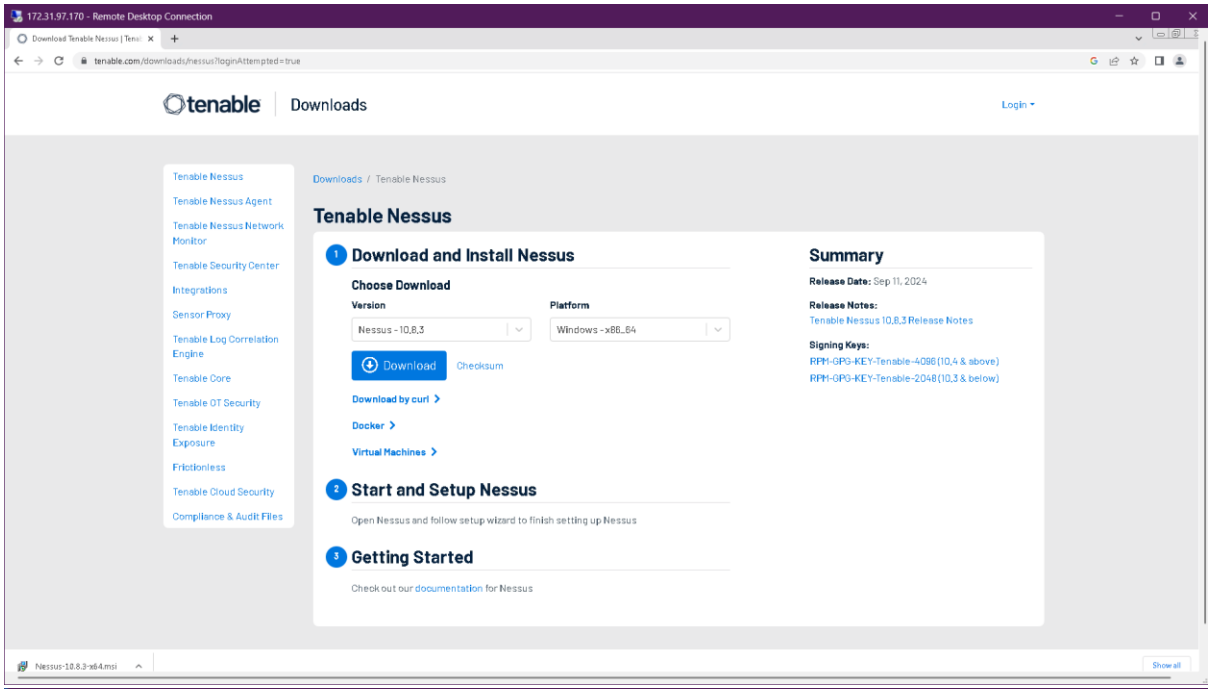
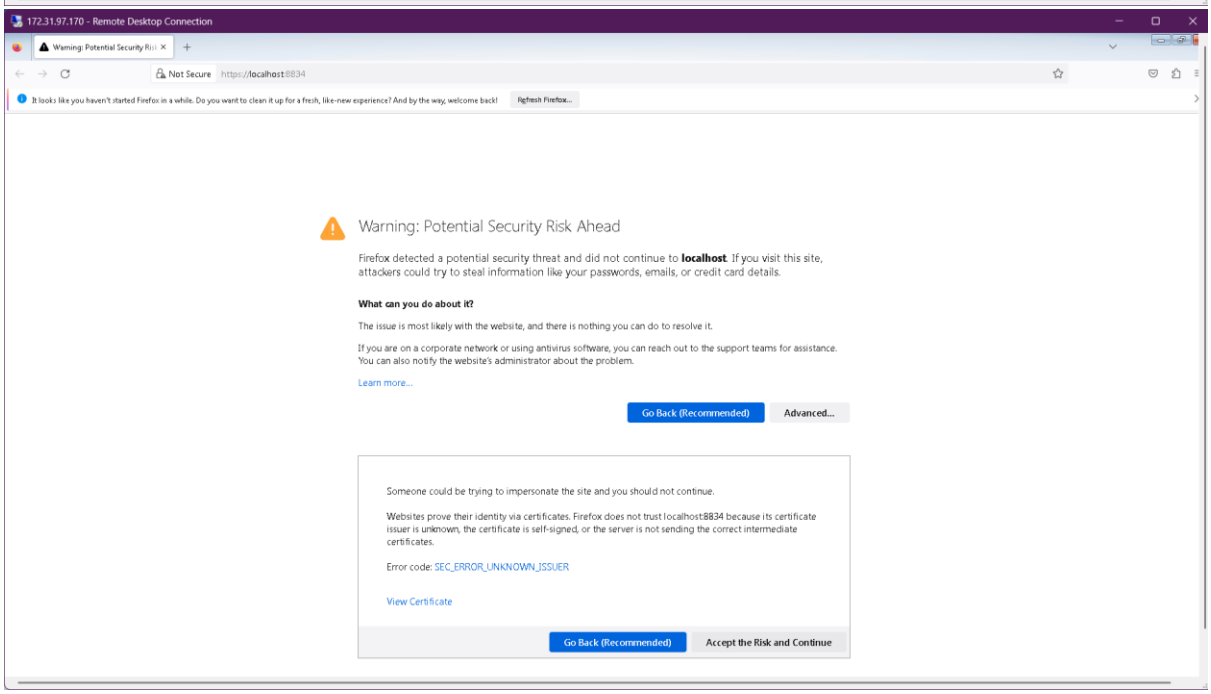
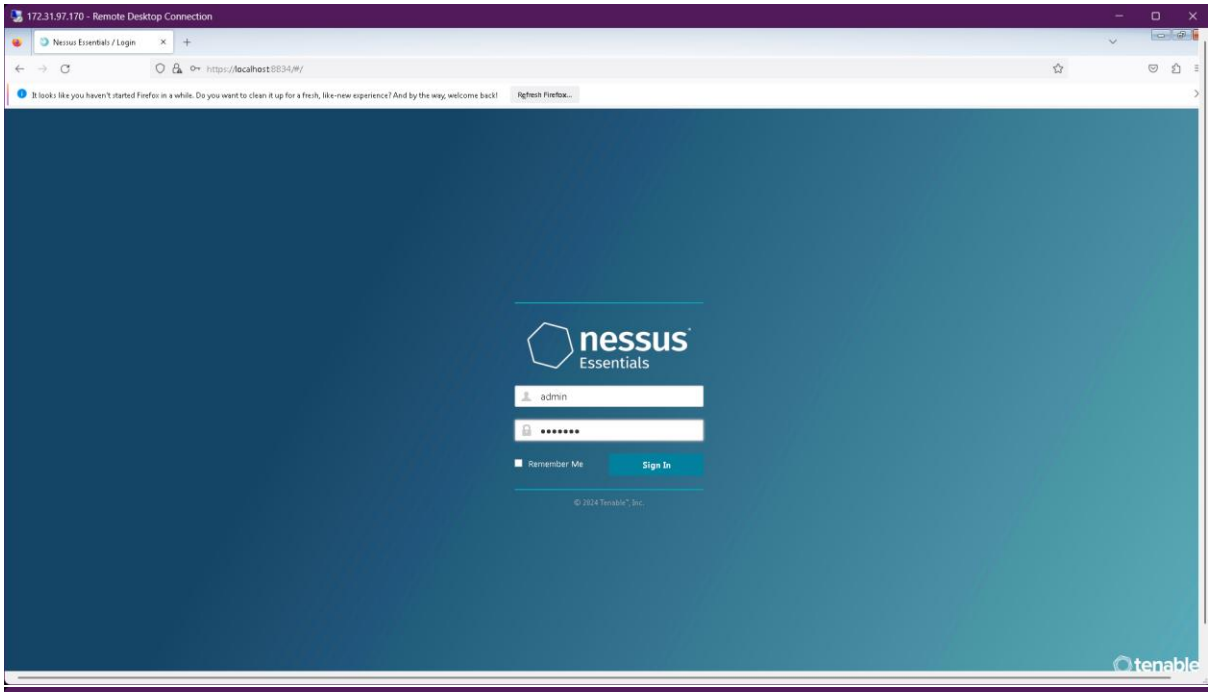
Submitted By Gurbaksh Lal

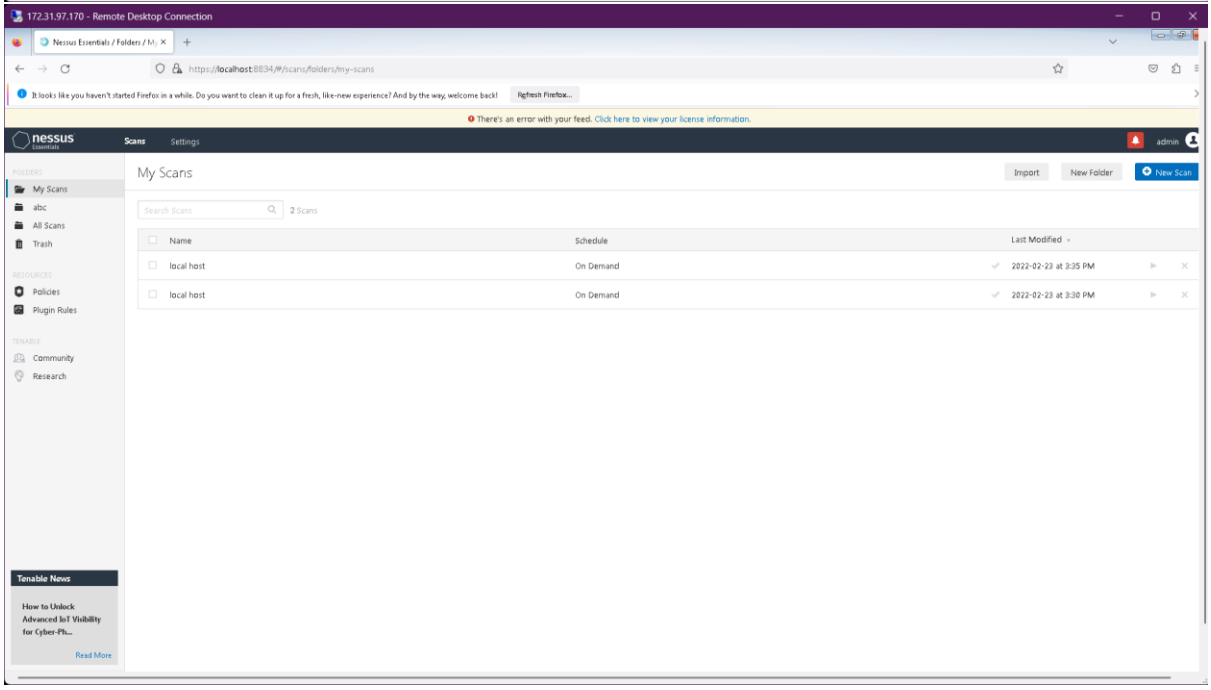
Roll No.: 2023PCS2029

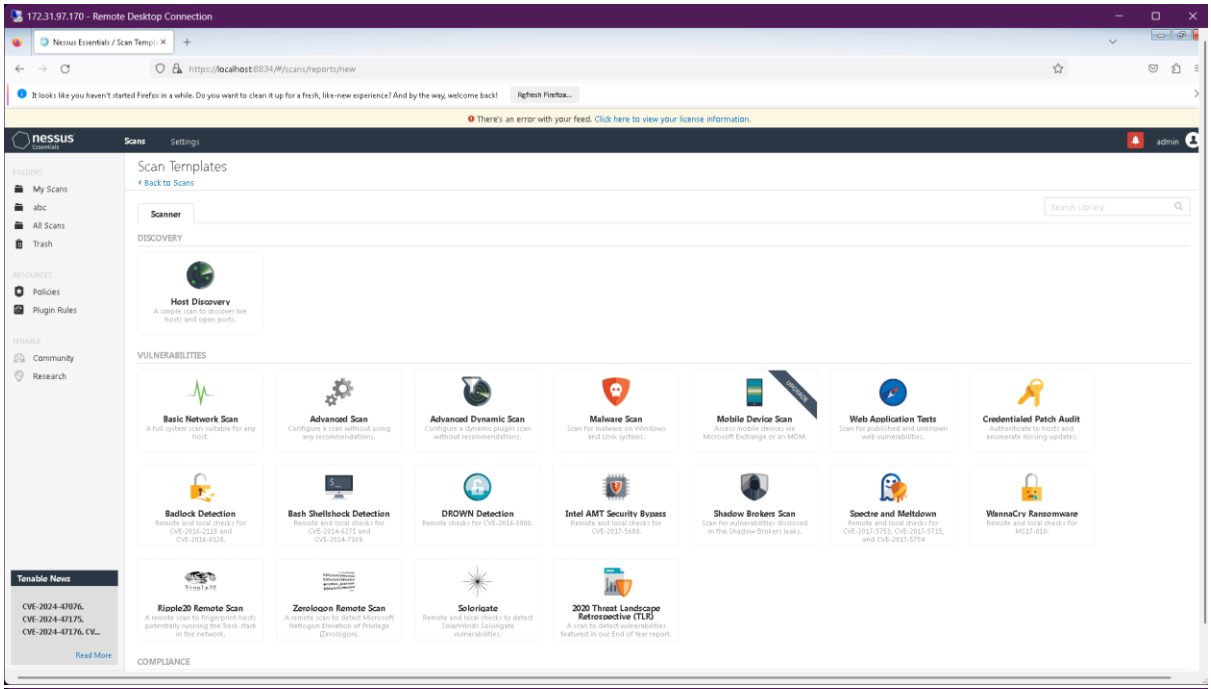
User id: gurbaksh.lal.pg23@nsut.ac.in

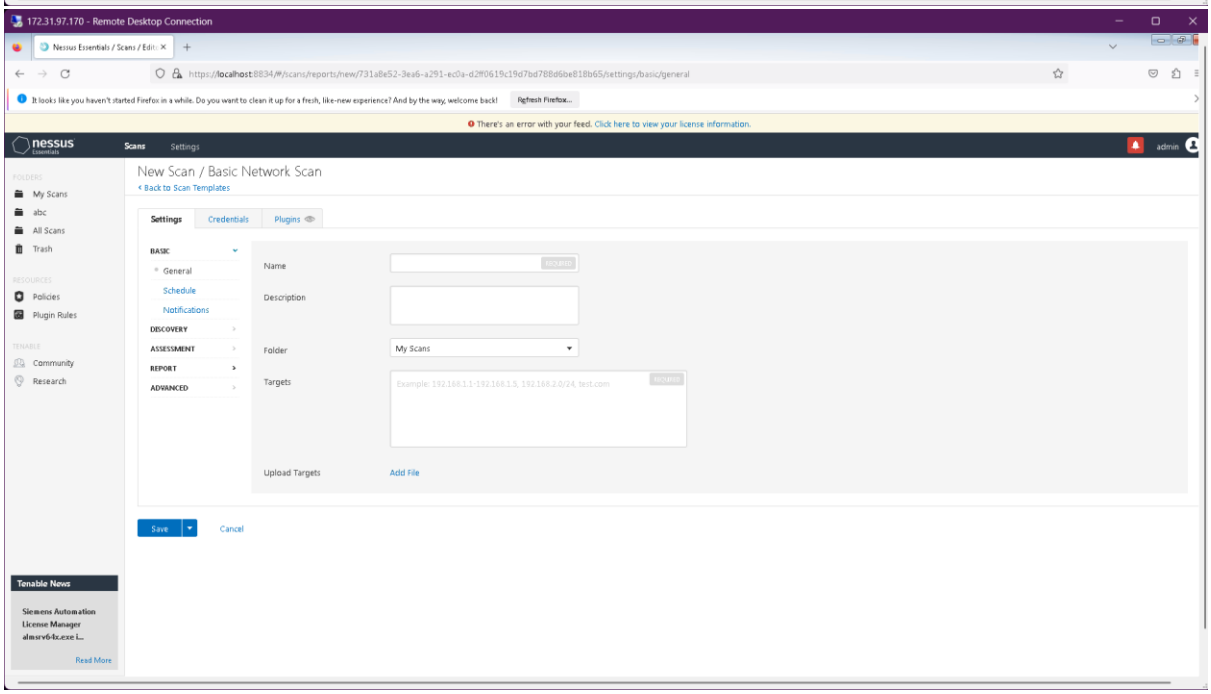


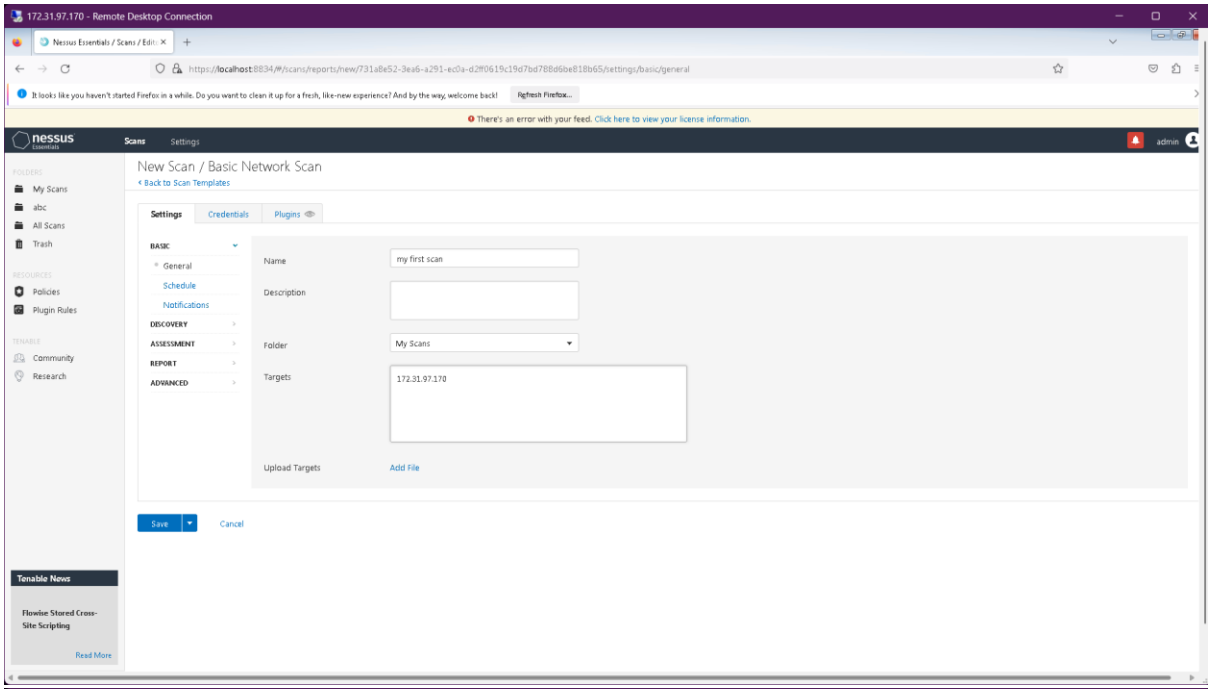


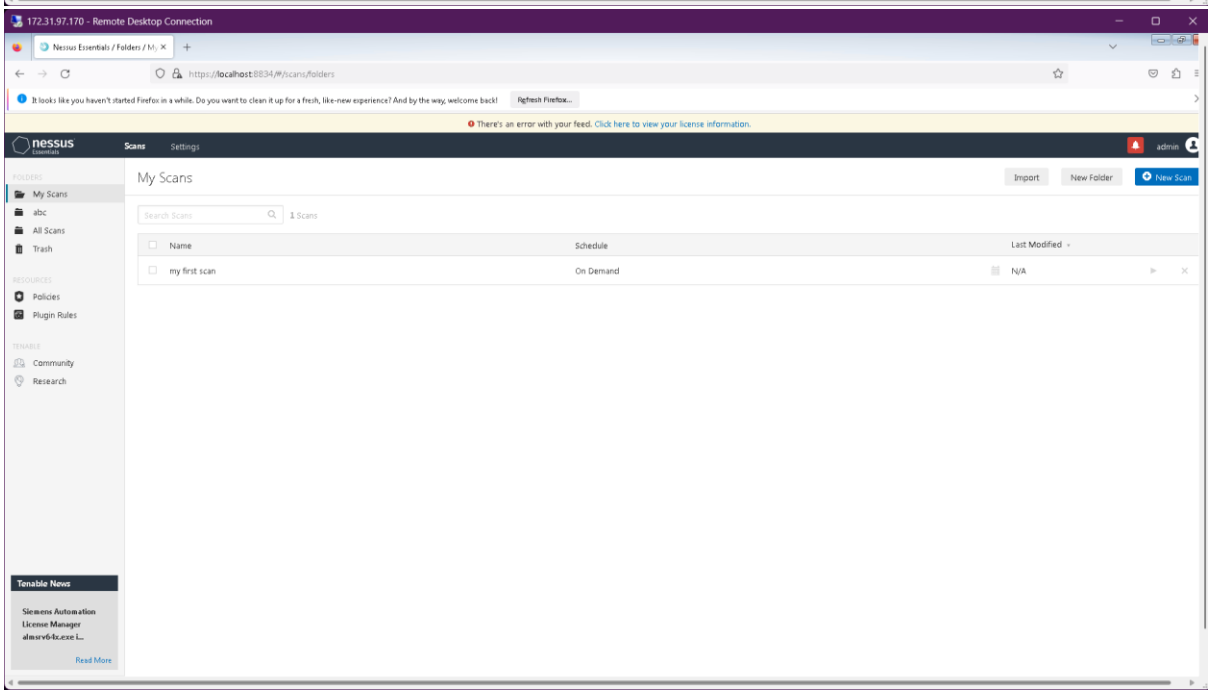

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Login
https://localhost:8834/#/
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
nessus
Essentials
admin
Remember Me
Sign In
© 2024 Tenable™, Inc.
tenable

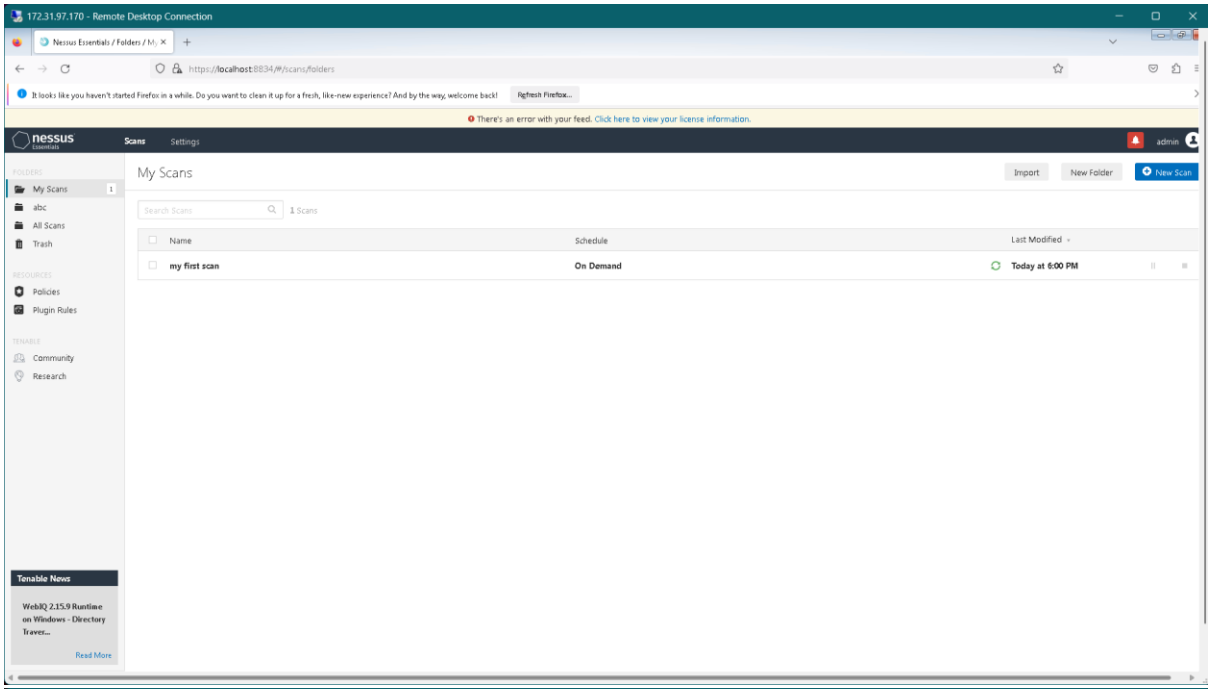

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Folders / My
https://localhost:8834/#/scans/folders/my-scans
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Essentials
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
My Scans
Import
New Folder
New Scan
Search Scans
2 Scans
Name
Schedule
Last Modified
local host
On Demand
2022-02-23 at 3:35 PM
local host
On Demand
2022-02-23 at 3:30 PM
Tenable News
How to Unlock Advanced IoT Visibility for Cyber-Ph...
Read More

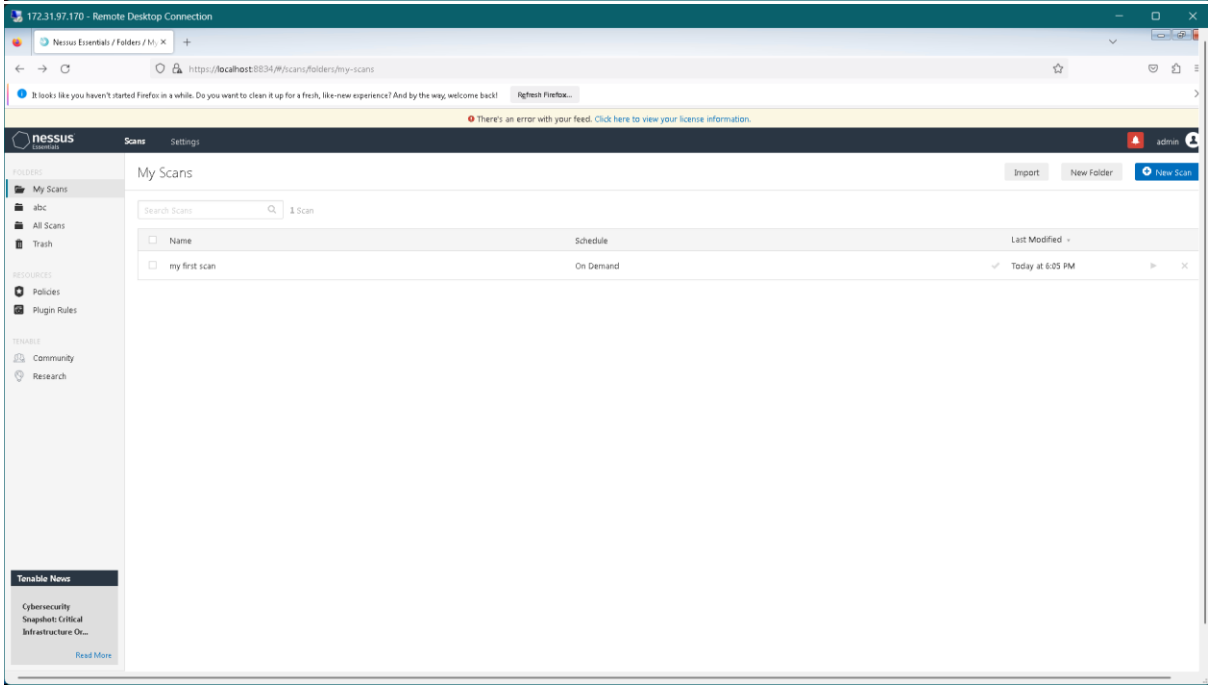

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Scan Templ
https://localhost:8834/#/scans/reports/new
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Scan Templates
Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Web Application Tests
Scan for published and unknown web vulnerabilities.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local check s for CVE-2014-6271 and CVE-2014-7169.
DROWN Detection
Remote checks for CVE-2016-0800.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
WannaCry Ransomware
Remote and local checks for MS17-010.
Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.
Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).
Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.
2020 Threat Landscape Retrospective (TLR)
A scan to detect vulnerabilities featured in our End of Year report.
COMPLIANCE
Tenable News
CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, CV...
Read More

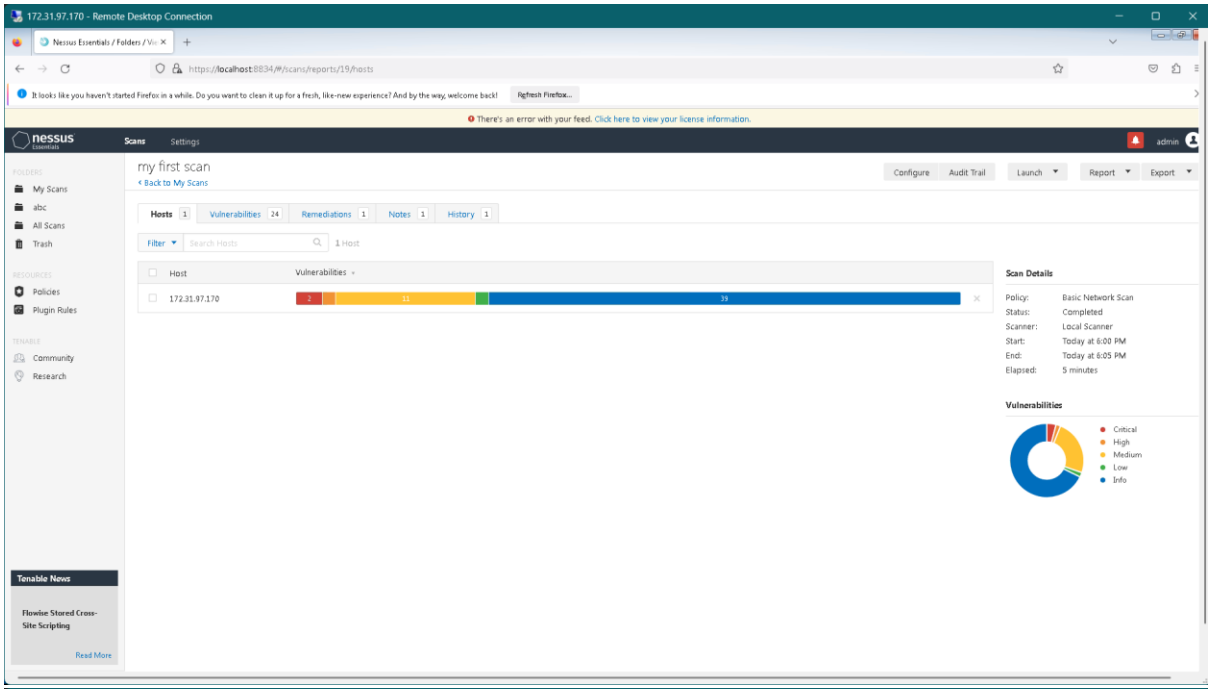

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Scans / Edit
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd7f8d6be818b65/settings/basic/general
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Description
Folder
My Scans
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
Upload Targets
Add File
Save
Cancel
Tenable News
Siemens Automation License Manager almsrv64x.exe i...
Read More

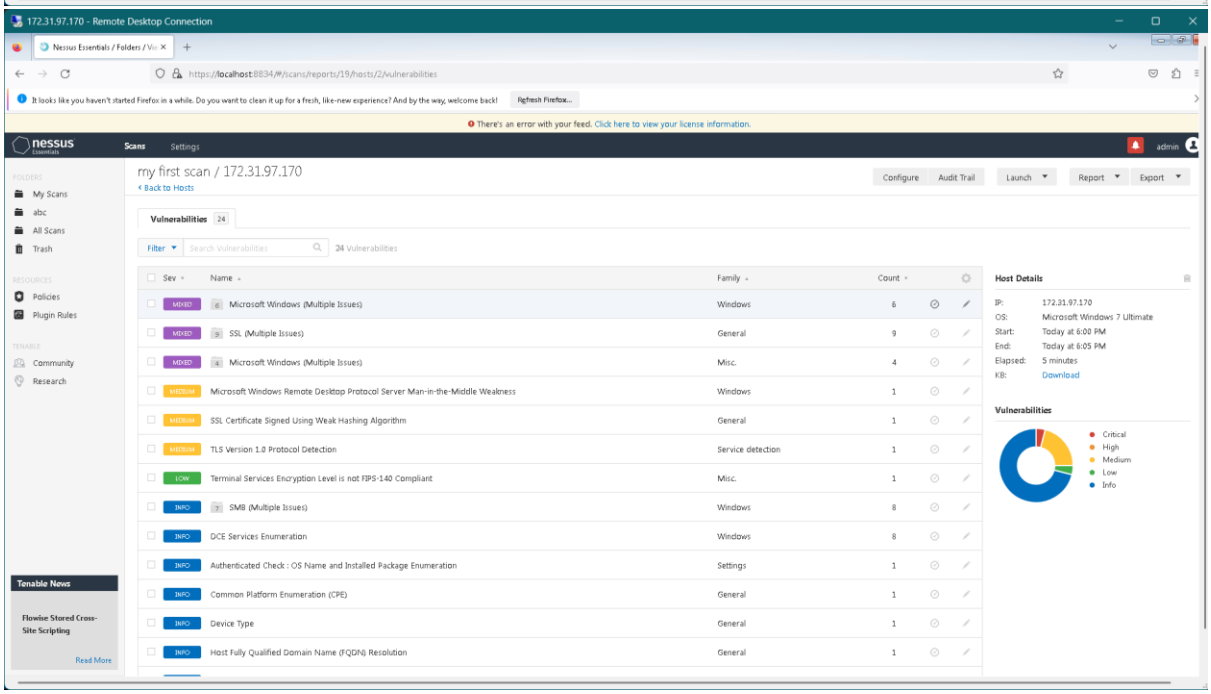

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Scans / Edit
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd7f8d6be818b65/settings/basic/general
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
my first scan
Description
Folder
My Scans
Targets
172.31.97.170
Upload Targets
Add File
Save
Cancel
Tenable News
Flowise Stored Cross-Site Scripting
Read More

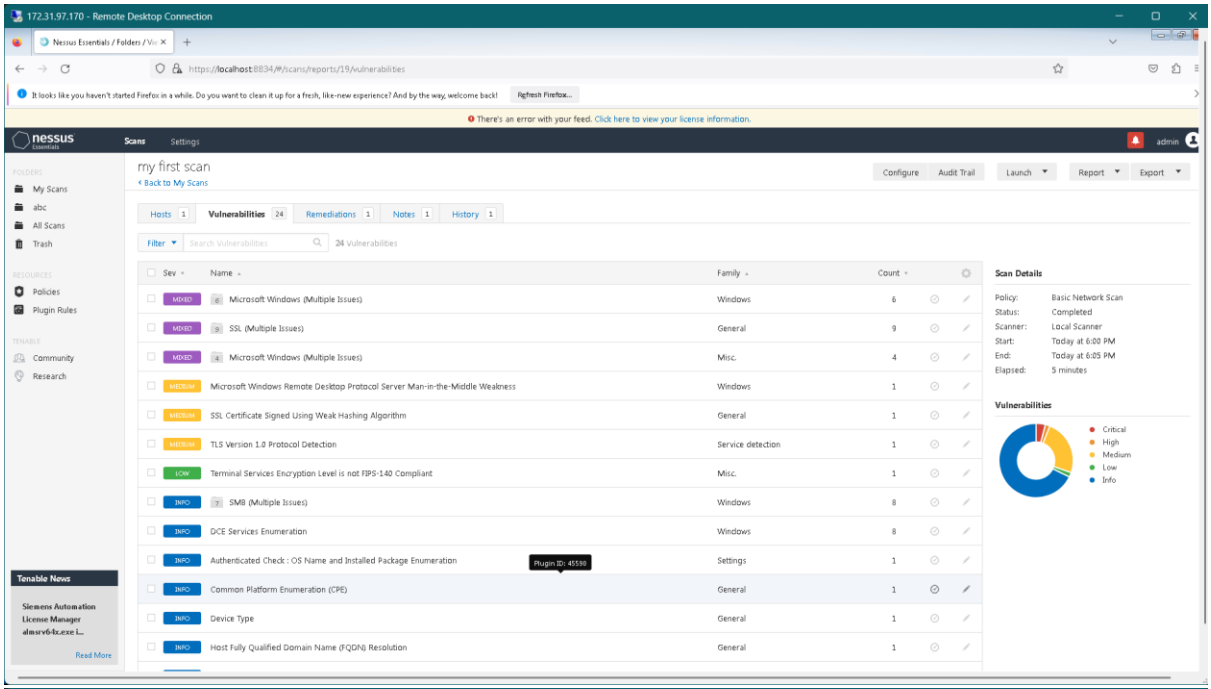

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Folders / My
https://localhost:8834/#/scans/folders
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
My Scans
Import
New Folder
New Scan
Search Scans
1 Scans
Name
Schedule
Last Modified
my first scan
On Demand
N/A
Tenable News
Siemens Automation License Manager almsrv64-lx.exe i...
Read More

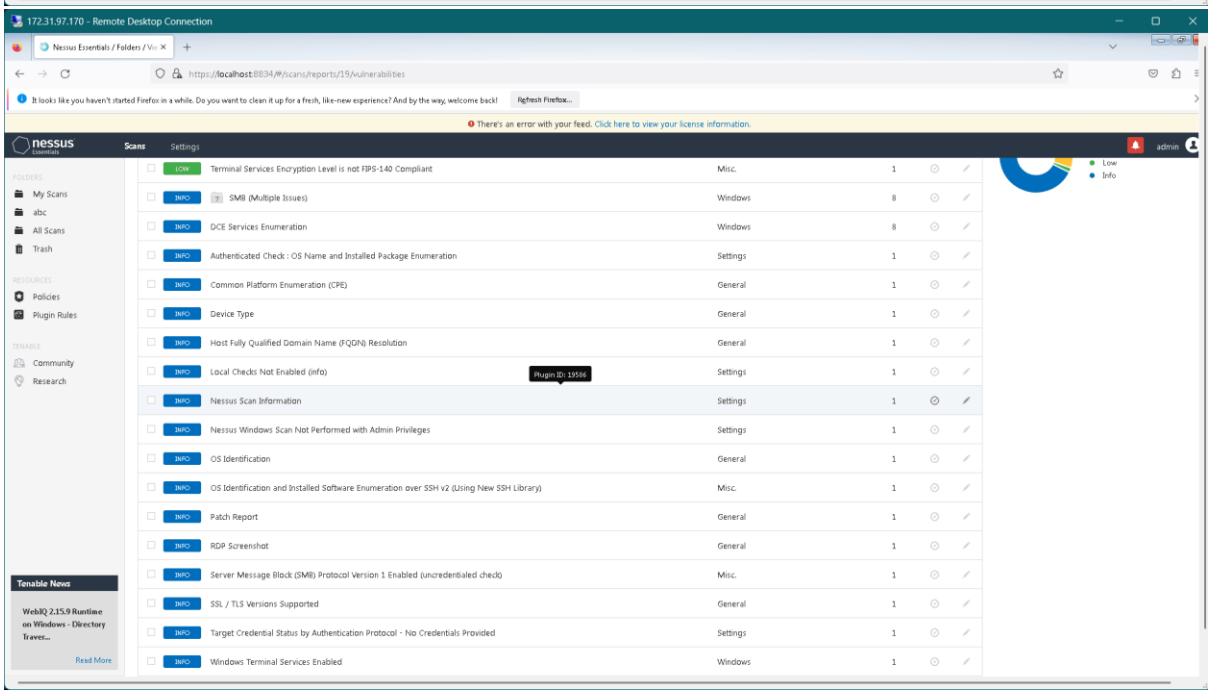

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Folders / My
https://localhost:8834/#/scans/folders
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Essentials
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
My Scans
Import
New Folder
New Scan
Search Scans
1 Scans
Name
Schedule
Last Modified
my first scan
On Demand
Today at 6:00 PM
Tenable News
WebIQ 2.15.9 Runtime on Windows - Directory Traver...
Read More

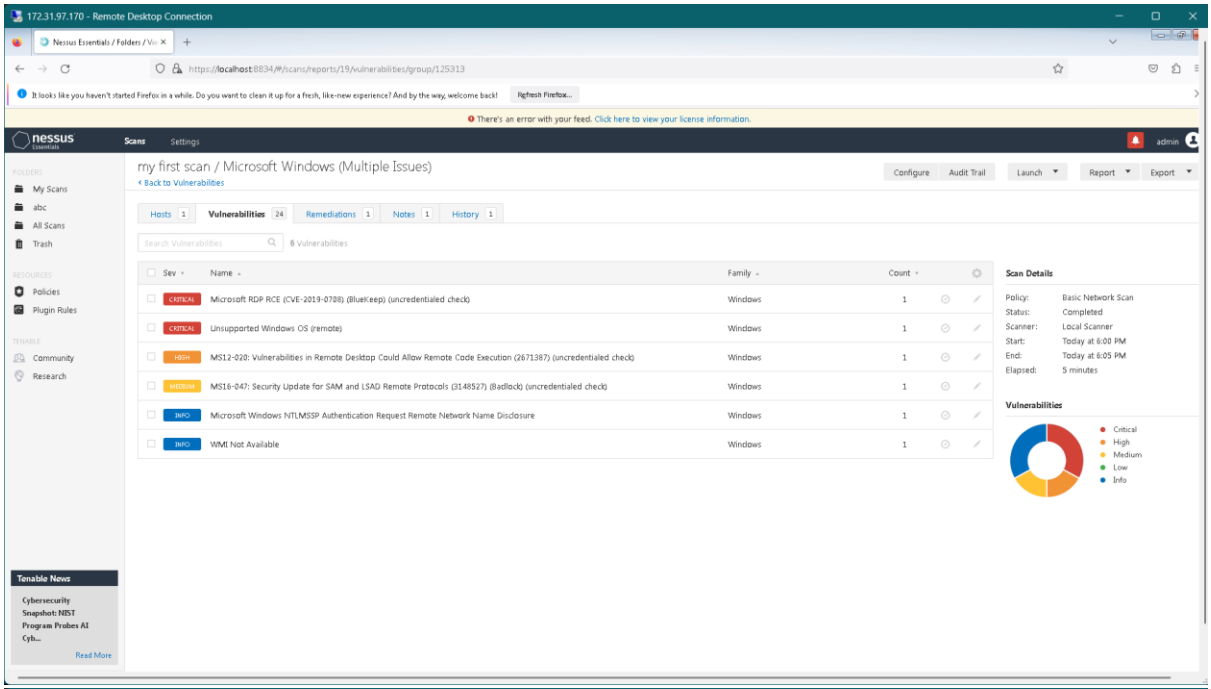

172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Folders / My
https://localhost:8834/#/scans/folders/my-scans
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Essentials
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
my first scan
On Demand
Today at 6:05 PM
Tenable News
Cybersecurity Snapshot: Critical Infrastructure Or...
Read More

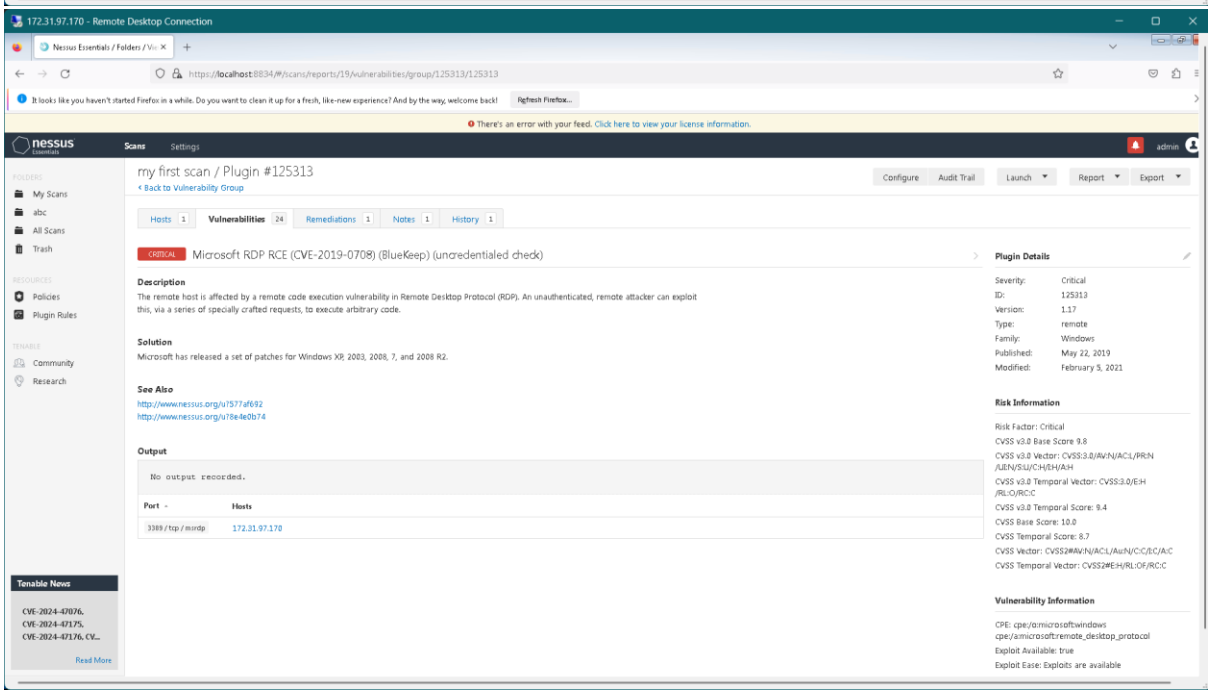

172.31.97.170 - Remote Desktop Connection
nessus
Scans
Settings
admin
my first scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 24
Remediations 1
Notes 1
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
172.31.97.170
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 6:00 PM
End: Today at 6:05 PM
Elapsed: 5 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
My Scans
abc
All Scans
Trash
Policies
Plugin Rules
Community
Research
Tenable News
Flowise Stored Cross-Site Scripting
Read More

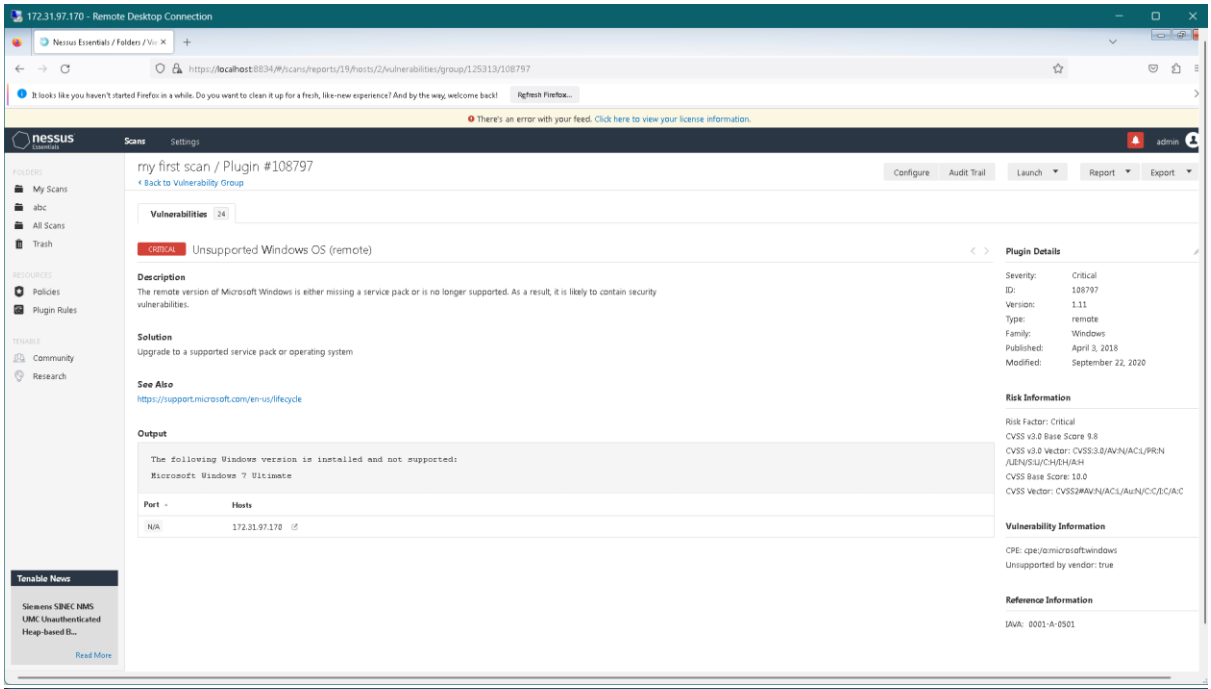

172.31.97.170 - Remote Desktop Connection
nessus
Scans
Settings
admin
my first scan / 172.31.97.170
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 24
Filter
Search Vulnerabilities
24 Vulnerabilities
Sev
Name
Family
Count
MIXED
Microsoft Windows (Multiple Issues)
Windows
6
MIXED
SSL (Multiple Issues)
General
9
MIXED
Microsoft Windows (Multiple Issues)
Misc.
4
MEDIUM
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Windows
1
MEDIUM
SSL Certificate Signed Using Weak Hashing Algorithm
General
1
MEDIUM
TLS Version 1.0 Protocol Detection
Service detection
1
LOW
Terminal Services Encryption Level is not FIPS-140 Compliant
Misc.
1
INFO
SMB (Multiple Issues)
Windows
8
INFO
DCE Services Enumeration
Windows
8
INFO
Authenticated Check : OS Name and Installed Package Enumeration
Settings
1
INFO
Common Platform Enumeration (CPE)
General
1
INFO
Device Type
General
1
INFO
Host Fully Qualified Domain Name (FQDN) Resolution
General
1
Host Details
IP: 172.31.97.170
OS: Microsoft Windows 7 Ultimate
Start: Today at 6:00 PM
End: Today at 6:05 PM
Elapsed: 5 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Flowise Stored Cross-Site Scripting
Read More

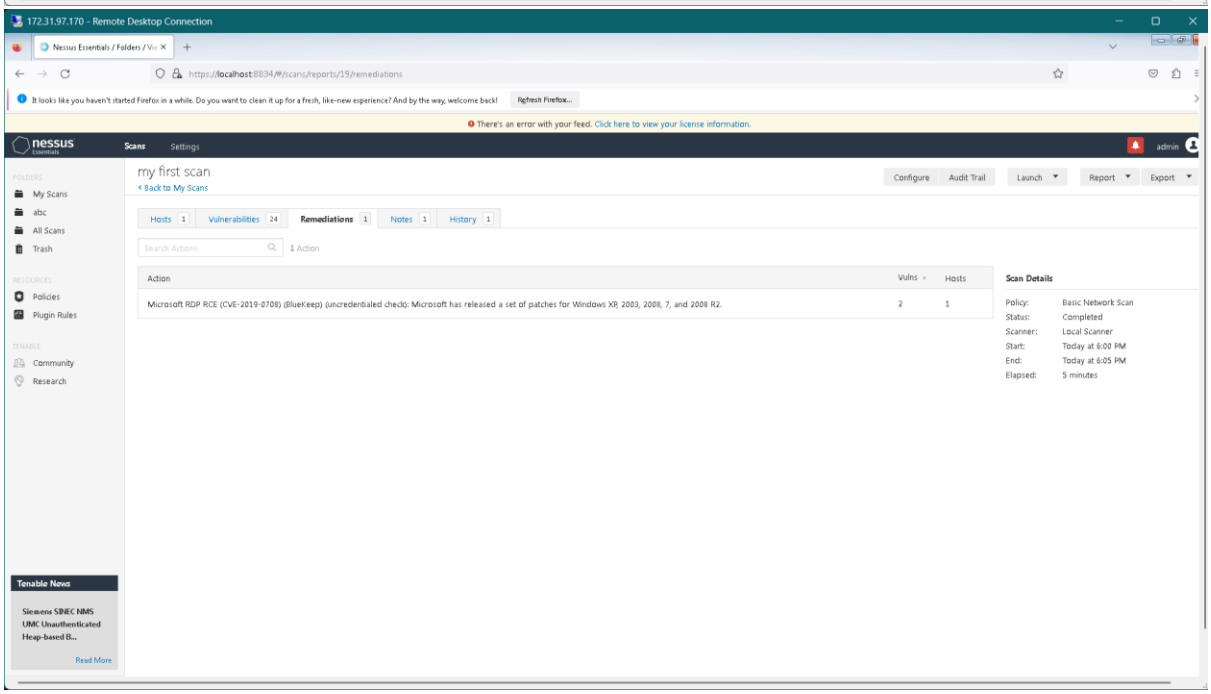

172.31.97.170 - Remote Desktop Connection
nessus
Scans
Settings
admin
my first scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 24
Remediations 1
Notes 1
History 1
Filter
Search Vulnerabilities
24 Vulnerabilities
Sev
Name
Family
Count
MIXED Microsoft Windows (Multiple Issues) Windows 6
MIXED SSL (Multiple Issues) General 9
MIXED Microsoft Windows (Multiple Issues) Misc. 4
MEDIUM Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness Windows 1
MEDIUM SSL Certificate Signed Using Weak Hashing Algorithm General 1
MEDIUM TLS Version 1.0 Protocol Detection Service detection 1
LOW Terminal Services Encryption Level is not FIPS-140 Compliant Misc. 1
INFO SMB (Multiple Issues) Windows 8
INFO DCE Services Enumeration Windows 8
INFO Authenticated Check : OS Name and Installed Package Enumeration Plugin ID: 45590 Settings 1
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Host Fully Qualified Domain Name (FQDN) Resolution General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 6:00 PM
End: Today at 6:05 PM
Elapsed: 5 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Siemens Automation License Manager almsrv64-lx.exe i...
Read More

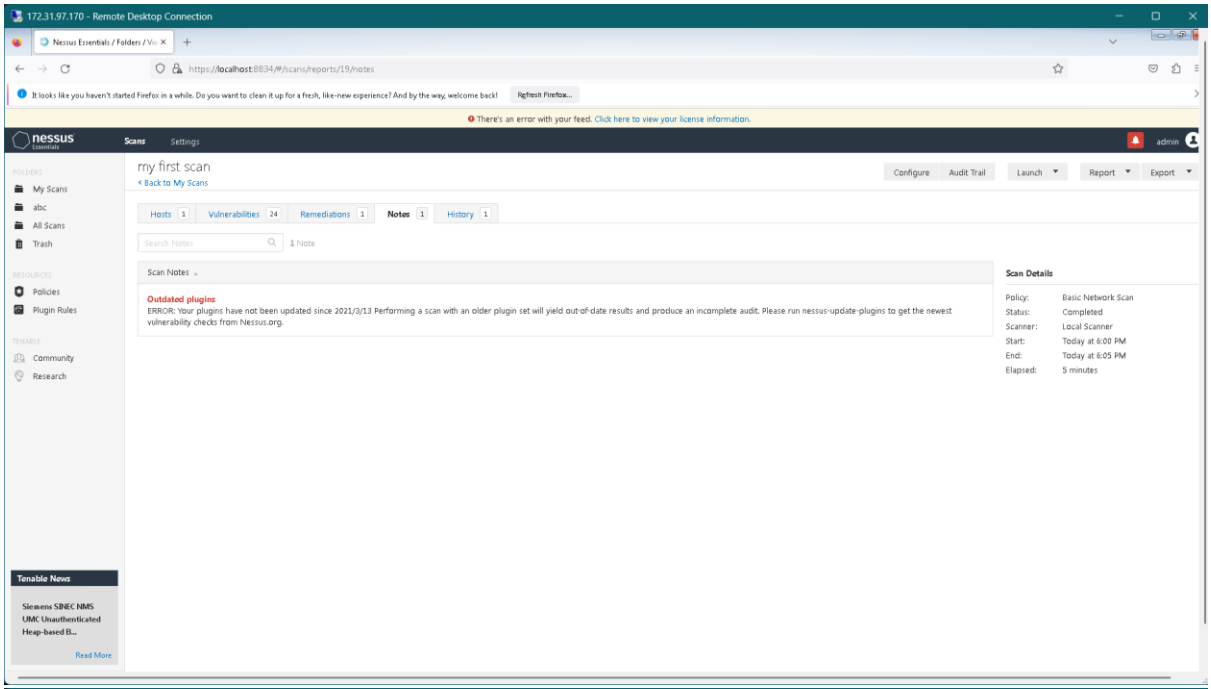

172.31.97.170 - Remote Desktop Connection
nessus
Scans
Settings
admin
LOW Terminal Services Encryption Level is not FIPS-140 Compliant Misc. 1
INFO SMB (Multiple Issues) Windows 8
INFO DCE Services Enumeration Windows 8
INFO Authenticated Check : OS Name and Installed Package Enumeration Settings 1
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Host Fully Qualified Domain Name (FQDN) Resolution General 1
INFO Local Checks Not Enabled (info) Plugin ID: 19506 Settings 1
INFO Nessus Scan Information Settings 1
INFO Nessus Windows Scan Not Performed with Admin Privileges Settings 1
INFO OS Identification General 1
INFO OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) Misc. 1
INFO Patch Report General 1
INFO RDP Screenshot General 1
INFO Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) Misc. 1
INFO SSL / TLS Versions Supported General 1
INFO Target Credential Status by Authentication Protocol - No Credentials Provided Settings 1
INFO Windows Terminal Services Enabled Windows 1
Low
Info
Tenable News
WebIQ 2.15.9 Runtime on Windows - Directory Traver...
Read More

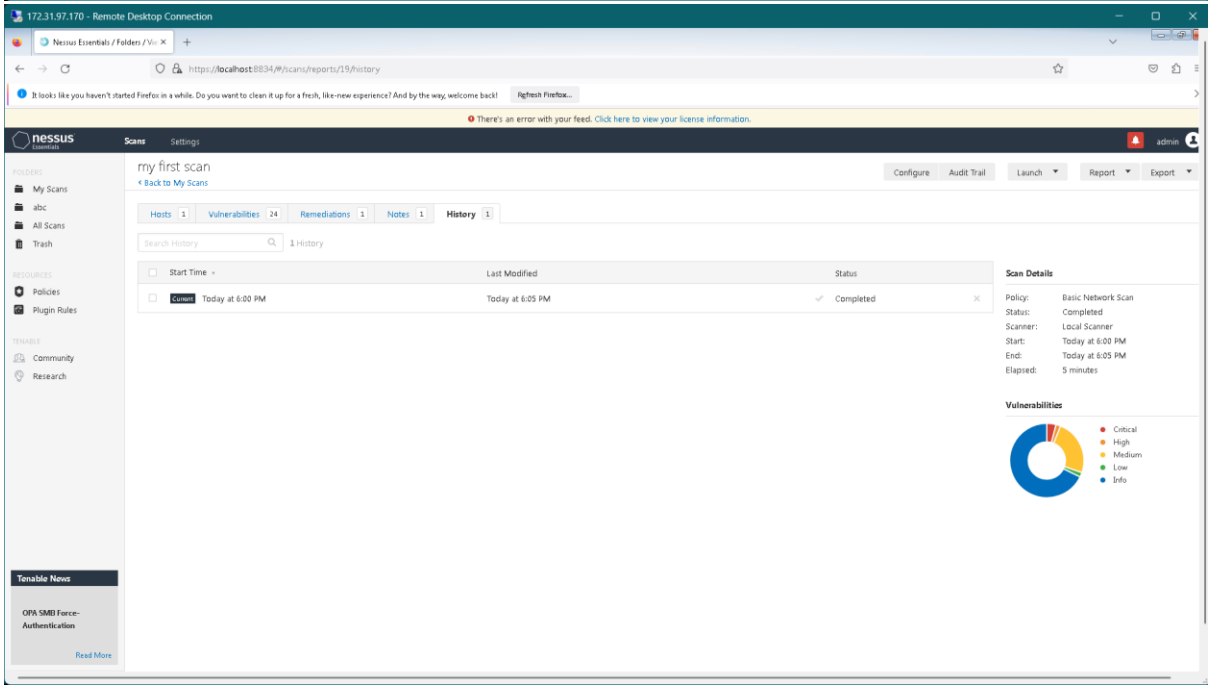

172.31.97.170 - Remote Desktop Connection
https://localhost:8834/#/scans/reports/19/vulnerabilities/group/125313
nessus
Scans
Settings
admin
my first scan / Microsoft Windows (Multiple Issues)
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 24
Remediations 1
Notes 1
History 1
6 Vulnerabilities
Sev
Name
Family
Count
CRITICAL
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
Windows
1
CRITICAL
Unsupported Windows OS (remote)
Windows
1
HIGH
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
Windows
1
MEDIUM
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Windows
1
INFO
Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Windows
1
INFO
WMI Not Available
Windows
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 6:00 PM
End: Today at 6:05 PM
Elapsed: 5 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Cybersecurity Snapshot: NIST Program Probes AI Cyb...
Read More


172.31.97.170 - Remote Desktop Connection
https://localhost:8834/#/scans/reports/19/vulnerabilities/group/125313/125313
nessus
Scans
Settings
admin
my first scan / Plugin #125313
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 24
Remediations 1
Notes 1
History 1
CRITICAL
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
Description
The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.
Solution
Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.
See Also
http://www.nessus.org/u?577af692
http://www.nessus.org/u?78e4e0b74
Output
No output recorded.
Port
Hosts
3389 / tcp / msrdp
172.31.97.170
Plugin Details
Severity: Critical
ID: 125313
Version: 1.17
Type: remote
Family: Windows
Published: May 22, 2019
Modified: February 5, 2021
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4
CVSS Base Score: 10.0
CVSS Temporal Score: 8.7
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:H/RL:OF/RC:C
Vulnerability Information
CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:remote_desktop_protocol
Exploit Available: true
Exploit Ease: Exploits are available
Tenable News
CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, CV...
Read More


172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Folders / Vu
https://localhost:8834/#/scans/reports/19/hosts/2/vulnerabilities/group/125313/108797
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Tenable News
Siemens SINEC NMS UMC Unauthenticated Heap-based B...
Read More
my first scan / Plugin #108797
Back to Vulnerability Group
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 24
CRITICAL
Unsupported Windows OS (remote)
Description
The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.
Solution
Upgrade to a supported service pack or operating system
See Also
https://support.microsoft.com/en-us/lifecycle
Output
The following Windows version is installed and not supported:
Microsoft Windows 7 Ultimate
Port
Hosts
N/A
172.31.97.170
Plugin Details
Severity: Critical
ID: 108797
Version: 1.11
Type: remote
Family: Windows
Published: April 3, 2018
Modified: September 22, 2020
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Vulnerability Information
CPE: cpe:/a:microsoft:windows
Unsupported by vendor: true
Reference Information
IAVA: 0001-A-0501


172.31.97.170 - Remote Desktop Connection
Nessus Essentials / Folders / Vu
https://localhost:8834/#/scans/reports/19/remediations
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
abc
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Tenable News
Siemens SINEC NMS UMC Unauthenticated Heap-based B...
Read More
my first scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 24
Remediations 1
Notes 1
History 1
Search Actions
1 Action
Action
Vulns
Hosts
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check): Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.
2
1
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 6:00 PM
End: Today at 6:05 PM
Elapsed: 5 minutes


172.31.97.170 - Remote Desktop Connection
https://localhost:8834/#/scans/reports/19/notes
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
admin
my first scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 24
Remediations 1
Notes 1
History 1
Search Notes
1 Note
Scan Notes
Outdated plugins
ERROR: Your plugins have not been updated since 2021/3/13 Performing a scan with an older plugin set will yield out-of-date results and produce an incomplete audit. Please run nessus-update-plugins to get the newest vulnerability checks from Nessus.org.
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 6:00 PM
End: Today at 6:05 PM
Elapsed: 5 minutes
My Scans
abc
All Scans
Trash
Policies
Plugin Rules
Community
Research
Tenable News
Siemens SINEC NMS UMC Unauthenticated Heap-based B...
Read More


172.31.97.170 - Remote Desktop Connection
https://localhost:8834/#/scans/reports/19/history
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
admin
my first scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 24
Remediations 1
Notes 1
History 1
Search History
1 History
Start Time
Last Modified
Status
Current
Today at 6:00 PM
Today at 6:05 PM
Completed
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 6:00 PM
End: Today at 6:05 PM
Elapsed: 5 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
My Scans
abc
All Scans
Trash
Policies
Plugin Rules
Community
Research
Tenable News
OPA SMB Force-Authentication
Read More