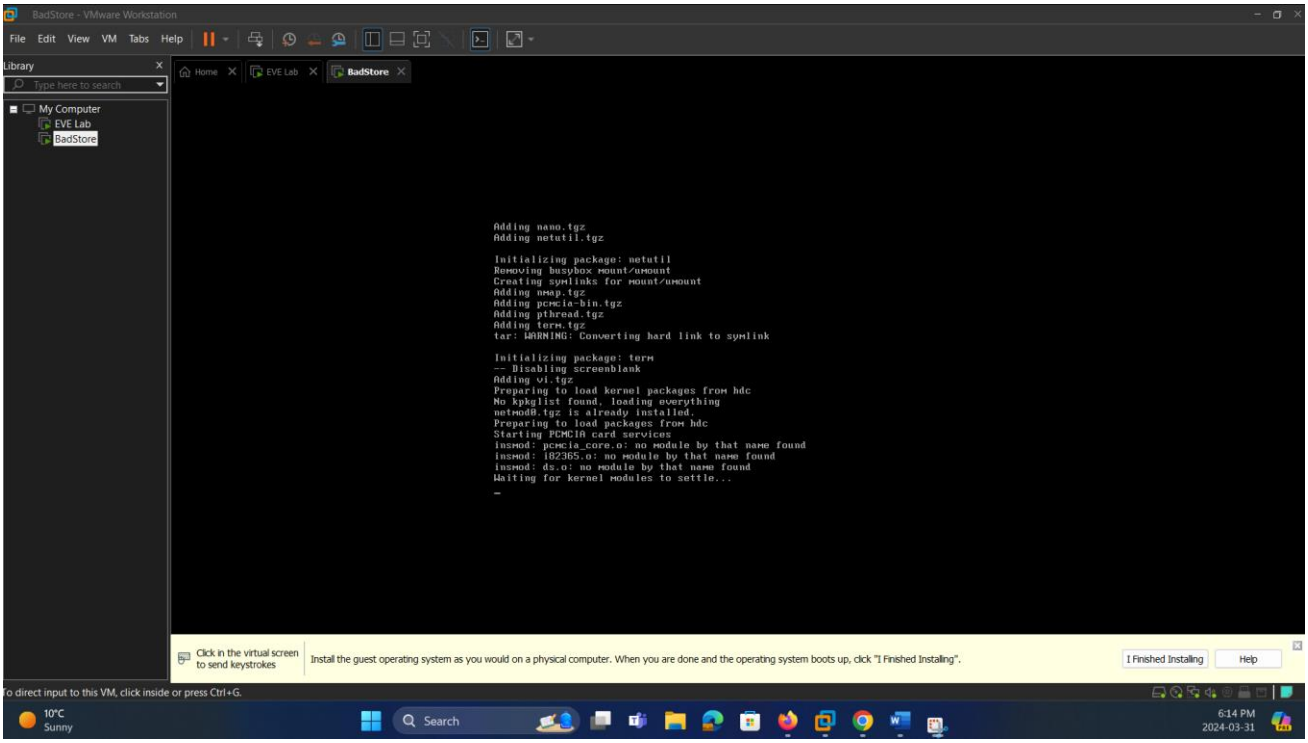
- **Objective**: Provide a roadmap to mitigate identified risks and strengthen the application's security.
- **Steps**: Developed recommendations focusing on secure coding practices, implementing secure cookie attributes, and updating protocols. Prioritized actions based on severity to address critical vulnerabilities first.

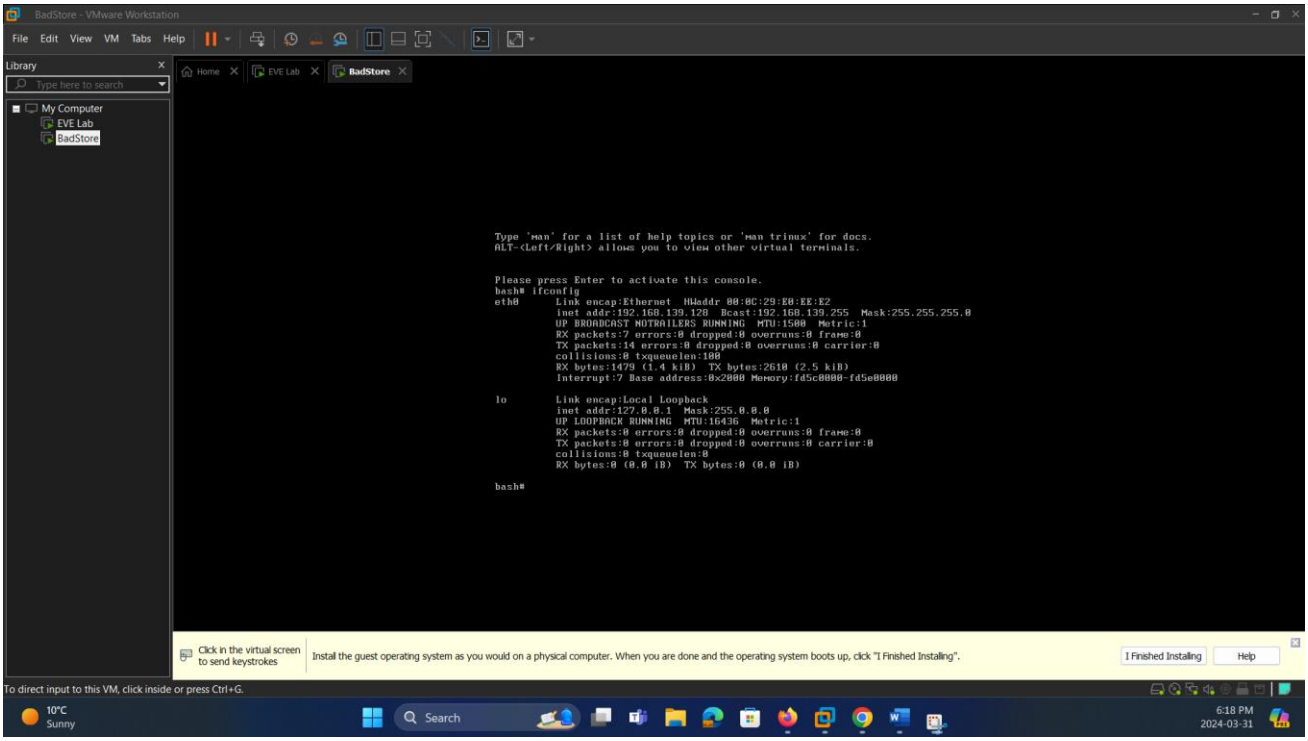
Lab Requirements

1. Configuring and Running Badstore in Virtual Machine Application (VMWare)

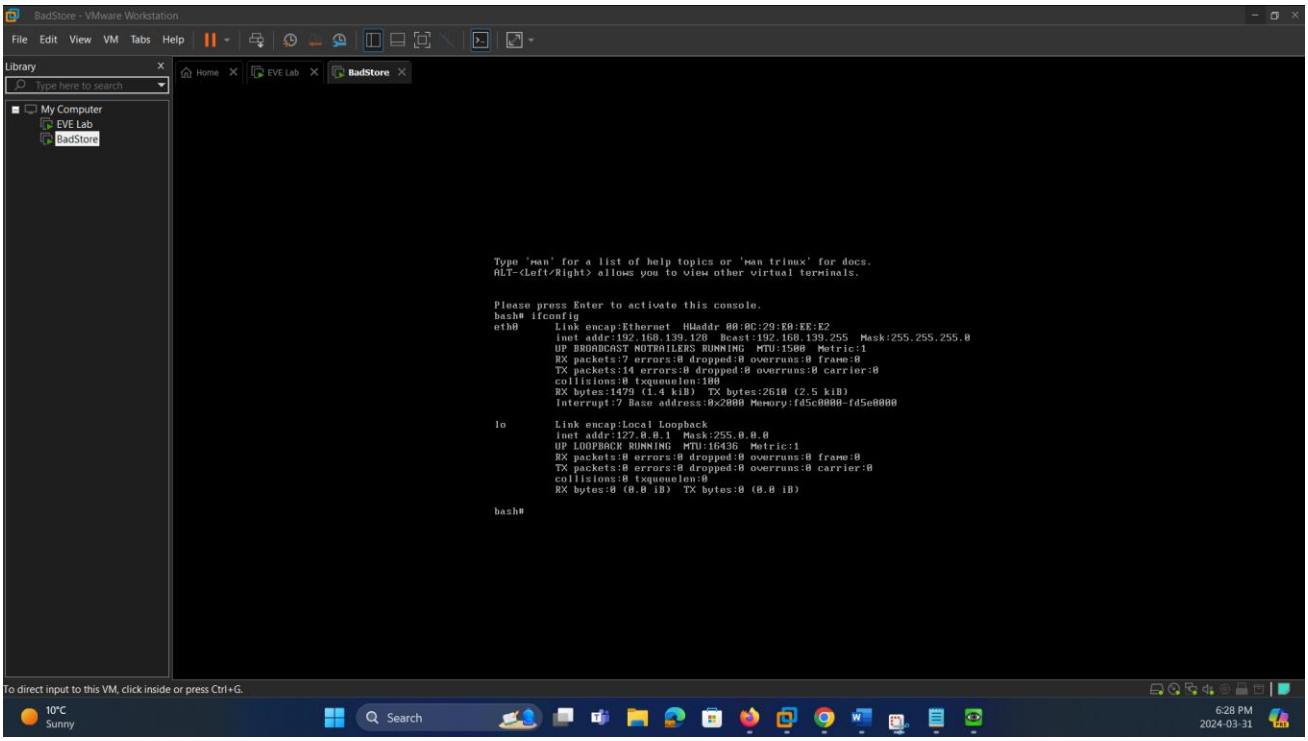


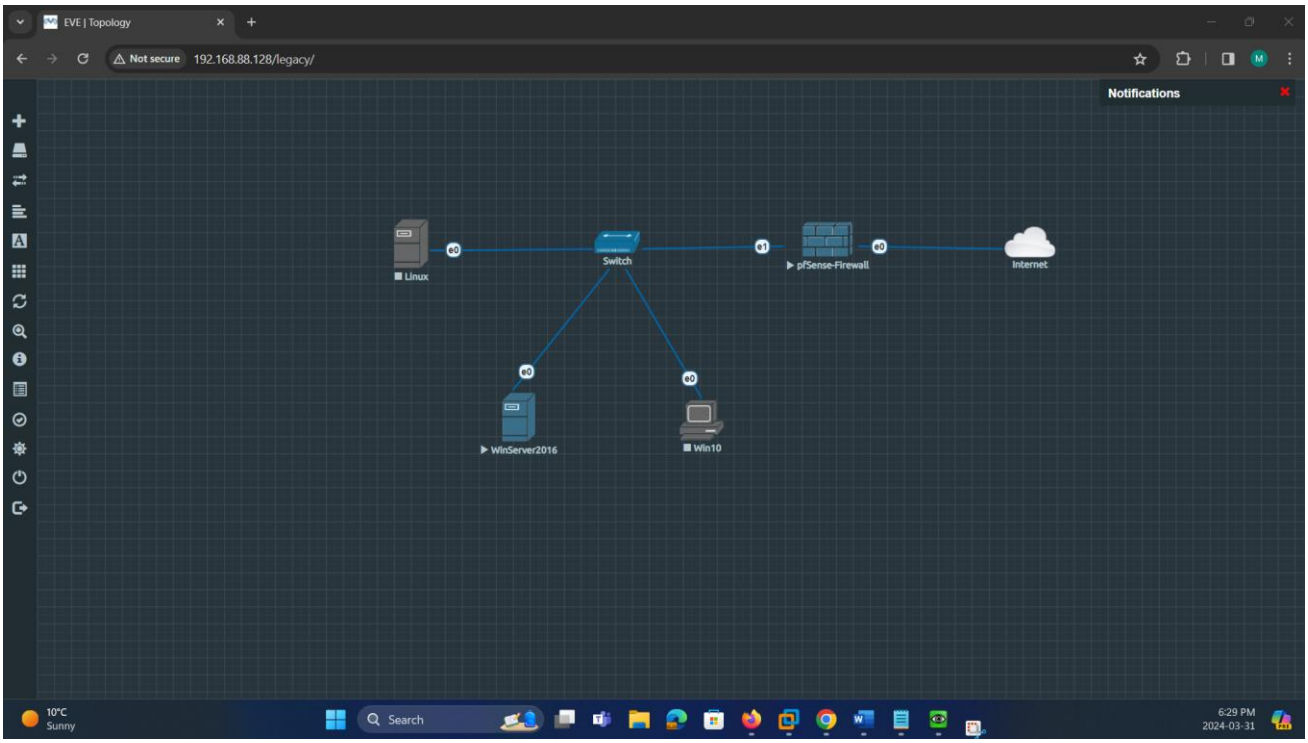


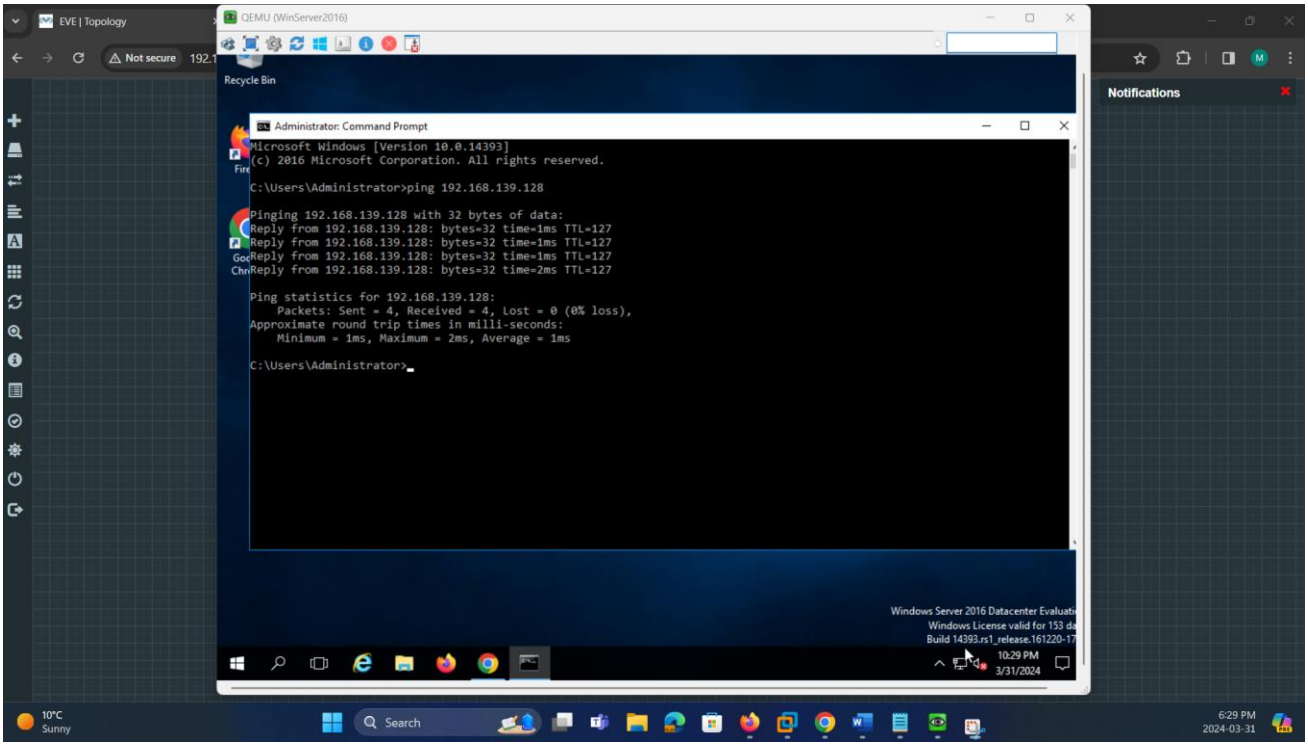




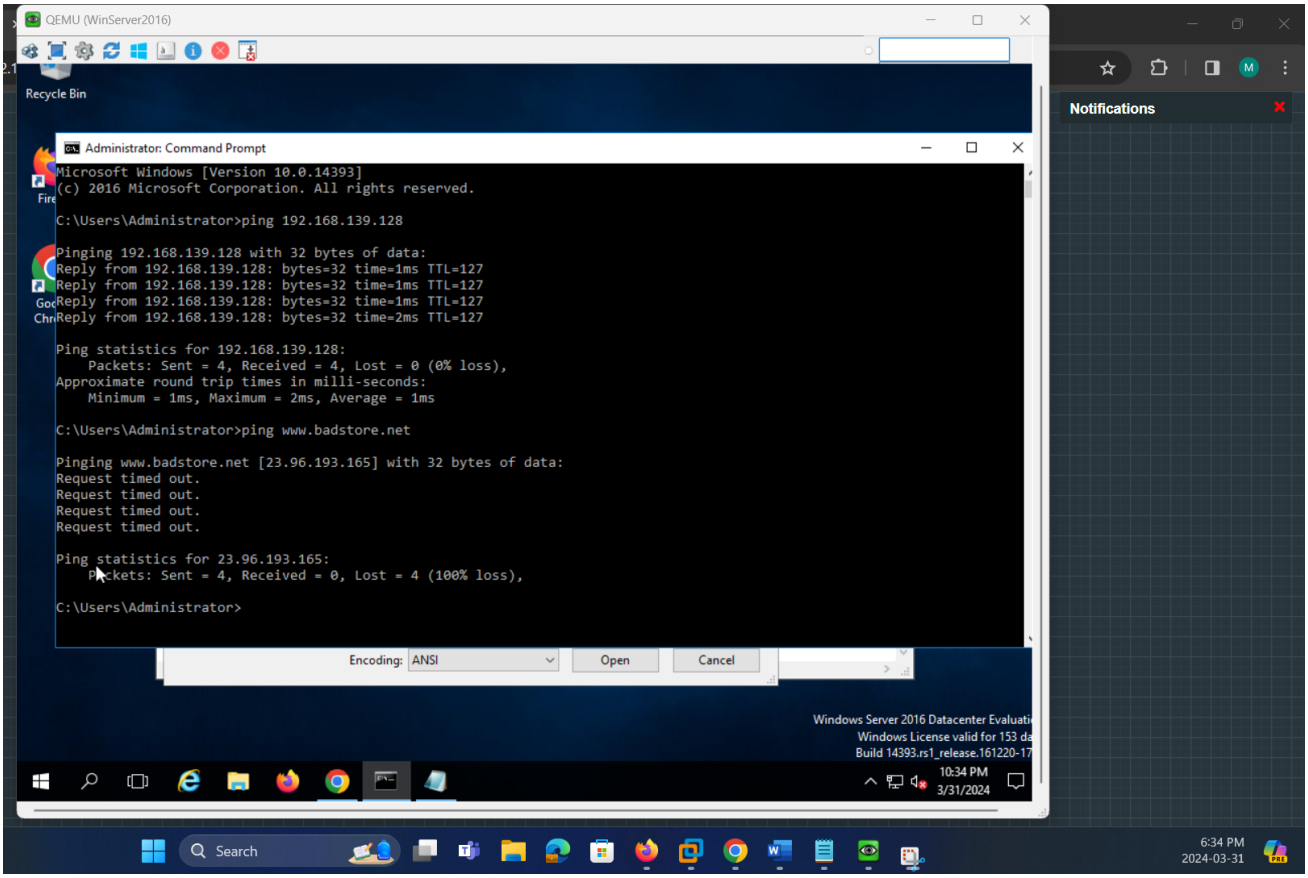
IP Address of Badstore: 192.168.139.128

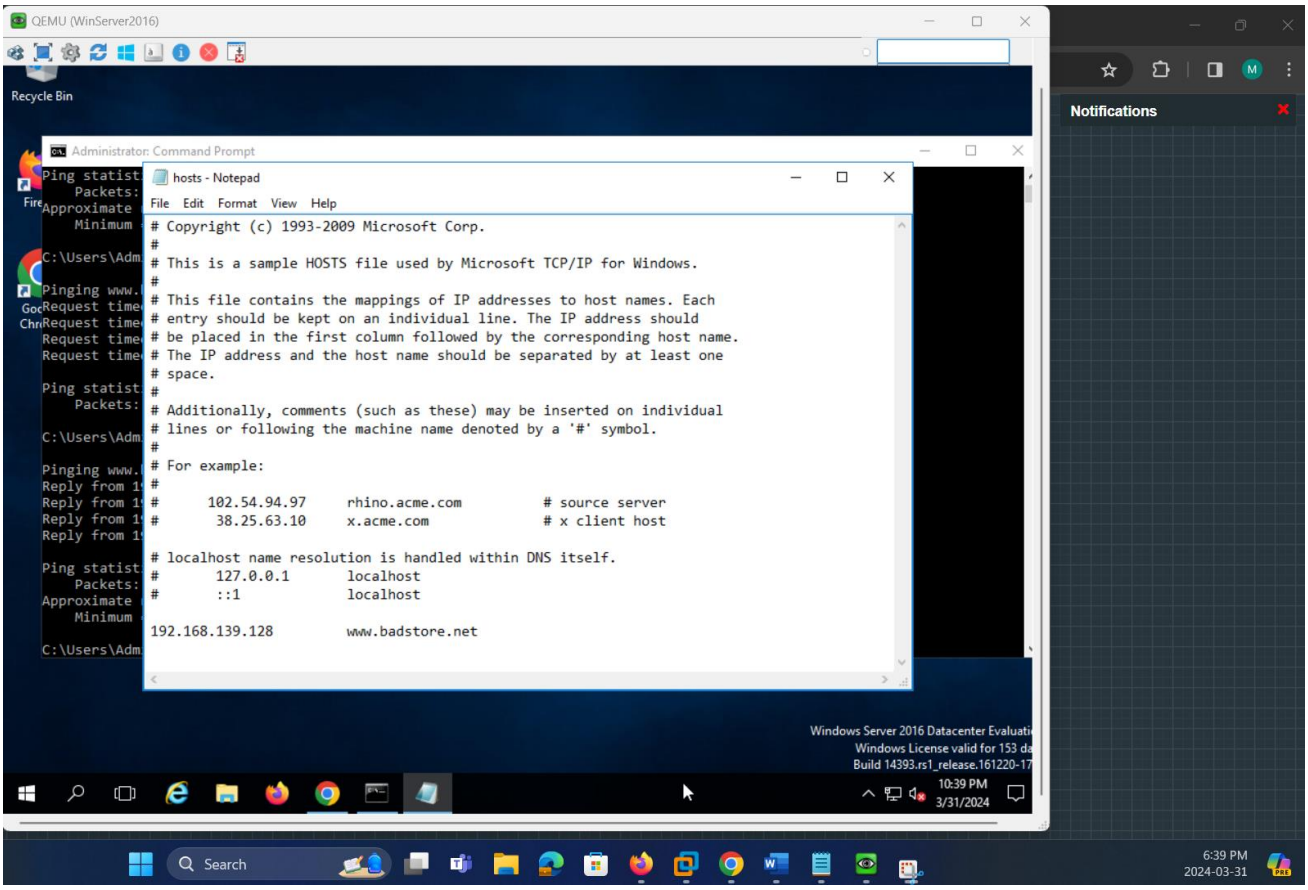

BadStore - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
EVE Lab
BadStore
Home
EVE Lab
BadStore
Type 'man' for a list of help topics or 'man trinux' for docs.
ALT-<Left/Right> allows you to view other virtual terminals.
Please press Enter to activate this console.
bash# ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:E0:EE:E2
inet addr:192.168.139.128 Bcast:192.168.139.255 Mask:255.255.255.0
UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
RX packets:7 errors:0 dropped:0 overruns:0 frame:0
TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:1479 (1.4 kiB) TX bytes:2610 (2.5 kiB)
Interrupt:7 Base address:0x2000 Memory:fd5c0000-fd5e0000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 iB) TX bytes:0 (0.0 iB)
bash#
To direct input to this VM, click inside or press Ctrl+G.
10°C
Sunny
Search
6:28 PM
2024-03-31

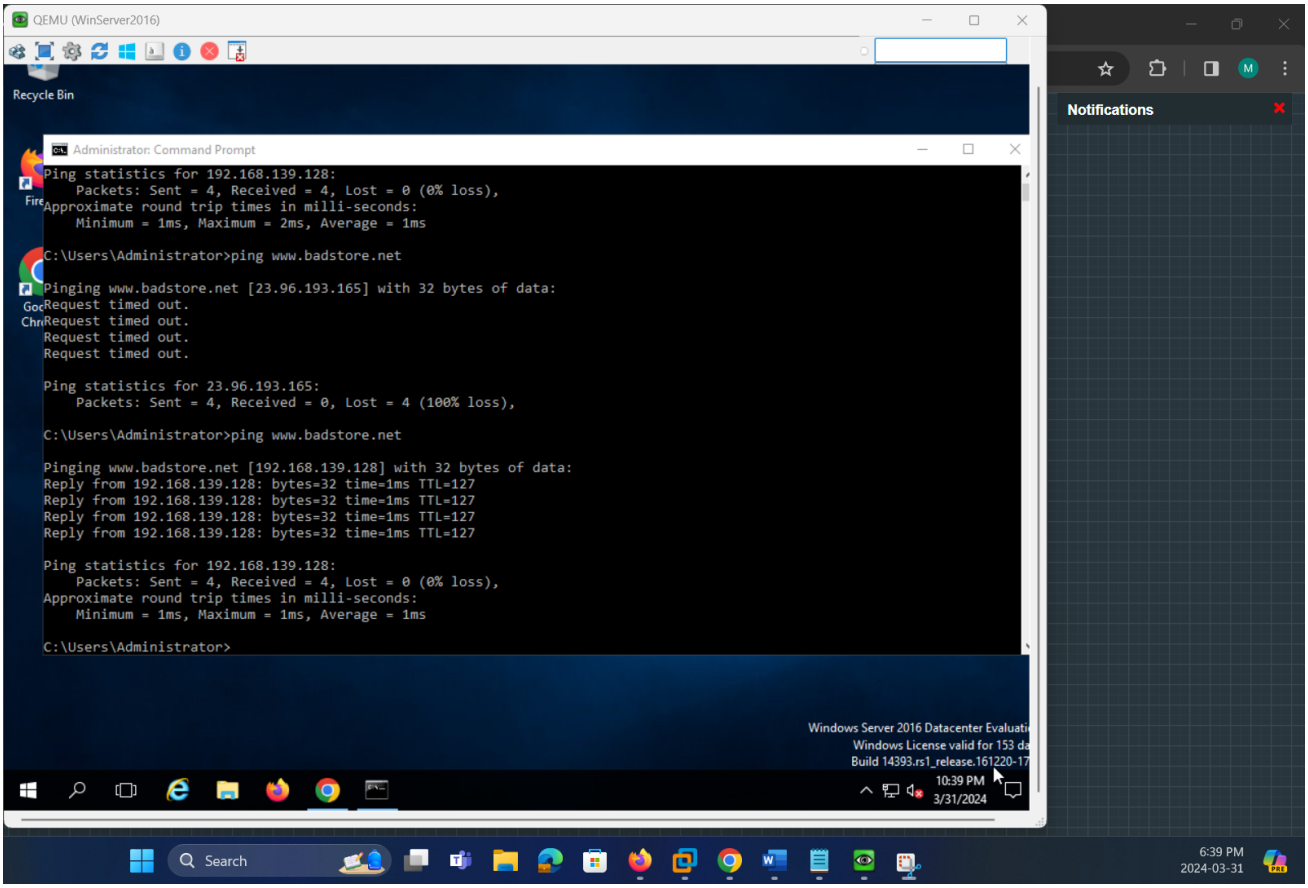

EVE | Topology
Not secure
192.168.88.128/legacy/
Notifications
Linux
Switch
pfSense-Firewall
Internet
WinServer2016
Win10
10°C
Sunny
Search
6:29 PM
2024-03-31

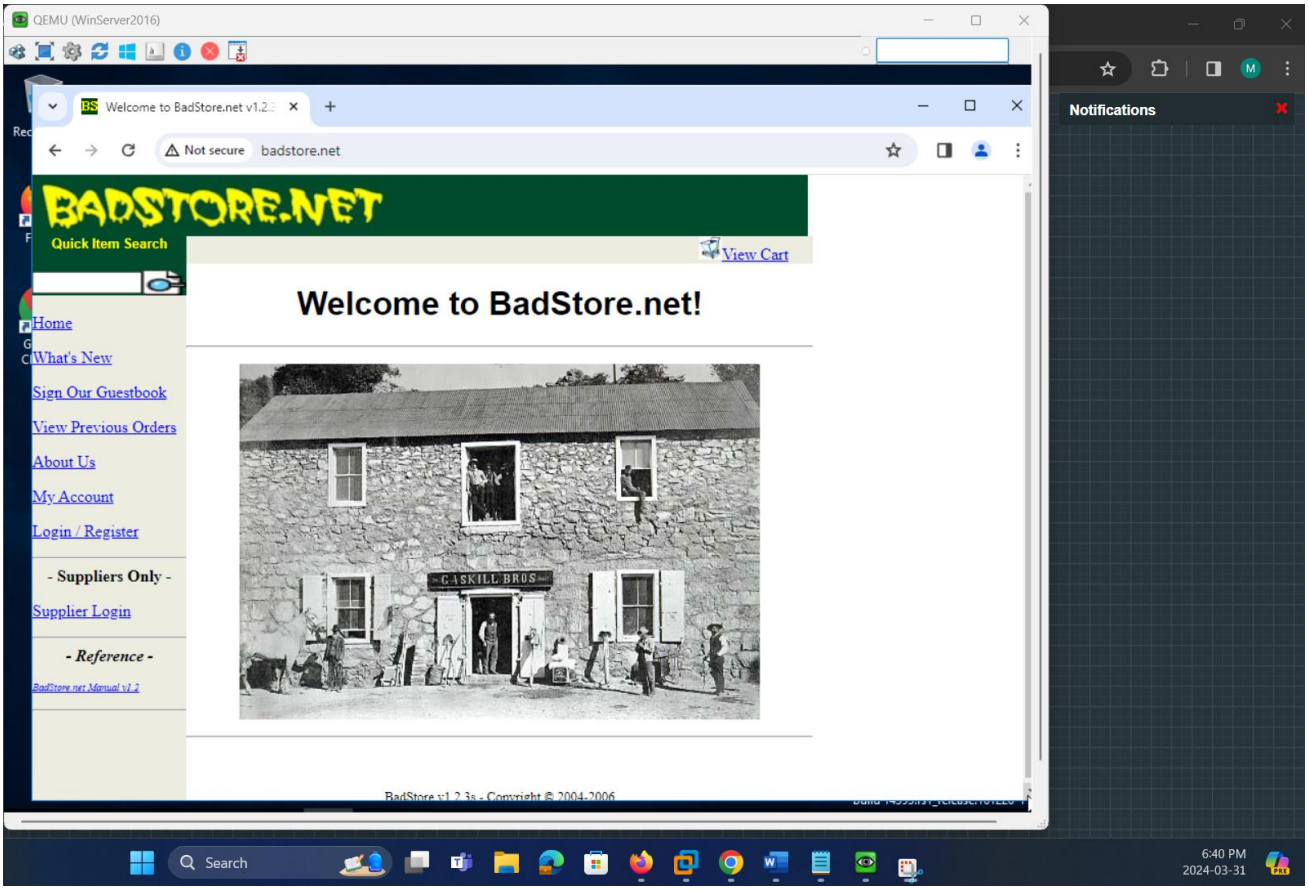


Conducted ping test to badstore IP Address from Windows 2016 Server VM – EVE Lab VM to BadStore VM



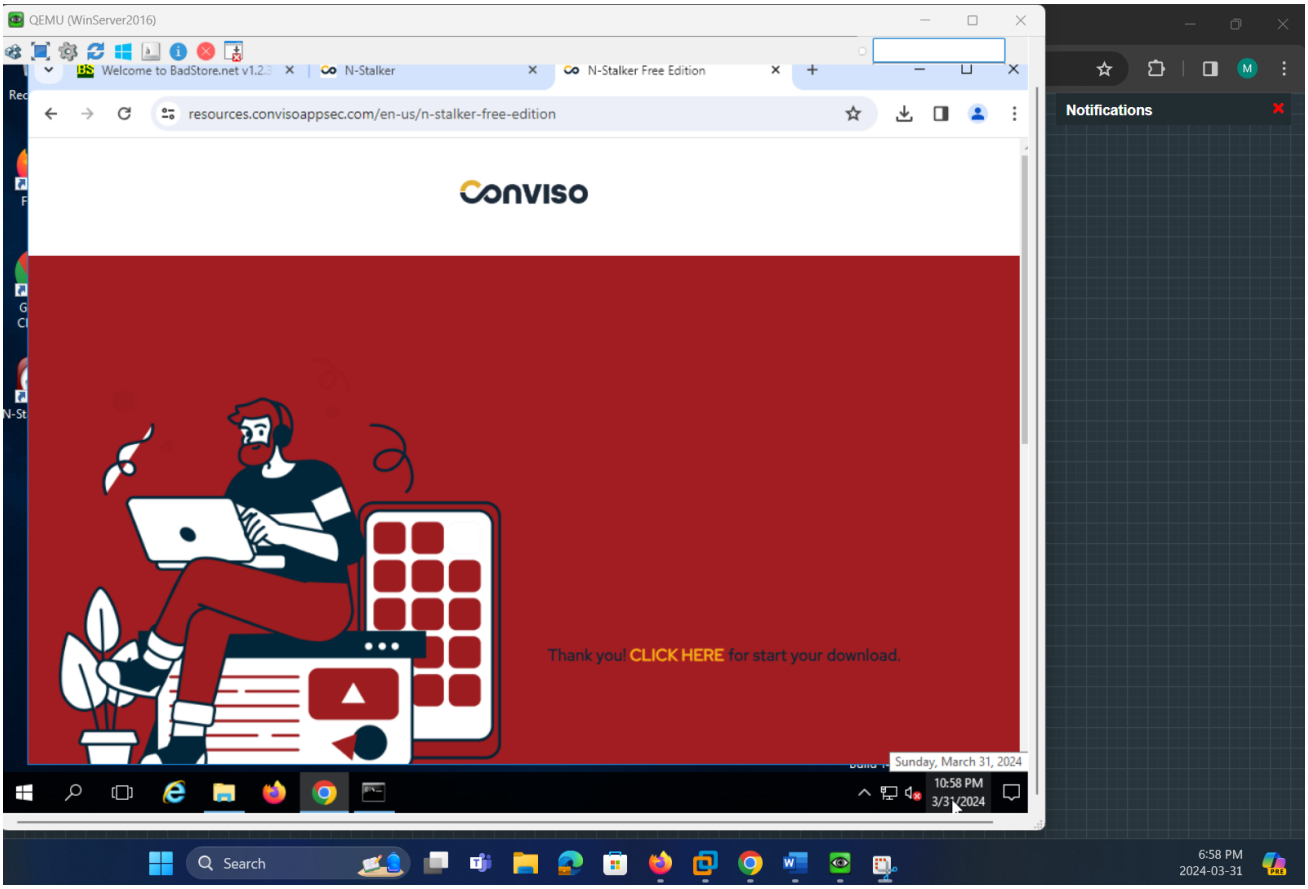

QEMU (WinServer2016)
Recycle Bin
Administrator: Command Prompt
hosts - Notepad
File Edit Format View Help
Copyright (c) 1993-2009 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97   rhino.acme.com   # source server
38.25.63.10   x.acme.com   # x client host
localhost name resolution is handled within DNS itself.
127.0.0.1   localhost
::1   localhost
192.168.139.128   www.badstore.net
Windows Server 2016 Datacenter Evaluati
Windows License valid for 153 da
Build 14393.rs1_release.161220-17
10:39 PM
3/31/2024
Notifications
Search
6:39 PM
2024-03-31

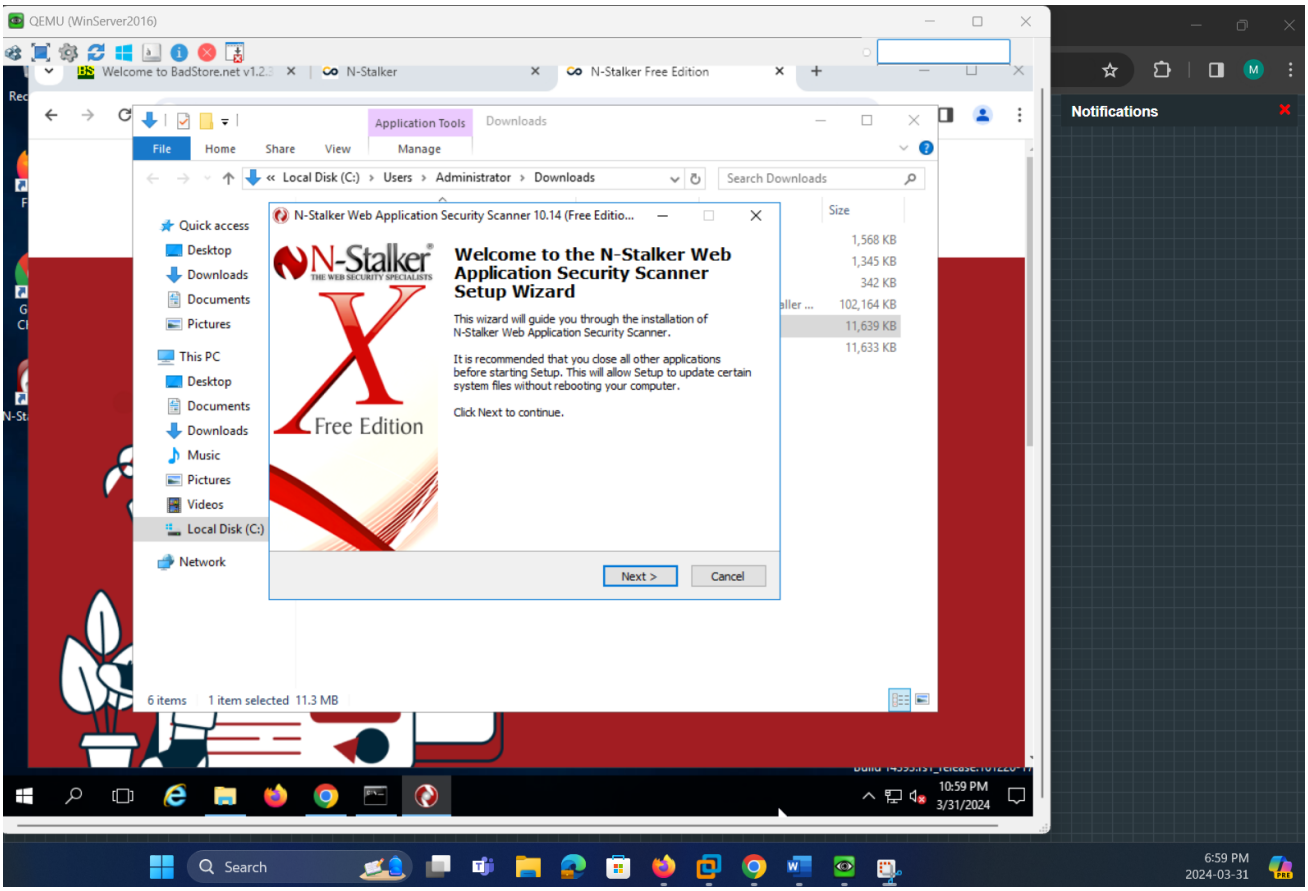

QEMU (WinServer2016)
Recycle Bin
Administrator: Command Prompt
Ping statistics for 192.168.139.128:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\Administrator>ping www.badstore.net
Pinging www.badstore.net [23.96.193.165] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 23.96.193.165:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Administrator>ping www.badstore.net
Pinging www.badstore.net [192.168.139.128] with 32 bytes of data:
Reply from 192.168.139.128: bytes=32 time=1ms TTL=127
Reply from 192.168.139.128: bytes=32 time=1ms TTL=127
Reply from 192.168.139.128: bytes=32 time=1ms TTL=127
Reply from 192.168.139.128: bytes=32 time=1ms TTL=127
Ping statistics for 192.168.139.128:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\Administrator>
Windows Server 2016 Datacenter Evaluati
Windows License valid for 153 da
Build 14393.rs1_release.161220-17
10:39 PM
3/31/2024
Notifications
Search
6:39 PM
2024-03-31

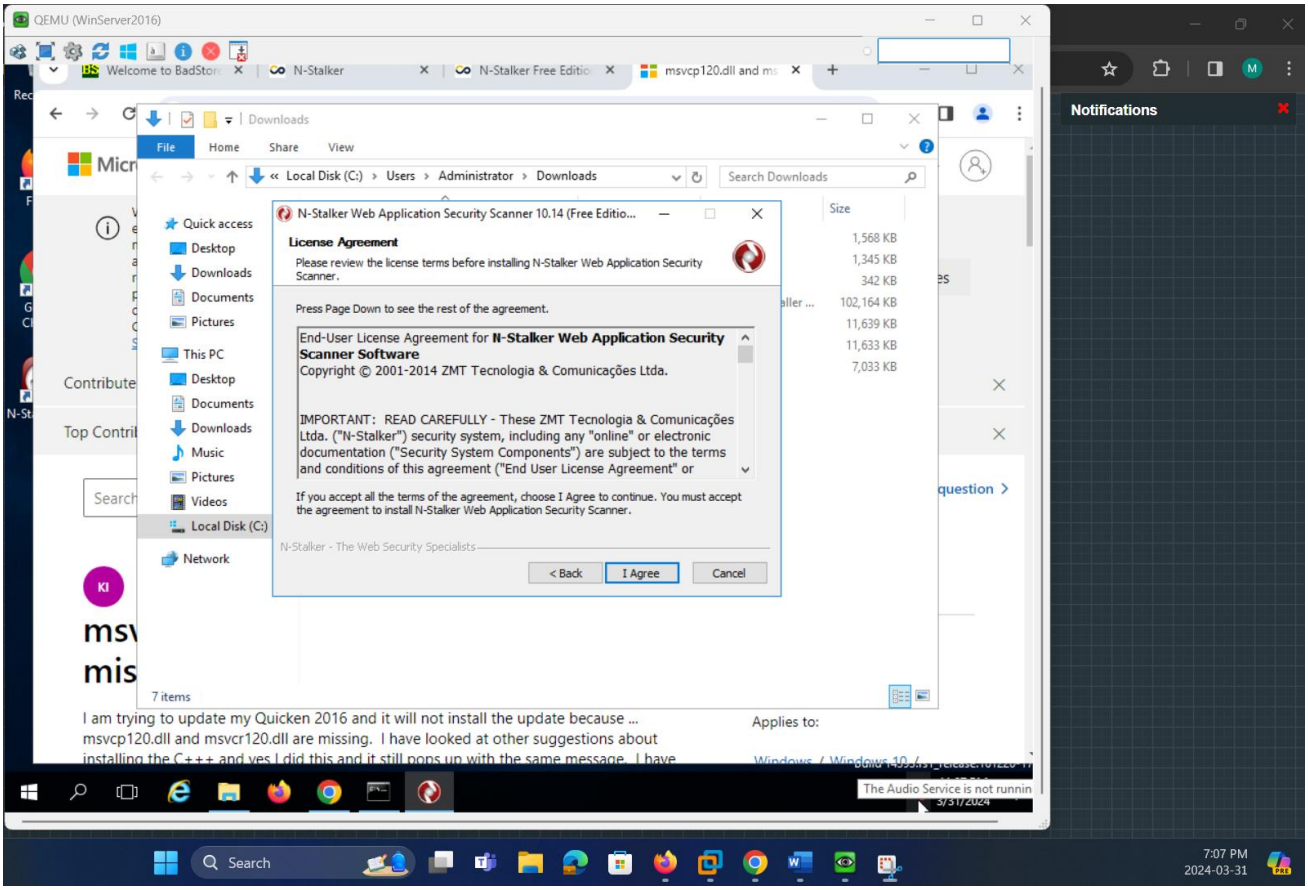


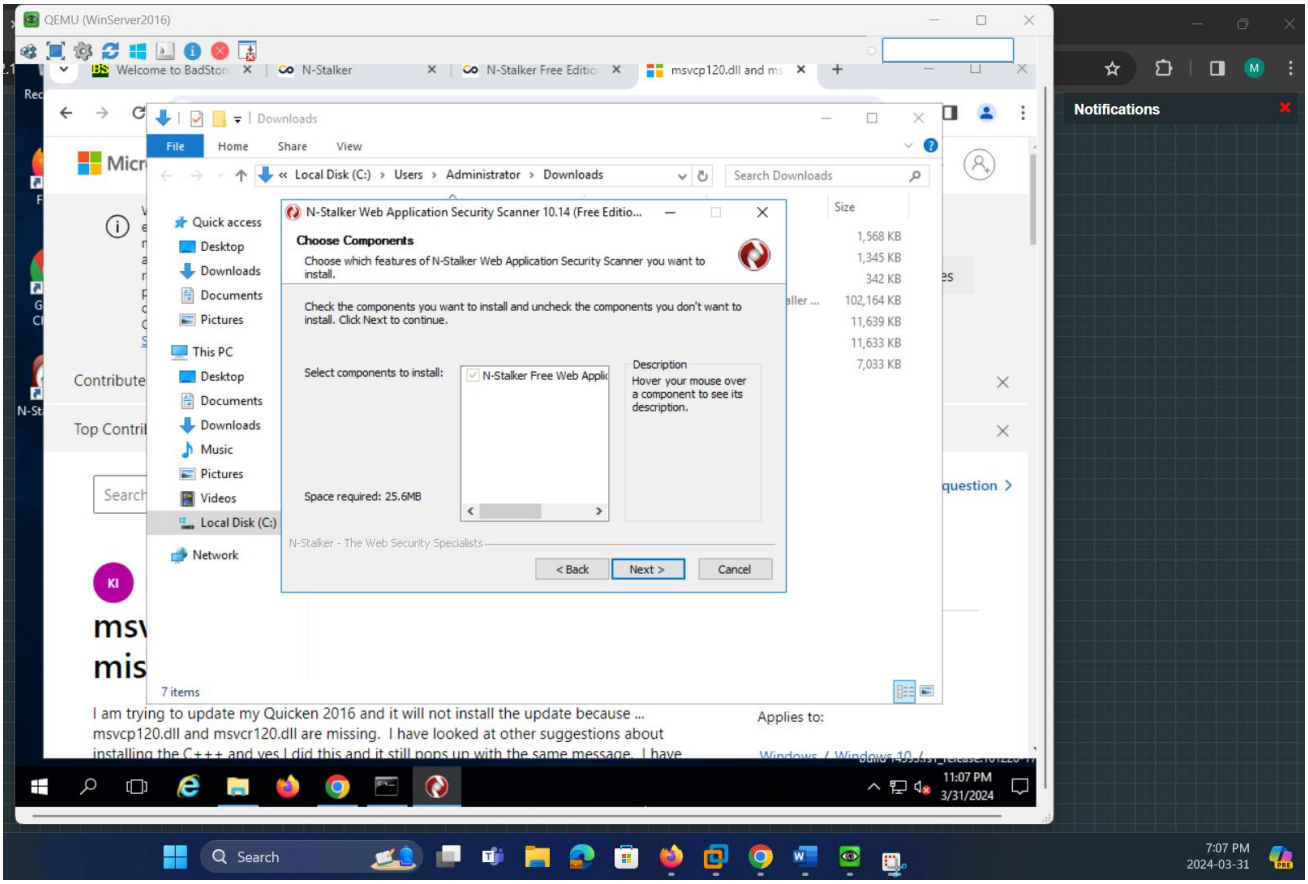
Configured hosts file of Windows Server 2016 and added IP Address of Badstore.Net for DNS Resolution
IP Address: 192.168.139.128 = www.badstore.net

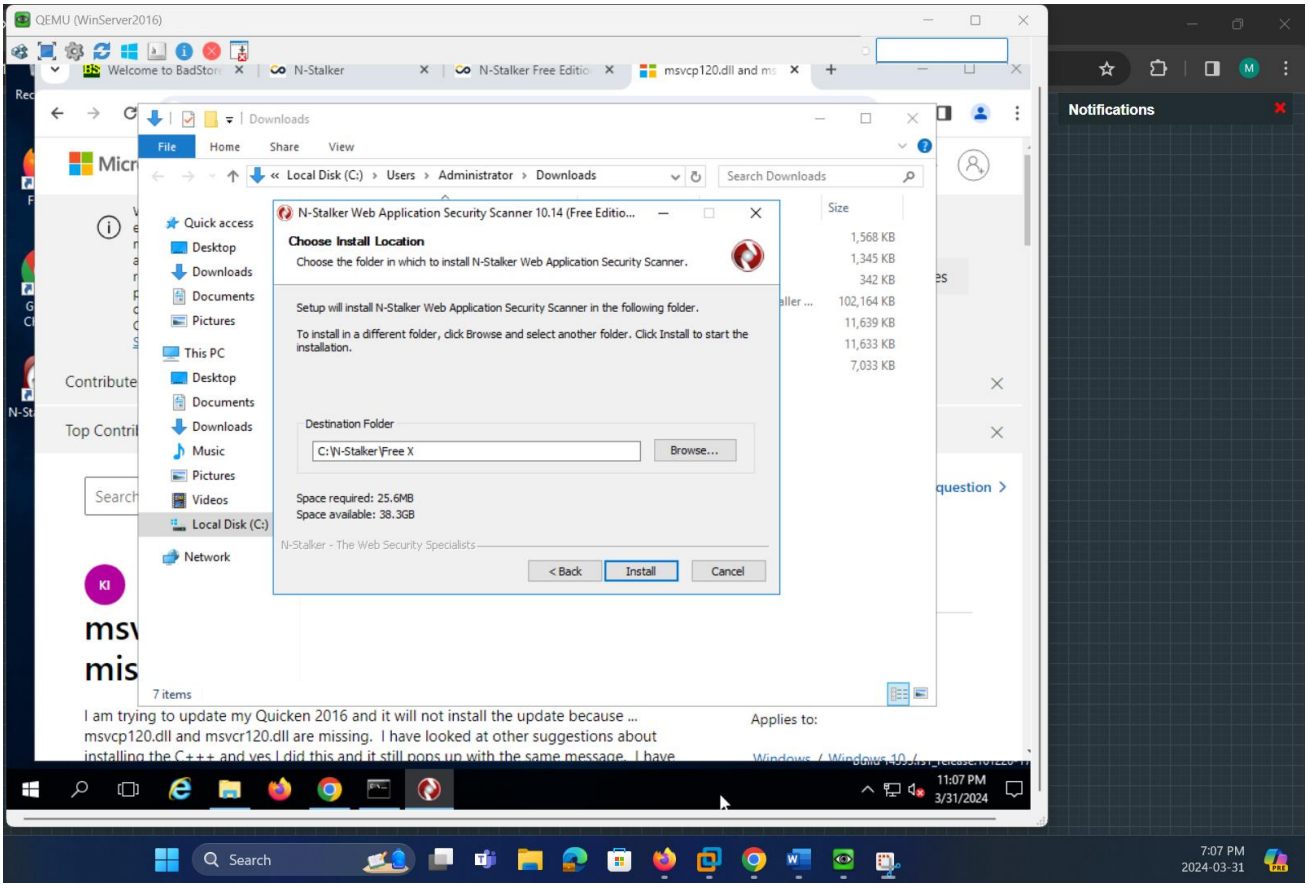
2. Downloading and Installing N-Stalker on Windows 2016 Server VM

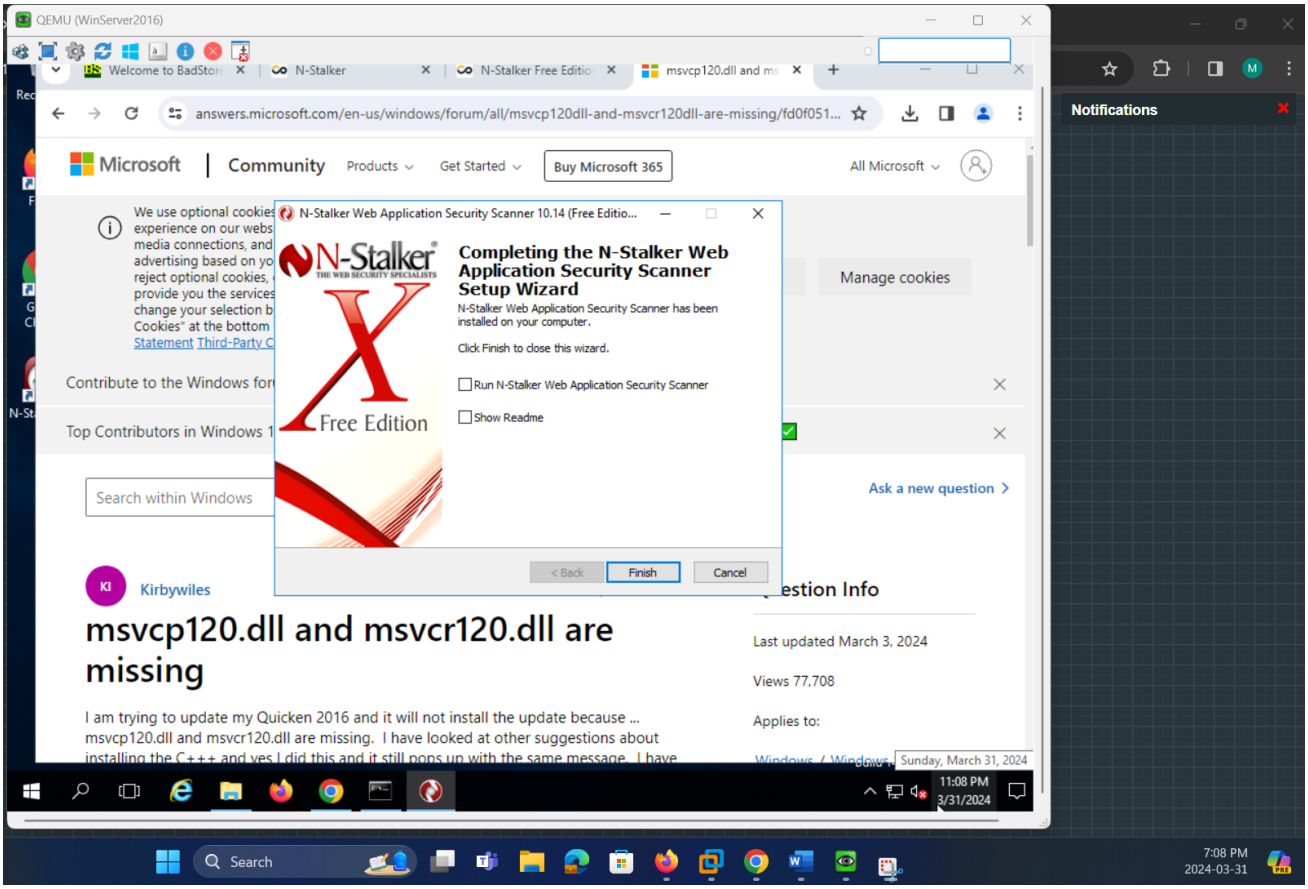

QEMU (WinServer2016)
Welcome to BadStore.net v1.2
N-Stalker
N-Stalker Free Edition
resources.convisoappsec.com/en-us/n-stalker-free-edition
Conviso
Thank you! CLICK HERE for start your download.
Sunday, March 31, 2024
10:58 PM
3/31/2024
Notifications
Search
6:58 PM
2024-03-31

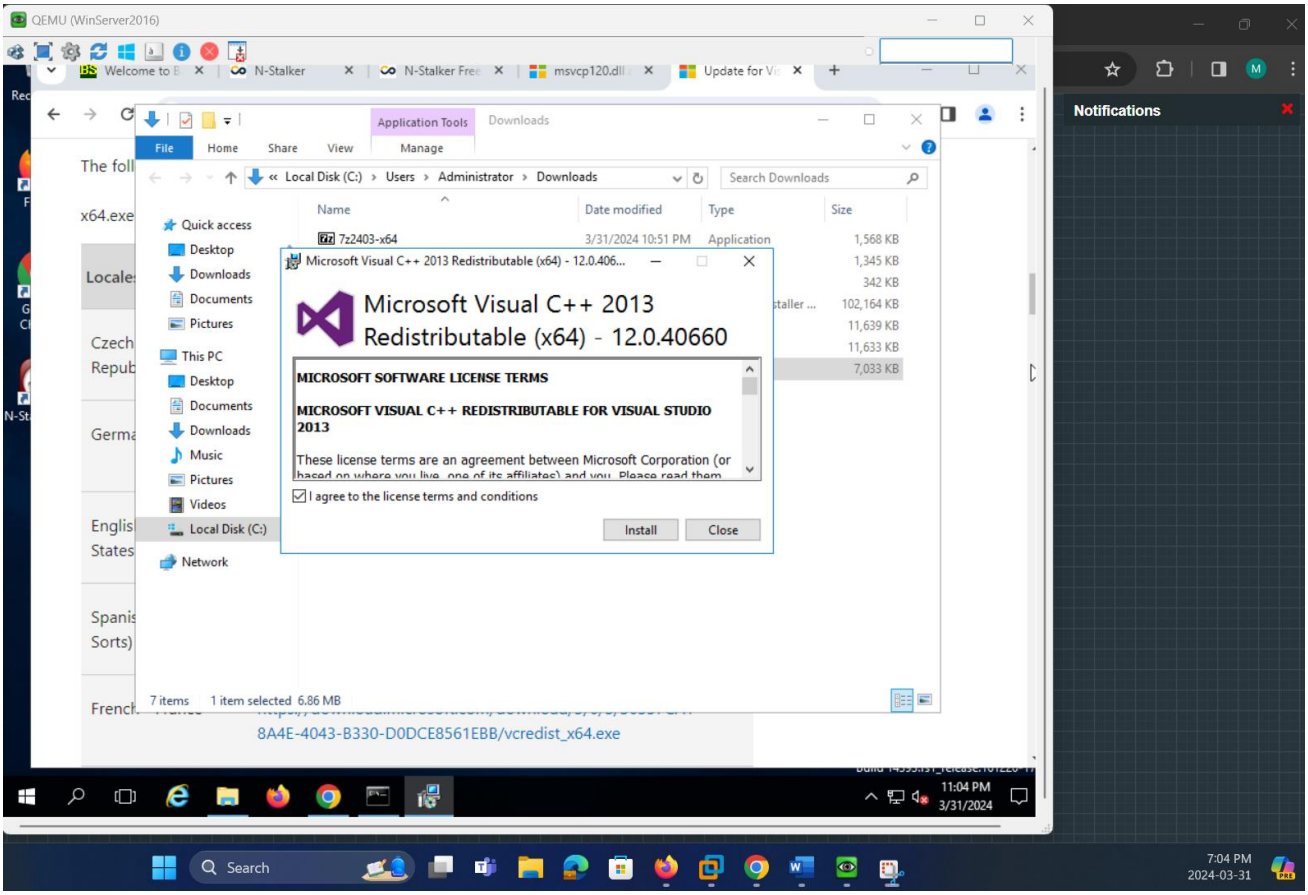

QEMU (WinServer2016)
Welcome to BadStore.net v1.2.2
N-Stalker
N-Stalker Free Edition
Application Tools
Downloads
File
Home
Share
View
Manage
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Size
1,568 KB
1,345 KB
342 KB
102,164 KB
11,639 KB
11,633 KB
6 items
1 item selected 11.3 MB
N-Stalker Web Application Security Scanner 10.14 (Free Editio...
N-Stalker
THE WEB SECURITY SPECIALISTS
X
Free Edition
Welcome to the N-Stalker Web Application Security Scanner Setup Wizard
This wizard will guide you through the installation of N-Stalker Web Application Security Scanner.
It is recommended that you close all other applications before starting Setup. This will allow Setup to update certain system files without rebooting your computer.
Click Next to continue.
Next >
Cancel
10:59 PM
3/31/2024
Notifications
Search
6:59 PM
2024-03-31

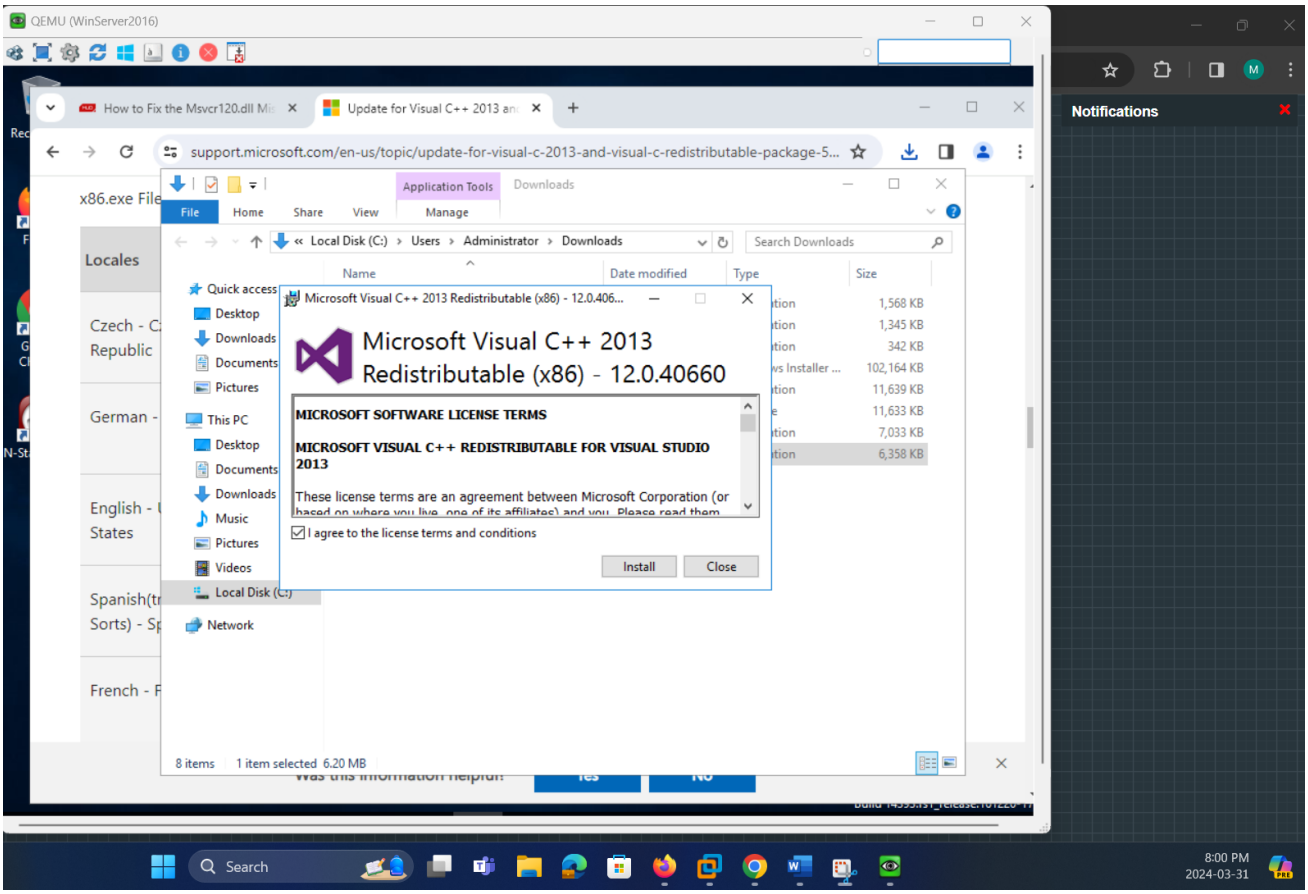

QEMU (WinServer2016)
Downloads
File
Home
Share
View
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Size
1,568 KB
1,345 KB
342 KB
102,164 KB
11,639 KB
11,633 KB
7,033 KB
7 items
N-Stalker Web Application Security Scanner 10.14 (Free Editio...
License Agreement
Please review the license terms before installing N-Stalker Web Application Security Scanner.
Press Page Down to see the rest of the agreement.
End-User License Agreement for N-Stalker Web Application Security Scanner Software
Copyright © 2001-2014 ZMT Tecnologia & Comunicações Ltda.
IMPORTANT: READ CAREFULLY - These ZMT Tecnologia & Comunicações Ltda. ("N-Stalker") security system, including any "online" or electronic documentation ("Security System Components") are subject to the terms and conditions of this agreement ("End User License Agreement" or
If you accept all the terms of the agreement, choose I Agree to continue. You must accept the agreement to install N-Stalker Web Application Security Scanner.
N-Stalker - The Web Security Specialists
< Back
I Agree
Cancel
I am trying to update my Quicken 2016 and it will not install the update because ... msvcp120.dll and msvcr120.dll are missing. I have looked at other suggestions about
Applies to:
Notifications
The Audio Service is not runnin
Search
7:07 PM
2024-03-31

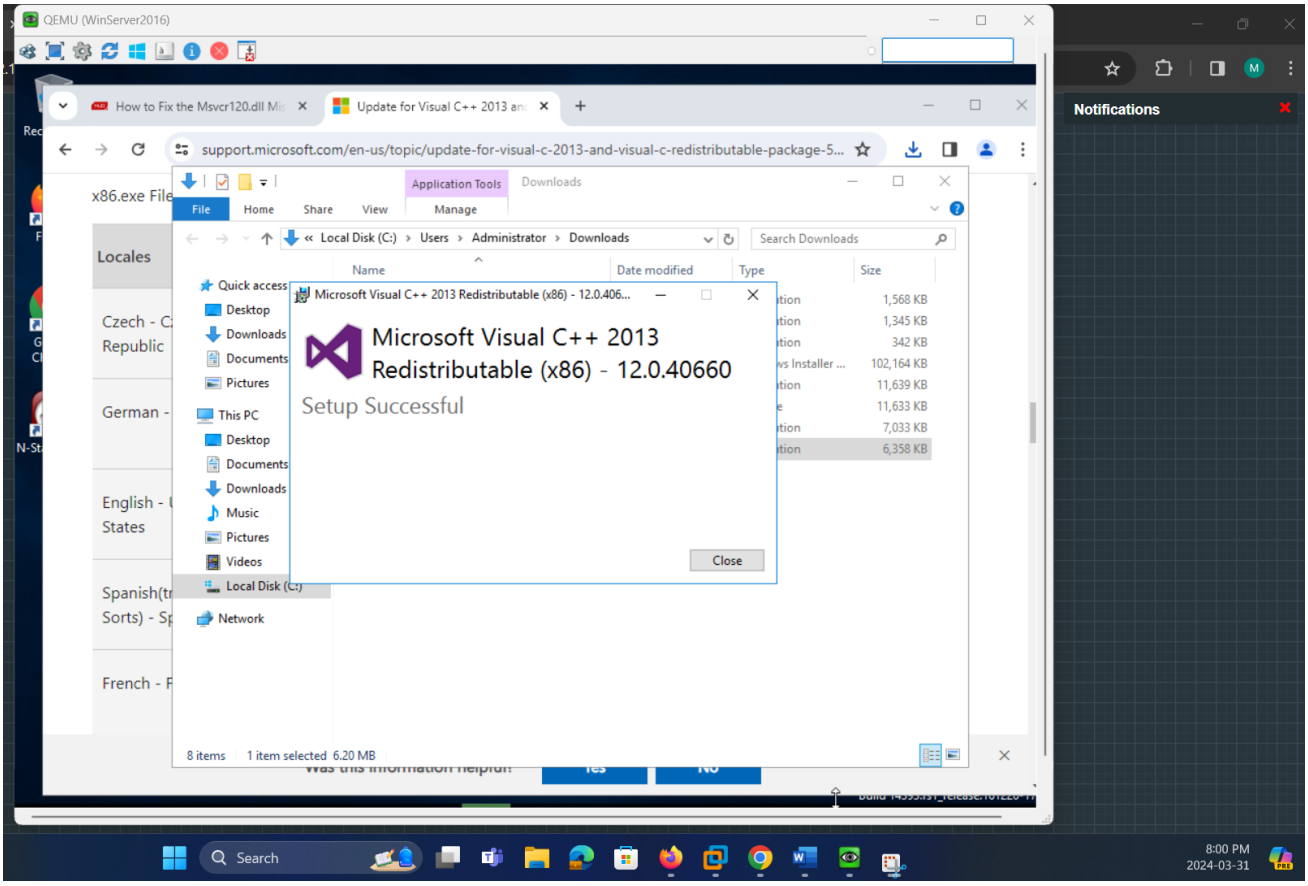

QEMU (WinServer2016)
Welcome to BadStore
N-Stalker
N-Stalker Free Editio
msvcp120.dll and ms
Notifications
Downloads
File
Home
Share
View
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Size
1,568 KB
1,345 KB
342 KB
102,164 KB
11,639 KB
11,633 KB
7,033 KB
N-Stalker Web Application Security Scanner 10.14 (Free Editio...
Choose Components
Choose which features of N-Stalker Web Application Security Scanner you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
N-Stalker Free Web Appli
Description
Hover your mouse over a component to see its description.
Space required: 25.6MB
N-Stalker - The Web Security Specialists
< Back
Next >
Cancel
7 items
I am trying to update my Quicken 2016 and it will not install the update because ... msvcp120.dll and msvcr120.dll are missing. I have looked at other suggestions about
Applies to:
11:07 PM
3/31/2024
Search
7:07 PM
2024-03-31

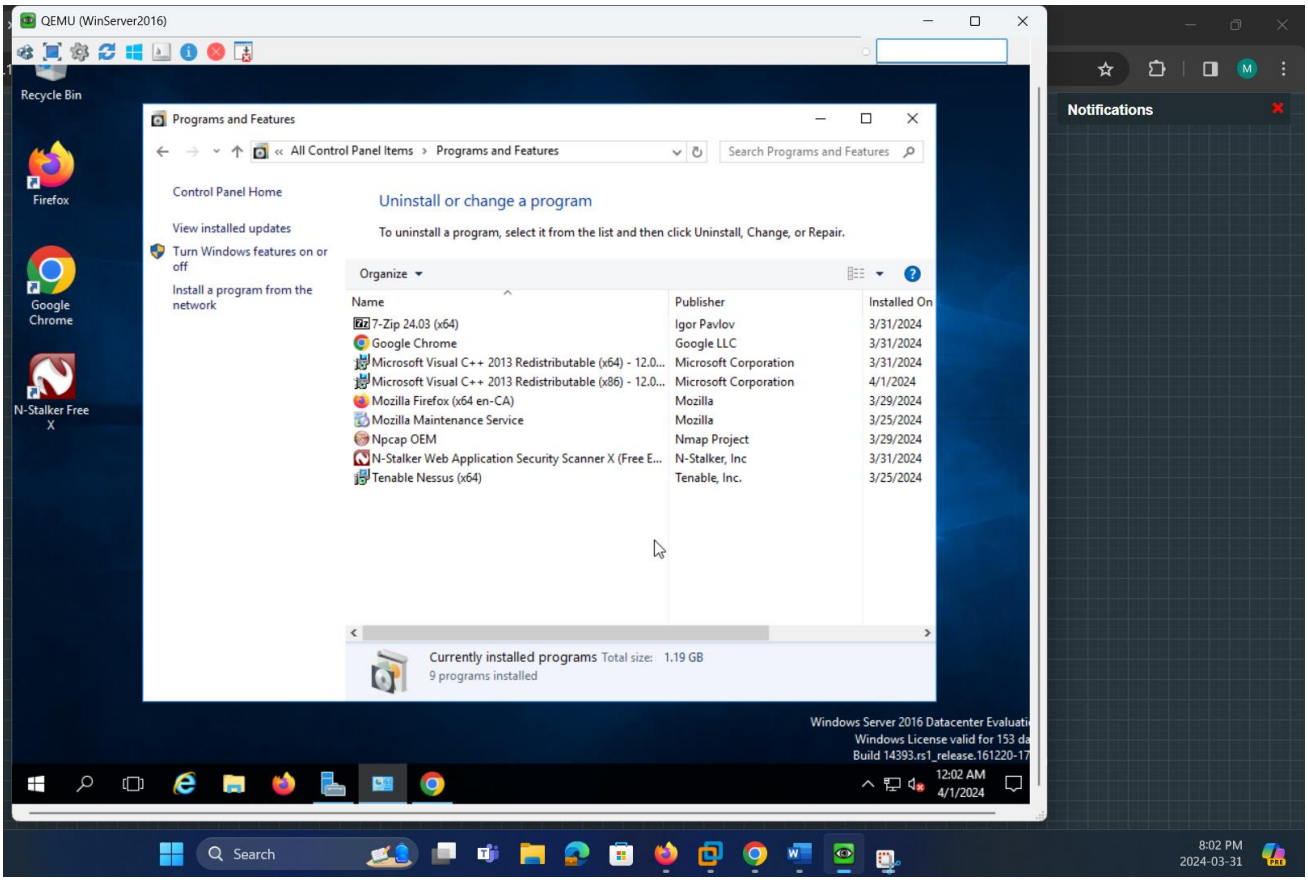

QEMU (WinServer2016)
Downloads
File
Home
Share
View
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Size
1,568 KB
1,345 KB
342 KB
102,164 KB
11,639 KB
11,633 KB
7,033 KB
7 items
N-Stalker Web Application Security Scanner 10.14 (Free Editio...
Choose Install Location
Choose the folder in which to install N-Stalker Web Application Security Scanner.
Setup will install N-Stalker Web Application Security Scanner in the following folder.
To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\N-Stalker\Free X
Browse...
Space required: 25.6MB
Space available: 38.3GB
N-Stalker - The Web Security Specialists
< Back
Install
Cancel
I am trying to update my Quicken 2016 and it will not install the update because ... msvcp120.dll and msvcr120.dll are missing. I have looked at other suggestions about
Applies to:
11:07 PM
3/31/2024
Notifications
Search
7:07 PM
2024-03-31


QEMU (WinServer2016)
Welcome to BadStore
N-Stalker
N-Stalker Free Edition
msvcp120.dll and ms
answers.microsoft.com/en-us/windows/forum/all/msvcp120dll-and-msvcr120dll-are-missing/fd0f051...
Microsoft
Community
Products
Get Started
Buy Microsoft 365
All Microsoft
Manage cookies
Contribute to the Windows for
Top Contributors in Windows 1
Search within Windows
Ask a new question
Kirbywiles
msvcp120.dll and msvcr120.dll are missing
I am trying to update my Quicken 2016 and it will not install the update because ... msvcp120.dll and msvcr120.dll are missing. I have looked at other suggestions about
Last updated March 3, 2024
Views 77,708
Applies to:
N-Stalker Web Application Security Scanner 10.14 (Free Editio...
N-Stalker
Free Edition
Completing the N-Stalker Web Application Security Scanner Setup Wizard
N-Stalker Web Application Security Scanner has been installed on your computer.
Click Finish to close this wizard.
Run N-Stalker Web Application Security Scanner
Show Readme
< Back
Finish
Cancel
Notifications
11:08 PM
3/31/2024
Sunday, March 31, 2024
Search
7:08 PM
2024-03-31


QEMU (WinServer2016)
Notifications
Application Tools
Downloads
File
Home
Share
View
Manage
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
Name
Date modified
Type
Size
7z2403-x64
3/31/2024 10:51 PM
Application
1,568 KB
1,345 KB
342 KB
102,164 KB
11,639 KB
11,633 KB
7,033 KB
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.406...
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40660
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013
These license terms are an agreement between Microsoft Corporation (or
I agree to the license terms and conditions
Install
Close
7 items
1 item selected 6.86 MB
8A4E-4043-B330-D0DCE8561EBB/vcredist_x64.exe
11:04 PM
3/31/2024
Search
7:04 PM
2024-03-31

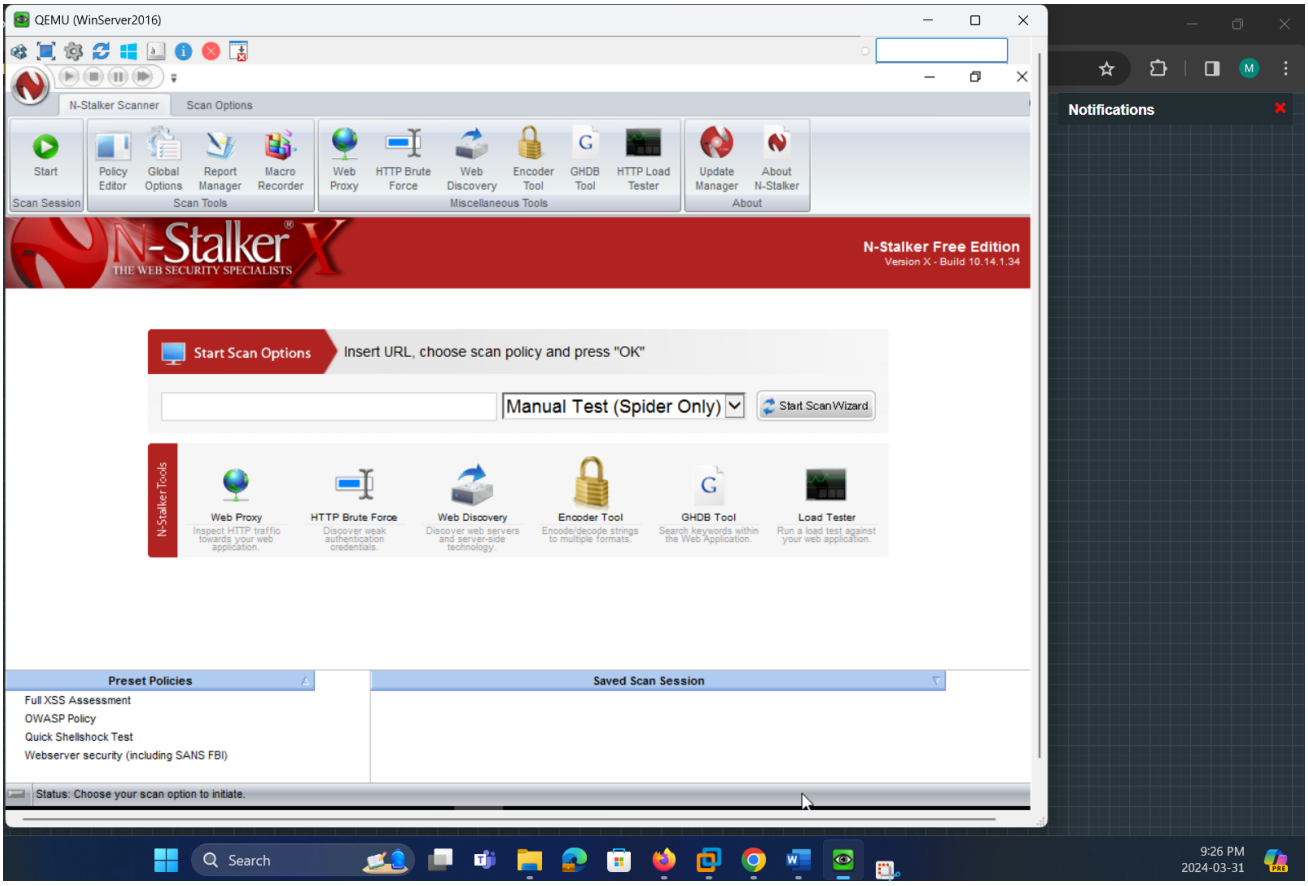

QEMU (WinServer2016)
Notifications
How to Fix the Msvcr120.dll Mi
Update for Visual C++ 2013 an
support.microsoft.com/en-us/topic/update-for-visual-c-2013-and-visual-c-redistributable-package-5...
x86.exe File
Locales
Czech - C
Republic
German -
English -
States
Spanish(t
Sorts) - Sp
French - F
Application Tools
Downloads
File
Home
Share
View
Manage
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
1,568 KB
1,345 KB
342 KB
102,164 KB
11,639 KB
11,633 KB
7,033 KB
6,358 KB
8 items
1 item selected 6.20 MB
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.406...
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40660
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013
These license terms are an agreement between Microsoft Corporation (or
I agree to the license terms and conditions
Install
Close
Search
8:00 PM
2024-03-31

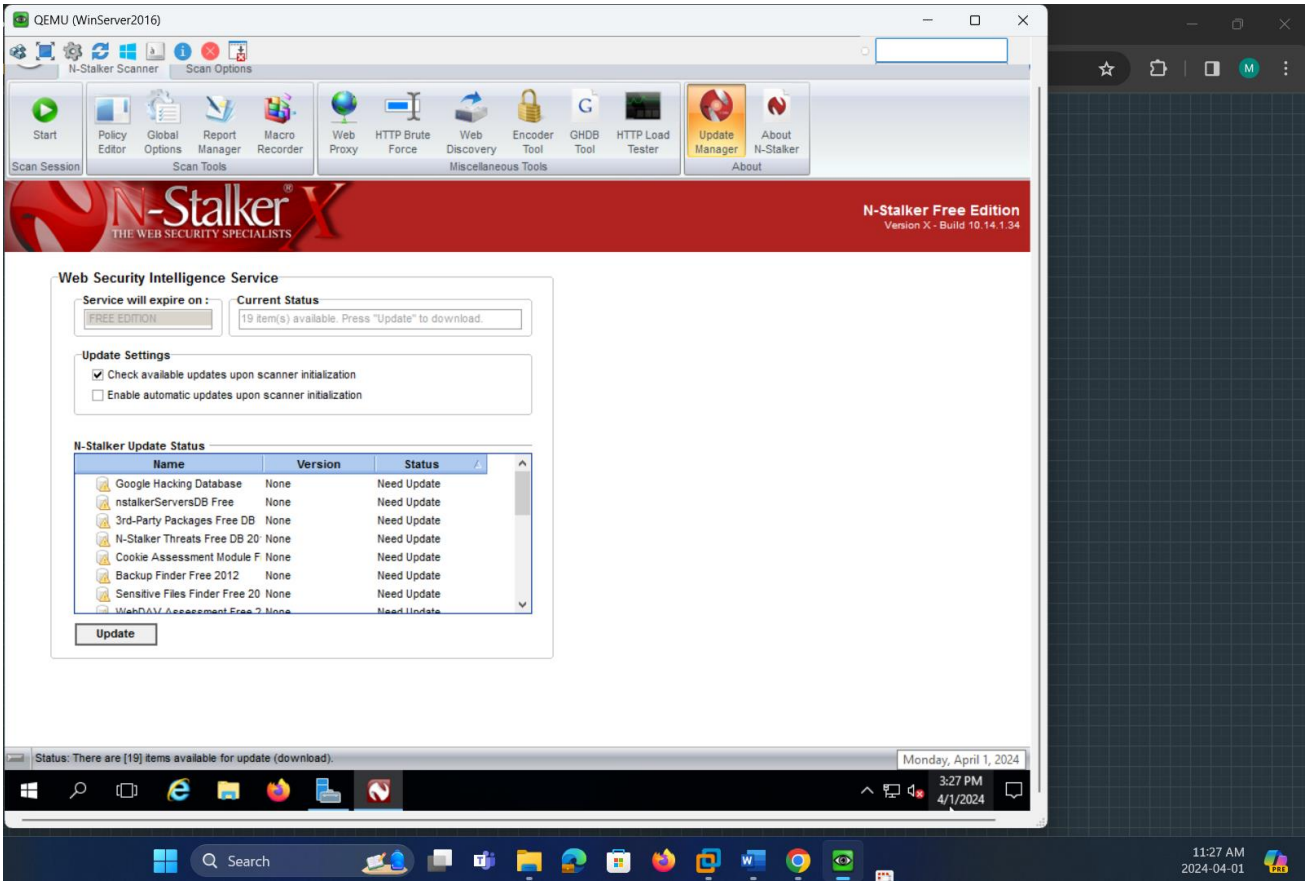

QEMU (WinServer2016)
How to Fix the Msvcr120.dll Mi
Update for Visual C++ 2013 an
support.microsoft.com/en-us/topic/update-for-visual-c-2013-and-visual-c-redistributable-package-5...
Notifications
x86.exe File
Locales
Czech - C
Republic
German -
English -
States
Spanish(tr
Sorts) - Sp
French - F
Application Tools
Downloads
File
Home
Share
View
Manage
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Network
1,568 KB
1,345 KB
342 KB
102,164 KB
11,639 KB
11,633 KB
7,033 KB
6,358 KB
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.406...
Microsoft Visual C++ 2013
Redistributable (x86) - 12.0.40660
Setup Successful
Close
8 items
1 item selected 6.20 MB
Search
8:00 PM
2024-03-31

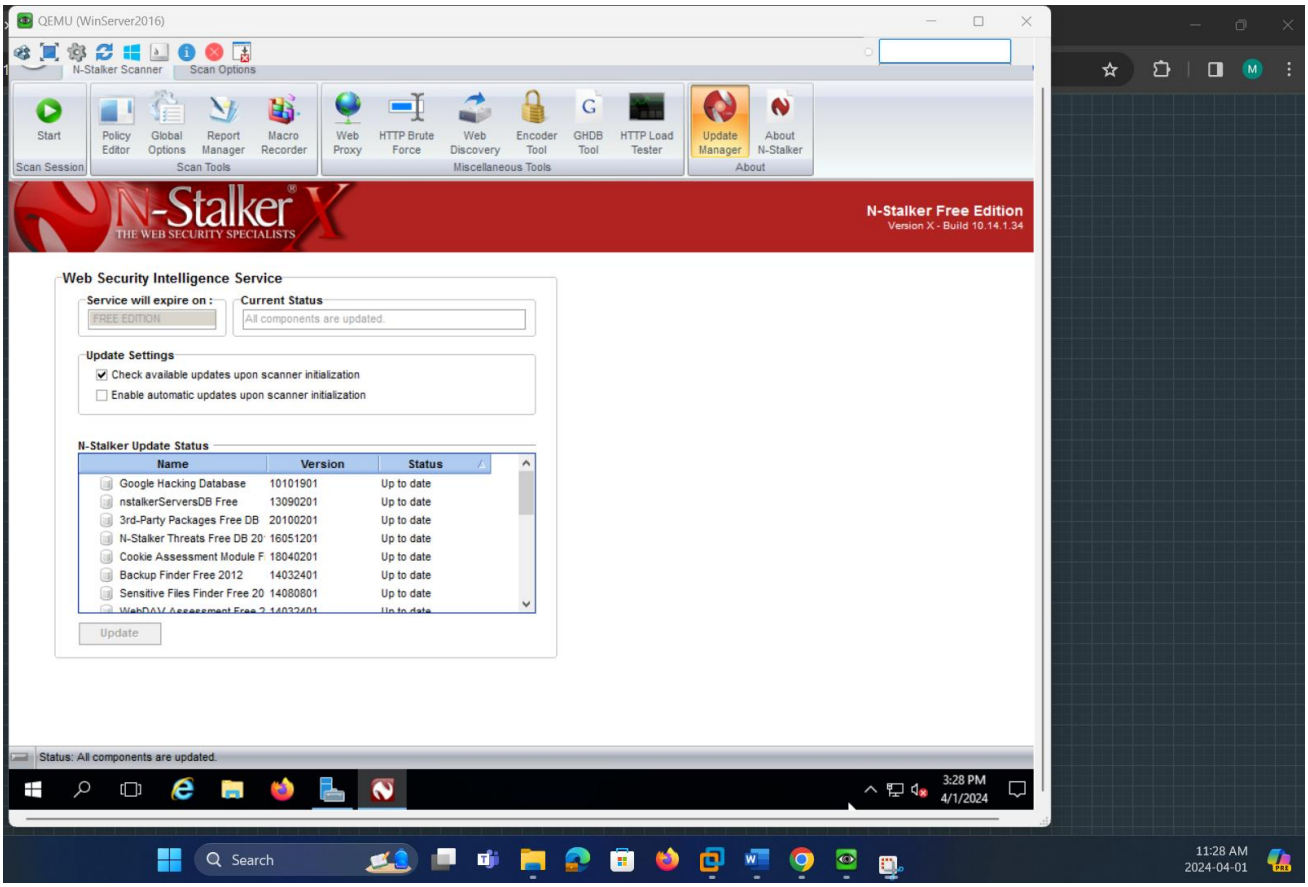


Installed required Visual C++ 2013 and Visual C++ Redistributable Packages x64 and x68 for Windows 2016 Server VM.

3. Running and Configuring N-Stalker Application in Windows 2016 Server VM

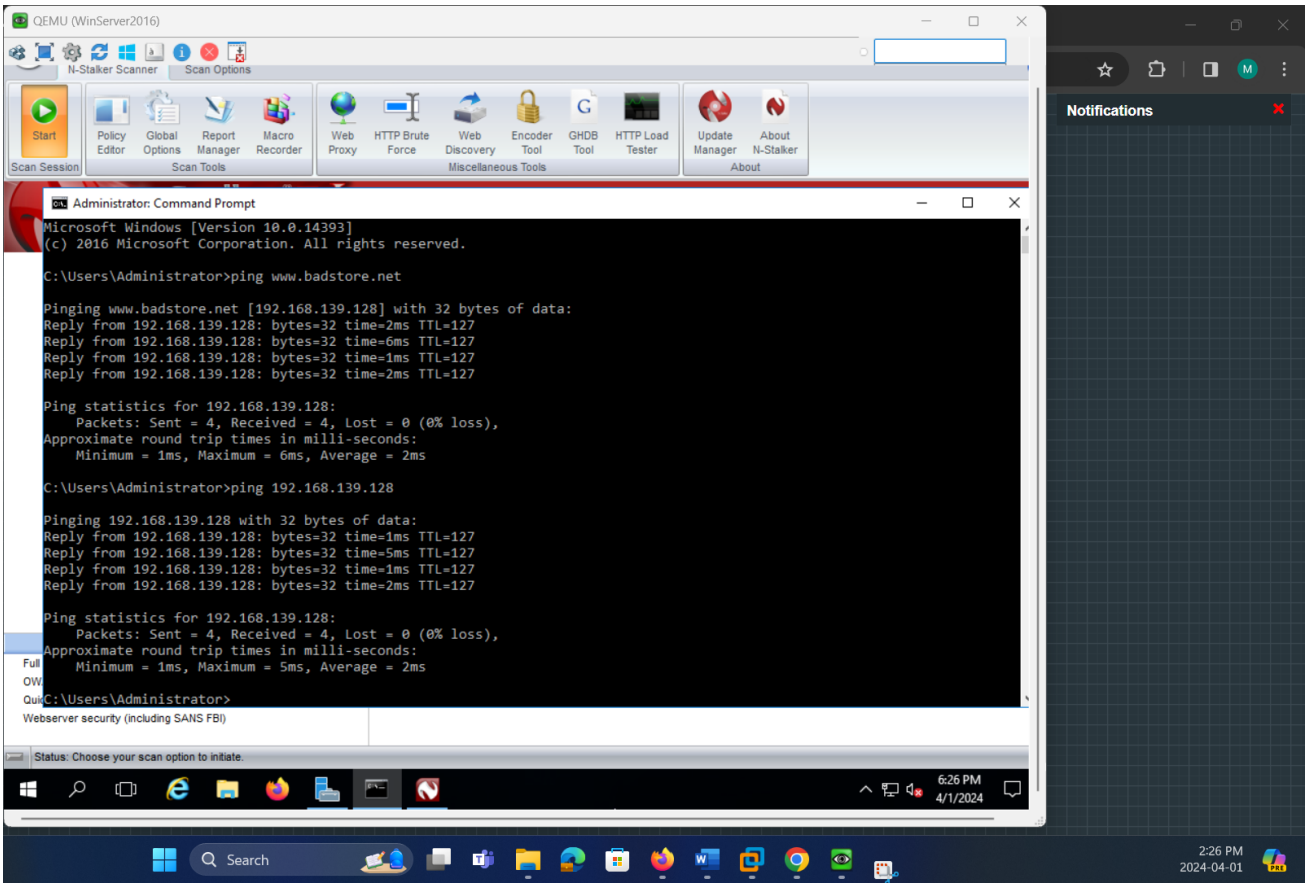

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Policy Editor
Global Options
Report Manager
Macro Recorder
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Update Manager
About N-Stalker
Scan Session
Scan Tools
Miscellaneous Tools
About
N-Stalker X
THE WEB SECURITY SPECIALISTS
N-Stalker Free Edition
Version X - Build 10.14.1.34
Start Scan Options
Insert URL, choose scan policy and press "OK"
Manual Test (Spider Only)
Start Scan Wizard
N-Stalker Tools
Web Proxy
Inspect HTTP traffic towards your web application.
HTTP Brute Force
Discover weak authentication credentials.
Web Discovery
Discover web servers and server-side technology.
Encoder Tool
Encode/decode strings to multiple formats.
GHDB Tool
Search keywords within the Web Application.
Load Tester
Run a load test against your web application.
Preset Policies
Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)
Saved Scan Session
Status: Choose your scan option to initiate.
Notifications
Search
9:26 PM
2024-03-31

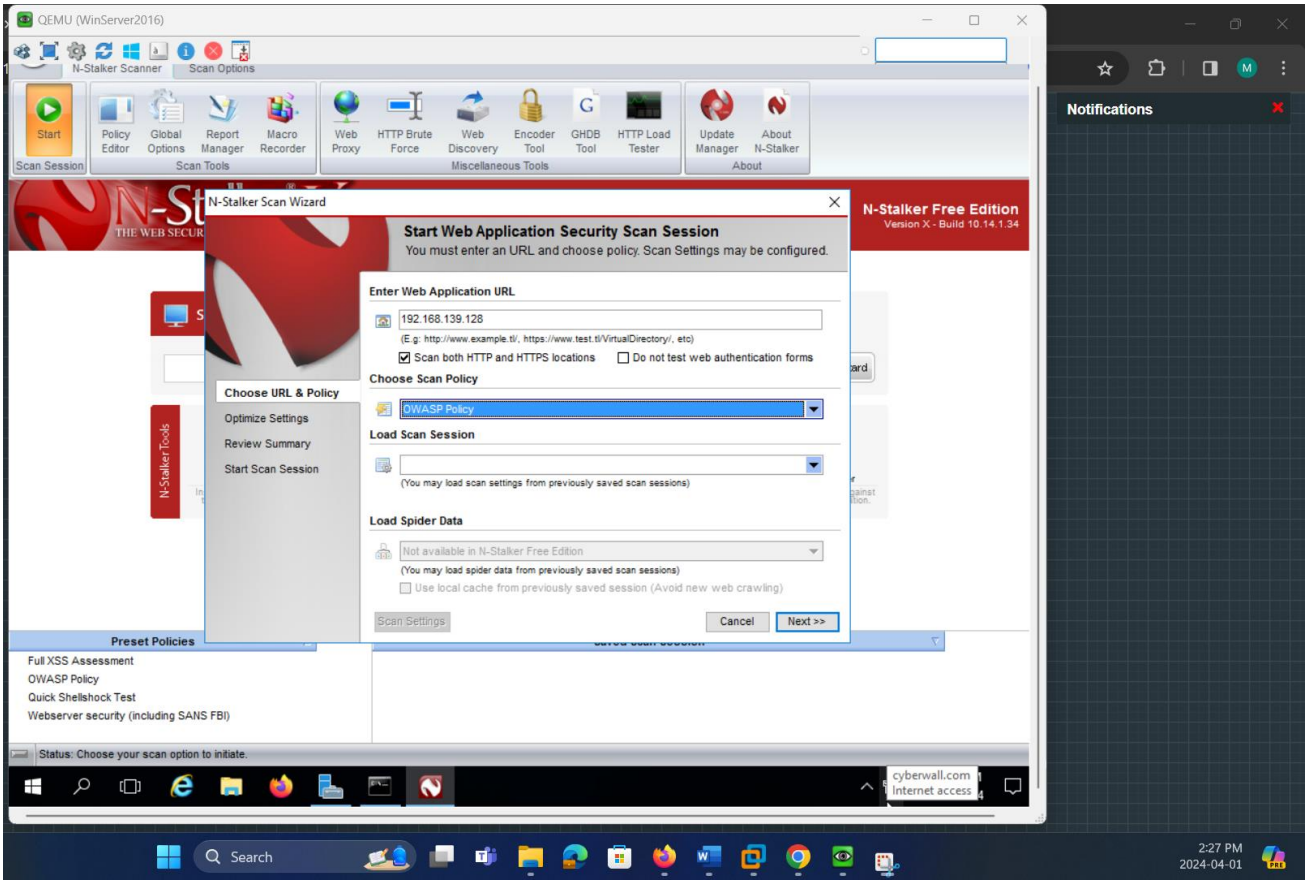

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Scan Session
Policy Editor
Global Options
Report Manager
Macro Recorder
Scan Tools
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Miscellaneous Tools
Update Manager
About N-Stalker
About
N-Stalker X
THE WEB SECURITY SPECIALISTS
N-Stalker Free Edition
Version X - Build 10.14.1.34
Web Security Intelligence Service
Service will expire on :
FREE EDITION
Current Status
19 item(s) available. Press "Update" to download.
Update Settings
Check available updates upon scanner initialization
Enable automatic updates upon scanner initialization
N-Stalker Update Status
Name
Version
Status
Google Hacking Database None Need Update
nstalkerServersDB Free None Need Update
3rd-Party Packages Free DB None Need Update
N-Stalker Threats Free DB 20 None Need Update
Cookie Assessment Module F None Need Update
Backup Finder Free 2012 None Need Update
Sensitive Files Finder Free 20 None Need Update
Update
Status: There are [19] items available for update (download).
Monday, April 1, 2024
3:27 PM
4/1/2024
Search
11:27 AM
2024-04-01

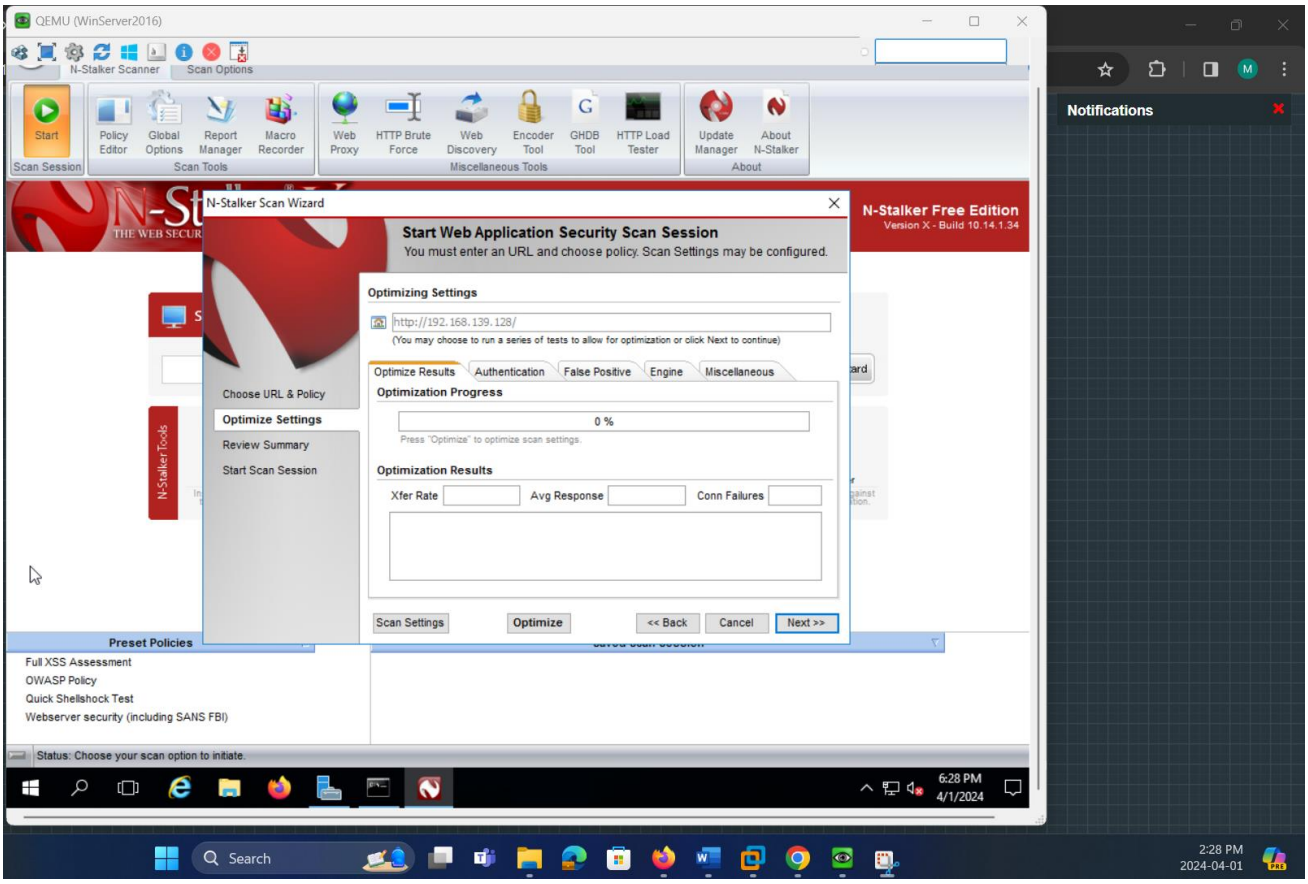


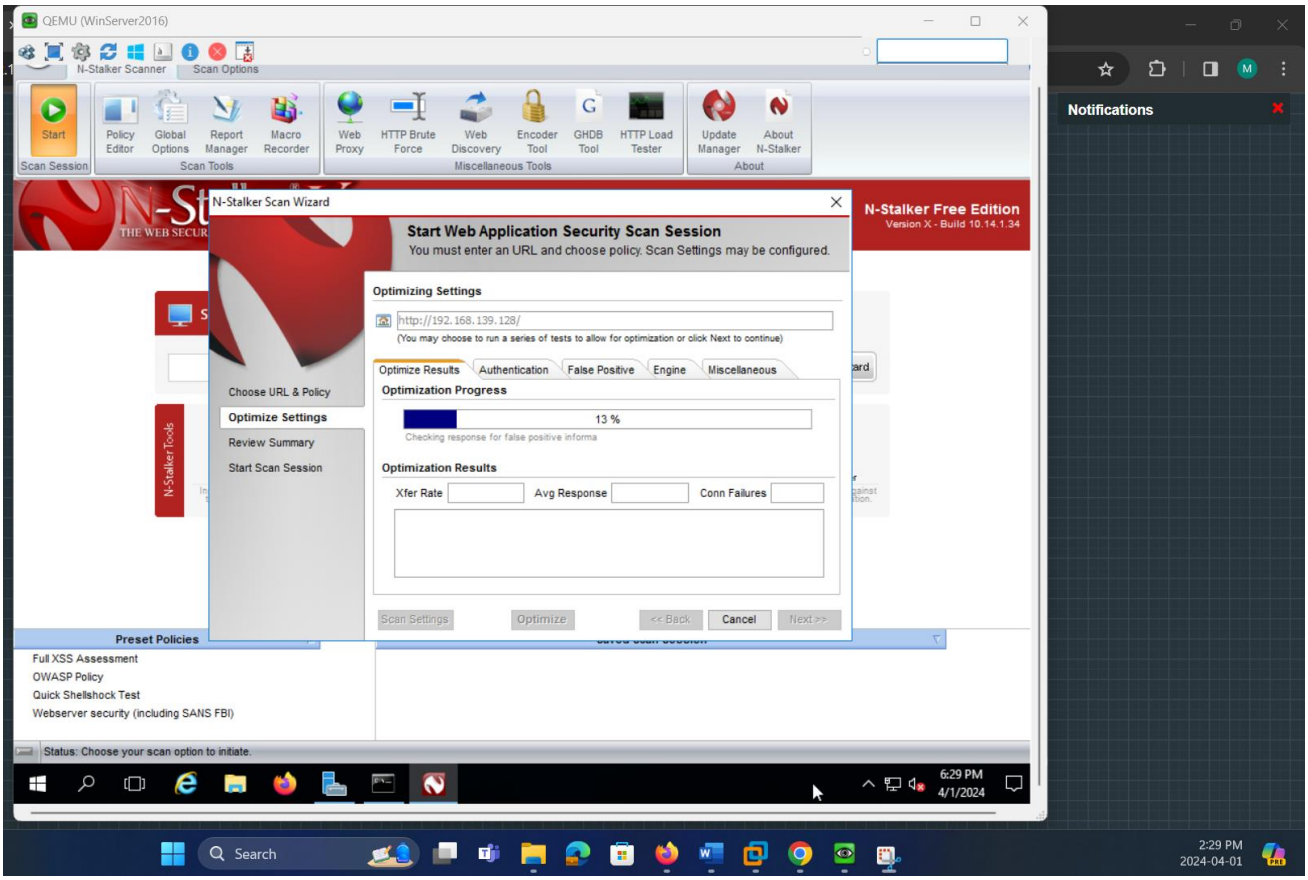
Updated Manager for Required Files and N-Stalker Updates

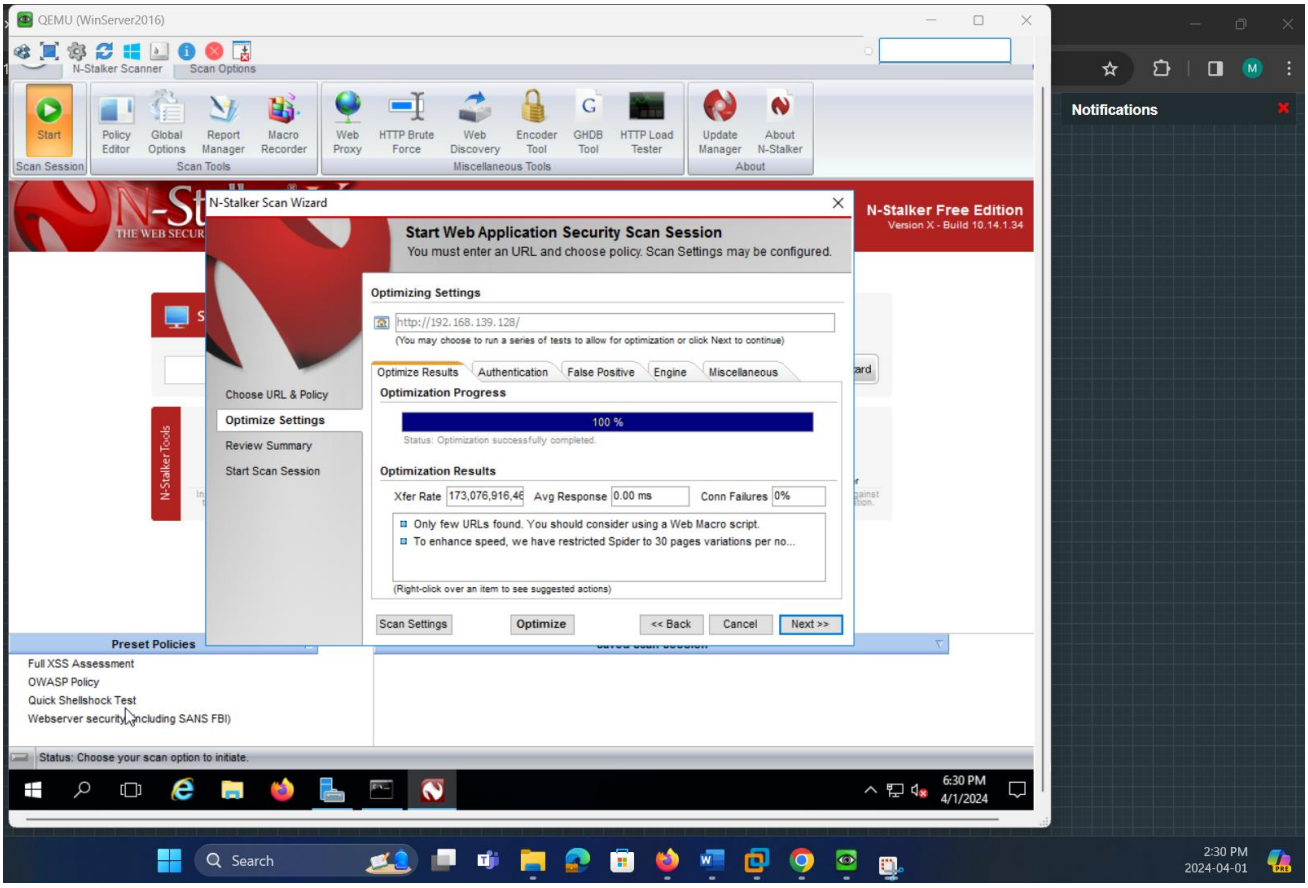
4. **Scanning www.badstore.net**

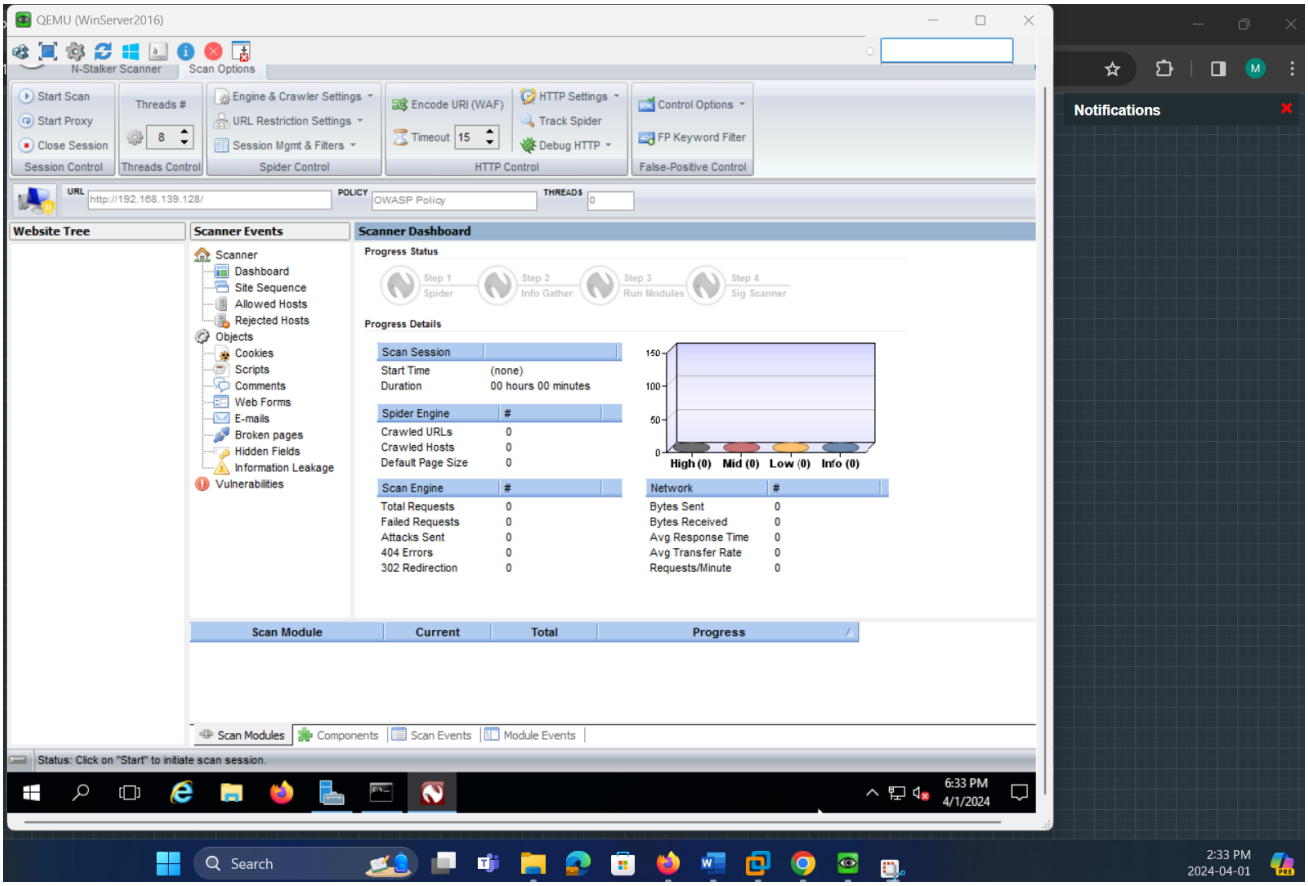

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Scan Session
Policy Editor
Global Options
Report Manager
Macro Recorder
Scan Tools
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Miscellaneous Tools
Update Manager
About N-Stalker
About
Notifications
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping www.badstore.net
Pinging www.badstore.net [192.168.139.128] with 32 bytes of data:
Reply from 192.168.139.128: bytes=32 time=2ms TTL=127
Reply from 192.168.139.128: bytes=32 time=6ms TTL=127
Reply from 192.168.139.128: bytes=32 time=1ms TTL=127
Reply from 192.168.139.128: bytes=32 time=2ms TTL=127
Ping statistics for 192.168.139.128:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 6ms, Average = 2ms
C:\Users\Administrator>ping 192.168.139.128
Pinging 192.168.139.128 with 32 bytes of data:
Reply from 192.168.139.128: bytes=32 time=1ms TTL=127
Reply from 192.168.139.128: bytes=32 time=5ms TTL=127
Reply from 192.168.139.128: bytes=32 time=1ms TTL=127
Reply from 192.168.139.128: bytes=32 time=2ms TTL=127
Ping statistics for 192.168.139.128:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\Administrator>
Webserver security (including SANS FBI)
Status: Choose your scan option to initiate.
6:26 PM
4/1/2024
Search
2:26 PM
2024-04-01

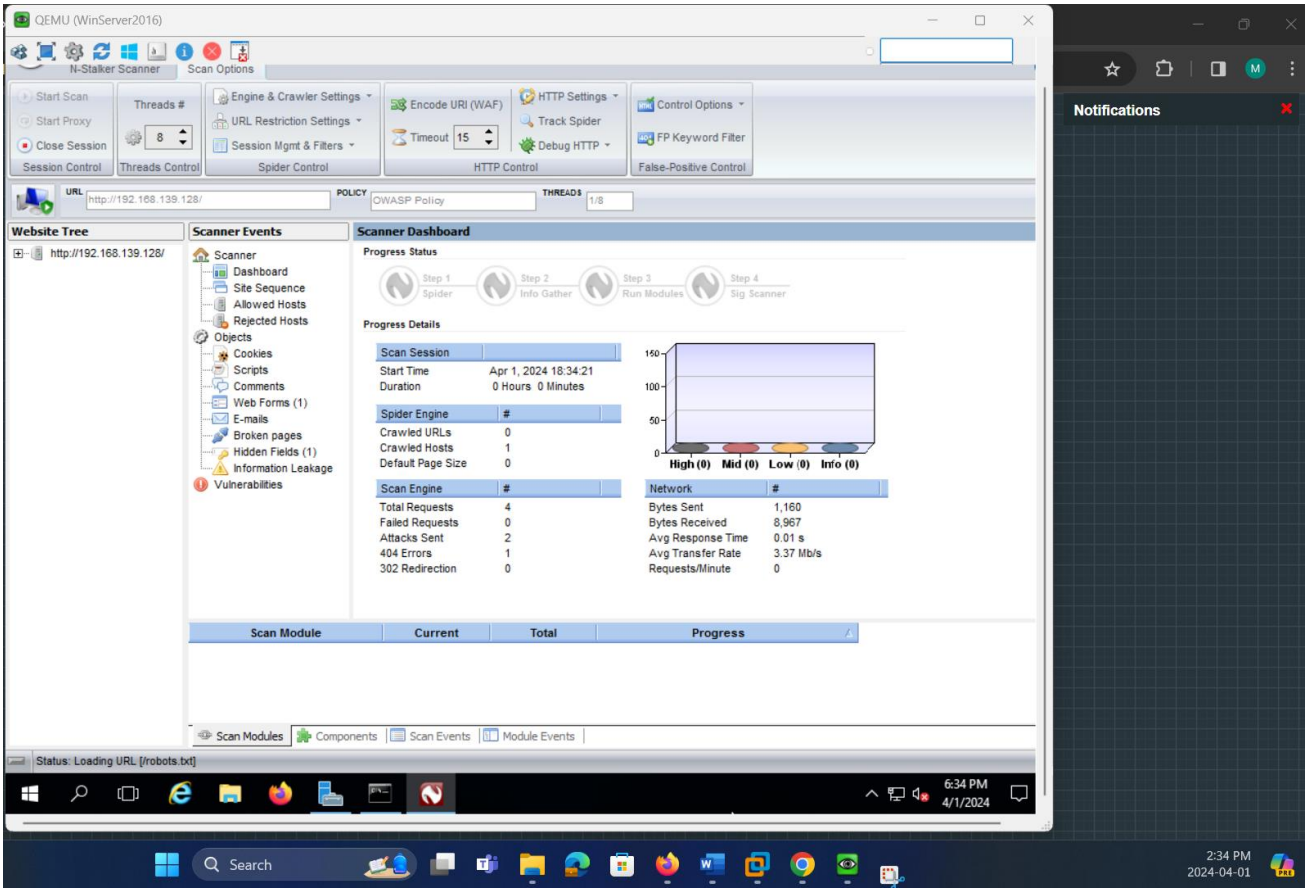

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Scan Session
Policy Editor
Global Options
Report Manager
Macro Recorder
Scan Tools
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Miscellaneous Tools
Update Manager
About N-Stalker
About
Notifications
N-Stalker Free Edition
Version X - Build 10.14.1.34
N-Stalker Scan Wizard
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.
Enter Web Application URL
192.168.139.128
(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)
Scan both HTTP and HTTPS locations
Do not test web authentication forms
Choose Scan Policy
OWASP Policy
Load Scan Session
(You may load scan settings from previously saved scan sessions)
Load Spider Data
Not available in N-Stalker Free Edition
(You may load spider data from previously saved scan sessions)
Use local cache from previously saved session (Avoid new web crawling)
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
Scan Settings
Cancel
Next >>
N-Stalker Tools
Preset Policies
Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)
Status: Choose your scan option to initiate.
cyberwall.com
Internet access
Search
2:27 PM
2024-04-01

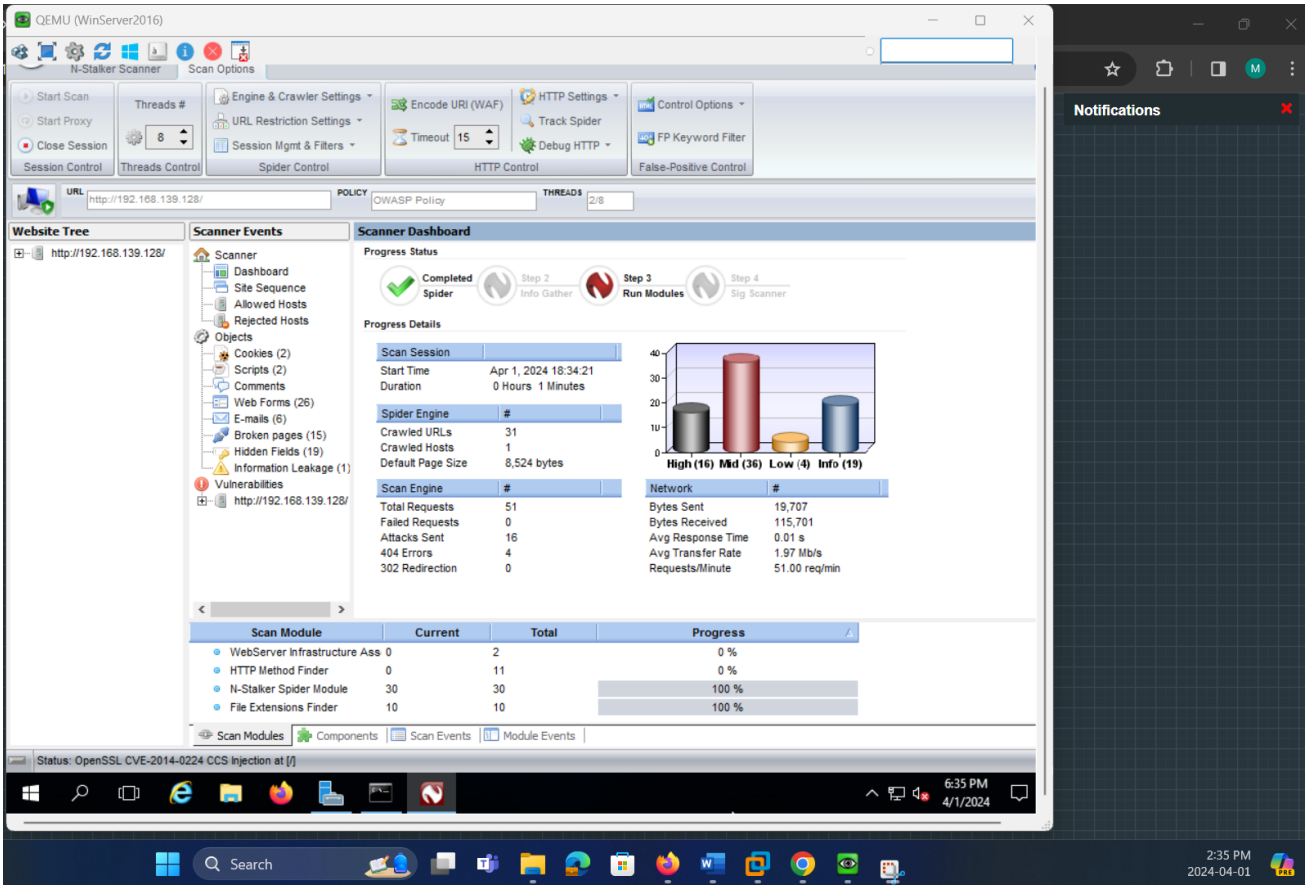

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Scan Session
Policy Editor
Global Options
Report Manager
Macro Recorder
Scan Tools
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Miscellaneous Tools
Update Manager
About N-Stalker
About
Notifications
N-Stalker Scan Wizard
N-Stalker Free Edition
Version X - Build 10.14.1.34
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.
Optimizing Settings
http://192.168.139.128/
(You may choose to run a series of tests to allow for optimization or click Next to continue)
Optimize Results
Authentication
False Positive
Engine
Miscellaneous
Optimization Progress
0 %
Press "Optimize" to optimize scan settings.
Optimization Results
Xfer Rate
Avg Response
Conn Failures
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
N-Stalker Tools
Scan Settings
Optimize
<< Back
Cancel
Next >>
Preset Policies
Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)
Status: Choose your scan option to initiate.
6:28 PM
4/1/2024
Search
2:28 PM
2024-04-01

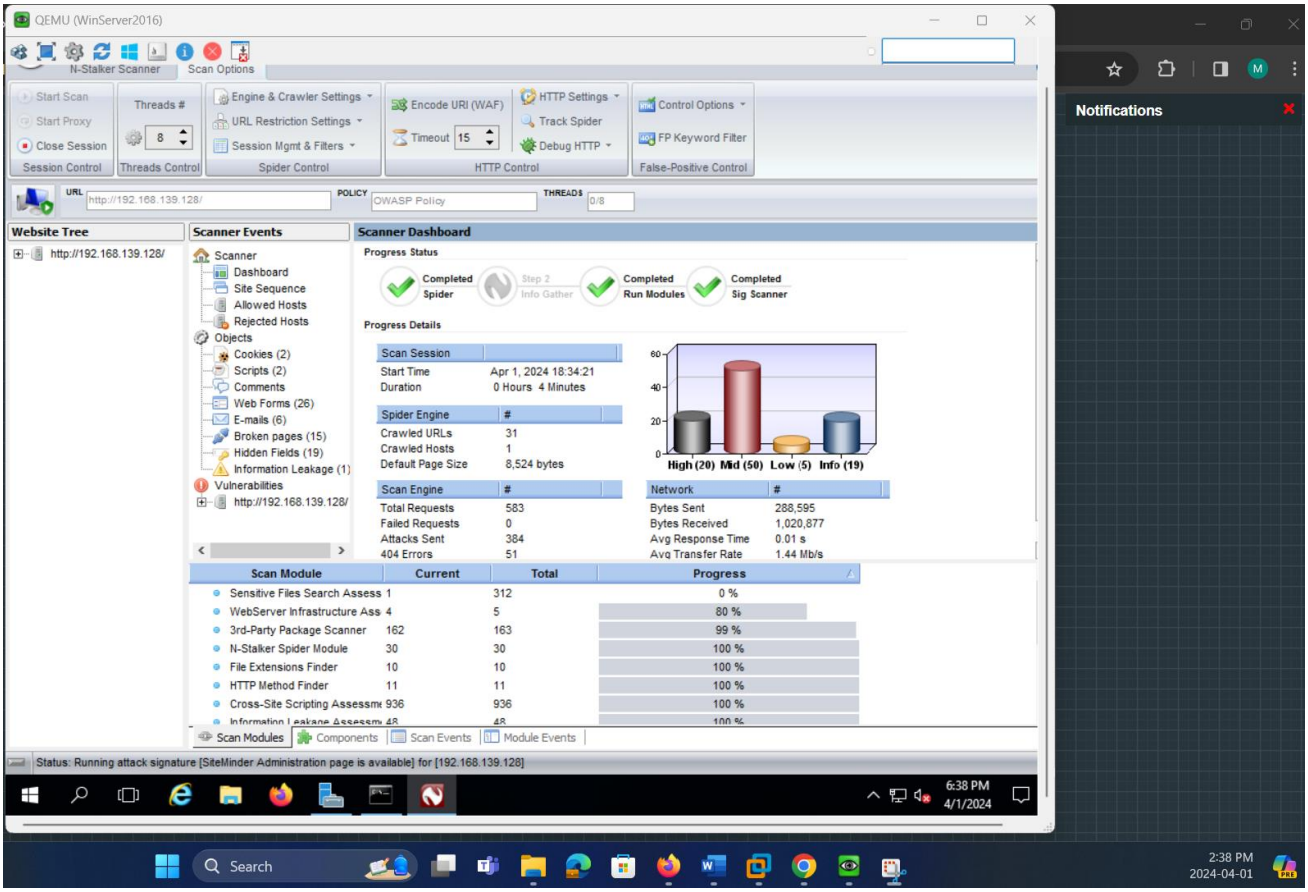

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Scan Session
Policy Editor
Global Options
Report Manager
Macro Recorder
Scan Tools
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Miscellaneous Tools
Update Manager
About N-Stalker
About
Notifications
N-Stalker Free Edition
Version X - Build 10.14.1.34
N-Stalker Scan Wizard
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.
Optimizing Settings
http://192.168.139.128/
(You may choose to run a series of tests to allow for optimization or click Next to continue)
Optimize Results
Authentication
False Positive
Engine
Miscellaneous
Optimization Progress
13 %
Checking response for false positive informa
Optimization Results
Xfer Rate
Avg Response
Conn Failures
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
Scan Settings
Optimize
<< Back
Cancel
Next >>
N-Stalker Tools
Preset Policies
Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)
Status: Choose your scan option to initiate.
6:29 PM
4/1/2024
Search
2:29 PM
2024-04-01

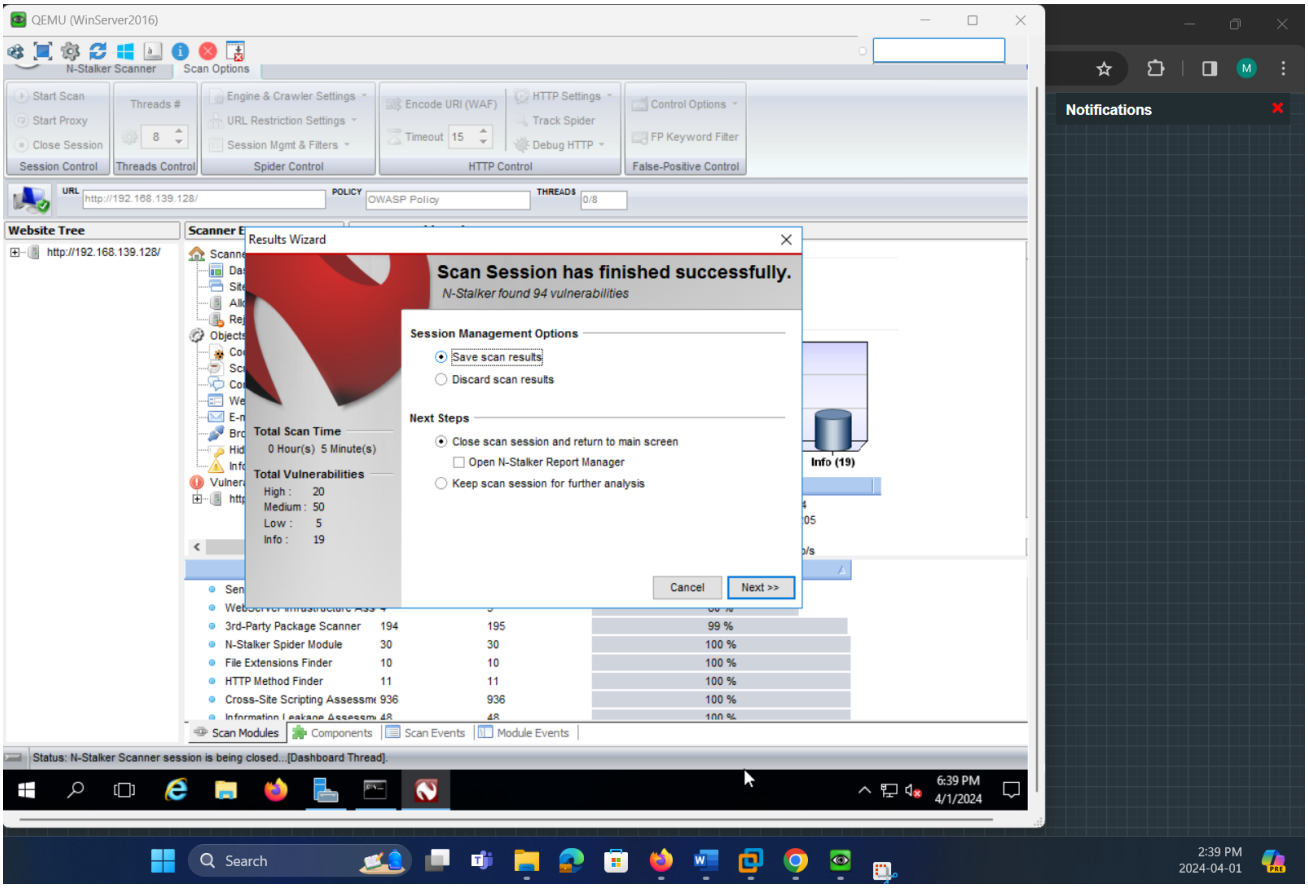

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Scan Session
Policy Editor
Global Options
Report Manager
Macro Recorder
Scan Tools
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Miscellaneous Tools
Update Manager
About N-Stalker
About
Notifications
N-Stalker Free Edition
Version X - Build 10.14.1.34
N-Stalker Scan Wizard
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.
Choose URL & Policy
Optimize Settings
Review Summary
Start Scan Session
Optimizing Settings
http://192.168.139.128/
(You may choose to run a series of tests to allow for optimization or click Next to continue)
Optimize Results
Authentication
False Positive
Engine
Miscellaneous
Optimization Progress
100 %
Status: Optimization successfully completed.
Optimization Results
Xfer Rate
173,076,916,46
Avg Response
0.00 ms
Conn Failures
0%
Only few URLs found. You should consider using a Web Macro script.
To enhance speed, we have restricted Spider to 30 pages variations per no...
(Right-click over an item to see suggested actions)
Scan Settings
Optimize
<< Back
Cancel
Next >>
N-Stalker Tools
Preset Policies
Full XSS Assessment
OWASP Policy
Quick Shellshock Test
Webserver security (including SANS FBI)
Status: Choose your scan option to initiate.
6:30 PM
4/1/2024
Search
2:30 PM
2024-04-01

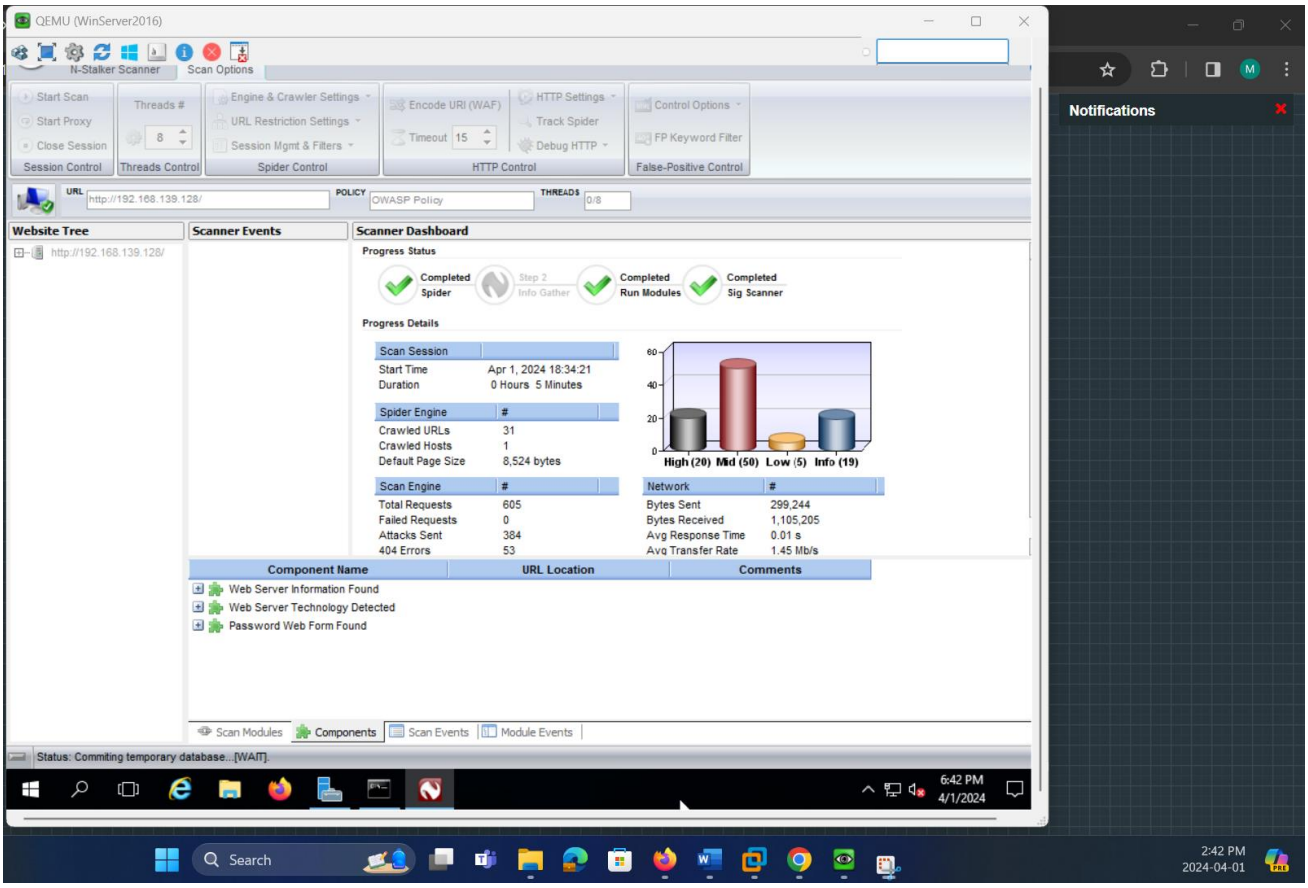

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
8
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
15
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
0
Website Tree
Scanner Events
Scanner Dashboard
Scanner
Dashboard
Site Sequence
Allowed Hosts
Rejected Hosts
Objects
Cookies
Scripts
Comments
Web Forms
E-mails
Broken pages
Hidden Fields
Information Leakage
Vulnerabilities
Progress Status
Step 1 Spider
Step 2 Info Gather
Step 3 Run Modules
Step 4 Sig Scanner
Progress Details
Scan Session
Start Time (none)
Duration 00 hours 00 minutes
Spider Engine #
Crawled URLs 0
Crawled Hosts 0
Default Page Size 0
Scan Engine #
Total Requests 0
Failed Requests 0
Attacks Sent 0
404 Errors 0
302 Redirection 0
150
100
50
0
High (0) Mid (0) Low (0) Info (0)
Network #
Bytes Sent 0
Bytes Received 0
Avg Response Time 0
Avg Transfer Rate 0
Requests/Minute 0
Scan Module
Current
Total
Progress
Scan Modules
Components
Scan Events
Module Events
Status: Click on "Start" to initiate scan session.
6:33 PM
4/1/2024
Notifications
Search
2:33 PM
2024-04-01

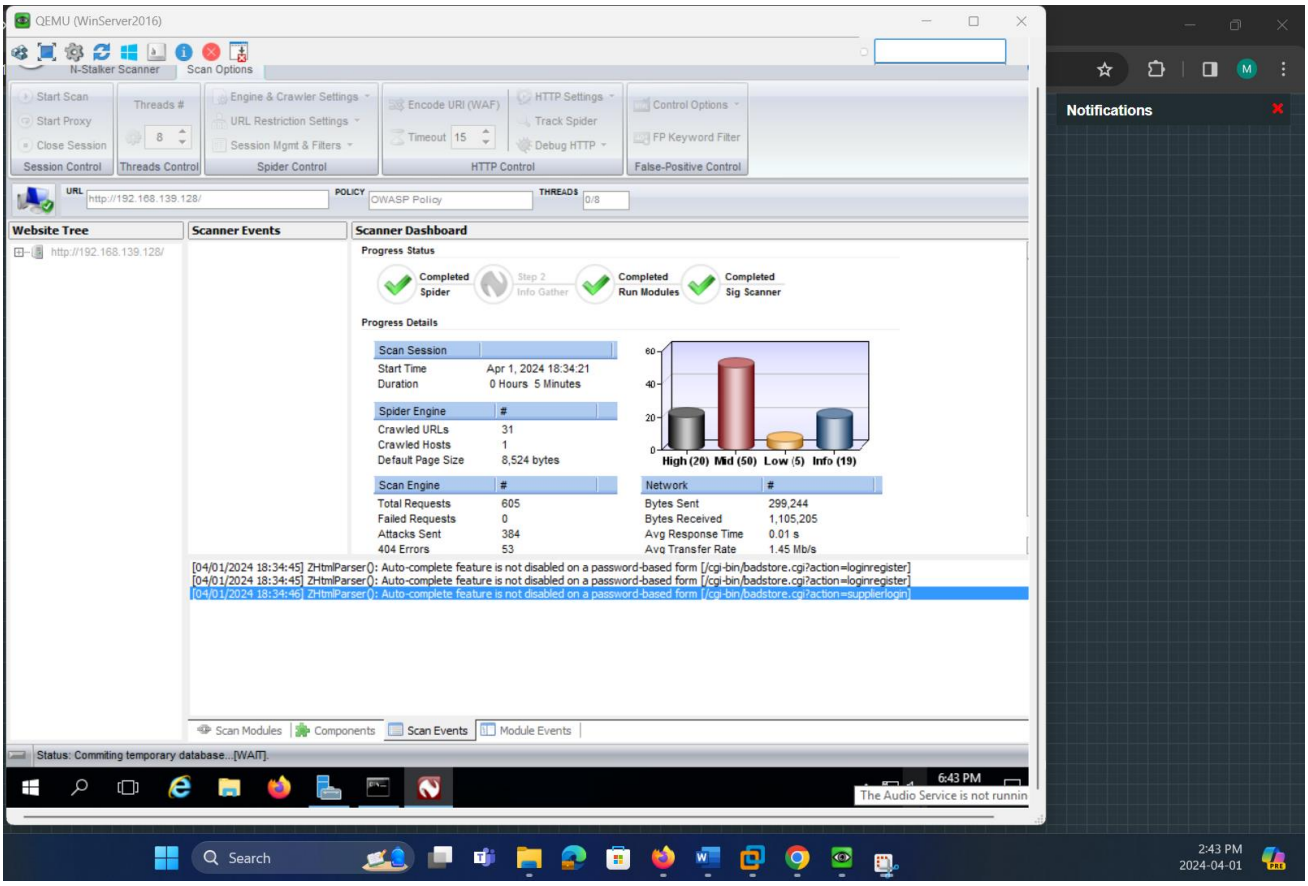

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
8
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout 15
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL http://192.168.139.128/
POLICY OWASP Policy
THREADS 1/8
Website Tree
http://192.168.139.128/
Scanner Events
Scanner
Dashboard
Site Sequence
Allowed Hosts
Rejected Hosts
Objects
Cookies
Scripts
Comments
Web Forms (1)
E-mails
Broken pages
Hidden Fields (1)
Information Leakage
Vulnerabilities
Scanner Dashboard
Progress Status
Step 1 Spider
Step 2 Info Gather
Step 3 Run Modules
Step 4 Sig Scanner
Progress Details
Scan Session
Start Time Apr 1, 2024 18:34:21
Duration 0 Hours 0 Minutes
Spider Engine #
Crawled URLs 0
Crawled Hosts 1
Default Page Size 0
Scan Engine #
Total Requests 4
Failed Requests 0
Attacks Sent 2
404 Errors 1
302 Redirection 0
150
100
50
0
High (0) Mid (0) Low (0) Info (0)
Network #
Bytes Sent 1,160
Bytes Received 8,967
Avg Response Time 0.01 s
Avg Transfer Rate 3.37 Mb/s
Requests/Minute 0
Scan Module
Current
Total
Progress
Scan Modules
Components
Scan Events
Module Events
Status: Loading URL [/robots.txt]
6:34 PM
4/1/2024
Notifications
Search
2:34 PM
2024-04-01

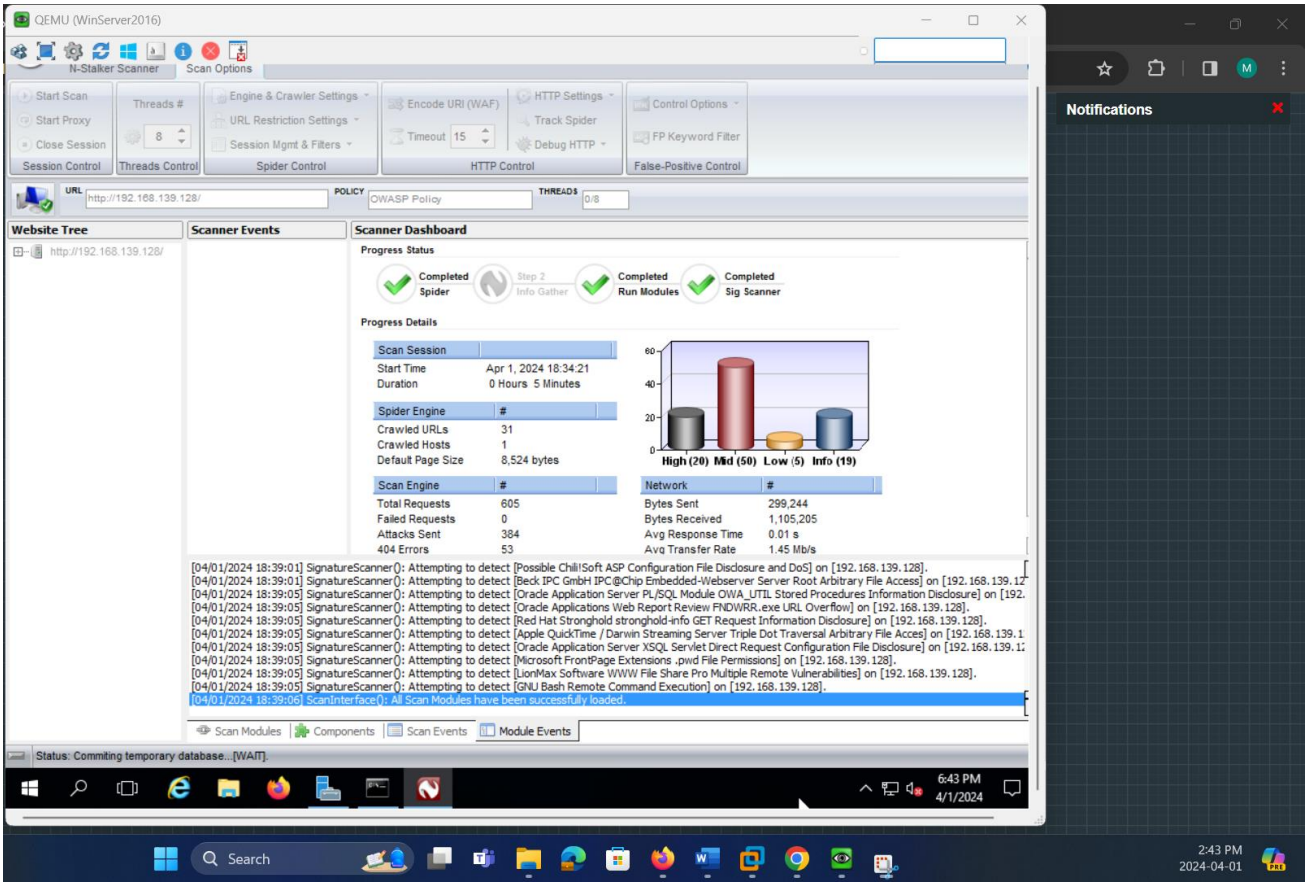

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
8
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
15
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
2/8
Website Tree
http://192.168.139.128/
Scanner Events
Scanner
Dashboard
Site Sequence
Allowed Hosts
Rejected Hosts
Objects
Cookies (2)
Scripts (2)
Comments
Web Forms (26)
E-mails (6)
Broken pages (15)
Hidden Fields (19)
Information Leakage (1)
Vulnerabilities
http://192.168.139.128/
Scanner Dashboard
Progress Status
Completed
Spider
Step 2
Info Gather
Step 3
Run Modules
Step 4
Sig Scanner
Progress Details
Scan Session
Start Time
Apr 1, 2024 18:34:21
Duration
0 Hours 1 Minutes
Spider Engine
#
Crawled URLs
31
Crawled Hosts
1
Default Page Size
8,524 bytes
Scan Engine
#
Total Requests
51
Failed Requests
0
Attacks Sent
16
404 Errors
4
302 Redirection
0
High (16) Mid (36) Low (4) Info (19)
Network
#
Bytes Sent
19,707
Bytes Received
115,701
Avg Response Time
0.01 s
Avg Transfer Rate
1.97 Mb/s
Requests/Minute
51.00 req/min
Scan Module
Current
Total
Progress
WebServer Infrastructure Ass
0
2
0 %
HTTP Method Finder
0
11
0 %
N-Stalker Spider Module
30
30
100 %
File Extensions Finder
10
10
100 %
Scan Modules
Components
Scan Events
Module Events
Status: OpenSSL CVE-2014-0224 CCS Injection at [/]
6:35 PM
4/1/2024
Notifications
Search
2:35 PM
2024-04-01

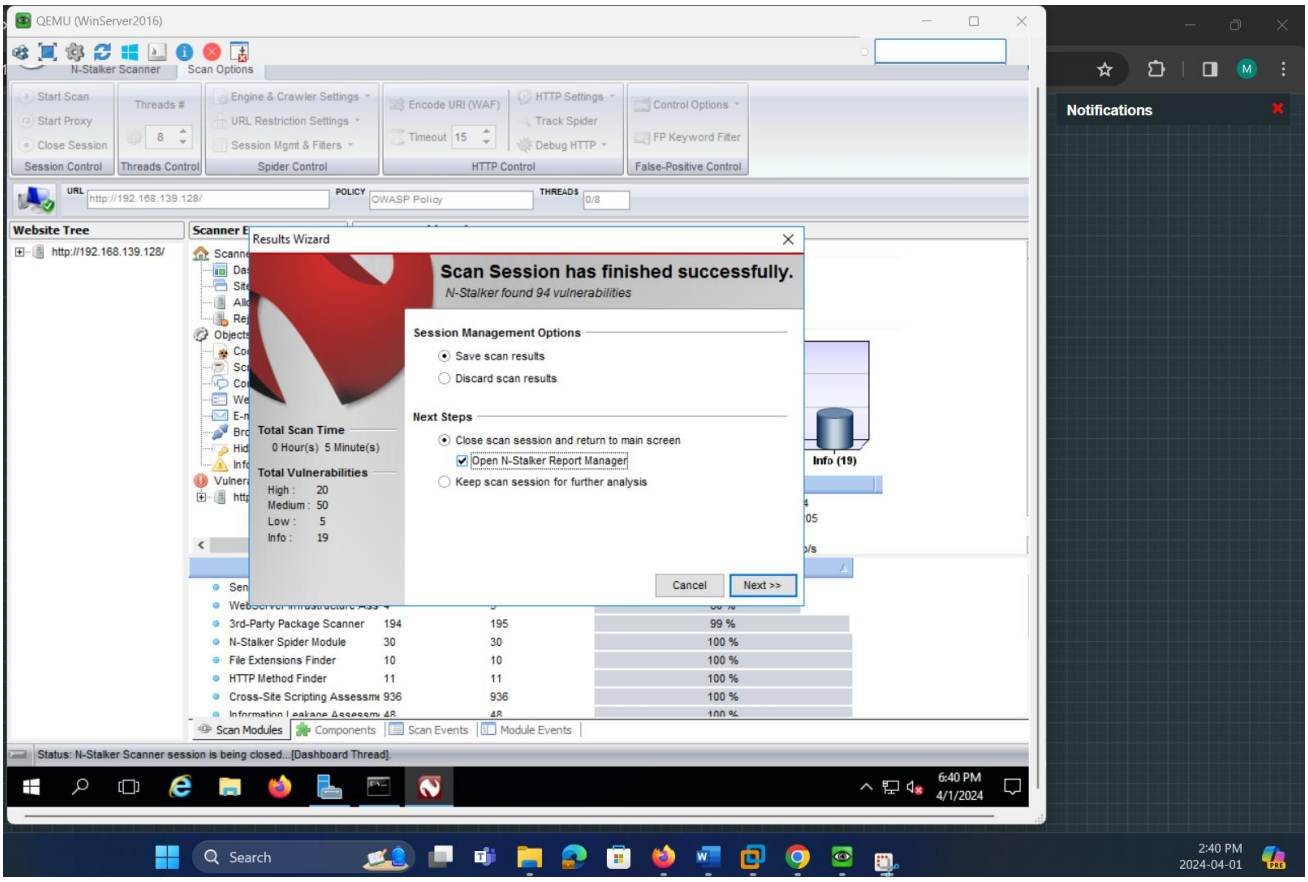

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
8
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout 15
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL http://192.168.139.128/
POLICY OWASP Policy
THREADS 0/8
Website Tree
http://192.168.139.128/
Scanner Events
Scanner
Dashboard
Site Sequence
Allowed Hosts
Rejected Hosts
Objects
Cookies (2)
Scripts (2)
Comments
Web Forms (26)
E-mails (6)
Broken pages (15)
Hidden Fields (19)
Information Leakage (1)
Vulnerabilities
http://192.168.139.128/
Scanner Dashboard
Progress Status
Completed Spider
Step 2 Info Gather
Completed Run Modules
Completed Sig Scanner
Progress Details
Scan Session
Start Time Apr 1, 2024 18:34:21
Duration 0 Hours 4 Minutes
Spider Engine #
Crawled URLs 31
Crawled Hosts 1
Default Page Size 8,524 bytes
Scan Engine #
Total Requests 583
Failed Requests 0
Attacks Sent 384
404 Errors 51
High (20) Mid (50) Low (5) Info (19)
Network #
Bytes Sent 288,595
Bytes Received 1,020,877
Avg Response Time 0.01 s
Avg Transfer Rate 1.44 Mb/s
Scan Module Current Total Progress
Sensitive Files Search Assess 1 312 0 %
WebServer Infrastructure Ass 4 5 80 %
3rd-Party Package Scanner 162 163 99 %
N-Stalker Spider Module 30 30 100 %
File Extensions Finder 10 10 100 %
HTTP Method Finder 11 11 100 %
Cross-Site Scripting Assessm 936 936 100 %
Scan Modules
Components
Scan Events
Module Events
Status: Running attack signature [SiteMinder Administration page is available] for [192.168.139.128]
6:38 PM
4/1/2024
Notifications
Search
2:38 PM
2024-04-01

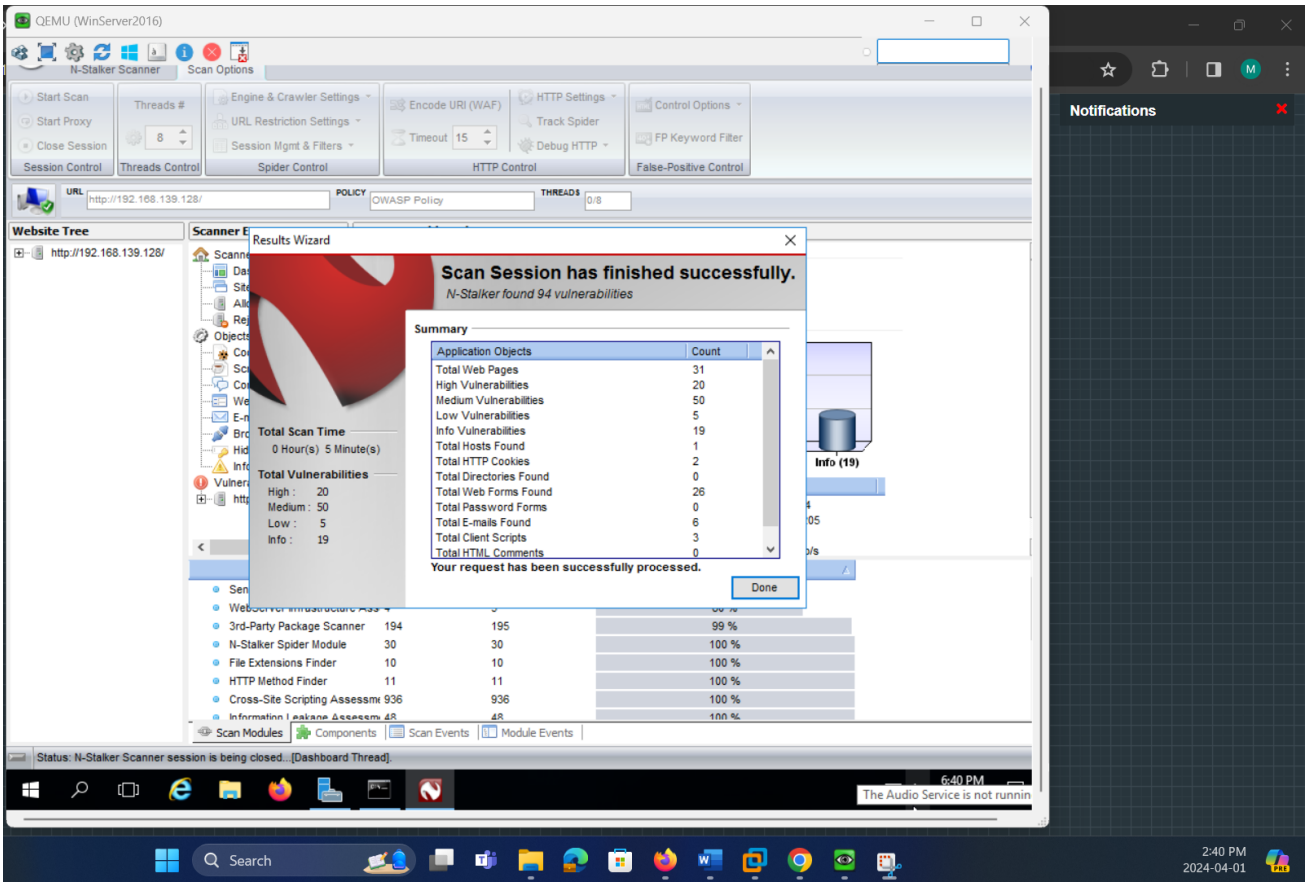

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
Website Tree
http://192.168.139.128/
Results Wizard
Scan Session has finished successfully.
N-Stalker found 94 vulnerabilities
Session Management Options
Save scan results
Discard scan results
Next Steps
Close scan session and return to main screen
Open N-Stalker Report Manager
Keep scan session for further analysis
Total Scan Time
0 Hour(s) 5 Minute(s)
Total Vulnerabilities
High : 20
Medium : 50
Low : 5
Info : 19
Cancel
Next >>
Info (19)
3rd-Party Package Scanner 194 195 99 %
N-Stalker Spider Module 30 30 100 %
File Extensions Finder 10 10 100 %
HTTP Method Finder 11 11 100 %
Cross-Site Scripting Assessm 936 936 100 %
Scan Modules
Components
Scan Events
Module Events
Status: N-Stalker Scanner session is being closed...[Dashboard Thread].
6:39 PM
4/1/2024
Notifications
Search
2:39 PM
2024-04-01

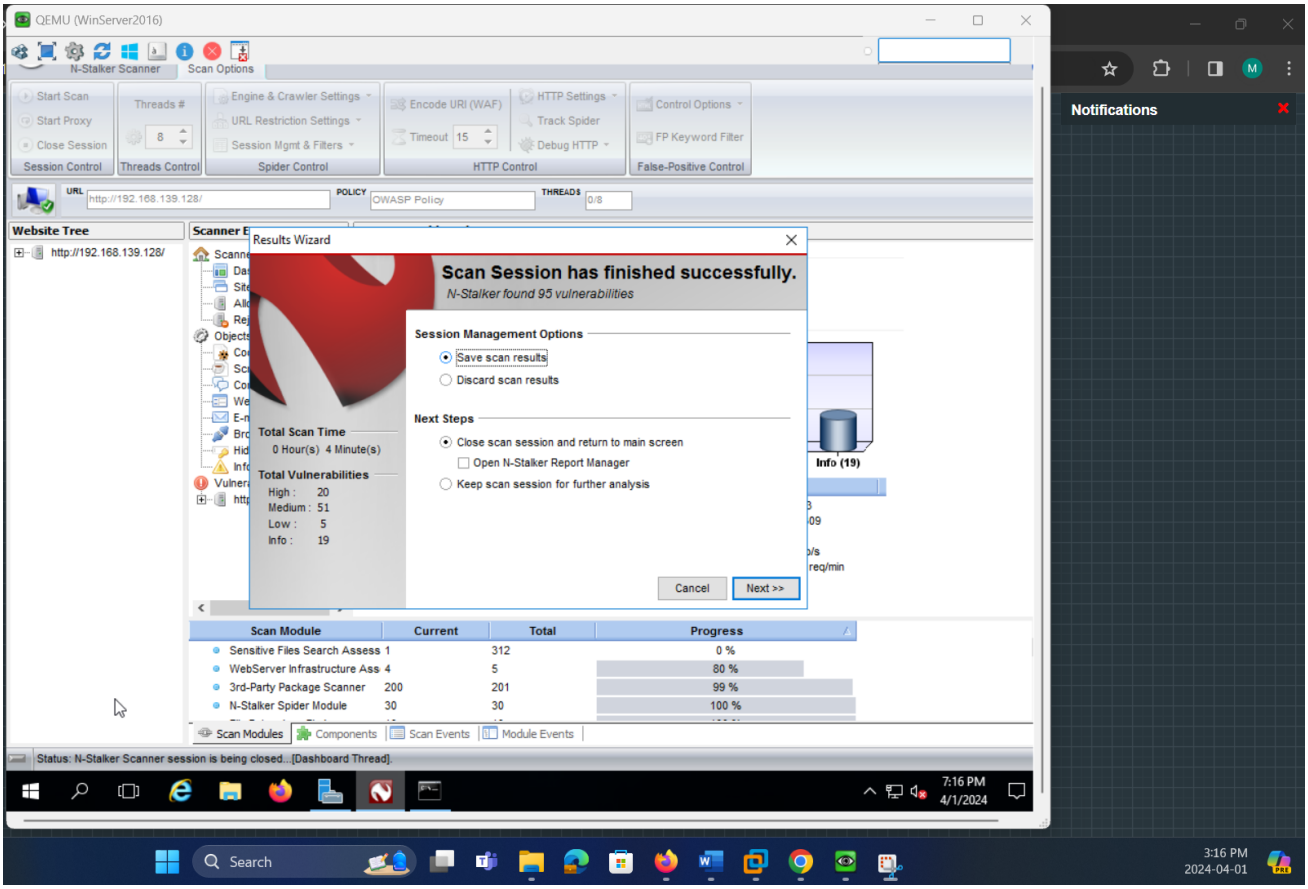

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
Website Tree
Scanner Events
Scanner Dashboard
Progress Status
Completed Spider
Step 2 Info Gather
Completed Run Modules
Completed Sig Scanner
Progress Details
Scan Session
Start Time Apr 1, 2024 18:34:21
Duration 0 Hours 5 Minutes
Spider Engine #
Crawled URLs 31
Crawled Hosts 1
Default Page Size 8,524 bytes
Scan Engine #
Total Requests 605
Failed Requests 0
Attacks Sent 384
404 Errors 53
High (20) Mid (50) Low (5) Info (19)
Network #
Bytes Sent 299,244
Bytes Received 1,105,205
Avg Response Time 0.01 s
Avg Transfer Rate 1.45 Mb/s
Component Name
URL Location
Comments
Web Server Information Found
Web Server Technology Detected
Password Web Form Found
Scan Modules
Components
Scan Events
Module Events
Status: Commiting temporary database...[WAIT].
6:42 PM
4/1/2024
Notifications
Search
2:42 PM
2024-04-01


QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
Website Tree
Scanner Events
Scanner Dashboard
Progress Status
Completed Spider
Step 2 Info Gather
Completed Run Modules
Completed Sig Scanner
Progress Details
Scan Session
Start Time Apr 1, 2024 18:34:21
Duration 0 Hours 5 Minutes
Spider Engine #
Crawled URLs 31
Crawled Hosts 1
Default Page Size 8,524 bytes
Scan Engine #
Total Requests 605
Failed Requests 0
Attacks Sent 384
404 Errors 53
High (20) Mid (50) Low (5) Info (19)
Network #
Bytes Sent 299,244
Bytes Received 1,105,205
Avg Response Time 0.01 s
Avg Transfer Rate 1.45 Mb/s
[04/01/2024 18:34:45] ZHtmlParser(): Auto-complete feature is not disabled on a password-based form [/cgi-bin/badstore.cgi?action=loginregister]
[04/01/2024 18:34:45] ZHtmlParser(): Auto-complete feature is not disabled on a password-based form [/cgi-bin/badstore.cgi?action=loginregister]
[04/01/2024 18:34:46] ZHtmlParser(): Auto-complete feature is not disabled on a password-based form [/cgi-bin/badstore.cgi?action=supplierlogin]
Scan Modules
Components
Scan Events
Module Events
Status: Commiting temporary database...[WAIT].
6:43 PM
The Audio Service is not runnin
Notifications
Search
2:43 PM
2024-04-01

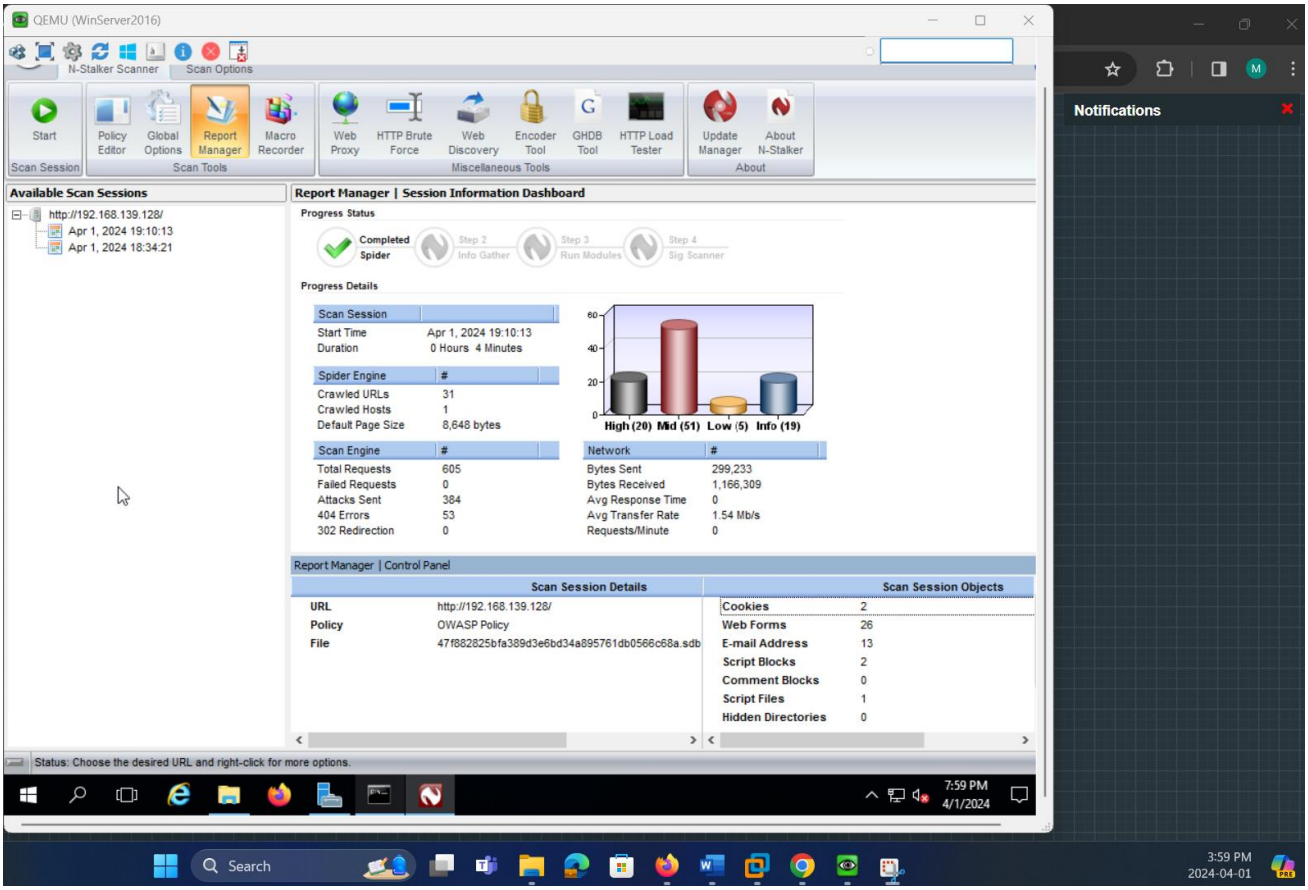

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
Website Tree
Scanner Events
Scanner Dashboard
Progress Status
Completed Spider
Step 2 Info Gather
Completed Run Modules
Completed Sig Scanner
Progress Details
Scan Session
Start Time Apr 1, 2024 18:34:21
Duration 0 Hours 5 Minutes
Spider Engine #
Crawled URLs 31
Crawled Hosts 1
Default Page Size 8,524 bytes
Scan Engine #
Total Requests 605
Failed Requests 0
Attacks Sent 384
404 Errors 53
High (20) Mid (50) Low (5) Info (19)
Network #
Bytes Sent 299,244
Bytes Received 1,105,205
Avg Response Time 0.01 s
Avg Transfer Rate 1.45 Mb/s
[04/01/2024 18:39:01] SignatureScanner(): Attempting to detect [Possible Chili!Soft ASP Configuration File Disclosure and DoS] on [192.168.139.128].
[04/01/2024 18:39:01] SignatureScanner(): Attempting to detect [Beck IPC GmbH IPC@Chip Embedded-Webserver Server Root Arbitrary File Access] on [192.168.139.12
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [Oracle Application Server PL/SQL Module OWA_UTIL Stored Procedures Information Disclosure] on [192.
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [Oracle Applications Web Report Review FNDWRR.exe URL Overflow] on [192.168.139.128].
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [Red Hat Stronghold stronghold-info GET Request Information Disclosure] on [192.168.139.128].
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [Apple QuickTime / Darwin Streaming Server Triple Dot Traversal Arbitrary File Acces] on [192.168.139.1
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [Oracle Application Server XSQL Servlet Direct Request Configuration File Disclosure] on [192.168.139.1
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [Microsoft FrontPage Extensions .pwd File Permissions] on [192.168.139.128].
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [LionMax Software WWW File Share Pro Multiple Remote Vulnerabilities] on [192.168.139.128].
[04/01/2024 18:39:05] SignatureScanner(): Attempting to detect [GNU Bash Remote Command Execution] on [192.168.139.128].
[04/01/2024 18:39:06] ScanInterface(): All Scan Modules have been successfully loaded.
Scan Modules
Components
Scan Events
Module Events
Status: Commiting temporary database...[WAIT].
6:43 PM
4/1/2024
Notifications
Search
2:43 PM
2024-04-01

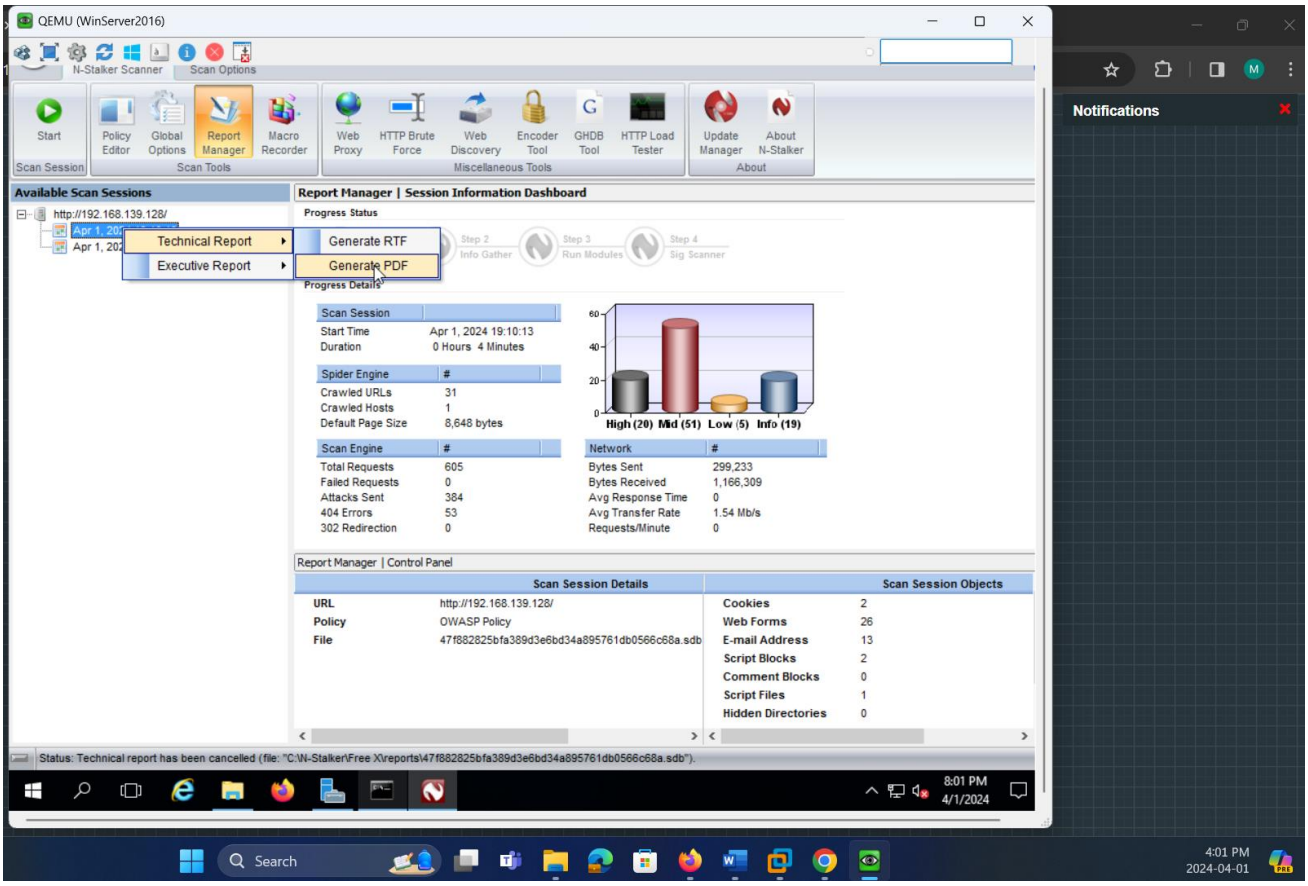

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
Website Tree
http://192.168.139.128/
Results Wizard
Scan Session has finished successfully.
N-Stalker found 94 vulnerabilities
Session Management Options
Save scan results
Discard scan results
Next Steps
Close scan session and return to main screen
Open N-Stalker Report Manager
Keep scan session for further analysis
Total Scan Time
0 Hour(s) 5 Minute(s)
Total Vulnerabilities
High : 20
Medium : 50
Low : 5
Info : 19
Cancel
Next >>
Info (19)
3rd-Party Package Scanner 194 195 99 %
N-Stalker Spider Module 30 30 100 %
File Extensions Finder 10 10 100 %
HTTP Method Finder 11 11 100 %
Cross-Site Scripting Assessm 936 936 100 %
Scan Modules
Components
Scan Events
Module Events
Status: N-Stalker Scanner session is being closed...[Dashboard Thread].
6:40 PM
4/1/2024
Notifications
Search
2:40 PM
2024-04-01

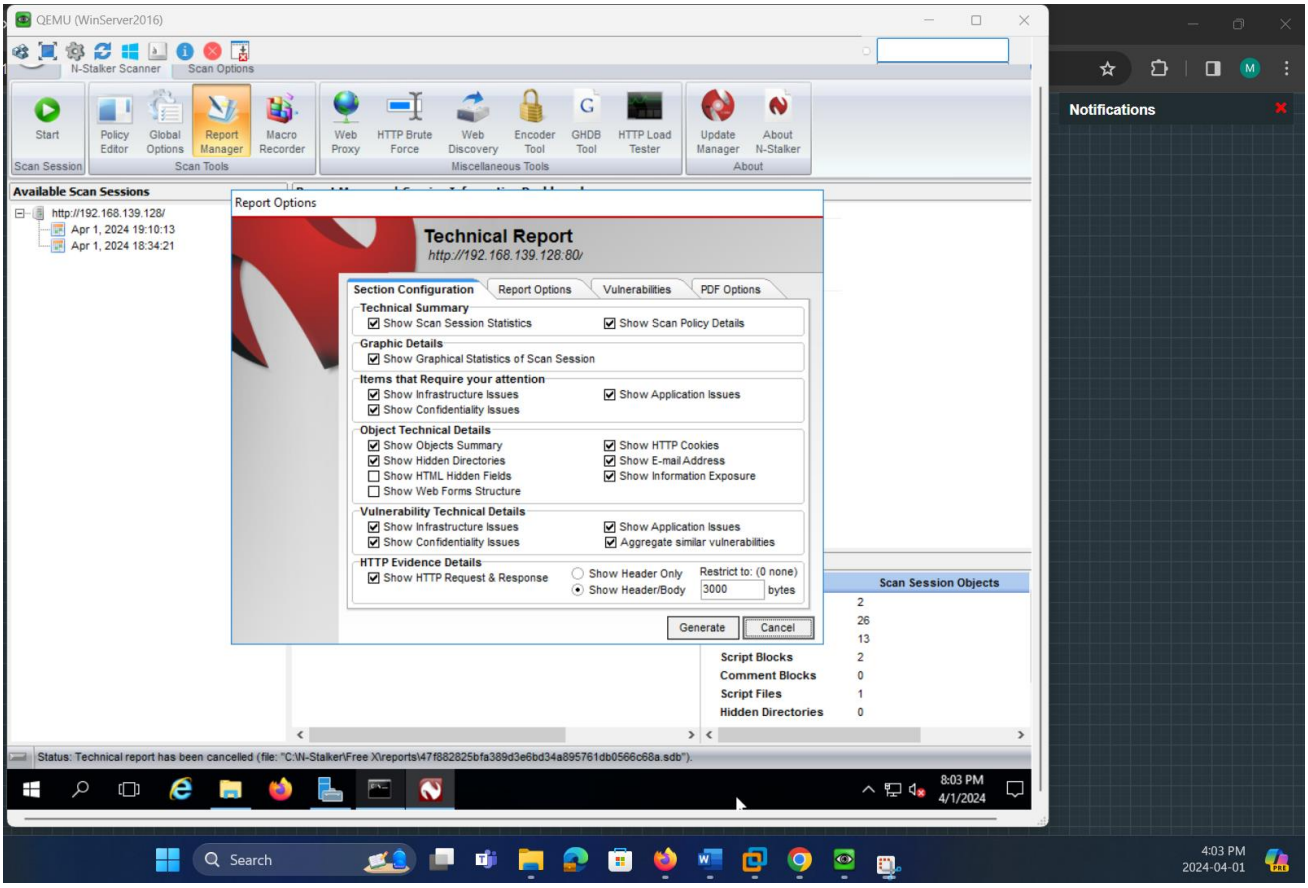

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start Scan
Start Proxy
Close Session
Session Control
Threads #
Threads Control
Engine & Crawler Settings
URL Restriction Settings
Session Mgmt & Filters
Spider Control
Encode URI (WAF)
Timeout
HTTP Settings
Track Spider
Debug HTTP
HTTP Control
Control Options
FP Keyword Filter
False-Positive Control
URL
http://192.168.139.128/
POLICY
OWASP Policy
THREADS
Website Tree
http://192.168.139.128/
Results Wizard
Scan Session has finished successfully.
N-Stalker found 94 vulnerabilities
Summary
Application Objects
Count
Total Web Pages 31
High Vulnerabilities 20
Medium Vulnerabilities 50
Low Vulnerabilities 5
Info Vulnerabilities 19
Total Hosts Found 1
Total HTTP Cookies 2
Total Directories Found 0
Total Web Forms Found 26
Total Password Forms 0
Total E-mails Found 6
Total Client Scripts 3
Total HTML Comments 0
Your request has been successfully processed.
Done
Total Scan Time
0 Hour(s) 5 Minute(s)
Total Vulnerabilities
High : 20
Medium : 50
Low : 5
Info : 19
Info (19)
3rd-Party Package Scanner 194 195 99 %
N-Stalker Spider Module 30 30 100 %
File Extensions Finder 10 10 100 %
HTTP Method Finder 11 11 100 %
Cross-Site Scripting Assessme 936 936 100 %
Scan Modules
Components
Scan Events
Module Events
Status: N-Stalker Scanner session is being closed...[Dashboard Thread].
6:40 PM
The Audio Service is not runnin
Notifications
Search
2:40 PM
2024-04-01

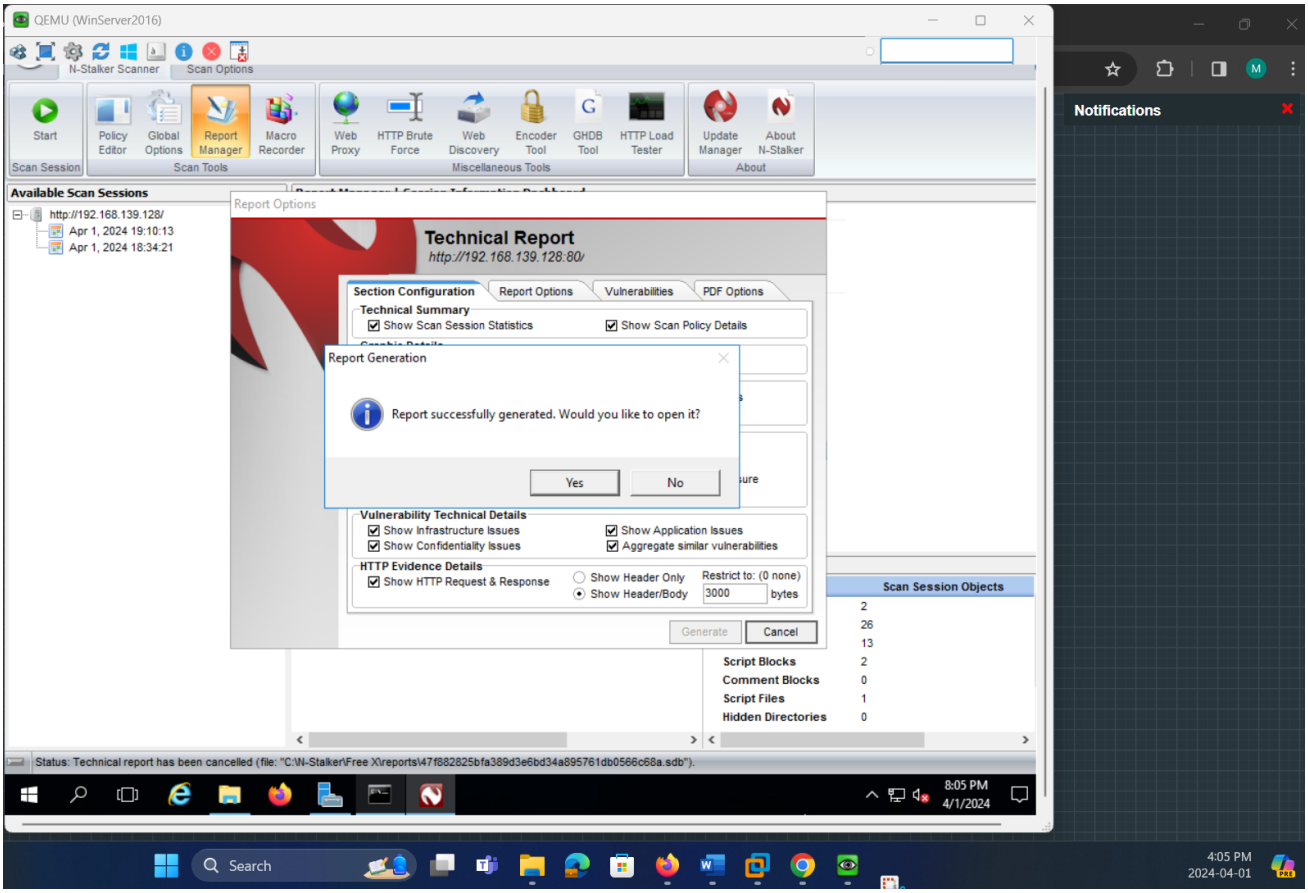


5. **Scan Results of www.badstore.net (192.168.139.128) – Generating Technical Report and Interpreting Reports**

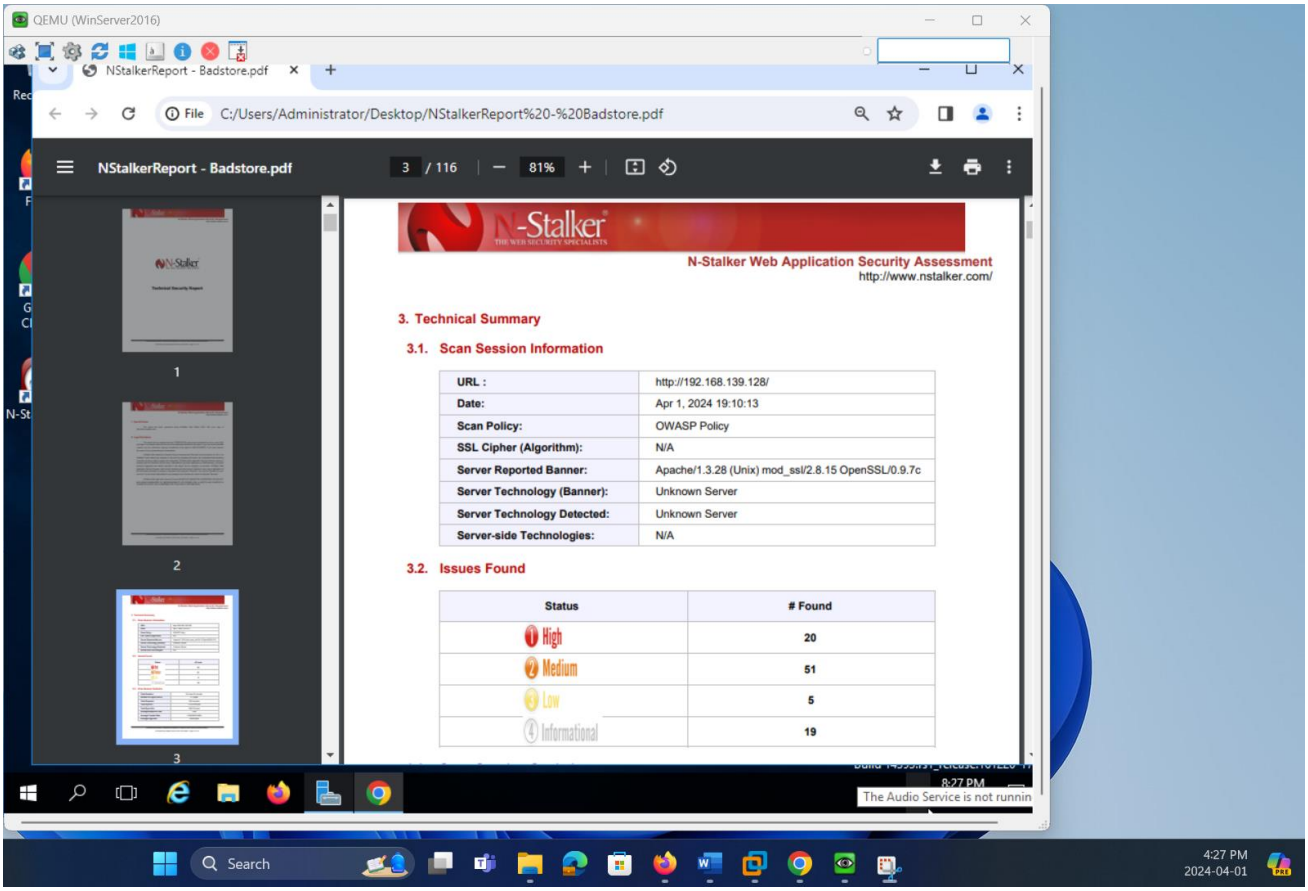

QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Policy Editor
Global Options
Report Manager
Macro Recorder
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Update Manager
About N-Stalker
Scan Session
Scan Tools
Miscellaneous Tools
About
Available Scan Sessions
http://192.168.139.128/
Apr 1, 2024 19:10:13
Apr 1, 2024 18:34:21
Report Manager | Session Information Dashboard
Progress Status
Completed Spider
Step 2 Info Gather
Step 3 Run Modules
Step 4 Sig Scanner
Progress Details
Scan Session
Start Time Apr 1, 2024 19:10:13
Duration 0 Hours 4 Minutes
Spider Engine #
Crawled URLs 31
Crawled Hosts 1
Default Page Size 8,648 bytes
Scan Engine #
Total Requests 605
Failed Requests 0
Attacks Sent 384
404 Errors 53
302 Redirection 0
High (20) Mid (51) Low (5) Info (19)
Network #
Bytes Sent 299,233
Bytes Received 1,166,309
Avg Response Time 0
Avg Transfer Rate 1.54 Mb/s
Requests/Minute 0
Report Manager | Control Panel
Scan Session Details
URL http://192.168.139.128/
Policy OWASP Policy
File 47f882825bfa389d3e6bd34a895761db0566c68a.sdb
Scan Session Objects
Cookies 2
Web Forms 26
E-mail Address 13
Script Blocks 2
Comment Blocks 0
Script Files 1
Hidden Directories 0
Status: Choose the desired URL and right-click for more options.
7:59 PM 4/1/2024
Notifications
Search
3:59 PM 2024-04-01


QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Policy Editor
Global Options
Report Manager
Macro Recorder
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Update Manager
About N-Stalker
Scan Session
Scan Tools
Miscellaneous Tools
About
Available Scan Sessions
http://192.168.139.128/
Technical Report
Executive Report
Generate RTF
Generate PDF
Report Manager | Session Information Dashboard
Progress Status
Progress Details
Scan Session
Start Time Apr 1, 2024 19:10:13
Duration 0 Hours 4 Minutes
Spider Engine #
Crawled URLs 31
Crawled Hosts 1
Default Page Size 8,648 bytes
Scan Engine #
Total Requests 605
Failed Requests 0
Attacks Sent 384
404 Errors 53
302 Redirection 0
High (20) Mid (51) Low (5) Info (19)
Network #
Bytes Sent 299,233
Bytes Received 1,166,309
Avg Response Time 0
Avg Transfer Rate 1.54 Mb/s
Requests/Minute 0
Report Manager | Control Panel
Scan Session Details
URL http://192.168.139.128/
Policy OWASP Policy
File 47f882825bfa389d3e6bd34a895761db0566c68a.sdb
Scan Session Objects
Cookies 2
Web Forms 26
E-mail Address 13
Script Blocks 2
Comment Blocks 0
Script Files 1
Hidden Directories 0
Status: Technical report has been cancelled (file: "C:\N-Stalker\Free X\reports\47f882825bfa389d3e6bd34a895761db0566c68a.sdb").
8:01 PM
4/1/2024
Notifications
Search
4:01 PM
2024-04-01


QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Scan Session
Policy Editor
Global Options
Report Manager
Macro Recorder
Scan Tools
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Miscellaneous Tools
Update Manager
About N-Stalker
About
Available Scan Sessions
http://192.168.139.128/
Apr 1, 2024 19:10:13
Apr 1, 2024 18:34:21
Report Options
Technical Report
http://192.168.139.128:80/
Section Configuration
Report Options
Vulnerabilities
PDF Options
Technical Summary
Show Scan Session Statistics
Show Scan Policy Details
Graphic Details
Show Graphical Statistics of Scan Session
Items that Require your attention
Show Infrastructure Issues
Show Application Issues
Show Confidentiality Issues
Object Technical Details
Show Objects Summary
Show HTTP Cookies
Show Hidden Directories
Show E-mail Address
Show HTML Hidden Fields
Show Information Exposure
Show Web Forms Structure
Vulnerability Technical Details
Show Infrastructure Issues
Show Application Issues
Show Confidentiality Issues
Aggregate similar vulnerabilities
HTTP Evidence Details
Show HTTP Request & Response
Show Header Only
Show Header/Body
Restrict to: (0 none)
3000
bytes
Generate
Cancel
Scan Session Objects
2
26
13
Script Blocks 2
Comment Blocks 0
Script Files 1
Hidden Directories 0
Status: Technical report has been cancelled (file: "C:\N-Stalker\Free X\reports\47f882825bfa389d3e6bd34a895761db0566c68a.sdb").
8:03 PM
4/1/2024
Notifications
Search
4:03 PM
2024-04-01


QEMU (WinServer2016)
N-Stalker Scanner
Scan Options
Start
Policy Editor
Global Options
Report Manager
Macro Recorder
Web Proxy
HTTP Brute Force
Web Discovery
Encoder Tool
GHDB Tool
HTTP Load Tester
Update Manager
About N-Stalker
Scan Session
Scan Tools
Miscellaneous Tools
About
Available Scan Sessions
http://192.168.139.128/
Apr 1, 2024 19:10:13
Apr 1, 2024 18:34:21
Report Options
Technical Report
http://192.168.139.128:80/
Section Configuration
Report Options
Vulnerabilities
PDF Options
Technical Summary
Show Scan Session Statistics
Show Scan Policy Details
Report Generation
Report successfully generated. Would you like to open it?
Yes
No
Vulnerability Technical Details
Show Infrastructure Issues
Show Application Issues
Show Confidentiality Issues
Aggregate similar vulnerabilities
HTTP Evidence Details
Show HTTP Request & Response
Show Header Only
Show Header/Body
Restrict to: (0 none)
3000
bytes
Generate
Cancel
Scan Session Objects
2
26
13
Script Blocks 2
Comment Blocks 0
Script Files 1
Hidden Directories 0
Status: Technical report has been cancelled (file: "C:\N-Stalker\Free X\reports\47f882825bfa389d3e6bd34a895761db0566c68a.sdb").
8:05 PM
4/1/2024
Notifications
Search
4:05 PM
2024-04-01


QEMU (WinServer2016)
NStalkerReport - Badstore.pdf
File C:/Users/Administrator/Desktop/NStalkerReport%20-%20Badstore.pdf
NStalkerReport - Badstore.pdf
1 / 116
81%
1
2
N-Stalker
THE WEB SECURITY SPECIALISTS
N-Stalker Web Application Security Assessment
http://www.nstalker.com/
N-Stalker
THE WEB SECURITY SPECIALISTS
Technical Security Report
Monday, April 1, 2024
8:26 PM
4/1/2024
Search
4:26 PM
2024-04-01



Based on the provided report from the N-Stalker Web Application Security Assessment, here is a general interpretation of the scan results:

1. **Vulnerable Server and Software**: The web server is running older, vulnerable versions of Apache, mod_ssl, and OpenSSL, which have numerous known security vulnerabilities. These vulnerabilities range from information disclosure to remote code execution and denial of service.
2. **Vulnerabilities Detected**:
    - **Cross-site Scripting (XSS)**: The report indicates multiple occurrences where XSS is possible, which could allow attackers to execute scripts in a user's browser to hijack sessions, deface web sites, or conduct phishing attacks. (CVSS Scores, n.d.)
    - **HTTP Parameter Pollution**: This vulnerability can lead to application behavior corruption by manipulating query parameters. (National Vulnerability Database, n.d.)
    - **Cross-site Request Forgery (CSRF)**: Identified vulnerabilities that could allow attackers to perform actions on behalf of legitimate users without their consent.
    - **Insecure Cookie Handling**: Some cookies are found without the HttpOnly flag, making them susceptible to access via client-side scripts. (mitre, n.d.)
    - **Clickjacking**: The application could be vulnerable to clickjacking, where a user is tricked into clicking something different from what the user perceives, effectively hijacking interactions meant to go to another site.

    - **Information Disclosure**: Several issues related to the disclosure of sensitive information have been found, including directory listings and downloadable objects that might contain sensitive data.
3. **Security Bypass and Information Exposure**: Multiple CVEs (Common Vulnerabilities and Exposures) are listed, each representing a different security risk. Many of these are related to OpenSSL and can lead to severe issues like security bypass, denial of service, information exposure, and potentially remote attacks.
4. **Recommended Actions**: Although the detailed remediation steps are not available in the report snippets (likely due to the use of the free edition of the scanner), the general recommendation is to update the vulnerable software to the latest, non-vulnerable versions. It's also advised to implement security best practices like disabling unnecessary HTTP methods, setting HttpOnly flags on cookies, and ensuring the application does not reveal detailed error messages or server versions.
5. **Risk of Unpatched Vulnerabilities**: The report suggests the presence of many outdated and unpatched vulnerabilities that can significantly compromise the security of the application and the server. It's essential to address these issues promptly.
6. **Confidentiality Risks**: The presence of exposed directories and downloadable files can pose significant risks if they contain sensitive information that should not be publicly accessible.

In summary, the report highlights critical security issues that need to be addressed to protect the web application and its users from potential exploits. It's crucial to review each finding in detail, prioritize based on risk, and apply the necessary security patches and configuration changes. For a complete and comprehensive resolution of these issues, upgrading to a full-featured version of the security scanner that provides detailed fixes and further information would be beneficial.

Conclusion and Recommendations:

The exercise using the N-Stalker Web Application Security Scanner has provided valuable insights into the security posture of the scanned web application – www.badstore.net. The results indicate several critical and high-risk vulnerabilities that must be addressed to protect the integrity, confidentiality, and availability of the web application and its underlying systems. Following are the general conclusions for the laboratory assignment:

1. **Outdated Software**: The web server and associated modules are running outdated versions with known vulnerabilities. Updating to the latest, secure versions is a critical step. (OWASP Top Ten, n.d.)
2. **Vulnerability Management**: There is a clear need for ongoing vulnerability management and regular security assessments to identify and remediate new and existing security risks.
3. **Security Hardening**: The web application requires security hardening measures, such as implementing secure cookie attributes, correcting server configurations to prevent clickjacking, and eliminating cross-site scripting vulnerabilities. (13 Best Practices for Improving Web Application Security, n.d.)
4. **Risk Mitigation**: Addressing the highlighted CVEs and other detected issues will greatly reduce the potential for exploitation by attackers.

5. **Compliance and Best Practices**: Ensuring compliance with industry security standards and best practices, like OWASP recommendations, will fortify the application's defense against common web threats. (15 Application Security Best Practices, n.d.) (Web Application Security Best Practices: A Developer's Guide, n.d.)
6. **Awareness and Training**: The exercise emphasizes the need for developer and administrator training on security awareness to prevent introducing vulnerabilities during development and maintenance.
7. **Security Culture**: Building a proactive security culture within the organization can lead to better security practices being followed consistently.
8. **Investment in Security Tools**: The results may suggest that investing in a full version of the security scanner or other advanced security tools could be beneficial for deeper insights and guidance on remediation.
9. **Regular Updates and Patching**: It's evident that regular software updates and patch management processes are vital to maintaining a secure environment.

Overall, the exercise serves as an important reminder of the necessity of web application security and the need for continuous improvement of security measures to safeguard against evolving cyber threats.

References

- *National Vulnerability Database*. (n.d.). Retrieved from nvd.nist.gov: https://nvd.nist.gov/vuln/search
- *13 Best Practices for Improving Web Application Security*. (n.d.). Retrieved from builtin.com: https://builtin.com/software-engineering-perspectives/web-application-security
- *15 Application Security Best Practices*. (n.d.). Retrieved from snyk.io: https://snyk.io/learn/application-security/best-practices/
- *CVSS Scores*. (n.d.). Retrieved from www.cvedetails.com: https://www.cvedetails.com/cvss-score-charts.php
- *mitre*. (n.d.). Retrieved from attack.mitre.org: https://attack.mitre.org/
- *OWASP Top Ten*. (n.d.). Retrieved from owasp.org: https://owasp.org/www-project-top-ten/
- *Web Application Security Best Practices: A Developer's Guide*. (n.d.). Retrieved from securityintelligence.com: https://securityintelligence.com/posts/web-application-security-best-practices-developers-guide/