Lab #5: Vulnerability Analysis

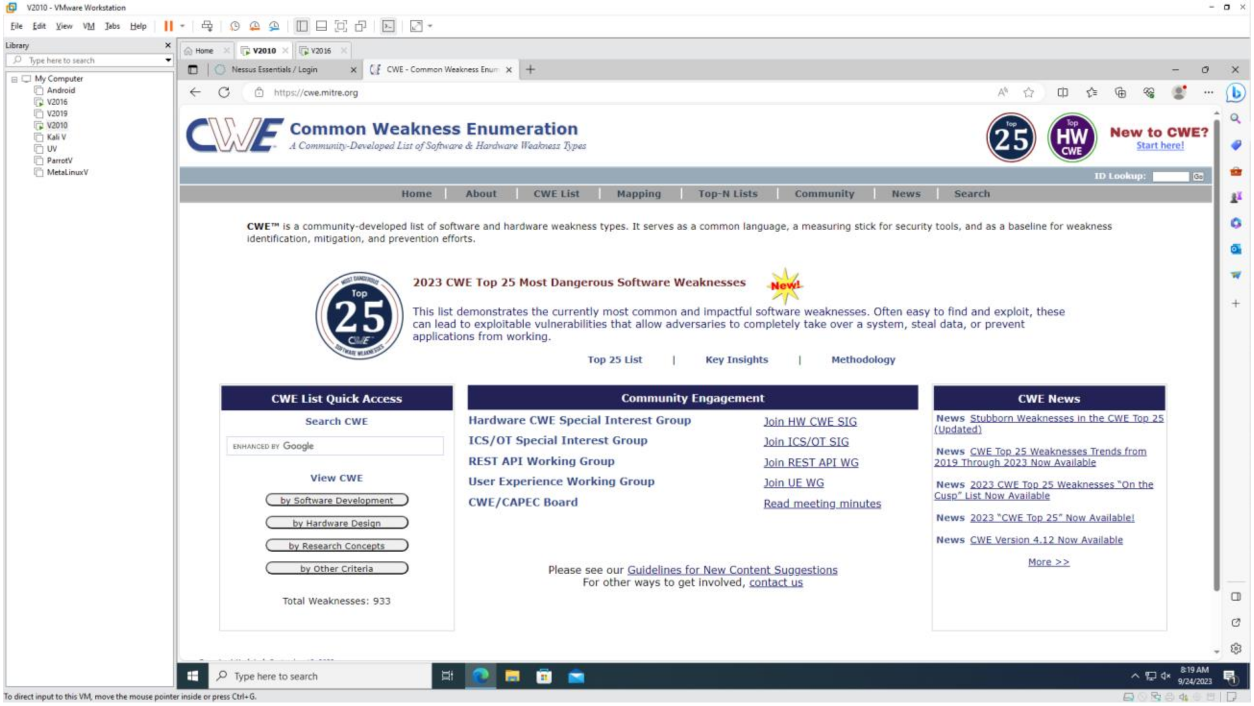
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 27/09/2023

Lab Tasks

1. Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)

- Open Windows 10
- Open Browser and search CWE



V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
Nessus Essentials / Login
CWE - Common Weakness Enum
https://cwe.mitre.org
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
Top 25
Top HW CWE
New to CWE?
Start here!
ID Lookup:
Go
Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

2023 CWE Top 25 Most Dangerous Software Weaknesses New!

This list demonstrates the currently most common and impactful software weaknesses. Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.

Please see our Guidelines for New Content Suggestions
For other ways to get involved, contact us

CWE News

News Stubborn Weaknesses in the CWE Top 25 (Updated)

News CWE Top 25 Weaknesses Trends from 2019 Through 2023 Now Available

News 2023 CWE Top 25 Weaknesses "On the Cusp" List Now Available

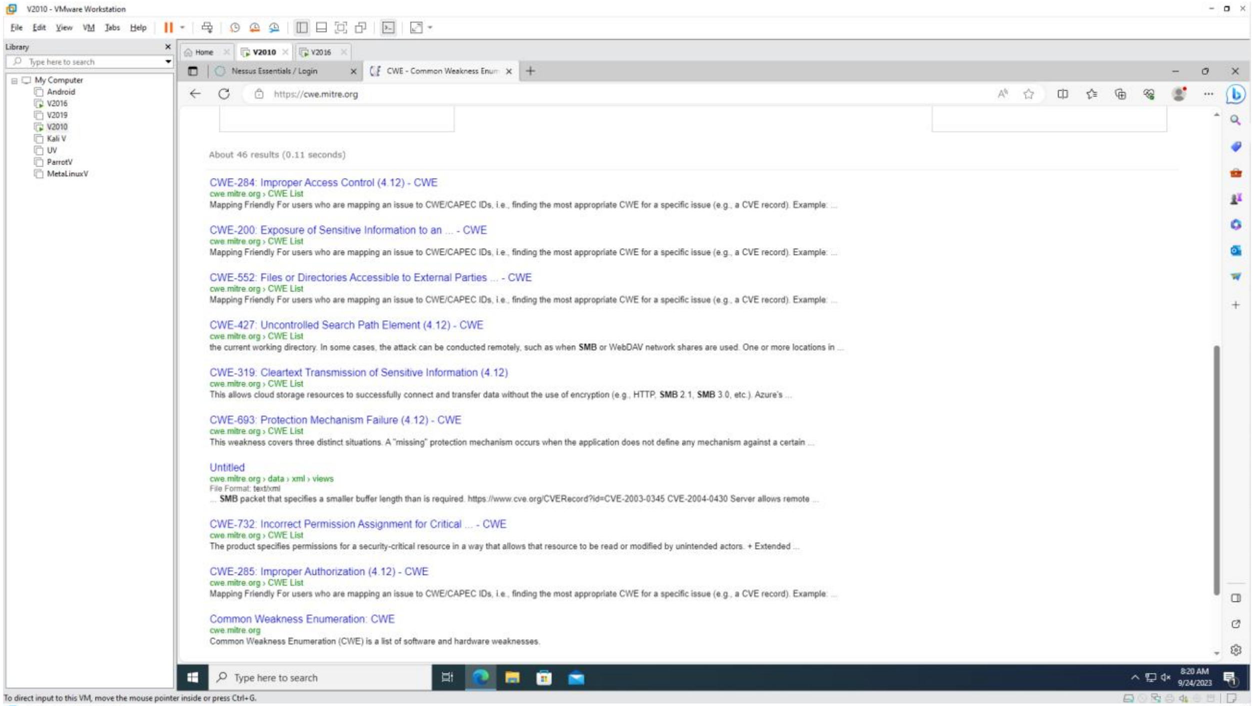
News 2023 "CWE Top 25" Now Available!

News CWE Version 4.12 Now Available

More >>

Type here to search
8:19 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Search SMB


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
Nessus Essentials / Login
CWE - Common Weakness Enum
https://cwe.mitre.org
Type here to search
8:20 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

About 46 results (0.11 seconds)

CWE-284: Improper Access Control (4.12) - CWE
cwe.mitre.org › CWE List
Mapping Friendly For users who are mapping an issue to CWE/CAPEC IDs, i.e., finding the most appropriate CWE for a specific issue (e.g., a CVE record). Example: ...

CWE-200: Exposure of Sensitive Information to an ... - CWE
cwe.mitre.org › CWE List
Mapping Friendly For users who are mapping an issue to CWE/CAPEC IDs, i.e., finding the most appropriate CWE for a specific issue (e.g., a CVE record). Example: ...

CWE-552: Files or Directories Accessible to External Parties ... - CWE
cwe.mitre.org › CWE List
Mapping Friendly For users who are mapping an issue to CWE/CAPEC IDs, i.e., finding the most appropriate CWE for a specific issue (e.g., a CVE record). Example: ...

CWE-427: Uncontrolled Search Path Element (4.12) - CWE
cwe.mitre.org › CWE List
the current working directory. In some cases, the attack can be conducted remotely, such as when **SMB** or WebDAV network shares are used. One or more locations in ...

CWE-319: Cleartext Transmission of Sensitive Information (4.12)
cwe.mitre.org › CWE List
This allows cloud storage resources to successfully connect and transfer data without the use of encryption (e.g., HTTP, **SMB** 2.1, **SMB** 3.0, etc.). Azure's ...

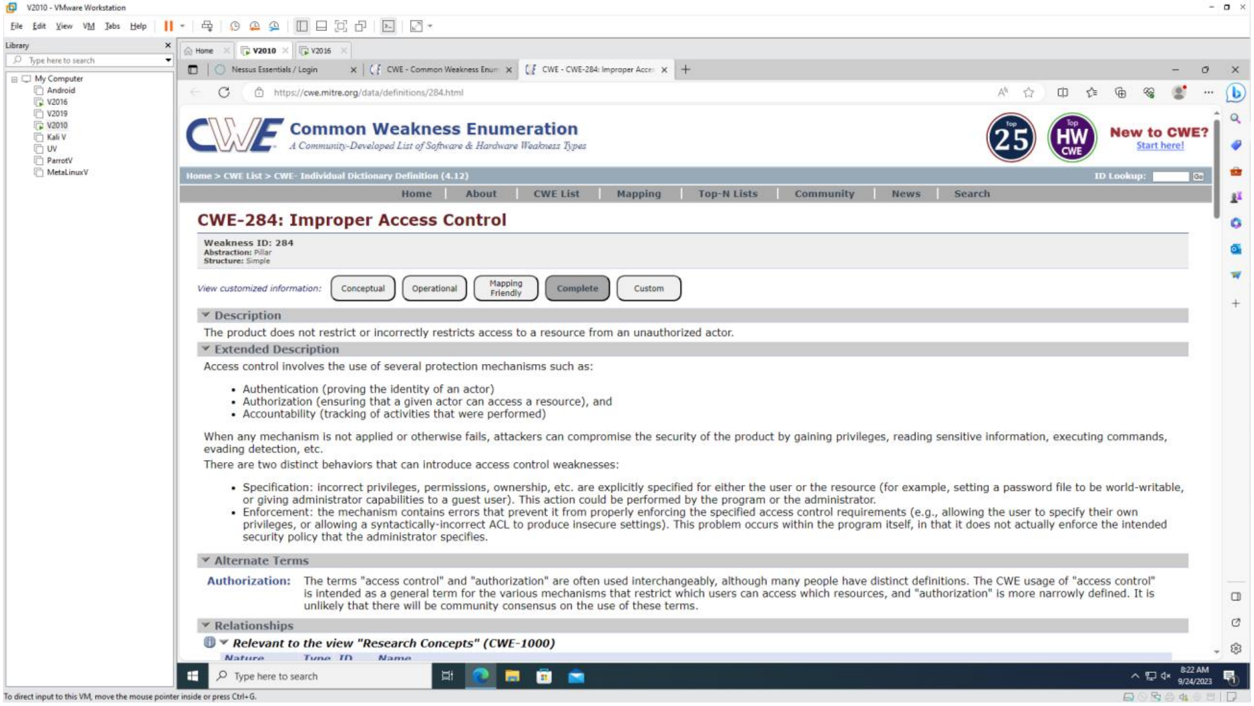
CWE-693: Protection Mechanism Failure (4.12) - CWE
cwe.mitre.org › CWE List
This weakness covers three distinct situations. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain ...

Untitled
cwe.mitre.org › data › xml › views
File Format: text/xml
... **SMB** packet that specifies a smaller buffer length than is required. https://www.cve.org/CVERecord?id=CVE-2003-0345 CVE-2004-0430 Server allows remote ...

CWE-732: Incorrect Permission Assignment for Critical ... - CWE
cwe.mitre.org › CWE List
The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors. + Extended ...

CWE-285: Improper Authorization (4.12) - CWE
cwe.mitre.org › CWE List
Mapping Friendly For users who are mapping an issue to CWE/CAPEC IDs, i.e., finding the most appropriate CWE for a specific issue (e.g., a CVE record). Example: ...

Common Weakness Enumeration: CWE
cwe.mitre.org
Common Weakness Enumeration (CWE) is a list of software and hardware weaknesses.


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
Nessus Essentials / Login
CWE - Common Weakness Enum
CWE - CWE-284: Improper Acce
https://cwe.mitre.org/data/definitions/284.html
Top 25
Top HW CWE
New to CWE?
Start here!
ID Lookup:
Go
Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search
Conceptual
Operational
Mapping Friendly
Complete
Custom
Type here to search
8:22 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE- Individual Dictionary Definition (4.12)

CWE-284: Improper Access Control

Weakness ID: 284
Abstraction: Pillar
Structure: Simple

View customized information:

Description

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Extended Description

Access control involves the use of several protection mechanisms such as:

- Authentication (proving the identity of an actor)
- Authorization (ensuring that a given actor can access a resource), and
- Accountability (tracking of activities that were performed)

When any mechanism is not applied or otherwise fails, attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc.

There are two distinct behaviors that can introduce access control weaknesses:

- Specification: incorrect privileges, permissions, ownership, etc. are explicitly specified for either the user or the resource (for example, setting a password file to be world-writable, or giving administrator capabilities to a guest user). This action could be performed by the program or the administrator.
- Enforcement: the mechanism contains errors that prevent it from properly enforcing the specified access control requirements (e.g., allowing the user to specify their own privileges, or allowing a syntactically-incorrect ACL to produce insecure settings). This problem occurs within the program itself, in that it does not actually enforce the intended security policy that the administrator specifies.

Alternate Terms

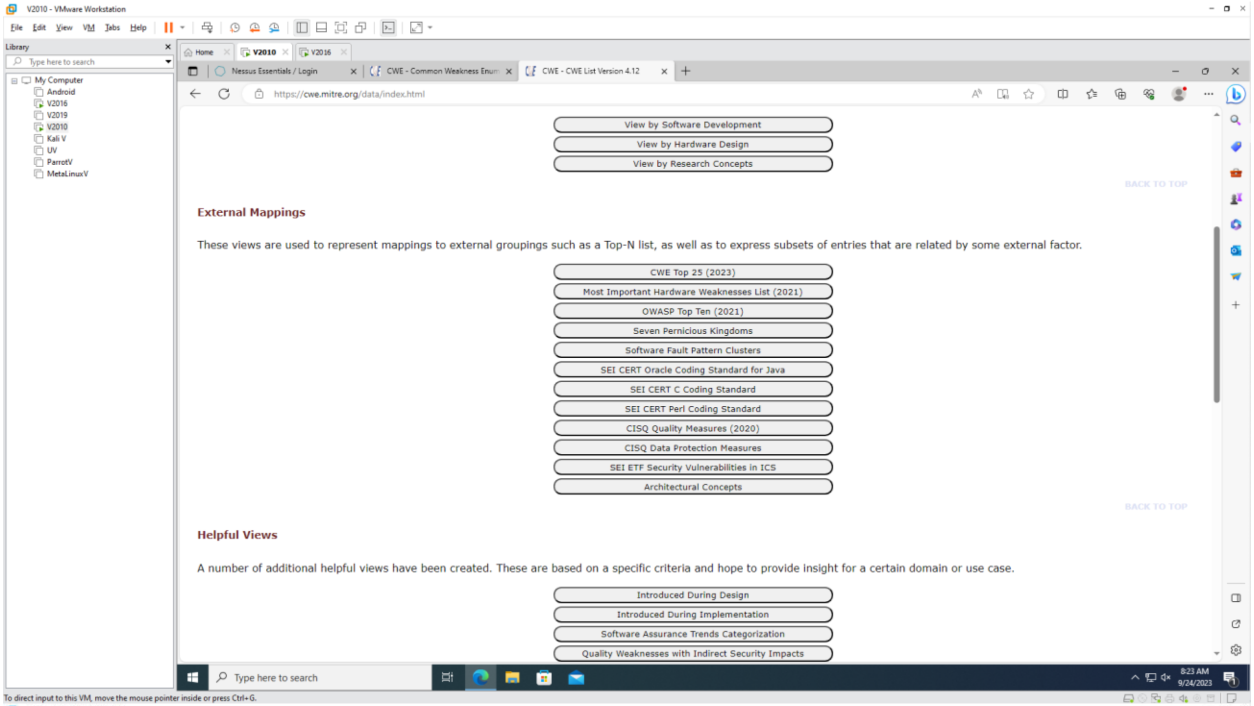
Authorization: The terms "access control" and "authorization" are often used interchangeably, although many people have distinct definitions. The CWE usage of "access control" is intended as a general term for the various mechanisms that restrict which users can access which resources, and "authorization" is more narrowly defined. It is unlikely that there will be community consensus on the use of these terms.

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature Type ID Name

- CWE list


https://cwe.mitre.org/data/index.html

View by Software Development
View by Hardware Design
View by Research Concepts

External Mappings

These views are used to represent mappings to external groupings such as a Top-N list, as well as to express subsets of entries that are related by some external factor.

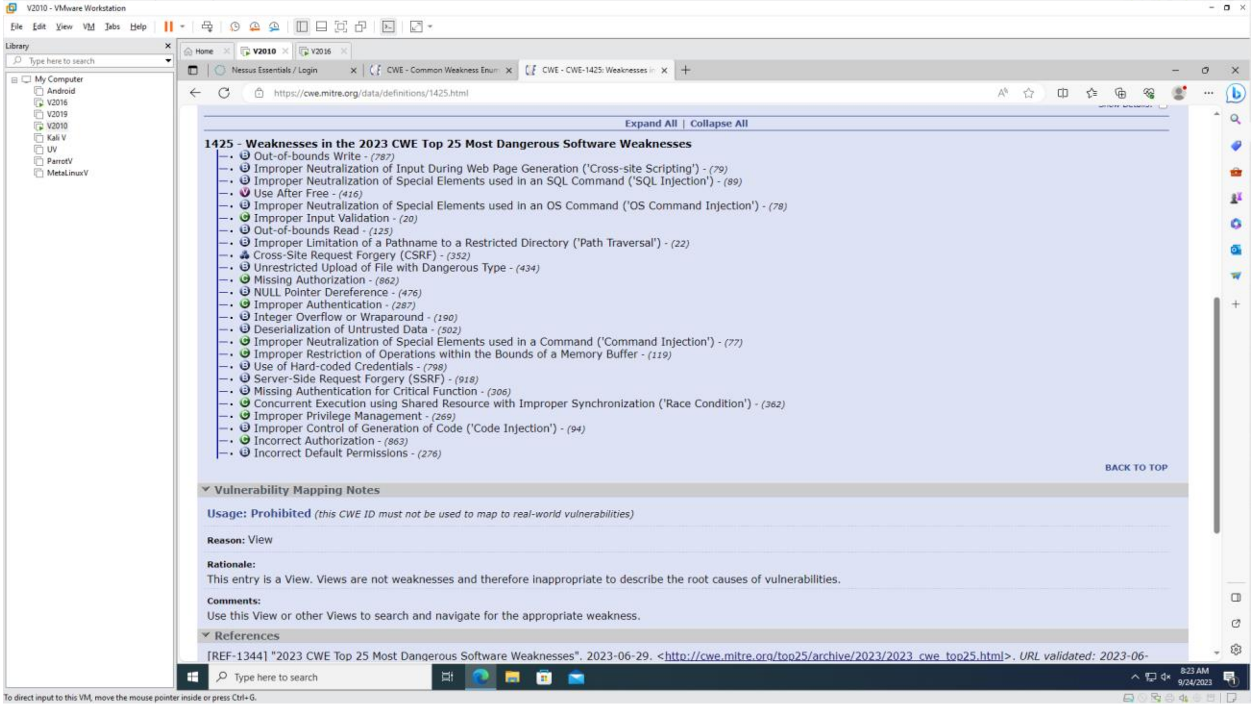
CWE Top 25 (2023)
Most Important Hardware Weaknesses List (2021)
OWASP Top Ten (2021)
Seven Pernicious Kingdoms
Software Fault Pattern Clusters
SEI CERT Oracle Coding Standard for Java
SEI CERT C Coding Standard
SEI CERT Perl Coding Standard
CISQ Quality Measures (2020)
CISQ Data Protection Measures
SEI ETF Security Vulnerabilities in ICS
Architectural Concepts

Helpful Views

A number of additional helpful views have been created. These are based on a specific criteria and hope to provide insight for a certain domain or use case.

Introduced During Design
Introduced During Implementation
Software Assurance Trends Categorization
Quality Weaknesses with Indirect Security Impacts

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
Nessus Essentials / Login
CWE - Common Weakness Enum
CWE - CWE List Version 4.12
BACK TO TOP
BACK TO TOP
Type here to search
8:23 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


https://cwe.mitre.org/data/definitions/1425.html

Expand All | Collapse All

1425 - Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses

- Out-of-bounds Write - *(787)*
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
- Use After Free - *(416)*
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
- Improper Input Validation - *(20)*
- Out-of-bounds Read - *(125)*
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - *(22)*
- Cross-Site Request Forgery (CSRF) - *(352)*
- Unrestricted Upload of File with Dangerous Type - *(434)*
- Missing Authorization - *(862)*
- NULL Pointer Dereference - *(476)*
- Improper Authentication - *(287)*
- Integer Overflow or Wraparound - *(190)*
- Deserialization of Untrusted Data - *(502)*
- Improper Neutralization of Special Elements used in a Command ('Command Injection') - *(77)*
- Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
- Use of Hard-coded Credentials - *(798)*
- Server-Side Request Forgery (SSRF) - *(918)*
- Missing Authentication for Critical Function - *(306)*
- Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') - *(362)*
- Improper Privilege Management - *(269)*
- Improper Control of Generation of Code ('Code Injection') - *(94)*
- Incorrect Authorization - *(863)*
- Incorrect Default Permissions - *(276)*

BACK TO TOP

Vulnerability Mapping Notes

Usage: Prohibited *(this CWE ID must not be used to map to real-world vulnerabilities)*

Reason: View

Rationale:
This entry is a View. Views are not weaknesses and therefore inappropriate to describe the root causes of vulnerabilities.

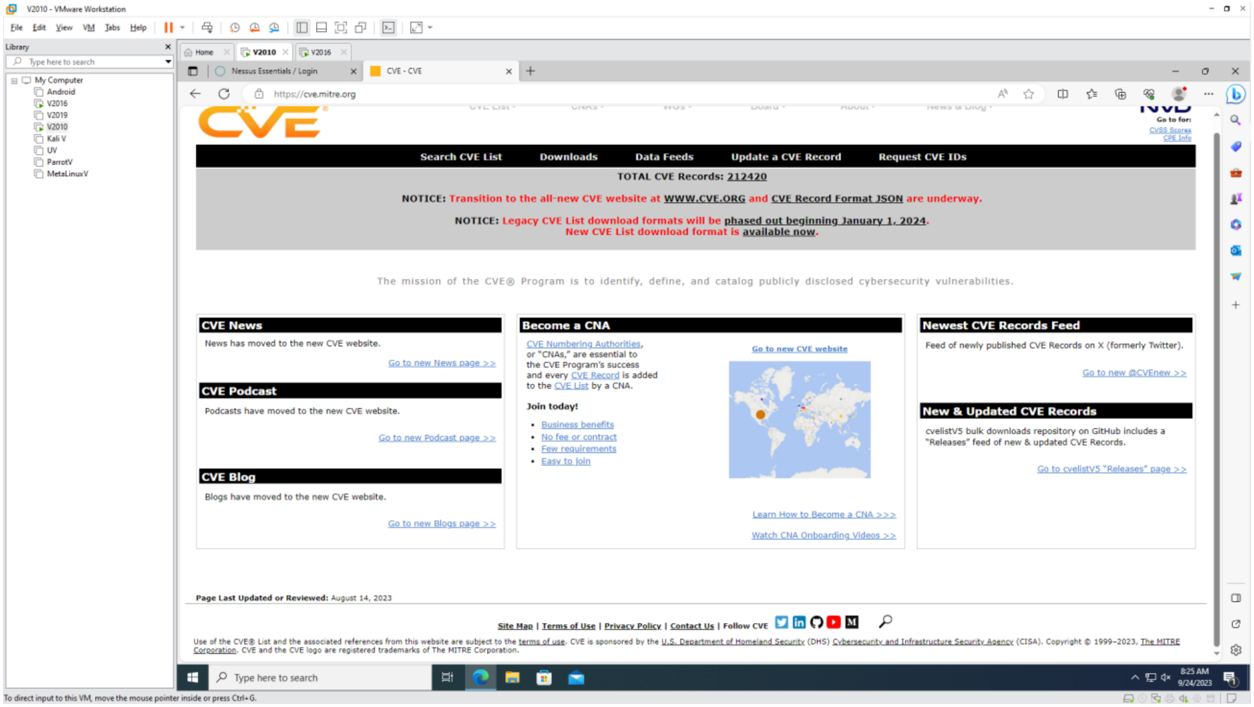
Comments:
Use this View or other Views to search and navigate for the appropriate weakness.

References

[REF-1344] "2023 CWE Top 25 Most Dangerous Software Weaknesses". 2023-06-29. <http://cwe.mitre.org/top25/archive/2023/2023_cwe_top25.html>. *URL validated: 2023-06-*

V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
Nessus Essentials / Login
CWE - Common Weakness Enum
CWE - CWE-1425: Weaknesses in
Type here to search
8:23 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)
- Open Windows 10
- Open Browser and search CVE



TOTAL CVE Records: 212420

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

Go to new News page >>

CVE Podcast

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

CVE Blog

Blogs have moved to the new CVE website.

Go to new Blogs page >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Go to new CVE website

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records Feed

Feed of newly published CVE Records on X (formerly Twitter).

Go to new @CVEnew >>

New & Updated CVE Records

cvelistV5 bulk downloads repository on GitHub includes a "Releases" feed of new & updated CVE Records.

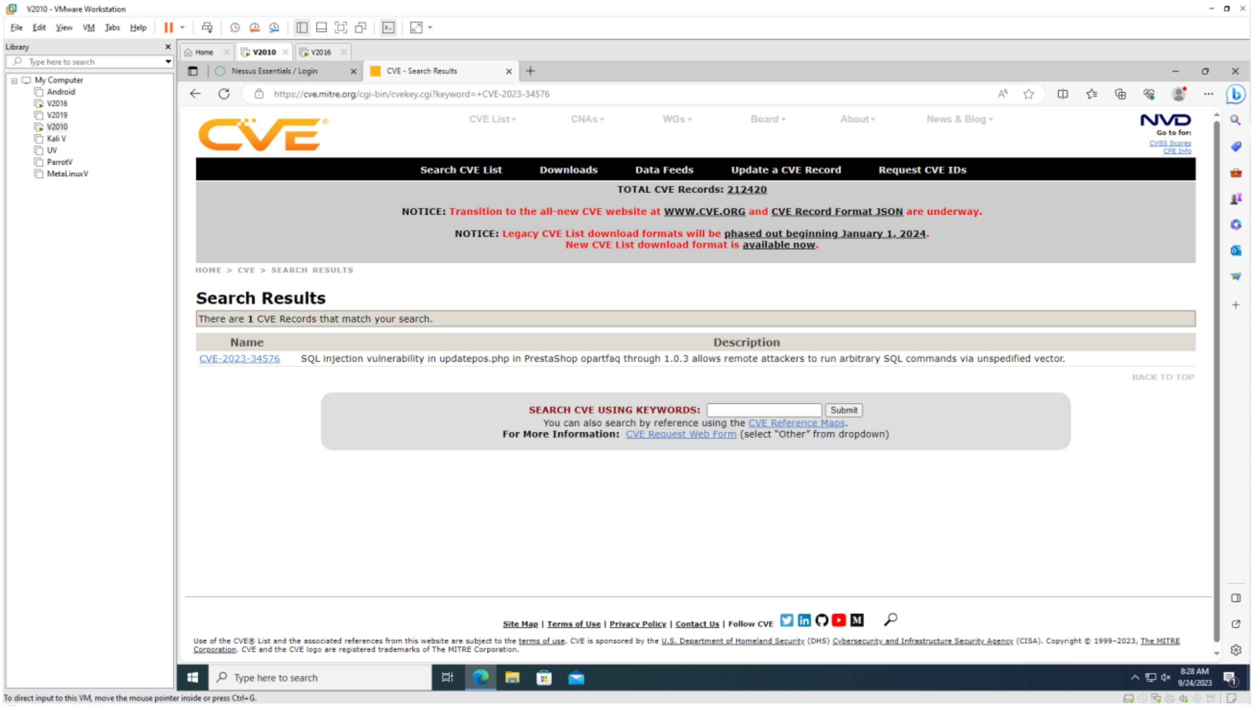
Go to cvelistV5 "Releases" page >>

Page Last Updated or Reviewed: August 14, 2023

Site Map | Terms of Use | Privacy Policy | Contact Us | Follow CVE

Use of the CVE® List and the associated references from this website are subject to the terms of use. CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2023, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.

- Search CVE



TOTAL CVE Records: 212420

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > SEARCH RESULTS

Search Results

There are **1** CVE Records that match your search.

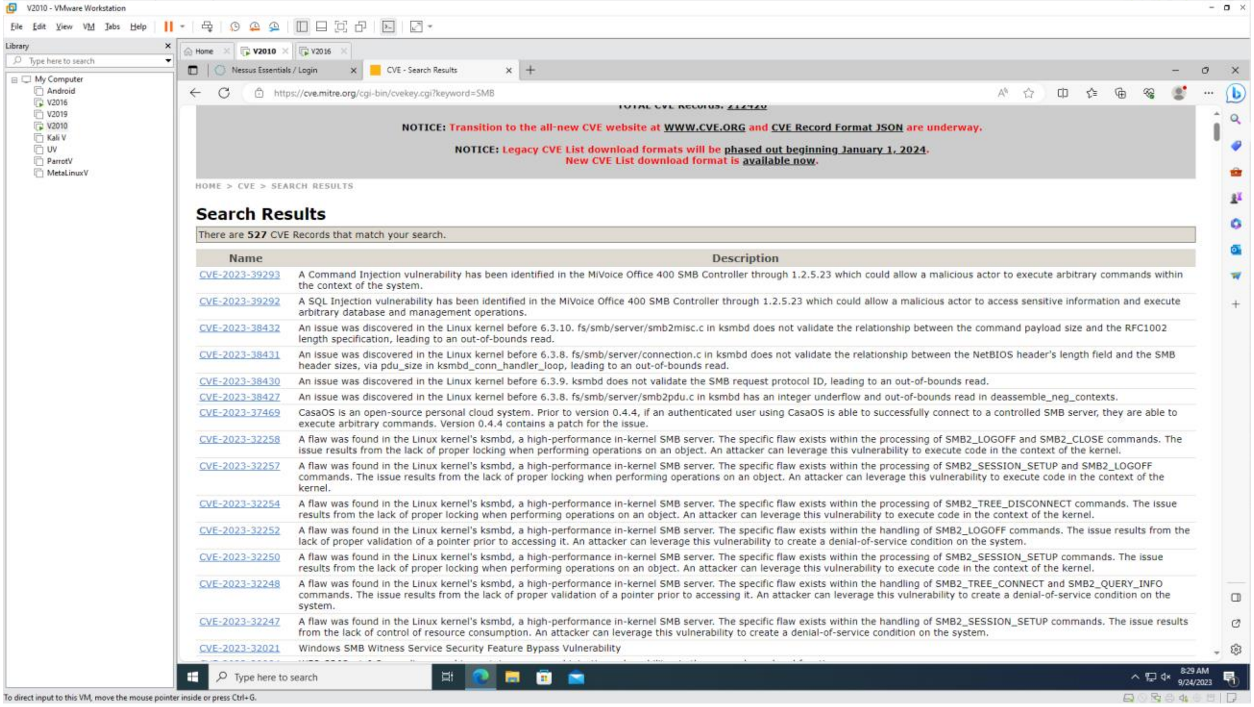
Name	Description
CVE-2023-34576	SQL injection vulnerability in updatepos.php in PrestaShop opartfaq through 1.0.3 allows remote attackers to run arbitrary SQL commands via unspedified vector.

BACK TO TOP

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.
For More Information: CVE Request Web Form (select "Other" from dropdown)

Site Map | Terms of Use | Privacy Policy | Contact Us | Follow CVE

Use of the CVE® List and the associated references from this website are subject to the terms of use. CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2023, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
Nessus Essentials / Login
CVE - Search Results
https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SMB
Type here to search
8:29 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

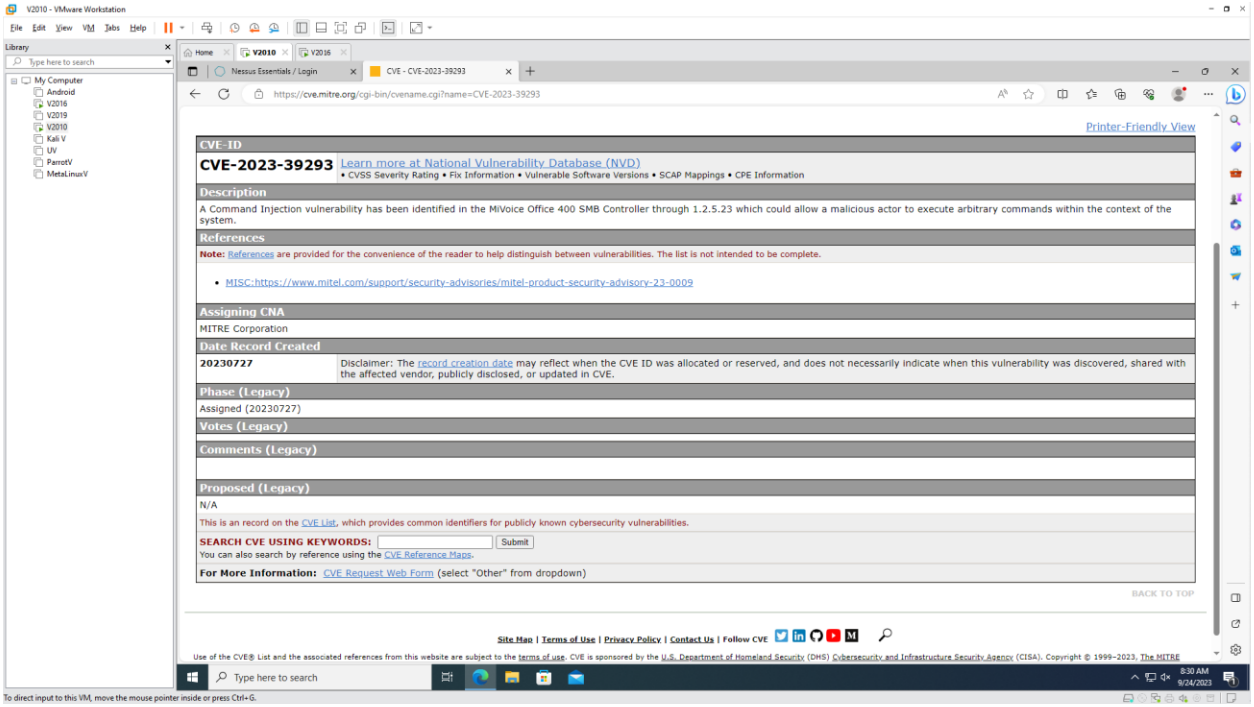
NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024.
New CVE List download format is available now.

HOME > CVE > SEARCH RESULTS

Search Results

There are **527** CVE Records that match your search.

Name	Description
CVE-2023-39293	A Command Injection vulnerability has been identified in the MiVoice Office 400 SMB Controller through 1.2.5.23 which could allow a malicious actor to execute arbitrary commands within the context of the system.
CVE-2023-39292	A SQL Injection vulnerability has been identified in the MiVoice Office 400 SMB Controller through 1.2.5.23 which could allow a malicious actor to access sensitive information and execute arbitrary database and management operations.
CVE-2023-38432	An issue was discovered in the Linux kernel before 6.3.10. fs/smb/server/smb2misc.c in ksmbd does not validate the relationship between the command payload size and the RFC1002 length specification, leading to an out-of-bounds read.
CVE-2023-38431	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/connection.c in ksmbd does not validate the relationship between the NetBIOS header's length field and the SMB header sizes, via pdu_size in ksmbd_conn_handler_loop, leading to an out-of-bounds read.
CVE-2023-38430	An issue was discovered in the Linux kernel before 6.3.9. ksmbd does not validate the SMB request protocol ID, leading to an out-of-bounds read.
CVE-2023-38427	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/smb2pdu.c in ksmbd has an integer underflow and out-of-bounds read in deassemble_neg_contexts.
CVE-2023-37469	CasaOS is an open-source personal cloud system. Prior to version 0.4.4, if an authenticated user using CasaOS is able to successfully connect to a controlled SMB server, they are able to execute arbitrary commands. Version 0.4.4 contains a patch for the issue.
CVE-2023-32258	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_LOGOFF and SMB2_CLOSE commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.
CVE-2023-32257	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP and SMB2_LOGOFF commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.
CVE-2023-32254	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_TREE_DISCONNECT commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.
CVE-2023-32252	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_LOGOFF commands. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.
CVE-2023-32250	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.
CVE-2023-32248	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_TREE_CONNECT and SMB2_QUERY_INFO commands. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.
CVE-2023-32247	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_SESSION_SETUP commands. The issue results from the lack of control of resource consumption. An attacker can leverage this vulnerability to create a denial-of-service condition on the system.
CVE-2023-32021	Windows SMB Witness Service Security Feature Bypass Vulnerability


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
Nessus Essentials / Login
CVE - CVE-2023-39293
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-39293
Type here to search
8:30 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Printer-Friendly View

CVE-ID	
CVE-2023-39293	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
A Command Injection vulnerability has been identified in the MiVoice Office 400 SMB Controller through 1.2.5.23 which could allow a malicious actor to execute arbitrary commands within the context of the system.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-23-0009	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20230727	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20230727)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: Submit You can also search by reference using the CVE Reference Maps.	
For More Information: CVE Request Web Form (select "Other" from dropdown)	

BACK TO TOP

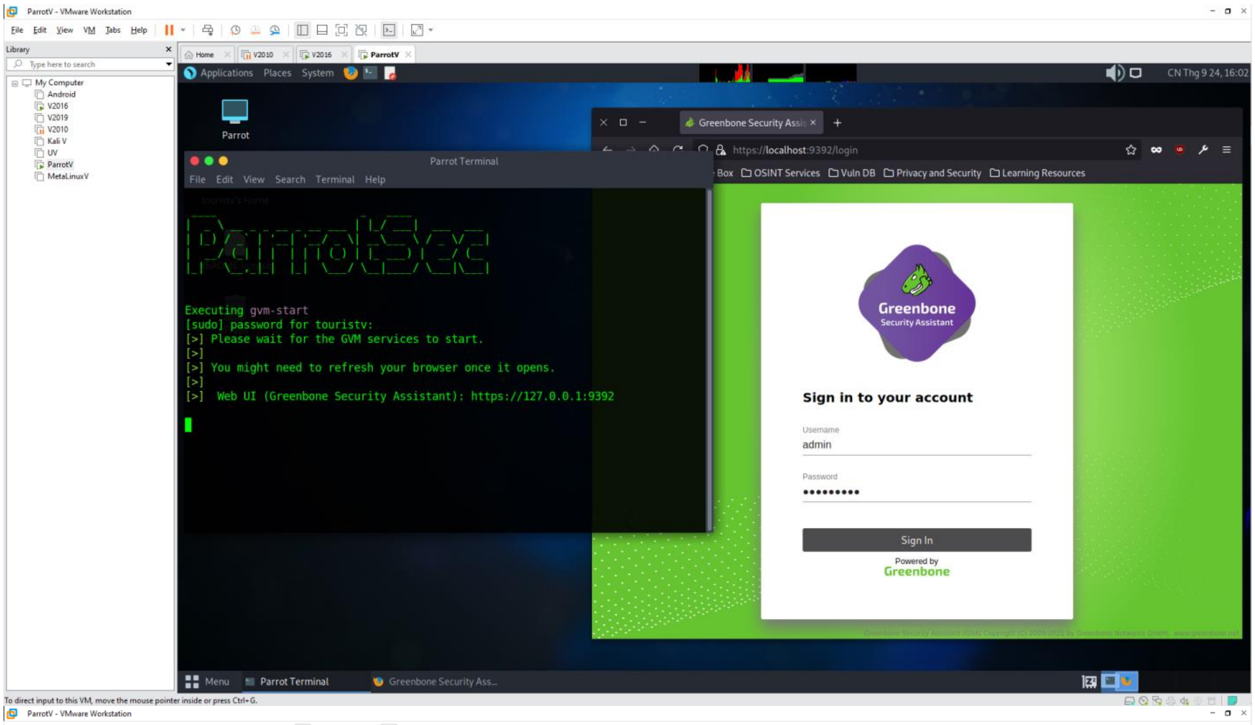
Site Map | Terms of Use | Privacy Policy | Contact Us | Follow CVE

Use of the CVE® List and the associated references from this website are subject to the terms of use. CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2023, The MITRE

2, Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

2.1 Perform Vulnerability Analysis using OpenVAS

- Open Parrot and Windows Server 2016



```
Executing gvm-start
[sudo] password for touristv:
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

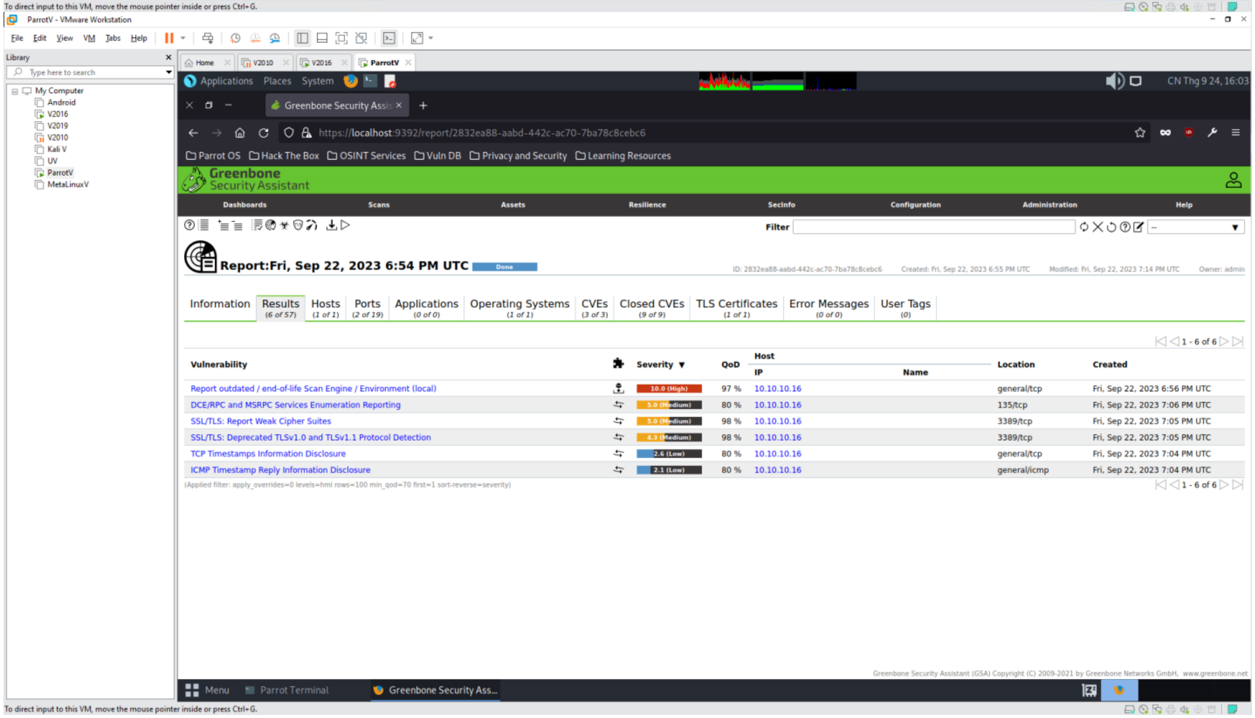
https://localhost:9392/login

Sign in to your account

Username: admin

Password: •••••••••

Sign In



https://localhost:9392/report/2832ea88-aabd-442c-ac70-7ba78c8cebc6

Report:Fri, Sep 22, 2023 6:54 PM UTC Done

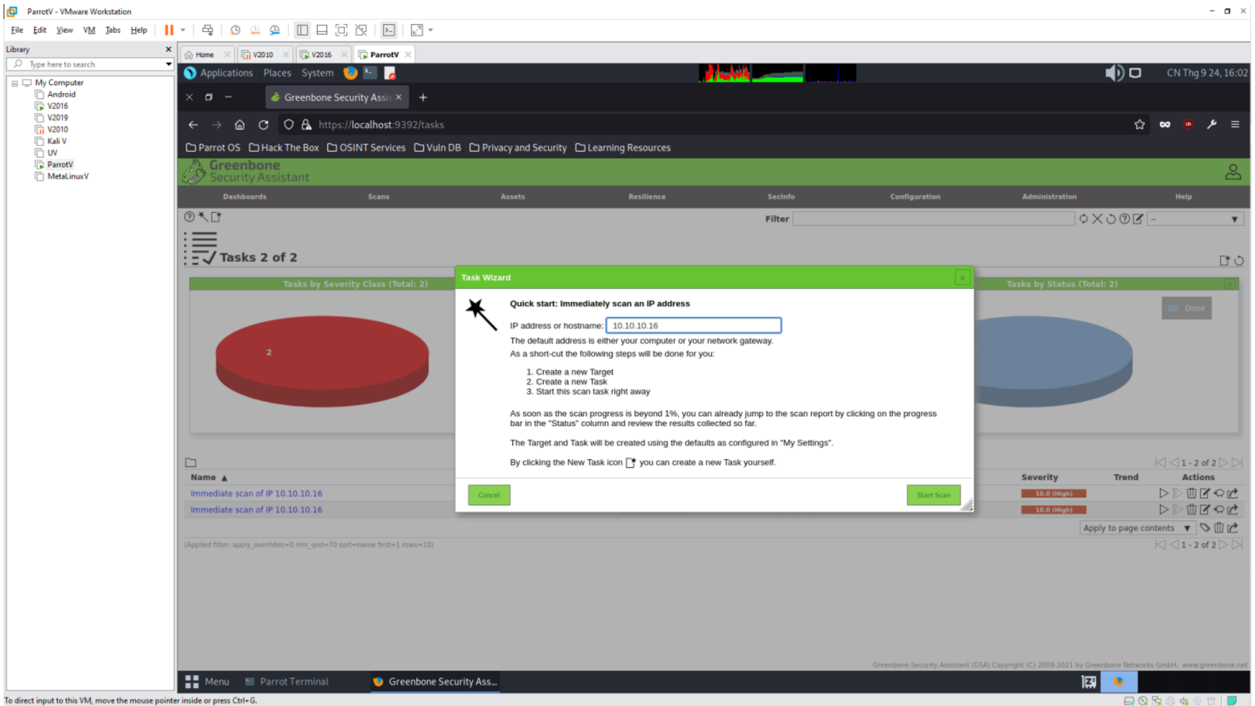
ID: 2832ea88-aabd-442c-ac70-7ba78c8cebc6 Created: Fri, Sep 22, 2023 6:55 PM UTC Modified: Fri, Sep 22, 2023 7:14 PM UTC Owner: admin

Information | Results (6 of 57) | Hosts (1 of 1) | Ports (2 of 19) | Applications (0 of 0) | Operating Systems (1 of 1) | CVEs (3 of 3) | Closed CVEs (9 of 9) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

1 - 6 of 6

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	10.10.10.16		general/tcp	Fri, Sep 22, 2023 6:56 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.10.10.16		135/tcp	Fri, Sep 22, 2023 7:06 PM UTC
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	98 %	10.10.10.16		3389/tcp	Fri, Sep 22, 2023 7:05 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	10.10.10.16		3389/tcp	Fri, Sep 22, 2023 7:05 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	10.10.10.16		general/tcp	Fri, Sep 22, 2023 7:04 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	10.10.10.16		general/icmp	Fri, Sep 22, 2023 7:04 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)



Task Wizard

Quick start: Immediately scan an IP address

IP address or hostname: 10.10.10.16

The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

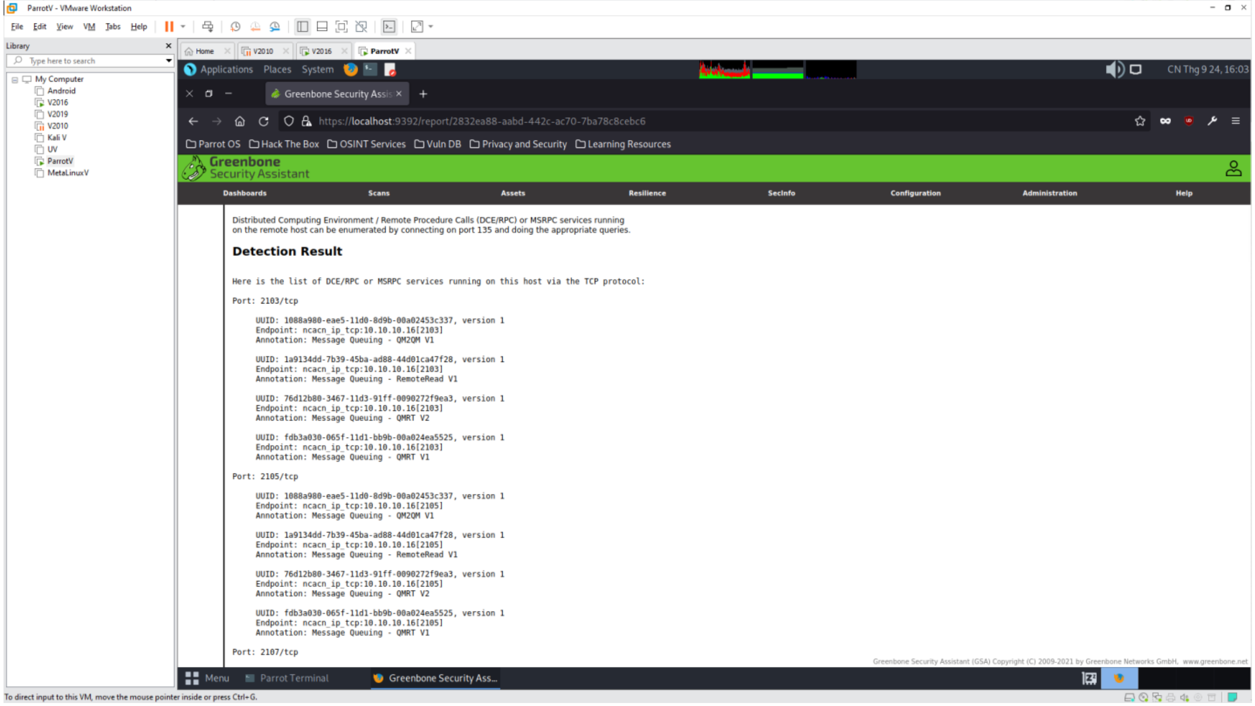
The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

Cancel | Start Scan

Name ▲	Severity
Immediate scan of IP 10.10.10.16	10.0 (High)
Immediate scan of IP 10.10.10.16	10.0 (High)

ParrotV - VMware Workstation
Tasks 2 of 2
Tasks by Severity Class (Total: 2)
Tasks by Status (Total: 2)
Done
https://localhost:9392/tasks
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help



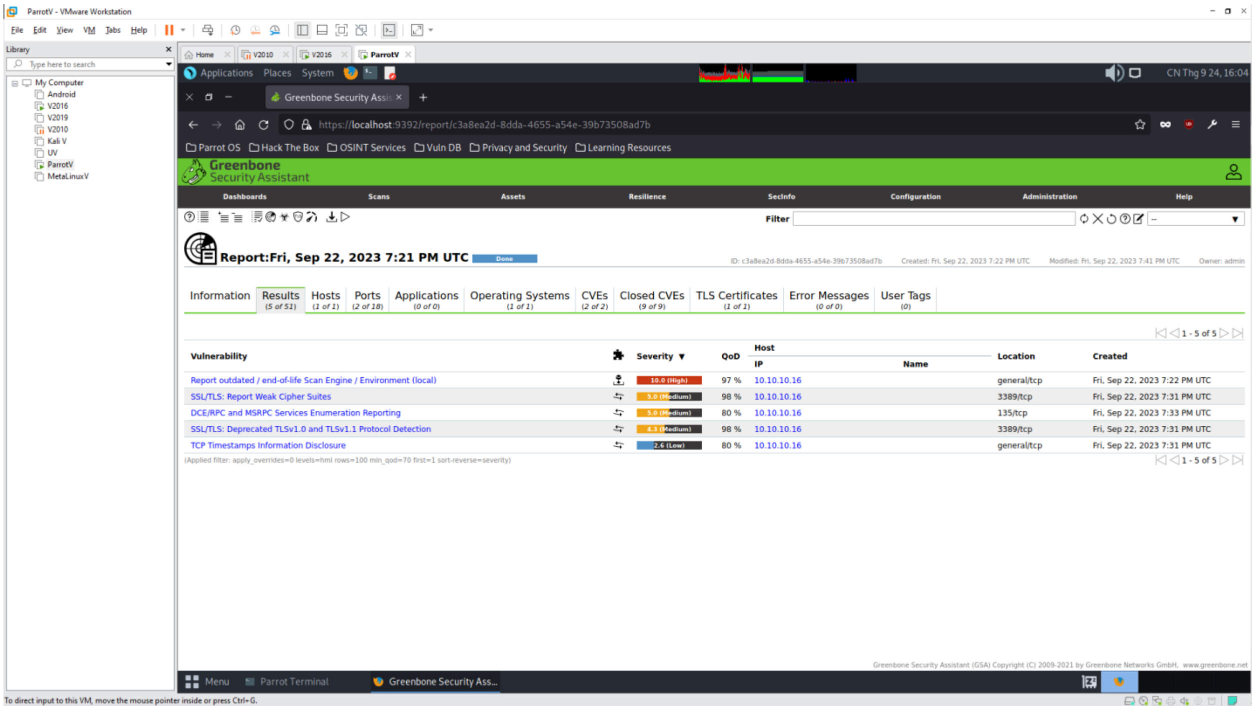
https://localhost:9392/report/2832ea88-aabd-442c-ac70-7ba78c8cebc6

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 2103/tcp

     UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2103]
     Annotation: Message Queuing - QM2QM V1

     UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2103]
     Annotation: Message Queuing - RemoteRead V1

     UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2103]
     Annotation: Message Queuing - QMRT V2

     UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2103]
     Annotation: Message Queuing - QMRT V1

Port: 2105/tcp

     UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2105]
     Annotation: Message Queuing - QM2QM V1

     UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2105]
     Annotation: Message Queuing - RemoteRead V1

     UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2105]
     Annotation: Message Queuing - QMRT V2

     UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1
     Endpoint: ncacn_ip_tcp:10.10.10.16[2105]
     Annotation: Message Queuing - QMRT V1

Port: 2107/tcp
```

- Turn on firewall on Windows Server 2016



Report:Fri, Sep 22, 2023 7:21 PM UTC Done

ID: c3a8ea2d-8dda-4655-a54e-39b73508ad7b Created: Fri, Sep 22, 2023 7:22 PM UTC Modified: Fri, Sep 22, 2023 7:41 PM UTC Owner: admin

Information | Results (5 of 51) | Hosts (1 of 1) | Ports (2 of 18) | Applications (0 of 0) | Operating Systems (1 of 1) | CVEs (2 of 2) | Closed CVEs (9 of 9) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0)

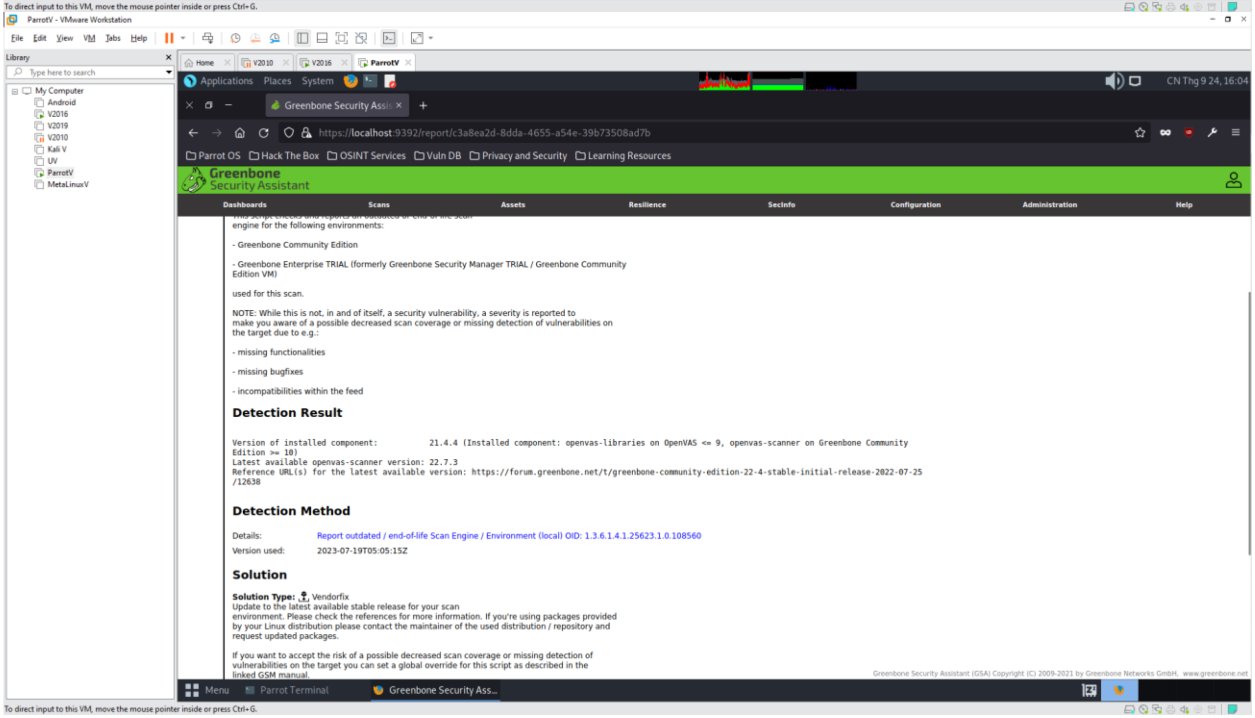
1 - 5 of 5

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	10.10.10.16		general/tcp	Fri, Sep 22, 2023 7:22 PM UTC
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	10.10.10.16		3389/tcp	Fri, Sep 22, 2023 7:31 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	10.10.10.16		135/tcp	Fri, Sep 22, 2023 7:33 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	10.10.10.16		3389/tcp	Fri, Sep 22, 2023 7:31 PM UTC
TCP Timestamps Information Disclosure	⇆	2.6 (Low)	80 %	10.10.10.16		general/tcp	Fri, Sep 22, 2023 7:31 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 5 of 5

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
ParrotV
Applications Places System
CN Thg 9 24, 16:04
Greenbone Security Assis
https://localhost:9392/report/c3a8ea2d-8dda-4655-a54e-39b73508ad7b
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net
Menu
Parrot Terminal
Greenbone Security Ass...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



This script checks and reports an outdated or end-of-life scan engine for the following environments:

- Greenbone Community Edition

- Greenbone Enterprise TRIAL (formerly Greenbone Security Manager TRIAL / Greenbone Community Edition VM)

used for this scan.

NOTE: While this is not, in and of itself, a security vulnerability, a severity is reported to make you aware of a possible decreased scan coverage or missing detection of vulnerabilities on the target due to e.g.:

- missing functionalities

- missing bugfixes

- incompatibilities within the feed

Detection Result

```
Version of installed component:          21.4.4 (Installed component: openvas-libraries on OpenVAS <= 9, openvas-scanner on Greenbone Community
Edition >= 10)
Latest available openvas-scanner version: 22.7.3
Reference URL(s) for the latest available version: https://forum.greenbone.net/t/greenbone-community-edition-22-4-stable-initial-release-2022-07-25
/12638
```

Detection Method

Details: Report outdated / end-of-life Scan Engine / Environment (local) OID: 1.3.6.1.4.1.25623.1.0.108560

Version used: 2023-07-19T05:05:15Z

Solution

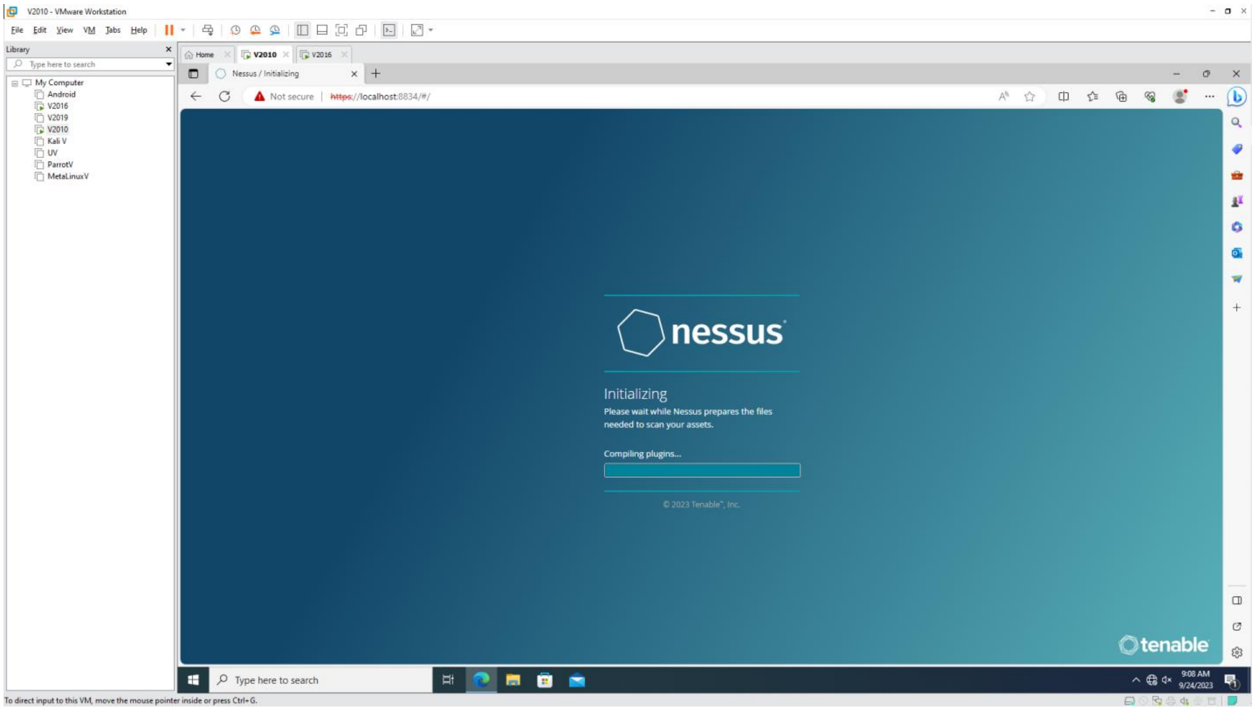
Solution Type: Vendorfix

Update to the latest available stable release for your scan environment. Please check the references for more information. If you're using packages provided by your Linux distribution please contact the maintainer of the used distribution / repository and request updated packages.

If you want to accept the risk of a possible decreased scan coverage or missing detection of vulnerabilities on the target you can set a global override for this script as described in the linked GSM manual.

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
V2016
ParrotV
Applications Places System
CN Thg 9 24, 16:04
Greenbone Security Assis
https://localhost:9392/report/c3a8ea2d-8dda-4655-a54e-39b73508ad7b
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net
Menu
Parrot Terminal
Greenbone Security Ass...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2.2 Perform Vulnerability Scanning using Nessus
- Open Windows 10 and Windows Server 2016
- Install Nessus



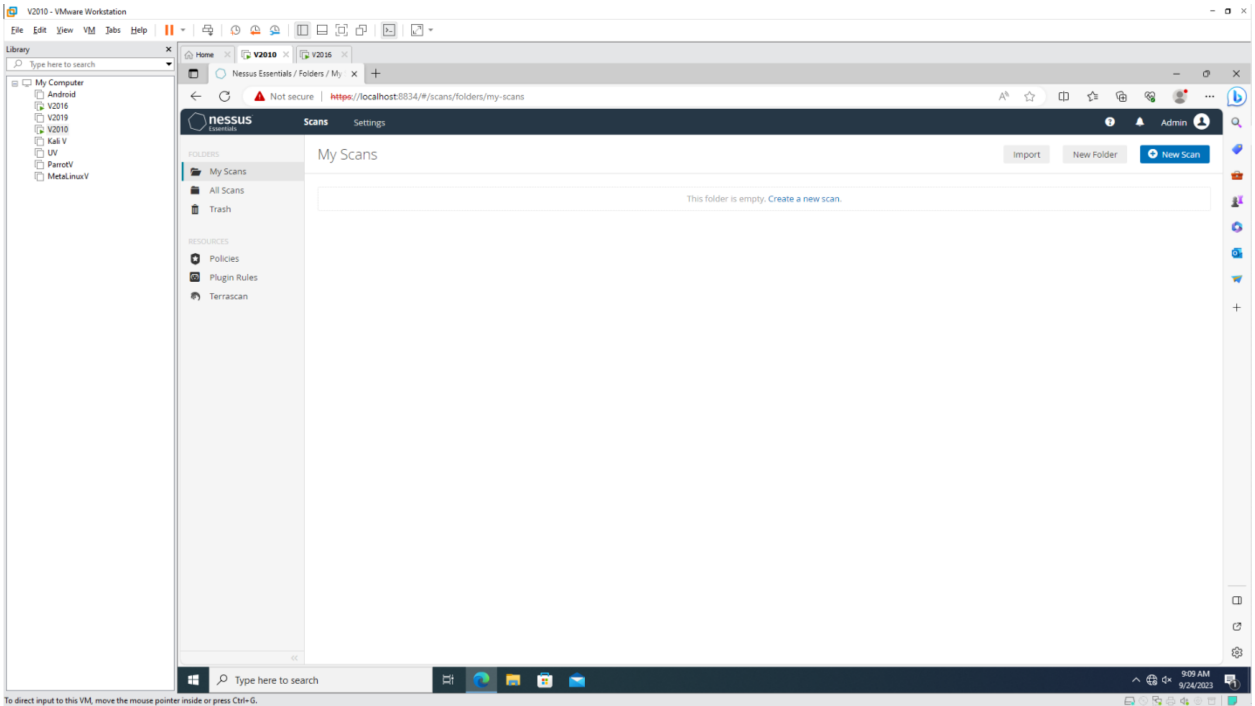
Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Compiling plugins...

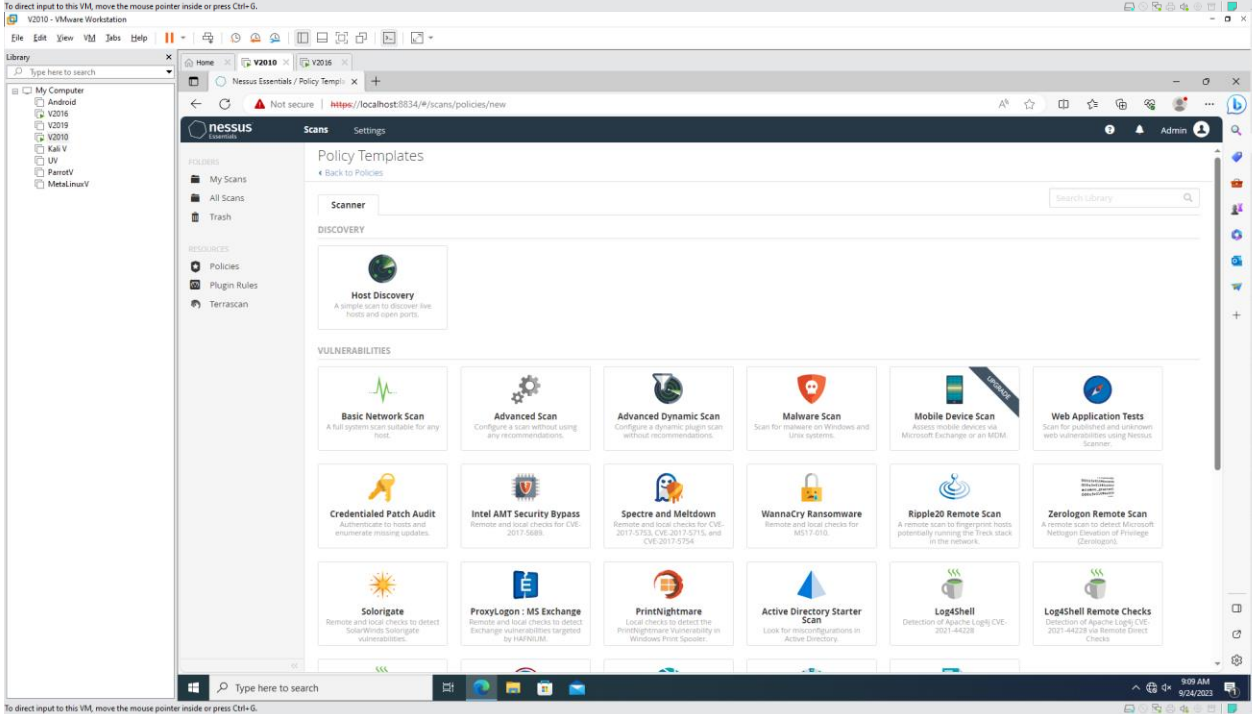
© 2023 Tenable®, Inc.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



My Scans

This folder is empty. Create a new scan.



Policy Templates

‹ Back to Policies

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.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

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.

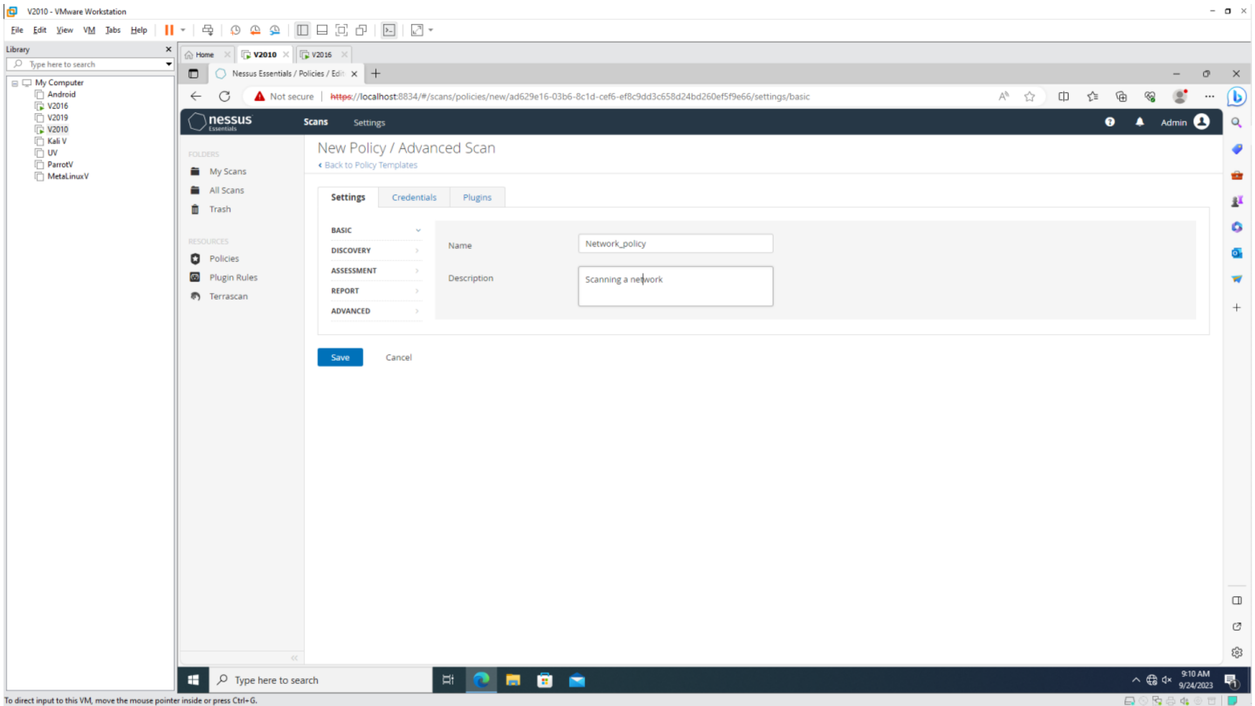
ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Log4Shell
Detection of Apache Log4j CVE-2021-44228

Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Nessus Essentials / Policies / Edit
Not secure
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/basic
nessus Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Type here to search
9:10 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

New Policy / Advanced Scan

‹ Back to Policy Templates

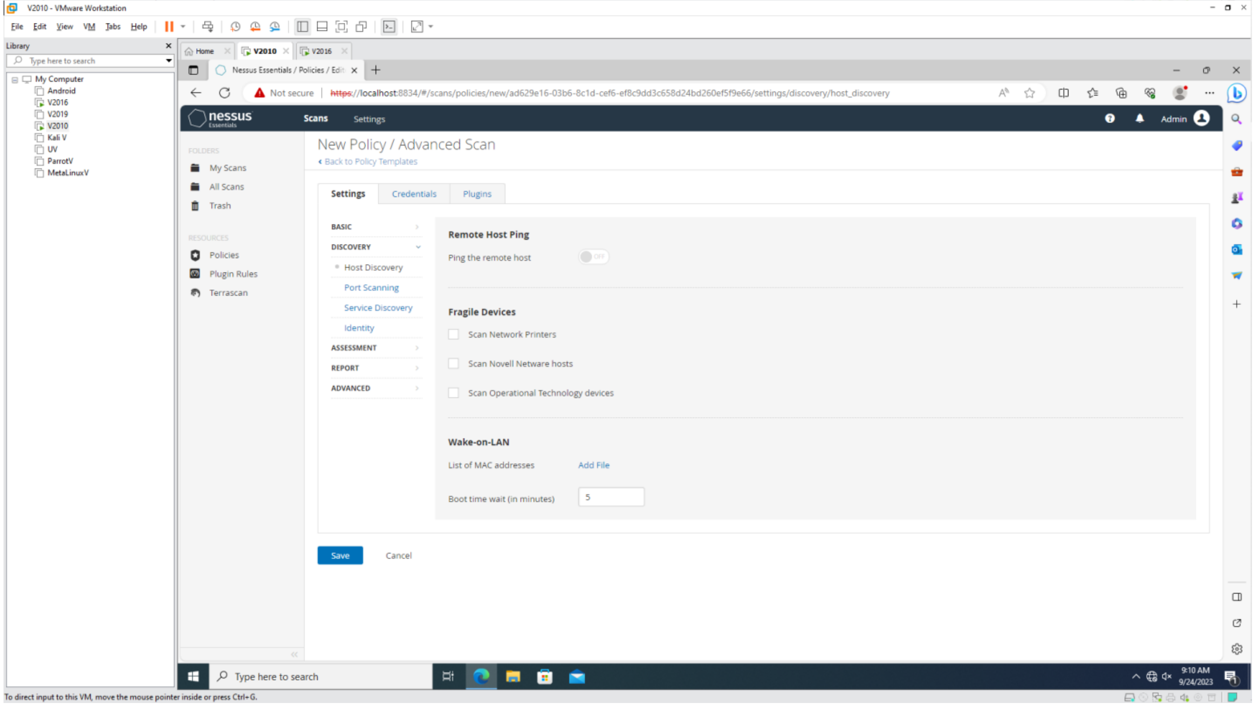
Settings | Credentials | Plugins

BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Name: Network_policy

Description: Scanning a network

Save | Cancel


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Nessus Essentials / Policies / Edit
Not secure
https://localhost:8834/#/scans/policies/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/discovery/host_discovery
nessus Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Type here to search
9:10 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

New Policy / Advanced Scan

‹ Back to Policy Templates

Settings | Credentials | Plugins

BASIC
DISCOVERY
- Host Discovery
- Port Scanning
- Service Discovery
- Identity

ASSESSMENT
REPORT
ADVANCED

Remote Host Ping

Ping the remote host: OFF

Fragile Devices

□ Scan Network Printers

□ Scan Novell Netware hosts

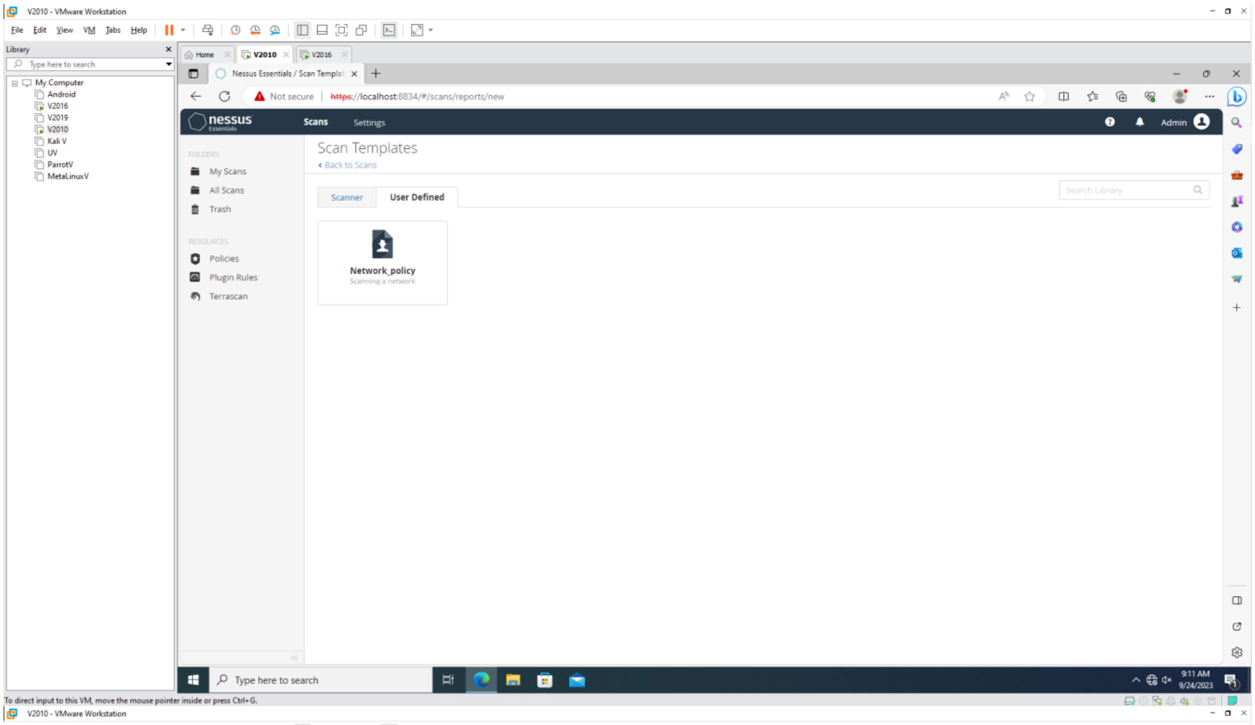
□ Scan Operational Technology devices

Wake-on-LAN

List of MAC addresses: Add File

Boot time wait (in minutes): 5

Save | Cancel



https://localhost:8834/#/scans/reports/new

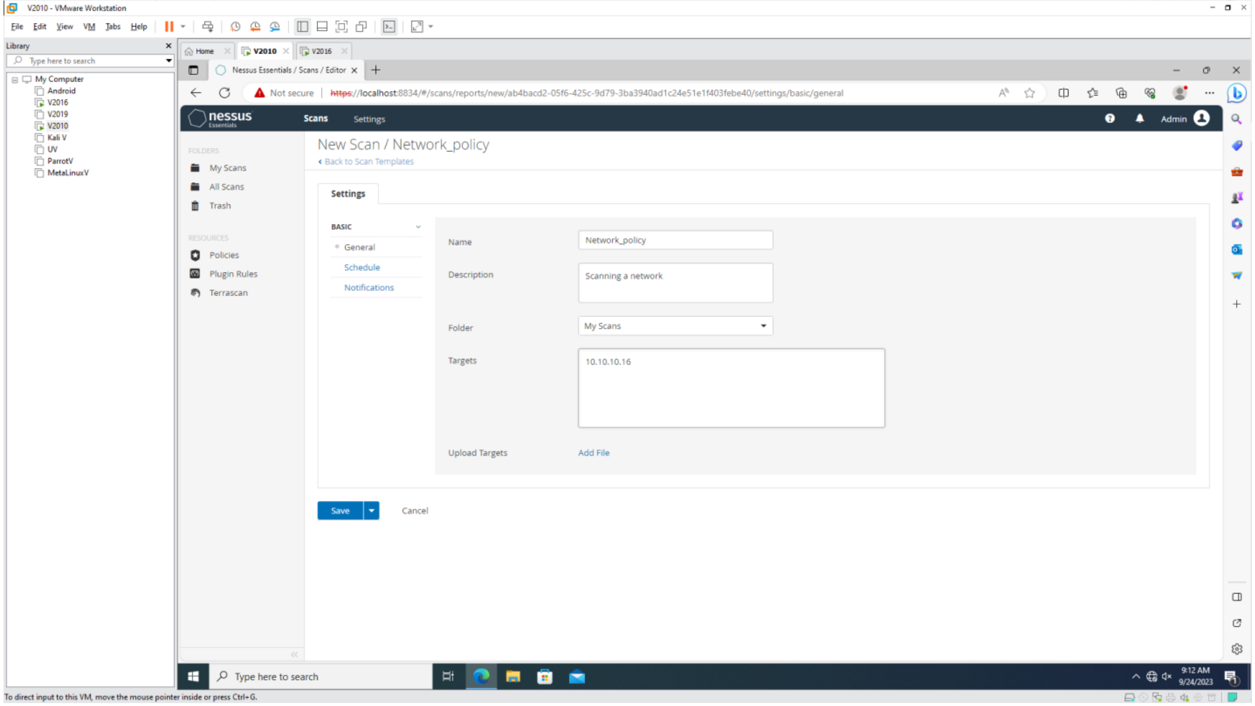
Scan Templates

‹ Back to Scans

Network_policy

Scanning a network

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



https://localhost:8834/#/scans/reports/new/ab4bacd2-05f6-425c-9d79-3ba3940ad1c24e51e1f403febe40/settings/basic/general

New Scan / Network_policy

‹ Back to Scan Templates

Name: Network_policy

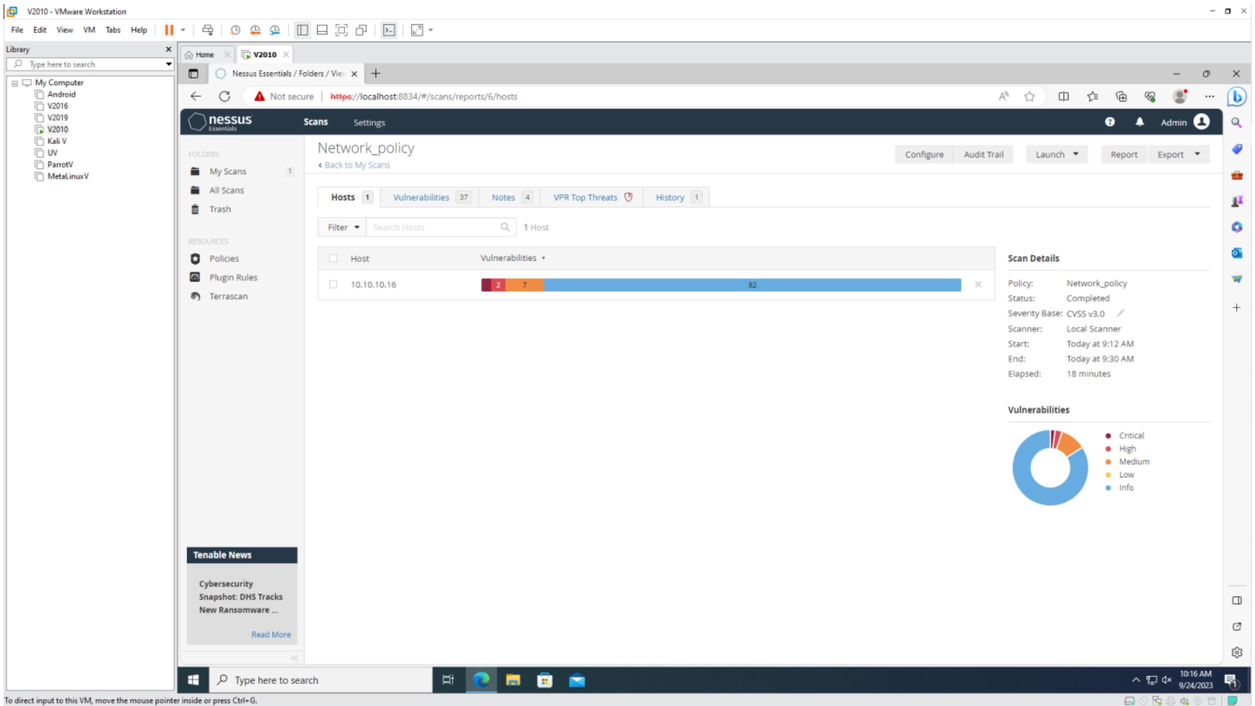
Description: Scanning a network

Folder: My Scans

Targets: 10.10.10.16

Upload Targets: Add File

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Not secure | https://localhost:8834/#/scans/reports/6/hosts

Network_policy

‹ Back to My Scans

Hosts 1 | Vulnerabilities 37 | Notes 4 | VPR Top Threats | History 1

Filter ▾ Search Hosts 1 Host

Host	Vulnerabilities ▾
10.10.10.16	2 7 82

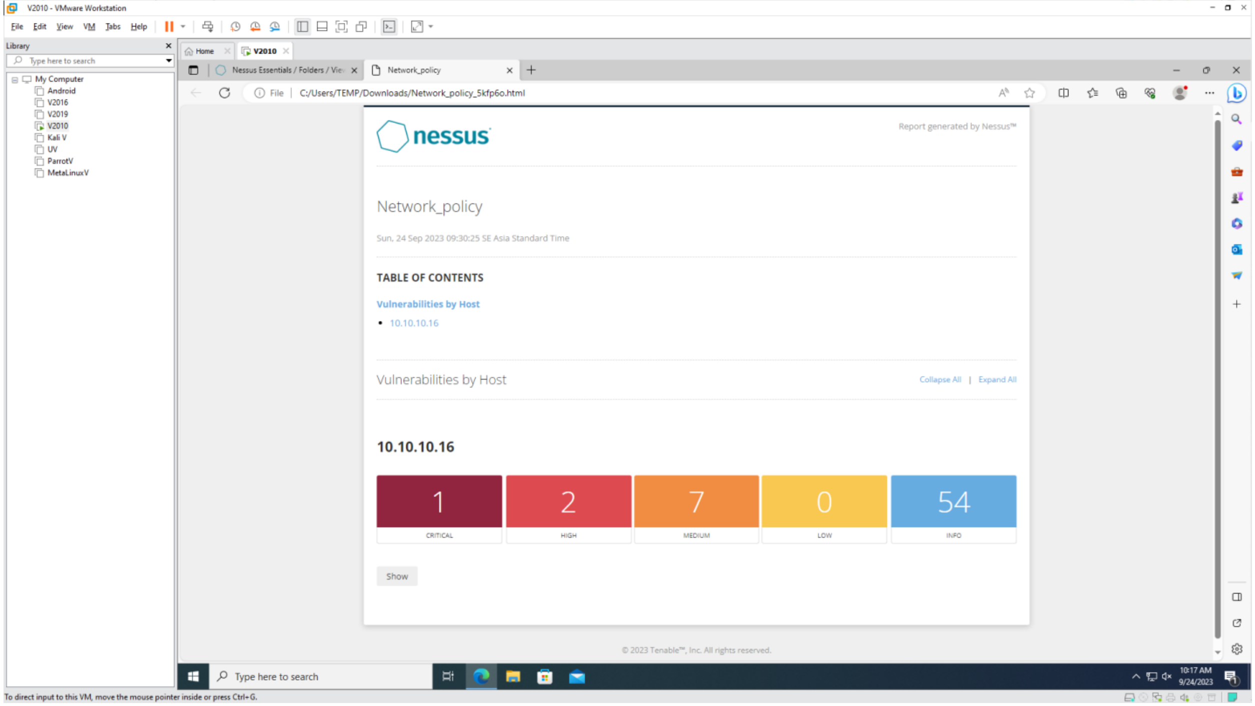
Scan Details

Policy:	Network_policy
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 9:12 AM
End:	Today at 9:30 AM
Elapsed:	18 minutes

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



File | C:/Users/TEMP/Downloads/Network_policy_5kfp6o.html

nessus

Report generated by Nessus™

Network_policy

Sun, 24 Sep 2023 09:30:25 SE Asia Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.10.10.16

Vulnerabilities by Host

Collapse All | Expand All

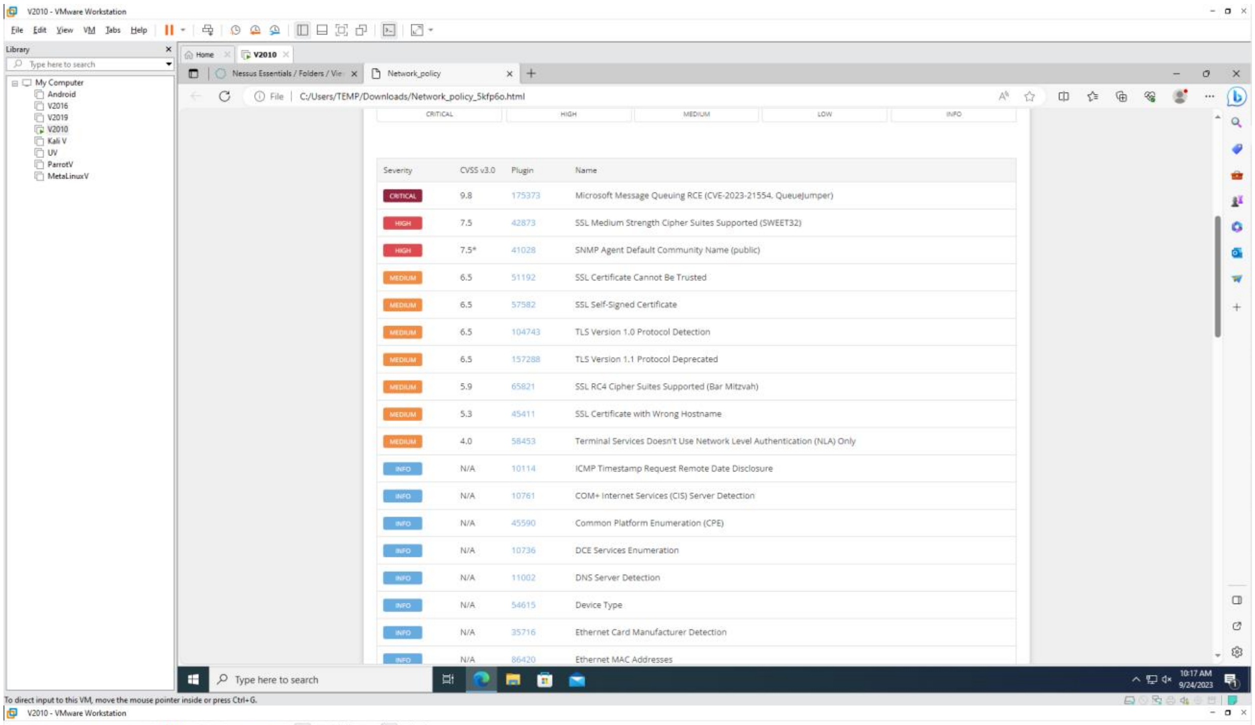
10.10.10.16

1	2	7	0	54
CRITICAL	HIGH	MEDIUM	LOW	INFO

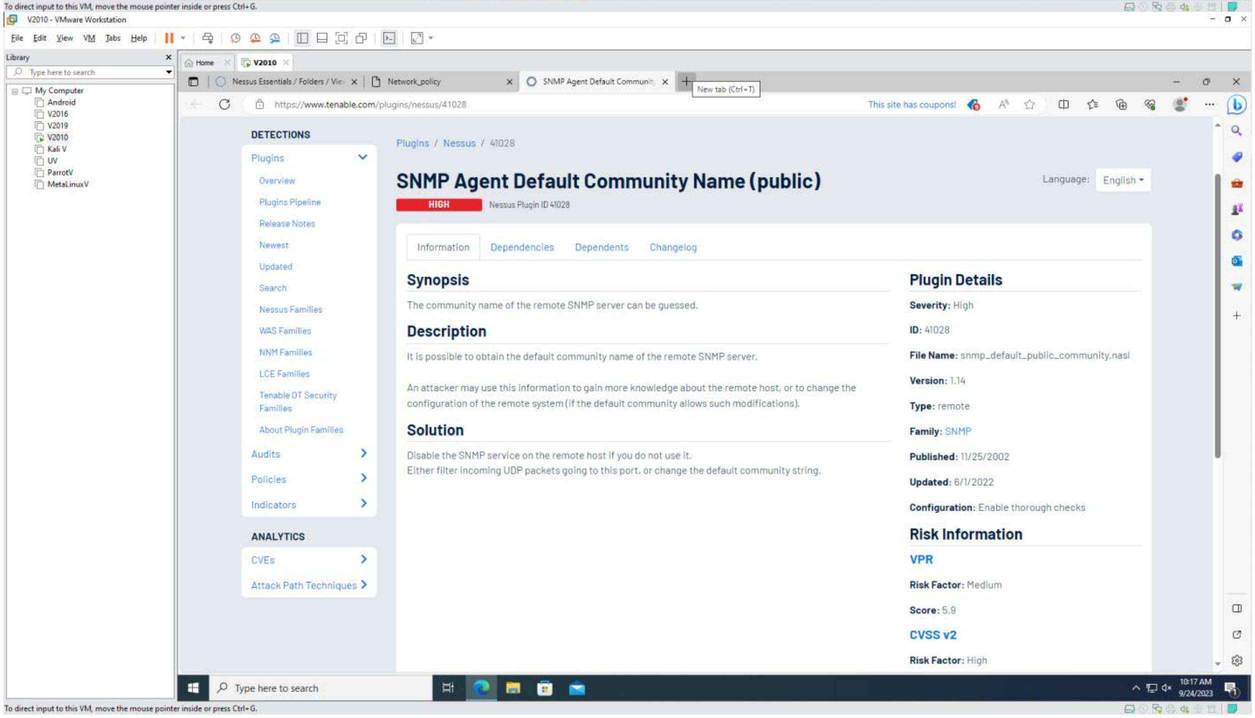
Show

© 2023 Tenable™, Inc. All rights reserved.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
V2010
Nessus Essentials / Folders / Vie
Network_policy
File C:/Users/TEMP/Downloads/Network_policy_5kfp6o.html
CRITICAL
HIGH
MEDIUM
LOW
INFO
Type here to search
10:17 AM
9/24/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	175373	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	57582	SSL Self-Signed Certificate
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.0	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10761	COM+ Internet Services (CIS) Server Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses



Plugins / Nessus / 41028

SNMP Agent Default Community Name (public)

HIGH Nessus Plugin ID 41028

Information Dependencies Dependents Changelog

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.

Plugin Details

Severity: High

ID: 41028

File Name: snmp_default_public_community.nasl

Version: 1.14

Type: remote

Family: SNMP

Published: 11/25/2002

Updated: 6/1/2022

Configuration: Enable thorough checks

Risk Information

VPR

Risk Factor: Medium

Score: 5.9

CVSS v2

Risk Factor: High