Course Title MCIS 6173 Information and Networking Security
Term: Spring 2025

Laboratory Exercise 4-3 – Vulnerability Scanning

1. Overview

For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable3 Environment to complete vulnerability scanning with Nessus, Nikto, and Metasploit.

2. Resources required

This exercise requires the Kali Linux with Metasploitable3 Environment running in the Cyber Range.

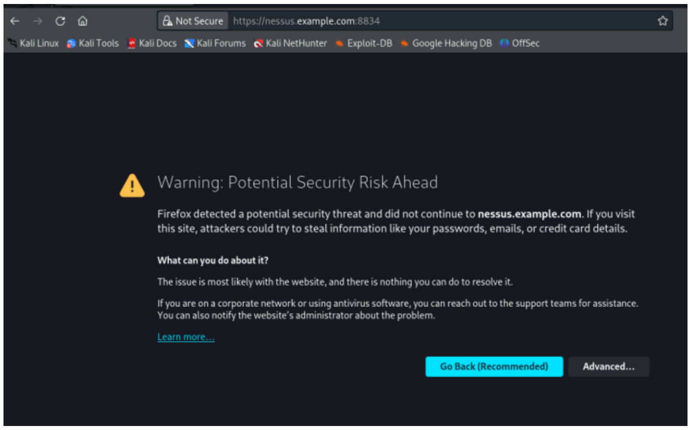
3. Initial Setup

For this exercise, you will log in to your Cyber Range account and select the Kali Linux with Metasploitable3 Environment, then click "start" to start your environment and "join" to get to your Linux desktop login.

4. Tasks

Task 1: Vulnerability Scanning with Nessus

Open a browser and navigate to https://nessus.example.com:8834



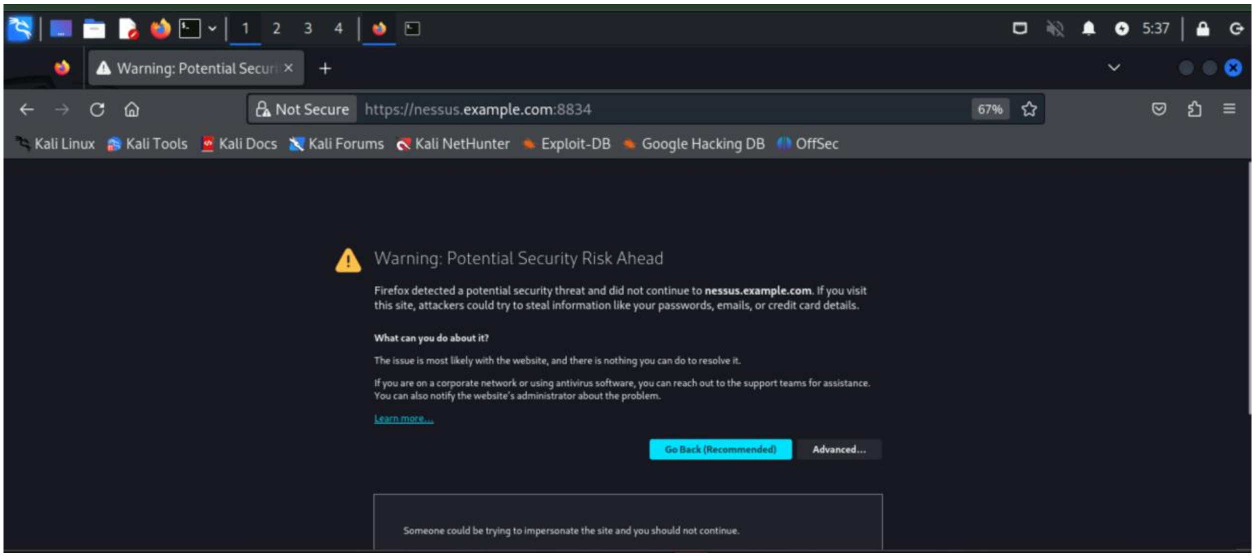
Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **nessus.example.com**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **nessus.example.com**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

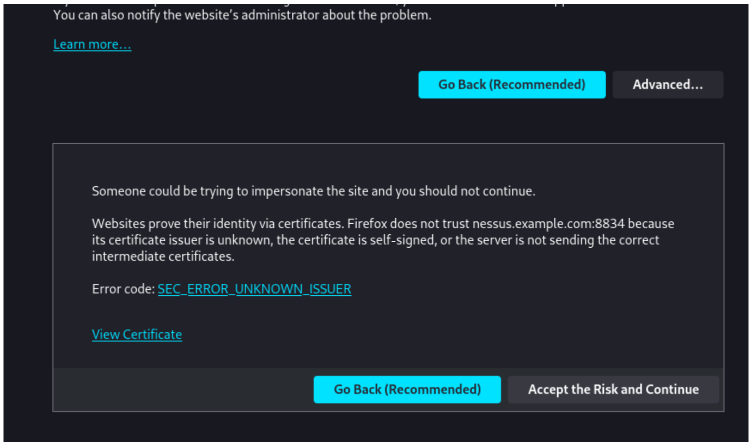
If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more…

Go Back (Recommended) Advanced…

Someone could be trying to impersonate the site and you should not continue.

Select the “Advanced” tab and then the “Accept the Risk and Continue” tab.



You can also notify the website's administrator about the problem.

Learn more…

Go Back (Recommended) Advanced…

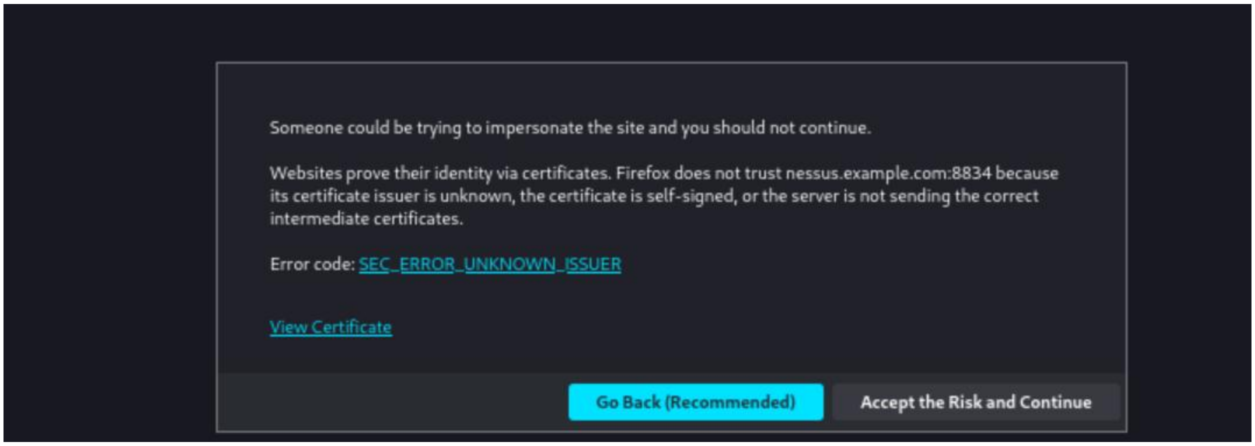
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust nessus.example.com:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

View Certificate

Go Back (Recommended) Accept the Risk and Continue



Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust nessus.example.com:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

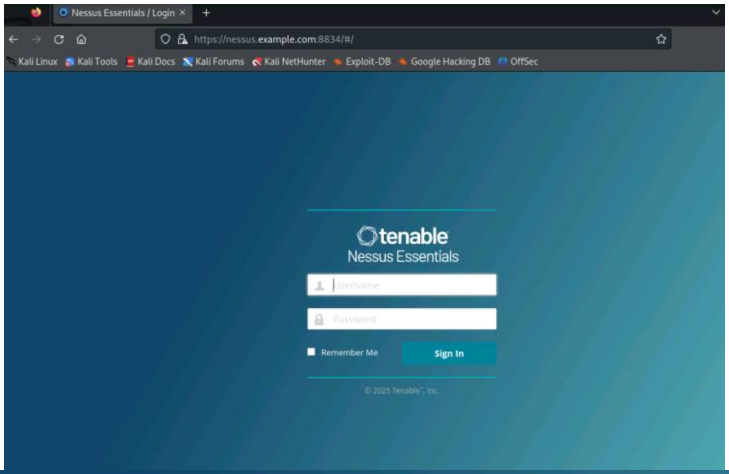
Error code: SEC_ERROR_UNKNOWN_ISSUER

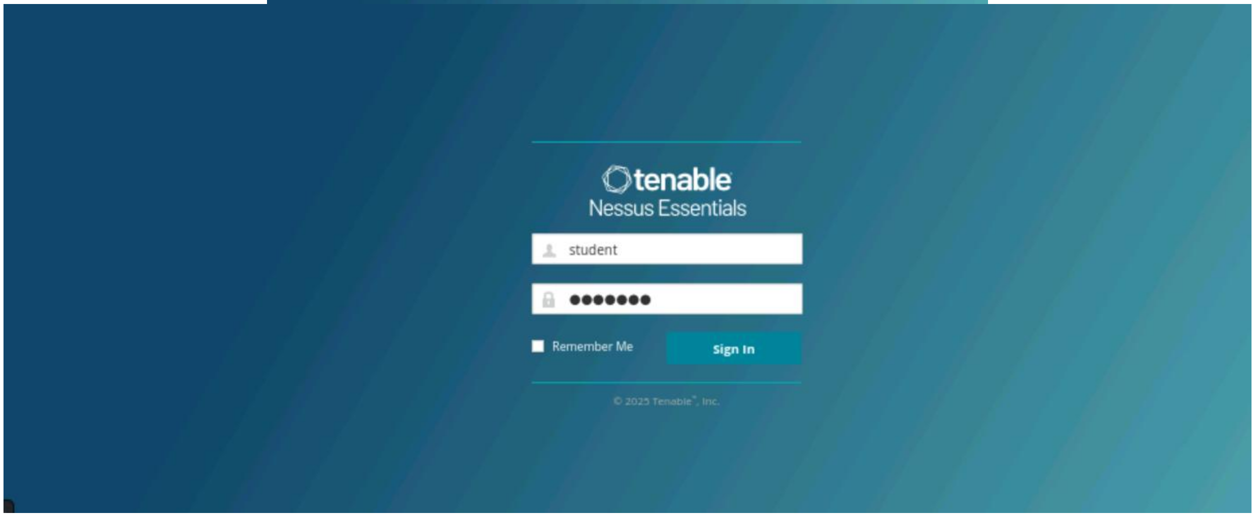
View Certificate

Go Back (Recommended) Accept the Risk and Continue

Sign In to the Tenable Nessus Essentials using these credentials:

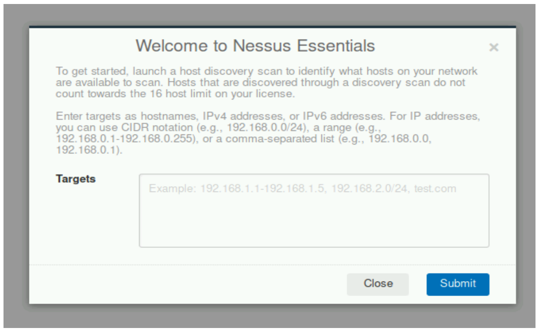
Username: **student**
Password: **student**





student
●●●●●●●

Close the Welcome to Nessus Essentials prompt.

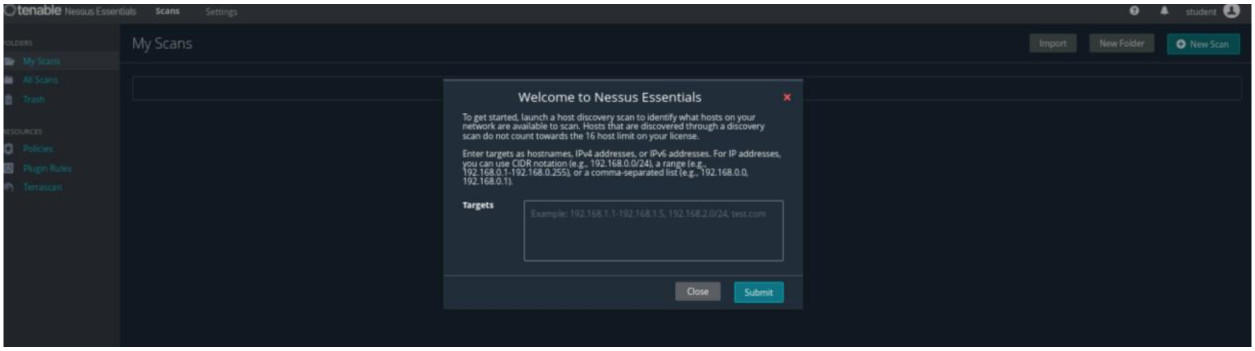


Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com



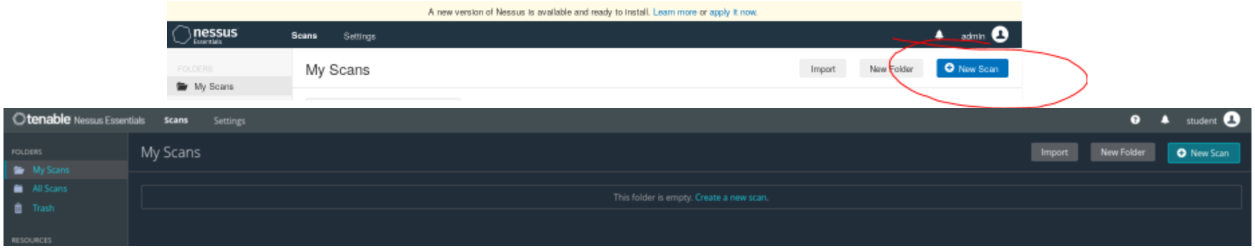
Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

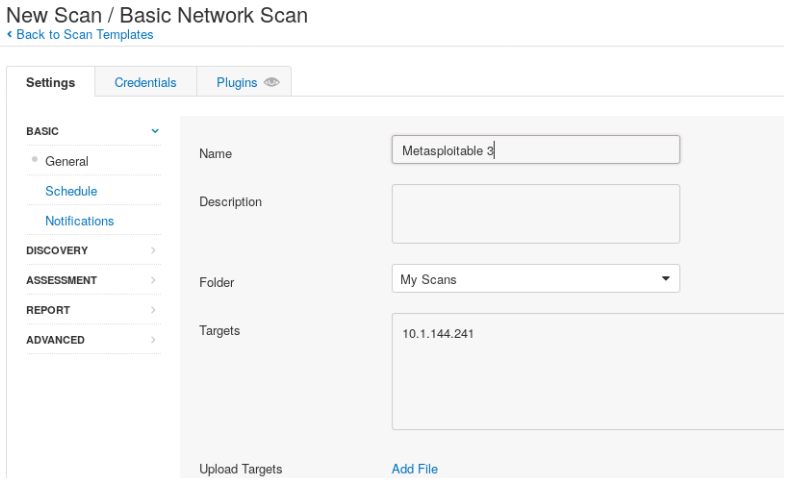
Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

On the top right-hand side, choose “New Scan.” Choose “Basic Network Scan'' and name it “Metasploitable 3.”


A new version of Nessus is available and ready to install. Learn more or apply it now.

This folder is empty. Create a new scan.

Type the Metasploitable IP into the target window.


New Scan / Basic Network Scan

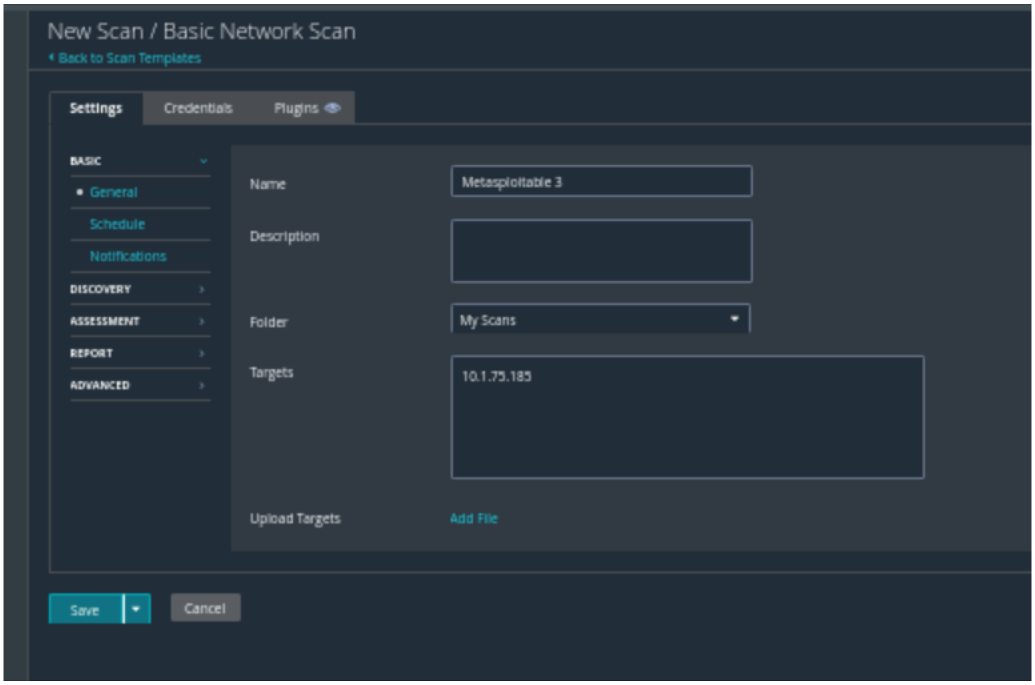
Name: Metasploitable 3

Description:

Folder: My Scans

Targets: 10.1.144.241

Upload Targets: Add File



New Scan / Basic Network Scan

Name: Metasploitable 3

Description:

Folder: My Scans

Targets: 10.1.75.185

Upload Targets

If you have forgotten your target IP open a new terminal tab, start the sql service, start Metasploit, switch to your workspace, and locate your IP address:

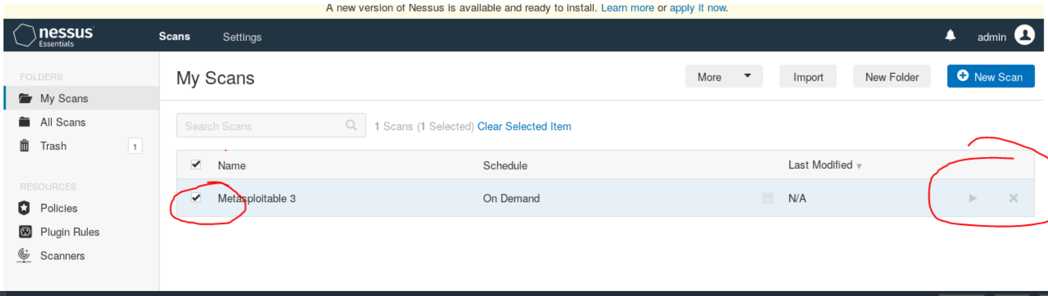
```
$sudo su
#service postgresql start
#msfdb init
#msfconsole

>db_status
>workspace —add metasploitable
>workspace
>ip addr show
```

Next, find the target Metasploitable machine. Open a new terminal window and become root. Type the following:

```
nmap -sS -Pn -v -p 22 your IP/20 | grep 'open'

nmap -sS -Pn -p 22 your IP/20 | grep -B4 'open'
```

Write down the IP address or copy and paste it into the form as the Target IP.

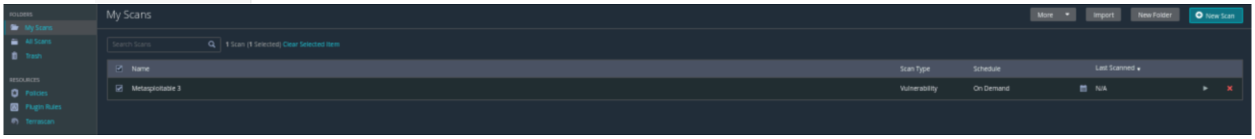
Check the target box and then click the play button on the top right-hand side of the dashboard. The scan may take some time to complete (~10 minutes). Once complete, review the results. Nessus should discover about 50-60% of vulnerabilities; however, this scan is not meant to replace manual human-based security checks. Many companies have made this mistake and paid the price, literally.



My Scans

1 Scans (1 Selected) Clear Selected Item

☑	Name	Schedule	Last Modified ▾
☑	Metasploitable 3	On Demand	N/A

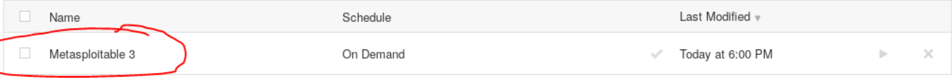


My Scans

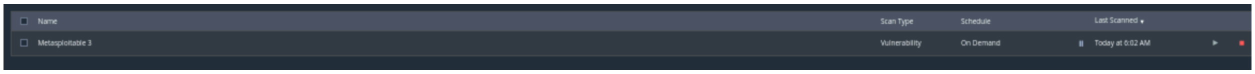
1 Scan (1 Selected) Clear Selected Item

☑	Name	Scan Type	Schedule	Last Scanned ▾
☑	Metasploitable 3	Vulnerability	On Demand	N/A

You can view the scan results live as Nessus finds vulnerabilities by clicking on the scan.

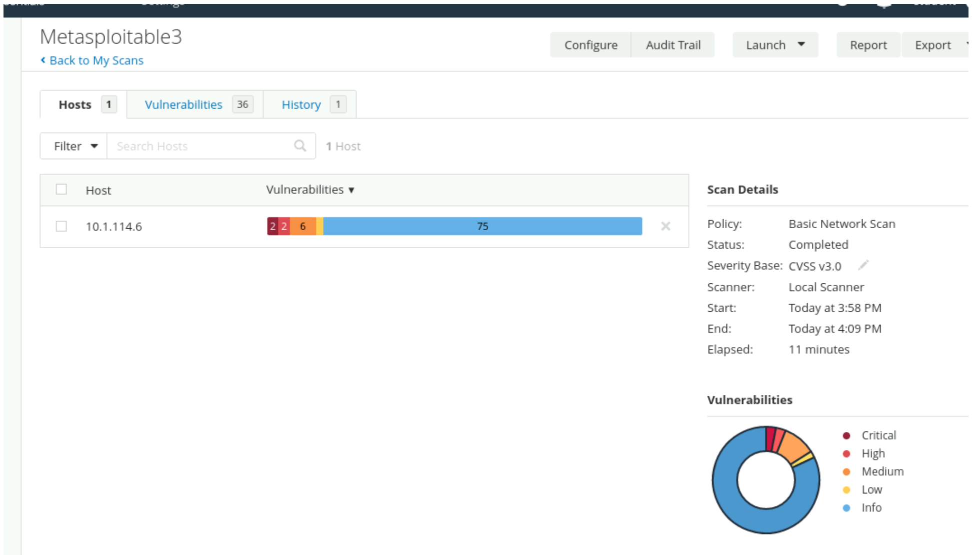


□	Name	Schedule	Last Modified ▾
□	Metasploitable 3	On Demand	Today at 6:00 PM



□	Name	Scan Type	Schedule	Last Scanned ▾
□	Metasploitable 3	Vulnerability	On Demand	Today at 6:02 AM

The first screen will provide an overview using the CVE score.



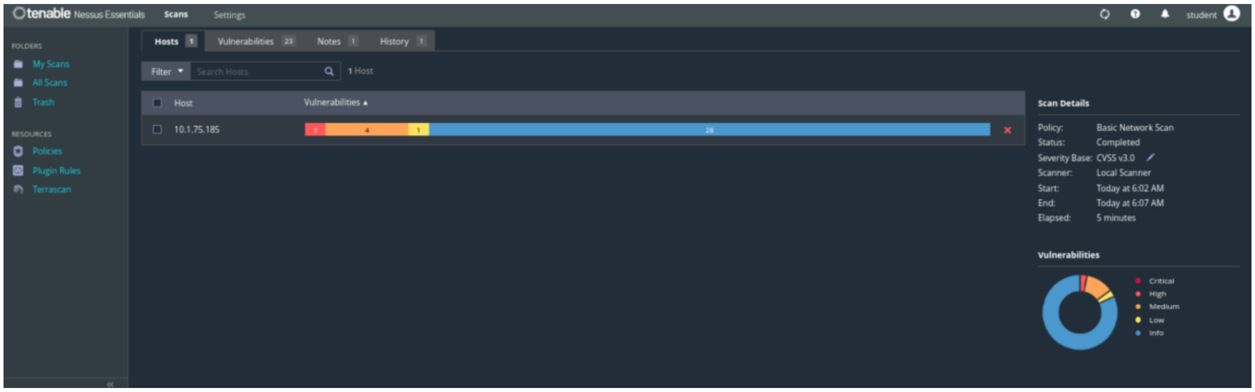
Metasploitable3
‹ Back to My Scans

1 Host

□	Host	Vulnerabilities ▾
□	10.1.114.6	2 2 6 75

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 3:58 PM
End:	Today at 4:09 PM
Elapsed:	11 minutes



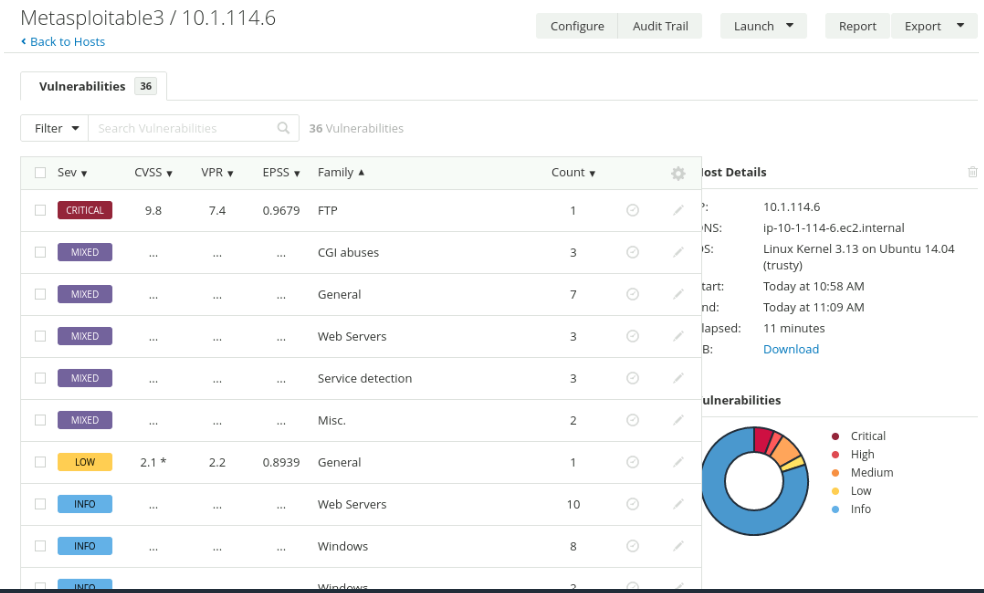
Host	Vulnerabilities ▲
10.1.75.185	1 4 1 28

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:02 AM
End: Today at 6:07 AM
Elapsed: 5 minutes

Vulnerabilities

Click on the IP to see the vulnerabilities and click on a vulnerability to view more details. The screenshots below show an FTP vulnerability that allows remote access using a Metasploit Module. In a later module, we will use the discovered critical vulnerability ProFTPD to exploit the Metasploitable 3 system.

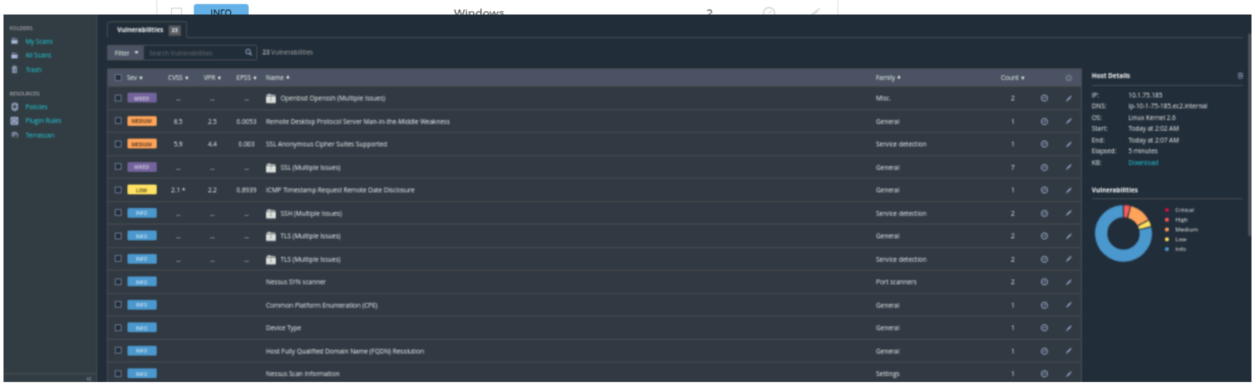

Metasploitable3 / 10.1.114.6

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Family ▲	Count ▾
CRITICAL	9.8	7.4	0.9679	FTP	1
MIXED	...	...	...	CGI abuses	3
MIXED	...	...	...	General	7
MIXED	...	...	...	Web Servers	3
MIXED	...	...	...	Service detection	3
MIXED	...	...	...	Misc.	2
LOW	2.1 *	2.2	0.8939	General	1
INFO	...	...	...	Web Servers	10
INFO	...	...	...	Windows	8
INFO				Windows	2

ost Details

P:	10.1.114.6
NS:	ip-10-1-114-6.ec2.internal
S:	Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
tart:	Today at 10:58 AM
nd:	Today at 11:09 AM
lapsed:	11 minutes
B:	Download

ulnerabilities

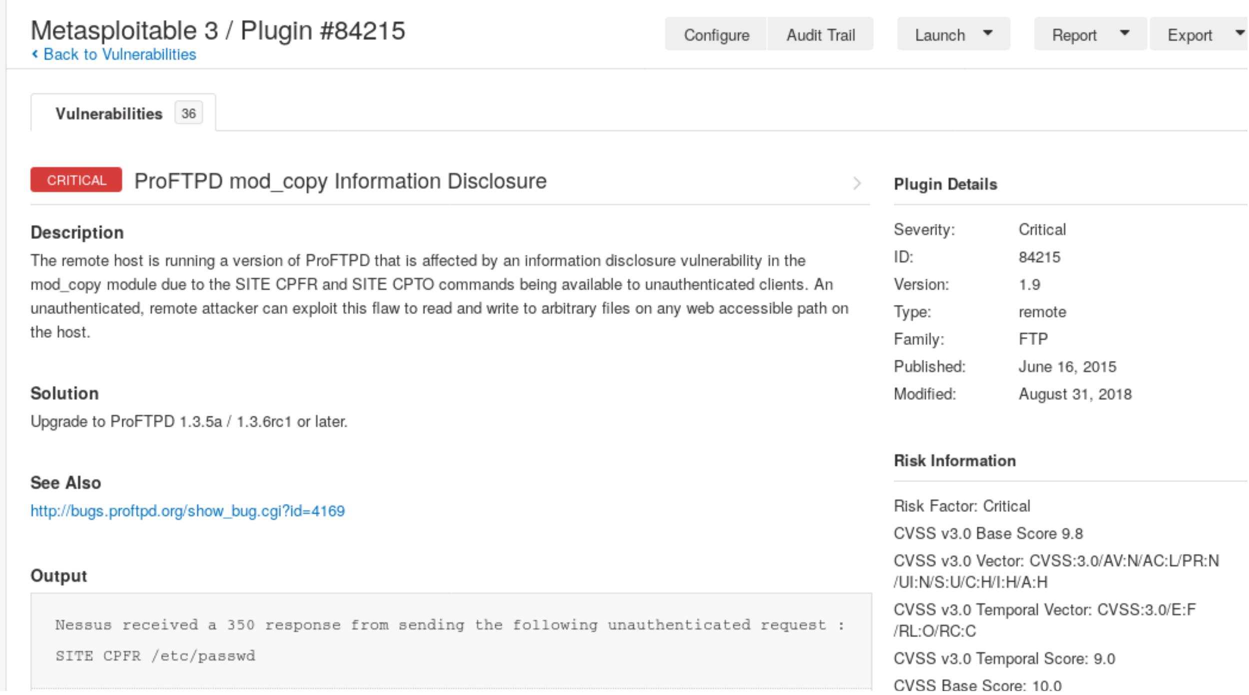


Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▲	Family ▲	Count ▾
MIXED	...	...	...	Openbsd Openssh (Multiple Issues)	Misc.	2
MEDIUM	6.5	2.5	0.0053	Remote Desktop Protocol Server Man-in-the-Middle Weakness	General	1
MEDIUM	5.9	4.4	0.003	SSL Anonymous Cipher Suites Supported	Service detection	1
MIXED	...	...	...	SSL (Multiple Issues)	General	7
LOW	2.1 *	2.2	0.8939	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	...	SSH (Multiple Issues)	Service detection	2
INFO	...	...	...	TLS (Multiple Issues)	General	2
INFO	...	...	...	TLS (Multiple Issues)	Service detection	2
INFO				Nessus SYN scanner	Port scanners	2
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO				Nessus Scan Information	Settings	1

Host Details

IP:	10.1.75.185
DNS:	ip-10-1-75-185.ec2.internal
OS:	Linux Kernel 2.6
Start:	Today at 2:02 AM
End:	Today at 2:07 AM
Elapsed:	5 minutes
KB:	Download

Vulnerabilities



Metasploitable 3 / Plugin #84215

ProFTPD mod_copy Information Disclosure

Description

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

Solution

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

See Also

http://bugs.proftpd.org/show_bug.cgi?id=4169

Output

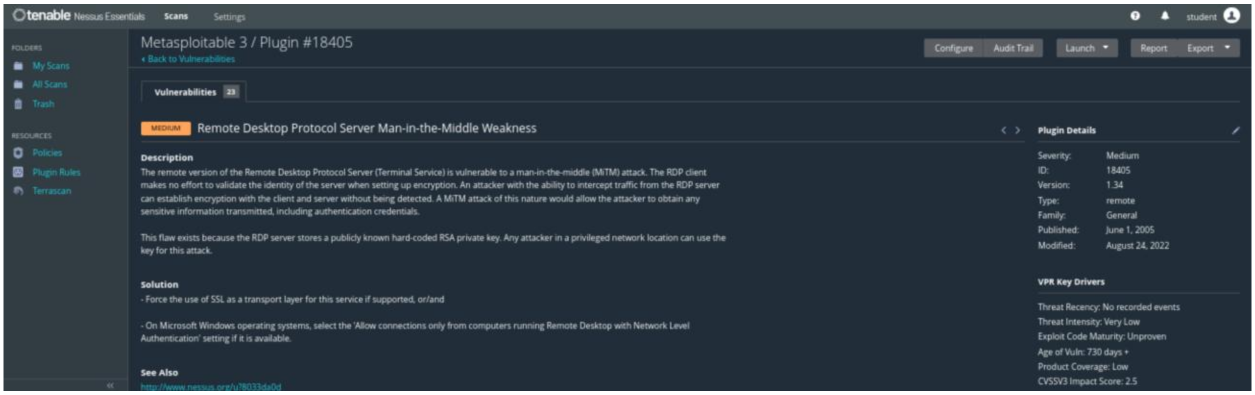
```
Nessus received a 350 response from sending the following unauthenticated request :

SITE CPFR /etc/passwd
```

Plugin Details

Severity: Critical
ID: 84215
Version: 1.9
Type: remote
Family: FTP
Published: June 16, 2015
Modified: August 31, 2018

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:F/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.0
CVSS Base Score: 10.0



Metasploitable 3 / Plugin #18405

Remote Desktop Protocol Server Man-in-the-Middle Weakness

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and

- On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

See Also

http://www.nessus.org/u?8033da0d

Plugin Details

Severity: Medium
ID: 18405
Version: 1.34
Type: remote
Family: General
Published: June 1, 2005
Modified: August 24, 2022

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 2.5

Task 2: Vulnerability Scanning with Nikto

Nikto is a web app vulnerability scanning tool that comes preinstalled in Kali Linux. It will scan any website for vulnerabilities and is simple to use. For this task, we will scan the Metasploitable Web app.

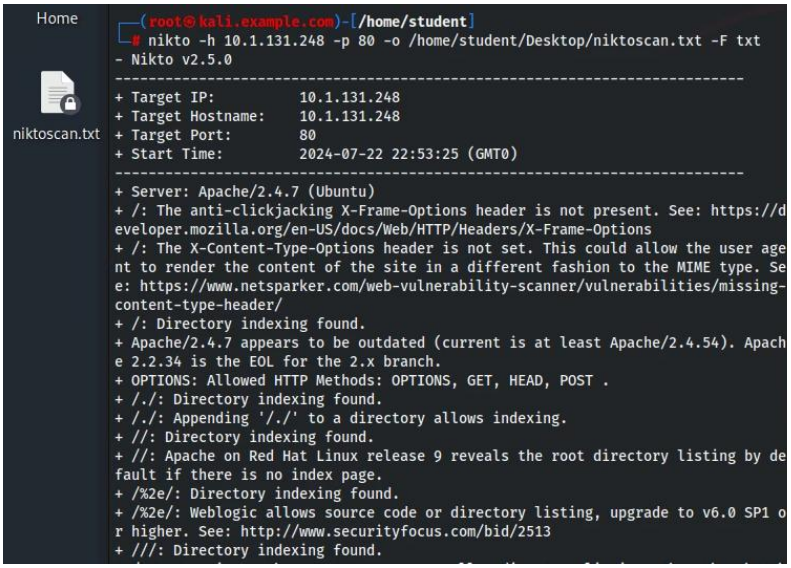
After opening a terminal on your Cyber Range Kali Linux VM, complete the following:

- Return to the terminal and, as root user, type;

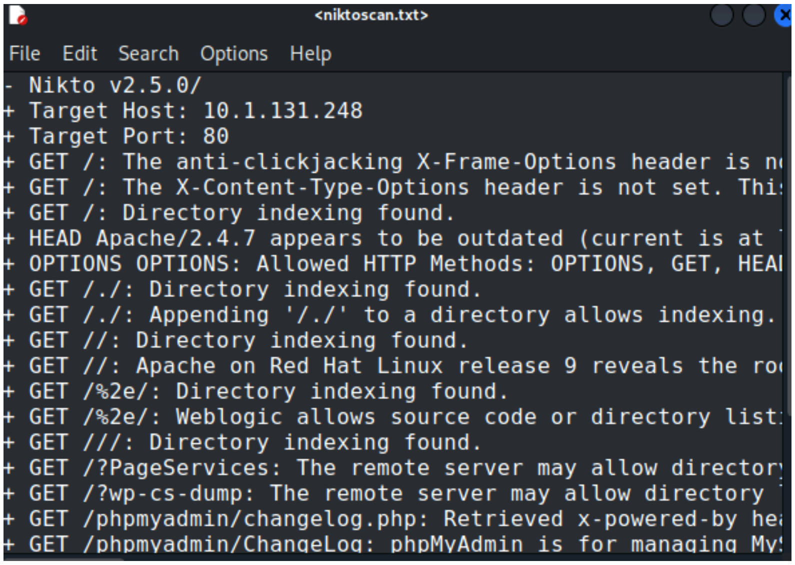
```
nikto -h <TargetIP> -p 80 /home/student/Desktop/niktoscan.txt -F txt
```

and hit enter.

This will scan the target and output the file to the Desktop as a text file. The file can be opened from the desktop by double-clicking on it. (See images below.) Vulnerabilities are listed by CVE numbers. Nikto will also list discovered directories and possible vulnerabilities such as SQL injections, session stealing, tokens/cookies, cross-site scripting, etc. Metasploitable 3 is very vulnerable by design. In a real situation, there would be less data.

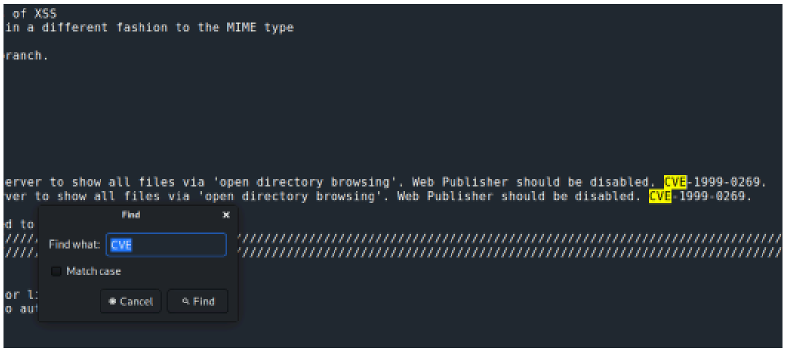


```
┌──(root㉿kali.example.com)-[/home/student]
└─# nikto -h 10.1.131.248 -p 80 -o /home/student/Desktop/niktoscan.txt -F txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.1.131.248
+ Target Hostname:    10.1.131.248
+ Target Port:        80
+ Start Time:         2024-07-22 22:53:25 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://d
eveloper.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type. Se
e: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-
content-type-header/
+ /: Directory indexing found.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apach
e 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by de
fault if there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 o
r higher. See: http://www.securityfocus.com/bid/2513
+ ///: Directory indexing found.
```



```
- Nikto v2.5.0/
+ Target Host: 10.1.131.248
+ Target Port: 80
+ GET /: The anti-clickjacking X-Frame-Options header is n
+ GET /: The X-Content-Type-Options header is not set. Thi
+ GET /: Directory indexing found.
+ HEAD Apache/2.4.7 appears to be outdated (current is at
+ OPTIONS OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEA
+ GET /./: Directory indexing found.
+ GET /./: Appending '/./' to a directory allows indexing.
+ GET //: Directory indexing found.
+ GET //: Apache on Red Hat Linux release 9 reveals the ro
+ GET /%2e/: Directory indexing found.
+ GET /%2e/: Weblogic allows source code or directory list
+ GET ///: Directory indexing found.
+ GET /?PageServices: The remote server may allow director
+ GET /?wp-cs-dump: The remote server may allow directory
+ GET /phpmyadmin/changelog.php: Retrieved x-powered-by he
+ GET /phpmyadmin/ChangeLog: phpMyAdmin is for managing My
```

You can press **CTRL+F** and type **CVE** to search. See the image below.



```
 of XSS
in a different fashion to the MIME type

ranch.






erver to show all files via 'open directory browsing'. Web Publisher should be disabled. CVE-1999-0269.
ver to show all files via 'open directory browsing'. Web Publisher should be disabled. CVE-1999-0269.

d to
////,                                                    '////////////////////////////////////////////////////////////////////////////
////,                                                    '////////////////////////////////////////////////////////////////////////////


or l:
o aut
```

Find what: CVE

□ Match case