EC-Council

codered
FROM EC-COUNCIL

CHAPTER 8

NETWORK SECURITY ASSESSMENT TECHNIQUES AND TOOLS

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 8:
Network Security Assessment Techniques and Tools

Exercise 1:
Collect Data through Search Engines 05

Exercise 2:
Gather Threat Intelligence Feed using threatfeeds.io 26

Exercise 3:
Perform Vulnerability Research in Common Weakness Enumeration (CWE) 35

Exercise 4:
Perform Vulnerability Assessment to Identify Security Vulnerabilities in the Target System or Network 43

SCENARIO

Network security assessment plays a vital role in safeguarding the networks, devices, and data pertaining to an organization. To protect these assets from the evolving landscape of cyberattacks, organizations require an understating of the current technical security posture of their network. Network security assessment helps organizations in identifying the existing security flaws and possible security threats and risks to their IT assets. It also helps in improving the integrity and resilience of both the internal and external networks.
Therefore, a security professional must perform network security assessment on a regular basis to ensure safety of the local network and the systems connected to it.

OBJECTIVE

The objective of this lab is to provide expert knowledge in assessing network security. This includes knowledge of the following tasks:

- Collecting data using search engines
- Gathering threat intelligence feed using threatfeeds.io
- Performing vulnerability research using Common Weakness Enumeration (CWE)
- Performing vulnerability assessment to identify vulnerabilities in the target system or network

OVERVIEW OF NETWORK SECURITY ASSESSMENT

Performing security assessments is the primary aim of a security professional. A security professional, attack a target network or organization with the knowledge and authorization of its management, to find loopholes in the security architecture. But the job does not end there. Finding such loopholes is a minor task. The most crucial task of security assessment is to apply the appropriate countermeasures in order to fix the loopholes. Conducting a security assessment to identify vulnerabilities can protect a network from sniffing attacks, MAC spoofing attack, ARP poisoning attack, etc.

LAB TASKS

Cyber security professional or a security professional uses numerous tools and techniques to examine network security. Recommended labs that will assist you in learning various techniques in network security assessment include the following:

01 Collect Data through Search Engines

02 Gather Threat Intelligence Feed using threatfeeds.io

03 Perform Vulnerability Research in Common Weakness Enumeration (CWE)

04 Perform Vulnerability Assessment to Identify Security Vulnerabilities in the Target System or Network

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: **COLLECT DATA THROUGH SEARCH ENGINES**

Search engines are one of the information sources to locate key information about threats and vulnerability scenarios.

LAB SCENARIO

An easy way to find threats and vulnerabilities in websites and applications is to Google them or use other search engines, which is a simple method adopted by attackers. Using search engines, hackers can identify crucial vulnerabilities in application code strings, providing the entry point they need to break through application security.
A security professional should use the same methods used by hackers such as to collect data regarding all the existing vulnerabilities in the organizational infrastructure and patch them before an attacker identifies and tries to exploit them.

OBJECTIVE

The objective of this lab is to demonstrate the following:

- Collecting data using Google Hacking Database
- Collecting data using ThreatCrowd
- Collecting data through deep and dark web searching using Tor Browser

OVERVIEW OF SEARCH ENGINES

Search engines play a major role in extracting critical details about a target from the Internet. They return a list of Search Engine Results Pages ('SERPs'). Security professionals and threat analysts use search engines to extract information about target threats and threat actors such as industry threats, technology threats, exploit used, exploit delivery method, harm caused, etc. which help them in analyzing the impact of the threat to the organization. These search engines can also be used to gather organizational information from an attacker point-of-view which helps in identifying the loopholes or vulnerabilities in the organization infrastructure.

Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on the Admin Machine-1 virtual machine.

2. Log in with the credentials Admin and admin@123.
Note: If Networks prompt appears once you have logged into the machine, click Yes.

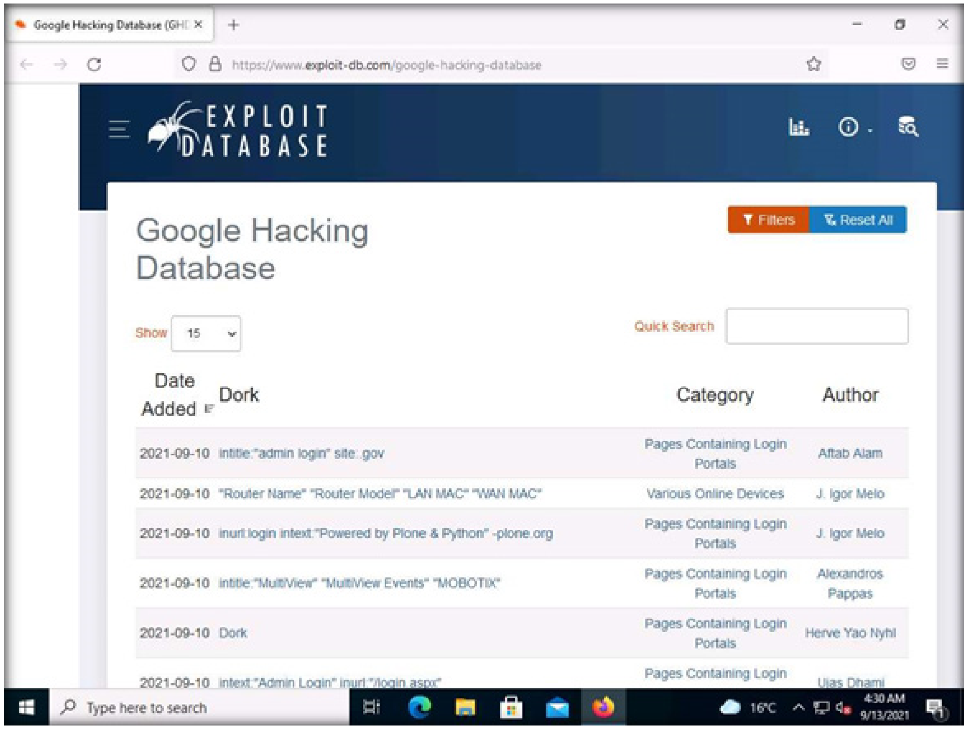
3. Launch any browser, in this lab, we are using the Mozilla Firefox browser. Double-click Firefox shortcut icon on the desktop.
Note: If an Update available pop-up appears, click on Dismiss.

4. In the address bar of the browser type https://www.exploit-db.com/google-hacking-database and press Enter. Google Hacking Database (GHDB) page appears.

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

Scroll down the page and review the latest entries. These are entries that have been discovered and submitted by the community. Take a few minutes and click on a few of them and see what you can discover. As you can see, these links can display quite a bit of information. Some of them may fail because the queries have been discovered, but you should be able to find valuable information when you are doing your testing.

5. Click Filters.
Note: If cookies pop-up appears in the lower-section of the window, Use necessary cookies only.


Google Hacking Database (GHI ×
https://www.exploit-db.com/google-hacking-database
EXPLOIT DATABASE
Filters
Reset All
Type here to search
16°C
4:30 AM
9/13/2021

Google Hacking Database

Show 15

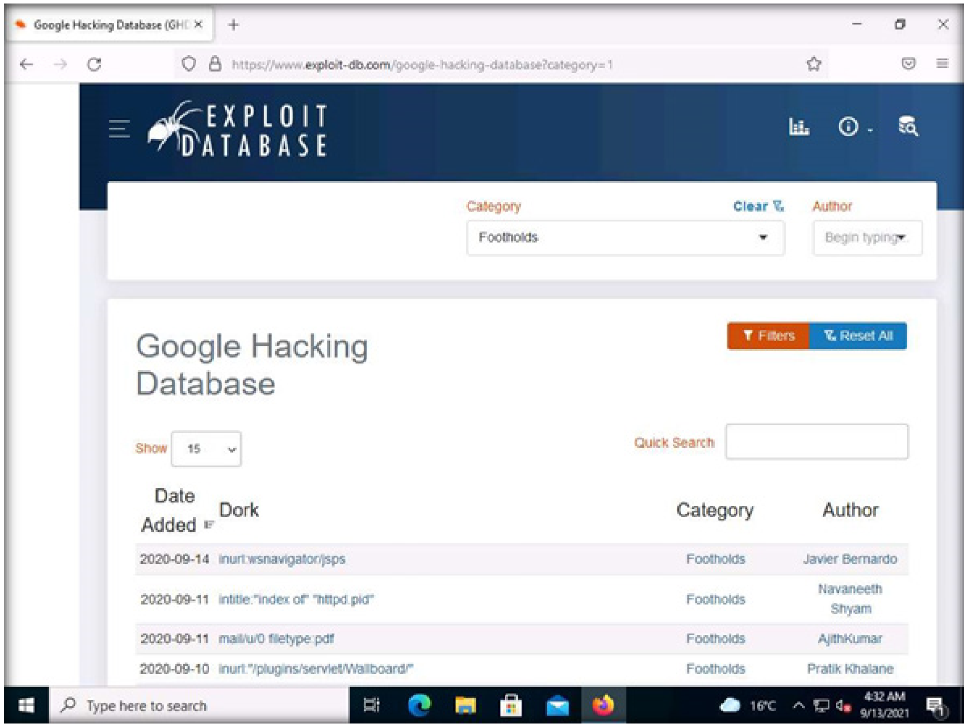
Quick Search

Date Added	Dork	Category	Author
2021-09-10	intitle:"admin login" site:.gov	Pages Containing Login Portals	Aftab Alam
2021-09-10	"Router Name" "Router Model" "LAN MAC" "WAN MAC"	Various Online Devices	J. Igor Melo
2021-09-10	inurl:login intext:"Powered by Plone & Python" -plone.org	Pages Containing Login Portals	J. Igor Melo
2021-09-10	intitle:"MultiView" "MultiView Events" "MOBOTIX"	Pages Containing Login Portals	Alexandros Pappas
2021-09-10	Dork	Pages Containing Login Portals	Herve Yao Nyhl
2021-09-10	intext:"Admin Login" inurl:"/login.aspx"	Pages Containing Login	Ujas Dhami

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

6. Click the drop-down menu in Category field to view the existing categories. Select Footholds category from the drop-down menu in Category field.

7. This will redirect you to the Footholds search results. What you would do in your testing is to create files of these queries. Then, with written authorization and permission to test the organizational site, you would use the string and enter the site that you are testing to see if there are any foothold weaknesses in the site. The foothold links are shown in the screenshot below.


Google Hacking Database (GHD
https://www.exploit-db.com/google-hacking-database?category=1
EXPLOIT DATABASE
Clear
Filters
Reset All
Type here to search
16°C
4:32 AM
9/13/2021

Category: Footholds

Author: Begin typing

Google Hacking Database

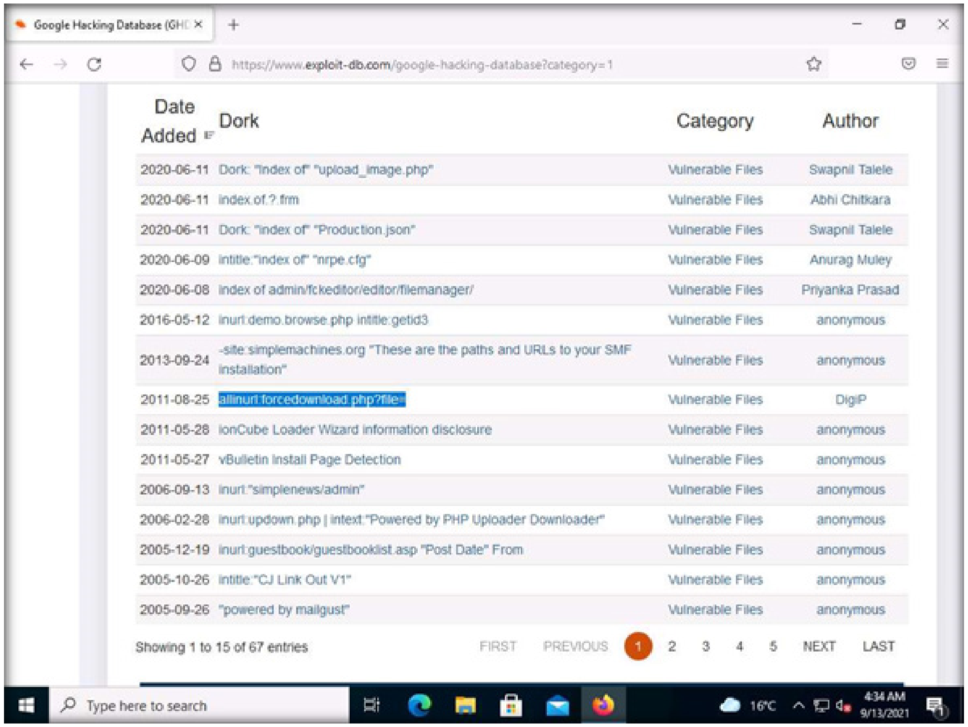
Show 15

Quick Search

Date Added	Dork	Category	Author
2020-09-14	inurl:wsnavigator/jsps	Footholds	Javier Bernardo
2020-09-11	intitle:"index of" "httpd.pid"	Footholds	Navaneeth Shyam
2020-09-11	mail/u/0 filetype:pdf	Footholds	AjithKumar
2020-09-10	inurl:"/plugins/servlet/Wallboard/"	Footholds	Pratik Khalane

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

8. After you have reviewed the entries, select Vulnerable Files from the Category drop-down menu. In the vulnerable files results, there is a query that shows “allinurl:forcedownload.php?file=”.
Note: The screenshots and search query results may vary in your environment, you may choose a query of your own and explore.


Google Hacking Database (GHD
https://www.exploit-db.com/google-hacking-database?category=1
Type here to search
16°C
4:34 AM
9/13/2021

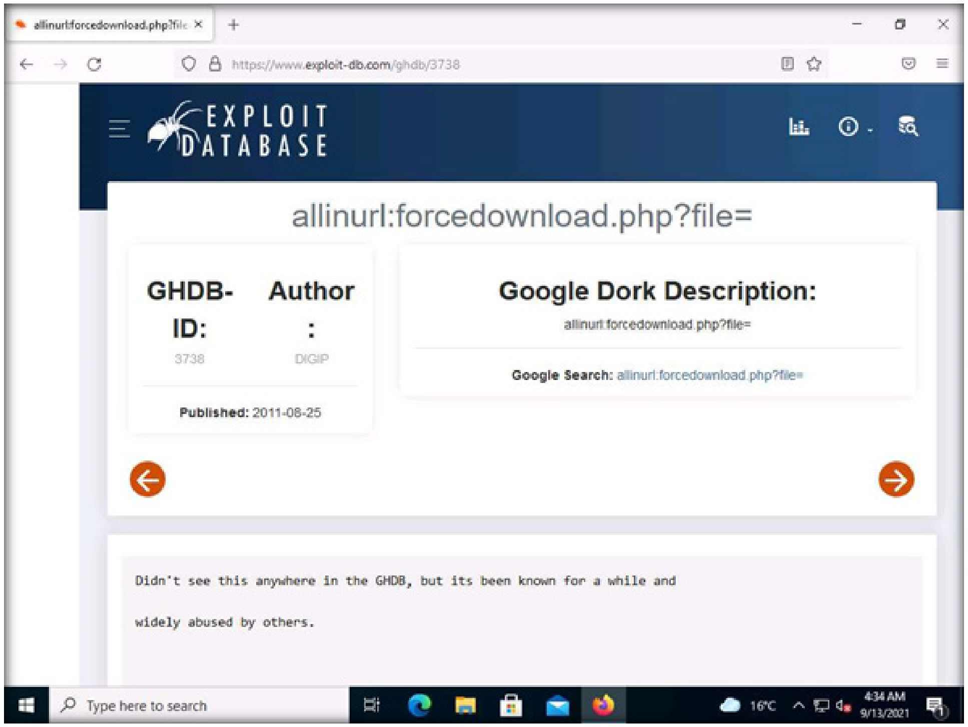
Date Added	Dork	Category	Author
2020-06-11	Dork: "index of" "upload_image.php"	Vulnerable Files	Swapnil Talele
2020-06-11	index.of.?.frm	Vulnerable Files	Abhi Chitkara
2020-06-11	Dork: "index of" "Production.json"	Vulnerable Files	Swapnil Talele
2020-06-09	intitle:"index of" "nrpe.cfg"	Vulnerable Files	Anurag Muley
2020-06-08	index of admin/fckeditor/editor/filemanager/	Vulnerable Files	Priyanka Prasad
2016-05-12	inurl:demo.browse.php intitle:getid3	Vulnerable Files	anonymous
2013-09-24	-site:simplemachines.org "These are the paths and URLs to your SMF installation"	Vulnerable Files	anonymous
2011-08-25	allinurl:forcedownload.php?file=	Vulnerable Files	DigiP
2011-05-28	ionCube Loader Wizard information disclosure	Vulnerable Files	anonymous
2011-05-27	vBulletin Install Page Detection	Vulnerable Files	anonymous
2006-09-13	inurl:"simplenews/admin"	Vulnerable Files	anonymous
2006-02-28	inurl:updown.php | intext:"Powered by PHP Uploader Downloader"	Vulnerable Files	anonymous
2005-12-19	inurl:guestbook/guestbooklist.asp "Post Date" From	Vulnerable Files	anonymous
2005-10-26	intitle:"CJ Link Out V1"	Vulnerable Files	anonymous
2005-09-26	"powered by mailgust"	Vulnerable Files	anonymous

Showing 1 to 15 of 67 entries

FIRST PREVIOUS 1 2 3 4 5 NEXT LAST

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

9. This query locates sites that use the forcedownload.php script and are vulnerable to URL manipulation. The site will spit out any file on the local site, including the PHP files, with all server-side code. We are not talking about the rendered page, but the source itself. This is most commonly used on WordPress sites to grab the wp-config.php file to gain access to the database but is not limited to WordPress sites. Many queries exist like this, and you are encouraged to develop your own and test whether the organization site is vulnerable.


allinurl:forcedownload.php?file ×
https://www.exploit-db.com/ghdb/3738
EXPLOIT DATABASE
Type here to search
16°C
4:34 AM
9/13/2021

allinurl:forcedownload.php?file=

GHDB-ID: 3738

Author: DIGIP

Published: 2011-08-25

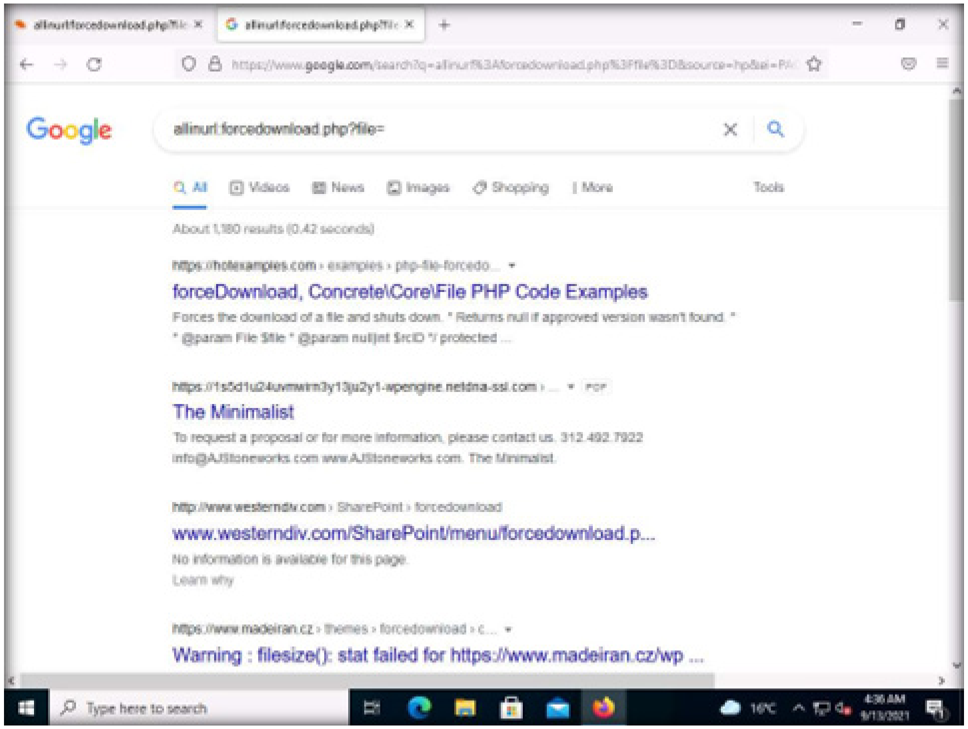
Google Dork Description:
allinurl:forcedownload.php?file=

Google Search: allinurl:forcedownload.php?file=

```
Didn't see this anywhere in the GHDB, but its been known for a while and

widely abused by others.
```

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

10. Now, open a new tab in the Firefox browser and open google.com website. In the Google search, type allinurl:forcedownload.php?file= and click Google Search. An example of Google search result of the above-mentioned query can be found in the screenshot below. Close the current tab in the browser window.


allinurl:forcedownload.php?file
allinurl:forcedownload.php?file
https://www.google.com/search?q=allinurl%3Aforcedownload.php%3Ffile%3D&source=hp&ei=PA
Google
allinurl:forcedownload.php?file=
All
Videos
News
Images
Shopping
More
Tools
Type here to search
16°C
4:36 AM
9/13/2021

About 1,180 results (0.42 seconds)

https://hotexamples.com › examples › php-file-forcedo...

forceDownload, Concrete\Core\File PHP Code Examples

Forces the download of a file and shuts down. * Returns null if approved version wasn't found. * * @param File $file * @param null|int $rcID */ protected ...

https://1s5d1u24uvmwim3y13ju2y1-wpengine.netdna-ssl.com › ... PDF

The Minimalist

To request a proposal or for more information, please contact us. 312.492.7922 info@AJStoneworks.com www.AJStoneworks.com. The Minimalist.

http://www.westerndiv.com › SharePoint › forcedownload

www.westerndiv.com/SharePoint/menu/forcedownload.p...

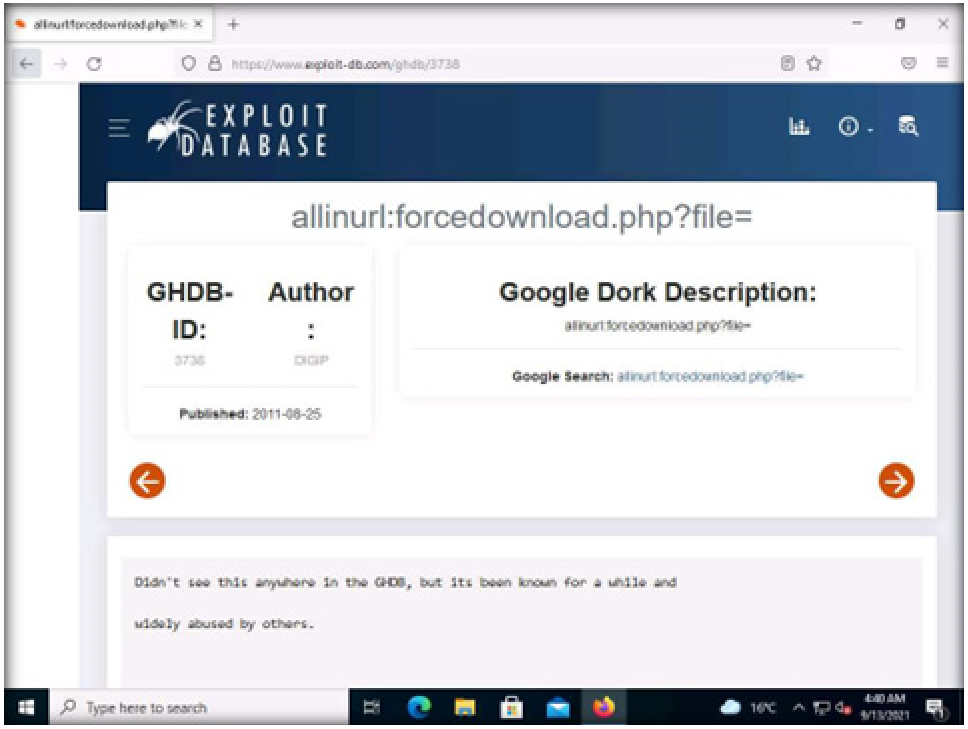
No information is available for this page.
Learn why

https://www.madeiran.cz › themes › forcedownload › c...

Warning : filesize(): stat failed for https://www.madeiran.cz/wp ...

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

11. In the Exploit Database website, click Go back one page icon ( ) to navigate back to the main page of site.



allinurl:forcedownload.php?file=

https://www.exploit-db.com/ghdb/3738

EXPLOIT DATABASE

allinurl:forcedownload.php?file=

GHDB-ID: 3738

Author: DIGIP

Published: 2011-08-25

Google Dork Description:

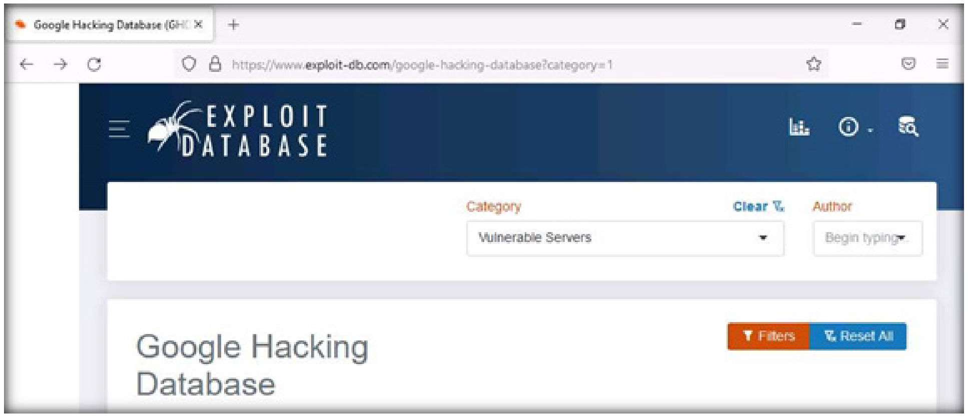
allinurl:forcedownload.php?file=

Google Search: allinurl:forcedownload.php?file=

```
Didn't see this anywhere in the GHDB, but its been known for a while and

widely abused by others.
```

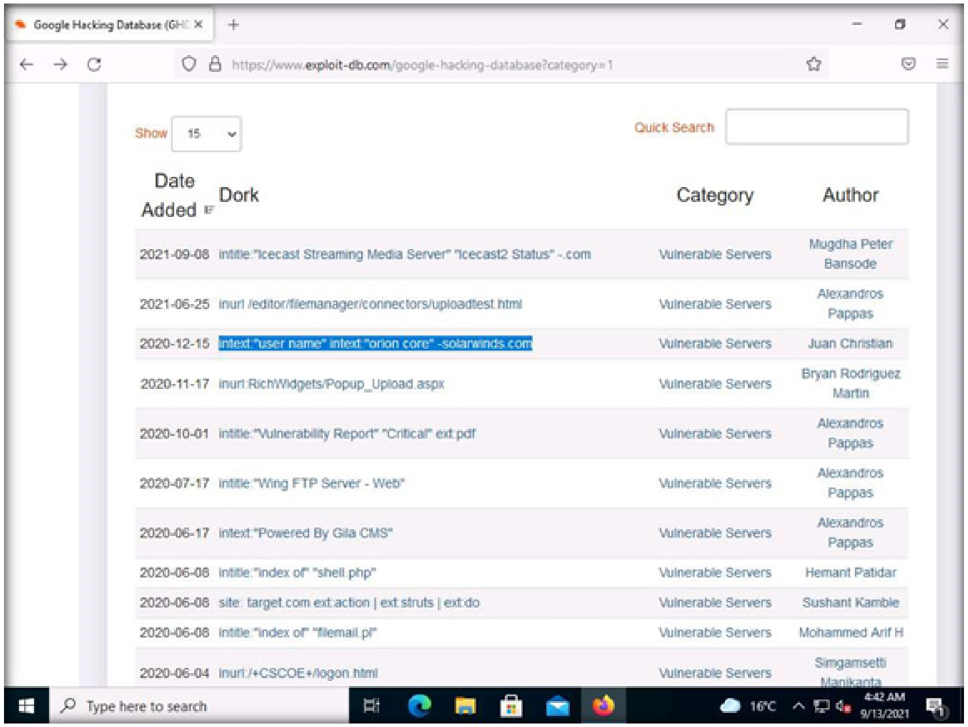
EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

12. In the landing page the next set of items, we want to check vulnerable servers; therefore, select Vulnerable Servers from the Category. The page will now display queries related to vulnerable servers.



EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

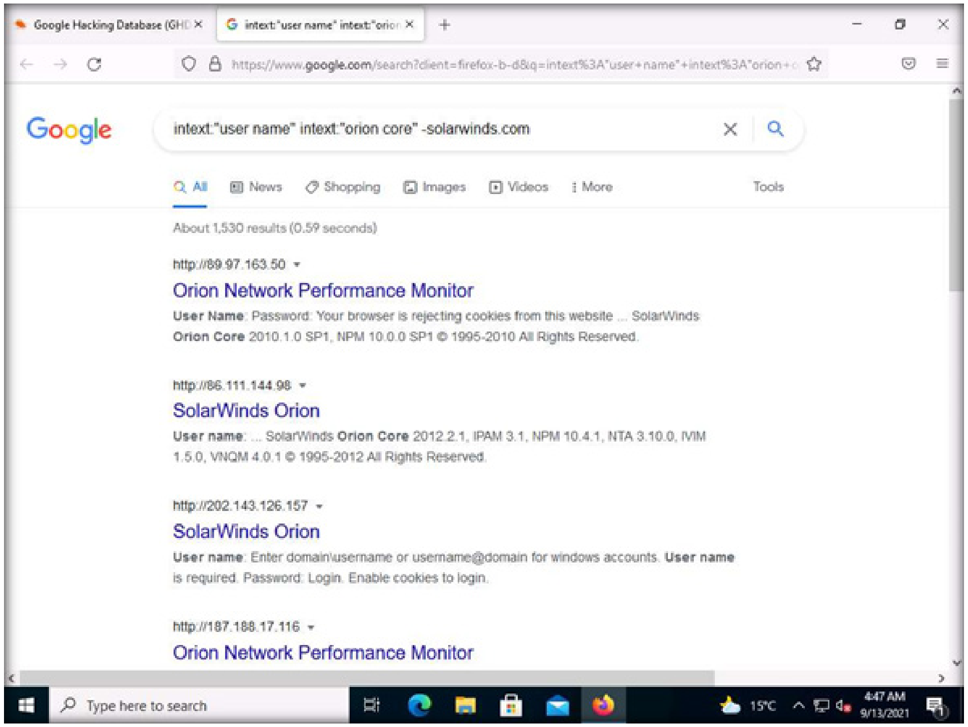
13. Once again, there are a number of queries we can use to identify potentially vulnerable servers. For example, we will look at the query intext:"user name" intext:"orion core" -solarwinds.com.
Note: The screenshots and search query results may when you perform this lab, you may choose a query of your own and explore.


Google Hacking Database (GH
https://www.exploit-db.com/google-hacking-database?category=1
Show 15
Quick Search
Type here to search
16°C
4:42 AM
9/13/2021

Date Added	Dork	Category	Author
2021-09-08	intitle:"Icecast Streaming Media Server" "Icecast2 Status" -.com	Vulnerable Servers	Mugdha Peter Bansode
2021-06-25	inurl /editor/filemanager/connectors/uploadtest.html	Vulnerable Servers	Alexandros Pappas
2020-12-15	intext:"user name" intext:"orion core" -solarwinds.com	Vulnerable Servers	Juan Christian
2020-11-17	inurl:RichWidgets/Popup_Upload.aspx	Vulnerable Servers	Bryan Rodriguez Martin
2020-10-01	intitle:"Vulnerability Report" "Critical" ext:pdf	Vulnerable Servers	Alexandros Pappas
2020-07-17	intitle:"Wing FTP Server - Web"	Vulnerable Servers	Alexandros Pappas
2020-06-17	intext:"Powered By Gila CMS"	Vulnerable Servers	Alexandros Pappas
2020-06-08	intitle:"index of" "shell.php"	Vulnerable Servers	Hemant Patidar
2020-06-08	site: target.com ext:action | ext:struts | ext:do	Vulnerable Servers	Sushant Kamble
2020-06-08	intitle:"index of" "filemail.pl"	Vulnerable Servers	Mohammed Arif H
2020-06-04	inurl:/+CSCOE+/logon.html	Vulnerable Servers	Singamsetti Manikanta

14. Open a new tab in the browser and open google.com website. In the Google search field, type intext:”user name” intext:”orion core” -solarwinds.com and click Google Search button. This query will look for SolarWinds Orion web consoles that are exposed to the Internet. The following screenshot shows the results of this query.

Close the current tab in the browser window.


Google Hacking Database (GHD
intext:"user name" intext:"orion
https://www.google.com/search?client=firefox-b-d&q=intext%3A"user+name"+intext%3A"orion+c
Google
All
News
Shopping
Images
Videos
More
Tools
Type here to search
15°C
4:47 AM
9/13/2021

intext:"user name" intext:"orion core" -solarwinds.com

About 1,530 results (0.59 seconds)

http://89.97.163.50
Orion Network Performance Monitor
User Name: Password: Your browser is rejecting cookies from this website ... SolarWinds **Orion Core** 2010.1.0 SP1, NPM 10.0.0 SP1 © 1995-2010 All Rights Reserved.

http://86.111.144.98
SolarWinds Orion
User name: ... SolarWinds **Orion Core** 2012.2.1, IPAM 3.1, NPM 10.4.1, NTA 3.10.0, IVIM 1.5.0, VNQM 4.0.1 © 1995-2012 All Rights Reserved.

http://202.143.126.157
SolarWinds Orion
User name: Enter domain\username or username@domain for windows accounts. **User name** is required. Password: Login. Enable cookies to login.

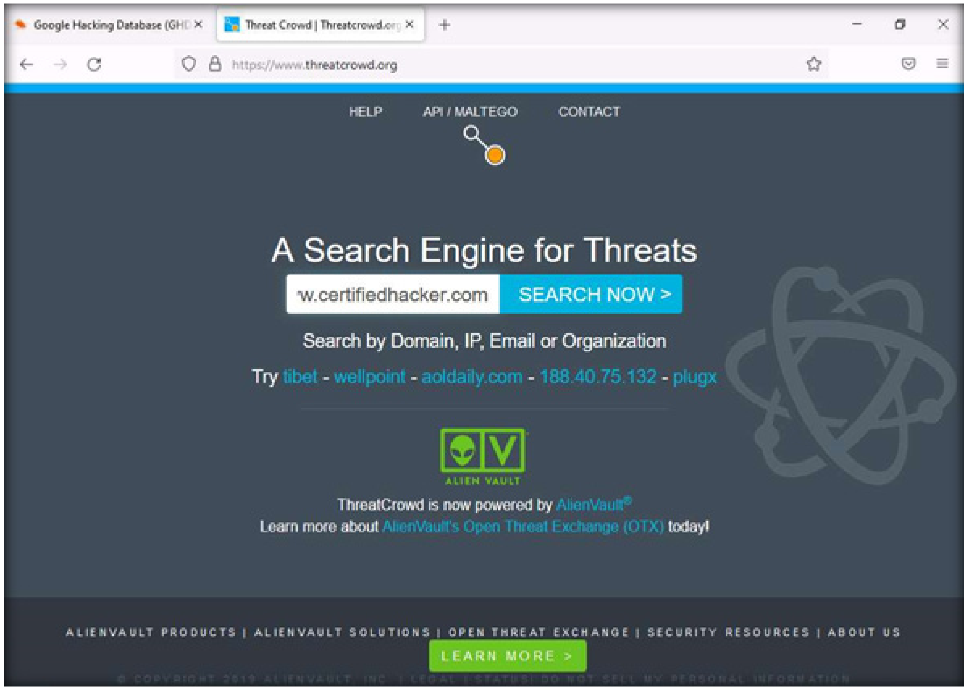
http://187.188.17.116
Orion Network Performance Monitor

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

15. In the Exploit Database website, click Go back one page icon ( ) to navigate back to the main page.

16. Similarly, you can explore other categories such as File Containing Usernames, Sensitive Directories, File Containing Passwords, etc.

17. Now, we shall perform the open-source intelligence gathering using ThreatCrowd. In a new tab, type https://www.threatcrowd.org in the address bar and press Enter. A Search Engine for Threats page appears as shown in the screenshot below.
In the search field, type the organization's URL that you wish to analyze (here, www.certifiedhacker.com) and click SEARCH NOW >.


Google Hacking Database (GHD
Threat Crowd | Threatcrowd.org
https://www.threatcrowd.org
HELP
API / MALTEGO
CONTACT
SEARCH NOW >
ALIEN VAULT
ALIENVAULT PRODUCTS | ALIENVAULT SOLUTIONS | OPEN THREAT EXCHANGE | SECURITY RESOURCES | ABOUT US
LEARN MORE >
© COPYRIGHT 2019 ALIENVAULT, INC. | LEGAL | STATUS| DO NOT SELL MY PERSONAL INFORMATION

A Search Engine for Threats

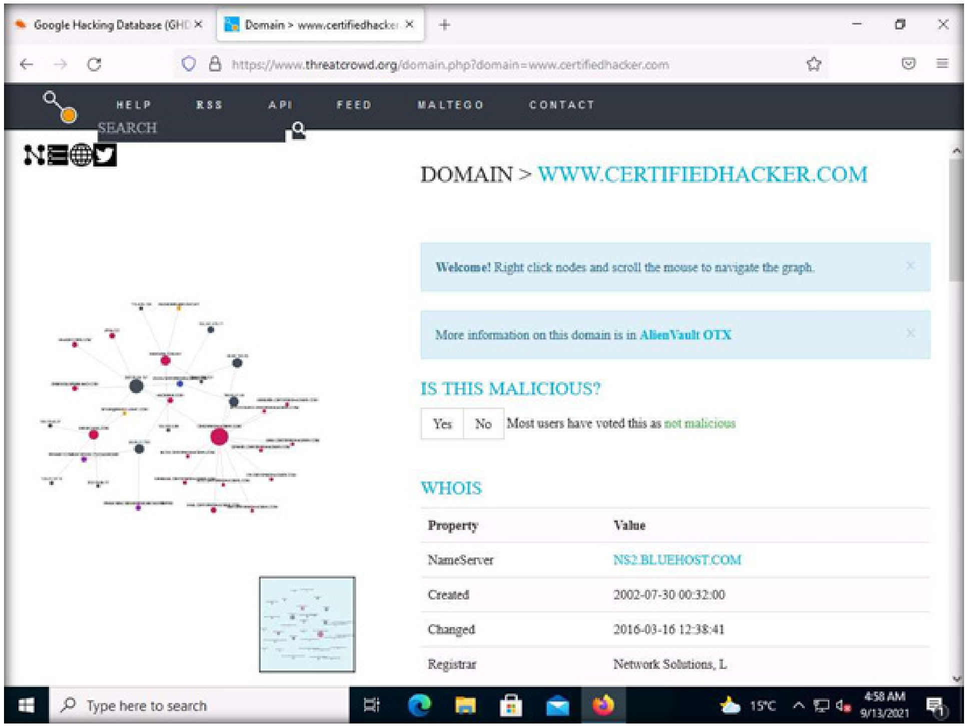
w.certifiedhacker.com

Search by Domain, IP, Email or Organization

Try tibet - wellpoint - aoldaily.com - 188.40.75.132 - plugx

ThreatCrowd is now powered by AlienVault®
Learn more about AlienVault's Open Threat Exchange (OTX) today!

18. You will see the detailed information regarding the provided URL including IP address, name servers, DNS resolutions, WhoIs results, etc. These details are present in the public domain and are important to gather such information as they can pose a threat. You can further conduct a series of queries and gather publicly available organizational information from the ThreatCrowd site.


Google Hacking Database (GHD
Domain > www.certifiedhacke
https://www.threatcrowd.org/domain.php?domain=www.certifiedhacker.com
HELP
RSS
API
FEED
MALTEGO
CONTACT
SEARCH
Type here to search
15°C
4:58 AM
9/13/2021

DOMAIN > WWW.CERTIFIEDHACKER.COM

Welcome! Right click nodes and scroll the mouse to navigate the graph.

More information on this domain is in **AlienVault OTX**

IS THIS MALICIOUS?

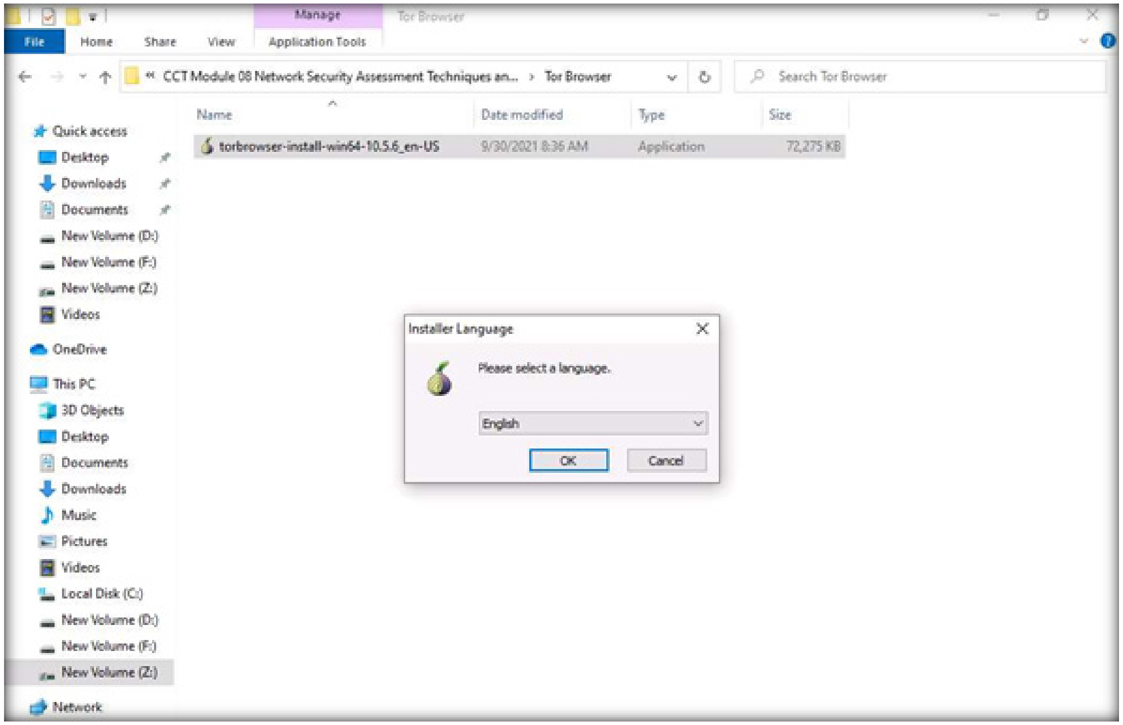
Yes No Most users have voted this as not malicious

WHOIS

Property	Value
NameServer	NS2.BLUEHOST.COM
Created	2002-07-30 00:32:00
Changed	2016-03-16 12:38:41
Registrar	Network Solutions, L

19. This concludes the demonstration showing how to gather open-source intelligence using Exploit Database and ThreatCrowd. Close all open windows.

20. Now, we shall perform the open-source intelligence gathering by deep and dark web searching using Tor Browser. Open a File Explorer and navigate to Z:\CCT-Tools\CCT Module 08 Network Security Assessment Techniques and Tools\Tor Browser and double-click torbrowser-install-win64-10.5.6_en-US.exe.
Installer Language window appears, select your preferred language (here, English) and click OK.
Note: If Open File – Security Warning window appears, click Run.
Note: If the User Account Control pop-up appears, click Yes.



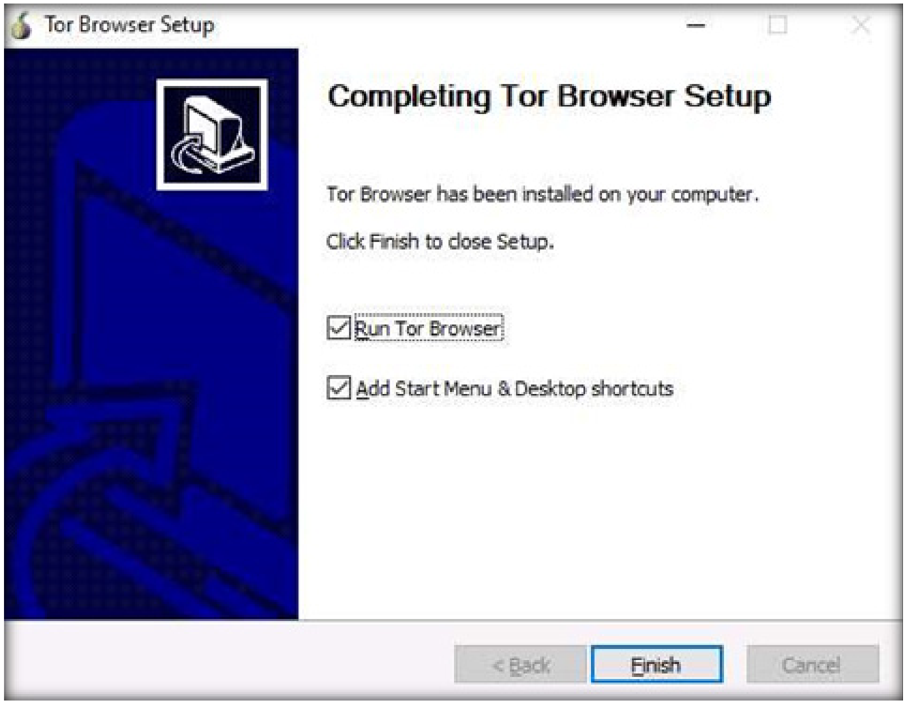
Name	Date modified	Type	Size
torbrowser-install-win64-10.5.6_en-US	9/30/2021 8:36 AM	Application	72,275 KB

Installer Language

Please select a language.

English

21. Follow the wizard steps (by selecting default options) to install Tor Browser. After the installation is complete, click Finish button to complete the installation and launch the Tor Browser as shown in the screenshot below.
Note: Make sure that Run Tor Browser option is checked.



Tor Browser Setup

Completing Tor Browser Setup

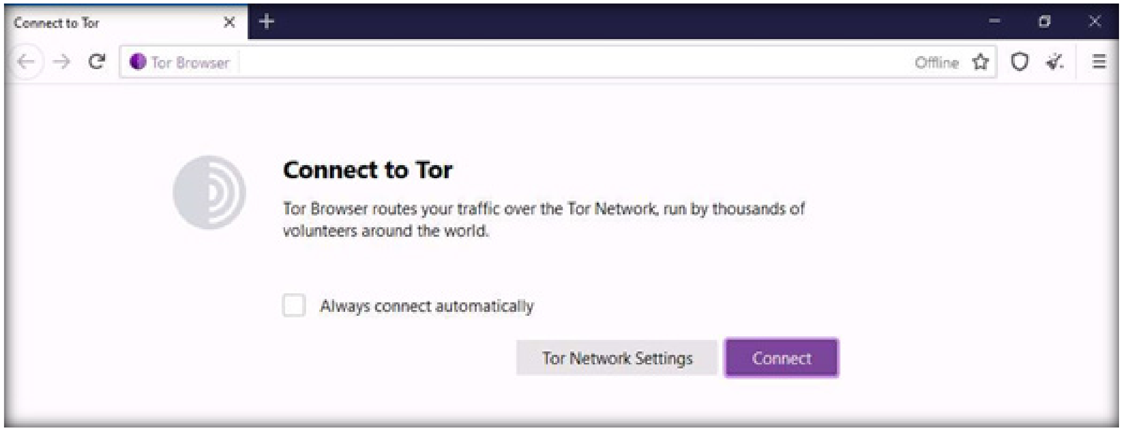
Tor Browser has been installed on your computer.

Click Finish to close Setup.

☑ Run Tor Browser

☑ Add Start Menu & Desktop shortcuts

22. Connect to Tor page appears. Click Connect button to browse through Tor browser default settings directly.
Note: If Tor is censored in your country or if you want to connect through Proxy, click Configure button here and continue.
Note: It might take a while to launch the Tor Browser.

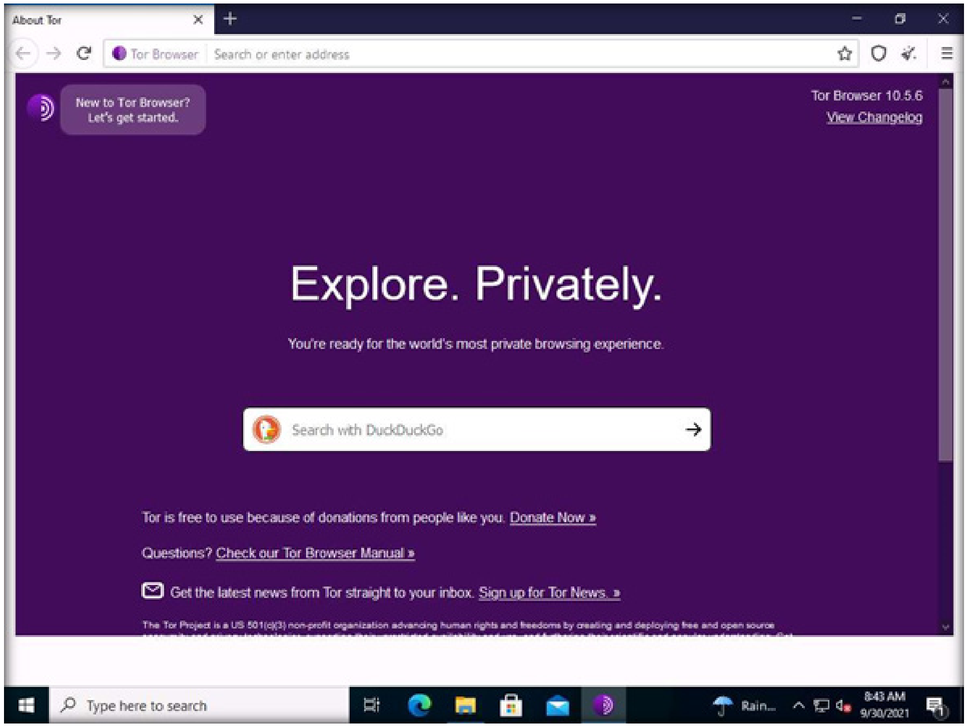


Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

23. After a few second, Tor browser home page appears. The main advantage of the Tor browser is that it maintains the anonymity of the user throughout the session.



Explore. Privately.

You're ready for the world's most private browsing experience.

Tor is free to use because of donations from people like you. Donate Now »

Questions? Check our Tor Browser Manual »

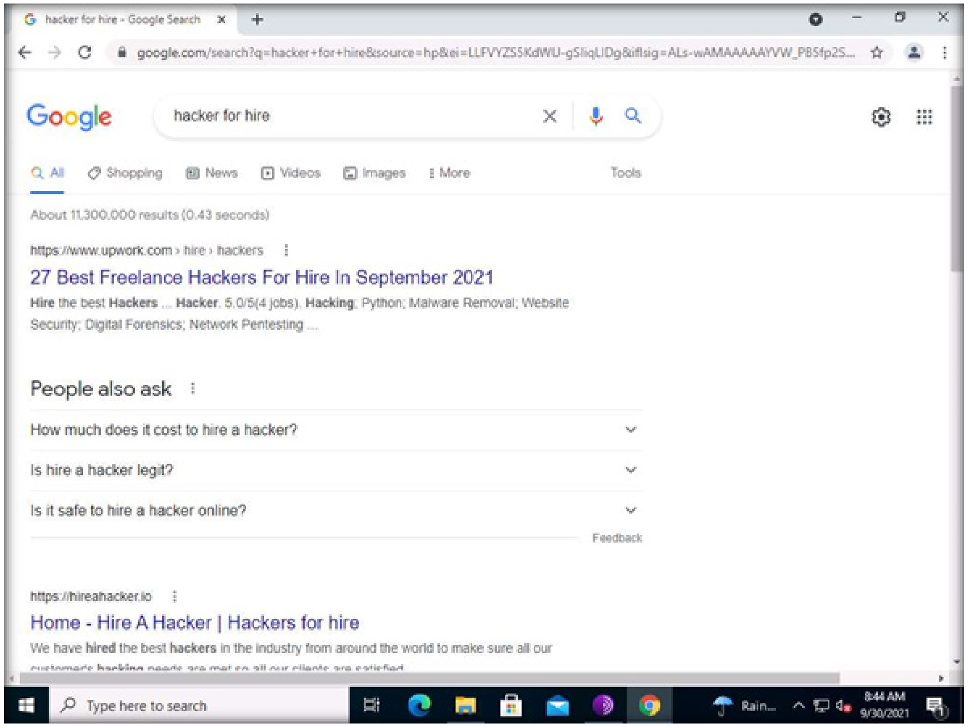
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

24. As a security professional, your job is to collect as much as information related to threats to the organization from the dark web. Before doing that, you must know the actual difference between surface web searching and dark web searching. Open Google Chrome. Navigate to www.google.com and in Google search, search for hacker for hire. You will be loaded with large amounts of irrelevant data as shown in the screenshot below.
Note: To launch Google Chrome, double-click Google Chrome shortcut present on the Desktop.


hacker for hire - Google Search
google.com/search?q=hacker+for+hire&source=hp&ei=LLFVYZS5KdWU-gSliqLIDg&iflsig=ALs-wAMAAAAAYVW_PB5fp2S...
Google
hacker for hire
All
Shopping
News
Videos
Images
More
Tools
Feedback
Type here to search
Rain...
8:44 AM
9/30/2021

About 11,300,000 results (0.43 seconds)

https://www.upwork.com › hire › hackers

27 Best Freelance Hackers For Hire In September 2021

Hire the best **Hackers** ... **Hacker**. 5.0/5(4 jobs). **Hacking**; Python; Malware Removal; Website Security; Digital Forensics; Network Pentesting ...

People also ask

How much does it cost to hire a hacker?

Is hire a hacker legit?

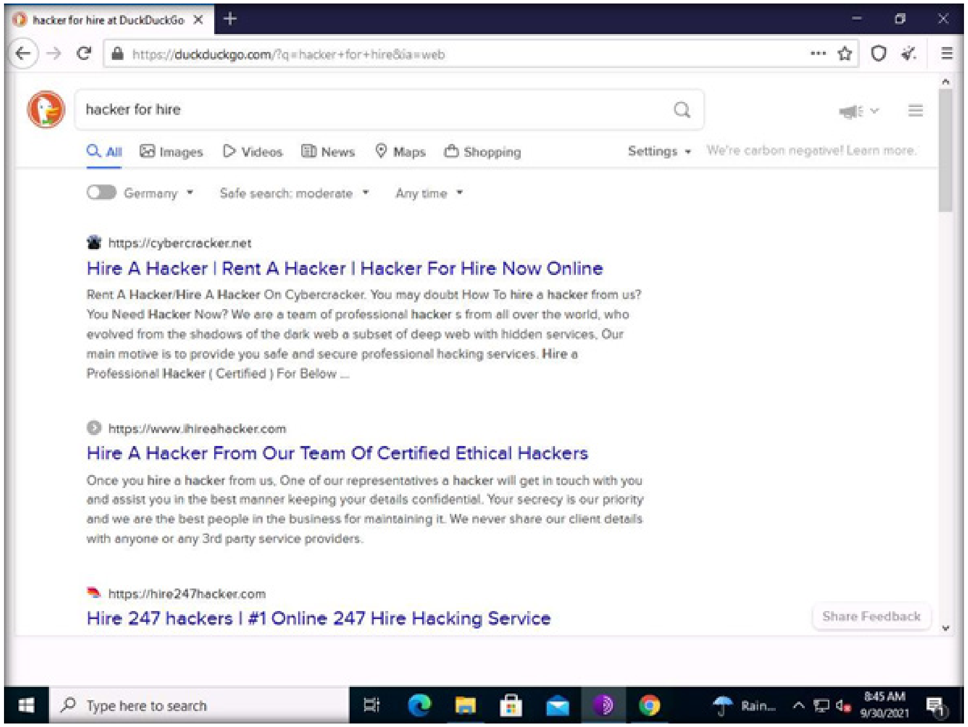
Is it safe to hire a hacker online?

https://hireahacker.io

Home - Hire A Hacker | Hackers for hire

We have **hired** the best **hackers** in the industry from around the world to make sure all our customer's **hacking** needs are met so all our clients are satisfied

25. Now switch to Tor browser and search for the same (i.e., hacker for hire). You will find the relevant links related to the professional hackers who operate underground through the dark web. Click and open any of the search results (here, hire247hacker.com).
Note: The search result may vary while you are performing the lab task.
Note: Tor uses DuckDuckGo search engine to perform a dark web search. The result may vary in your environment.



hacker for hire

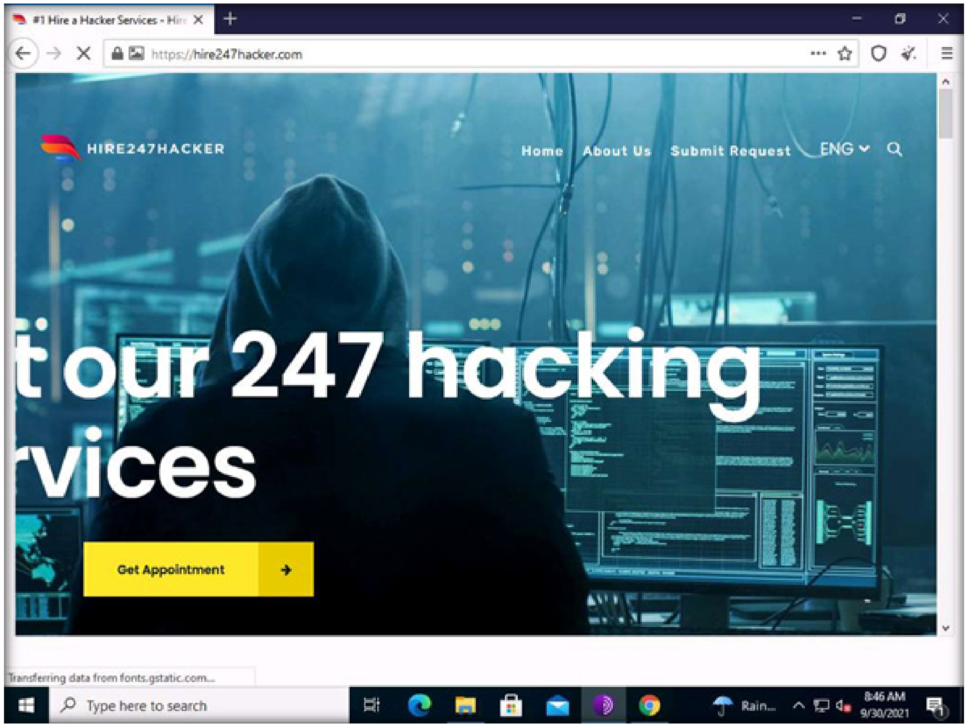
https://cybercracker.net
Hire A Hacker | Rent A Hacker | Hacker For Hire Now Online
Rent A Hacker/Hire A Hacker On Cybercracker. You may doubt How To hire a hacker from us? You Need Hacker Now? We are a team of professional hacker s from all over the world, who evolved from the shadows of the dark web a subset of deep web with hidden services. Our main motive is to provide you safe and secure professional hacking services. Hire a Professional Hacker (Certified) For Below ...

https://www.ihireahacker.com
Hire A Hacker From Our Team Of Certified Ethical Hackers
Once you hire a hacker from us, One of our representatives a hacker will get in touch with you and assist you in the best manner keeping your details confidential. Your secrecy is our priority and we are the best people in the business for maintaining it. We never share our client details with anyone or any 3rd party service providers.

https://hire247hacker.com
Hire 247 hackers | #1 Online 247 Hire Hacking Service

EXERCISE 1: COLLECT DATA THROUGH SEARCH ENGINES

26. The hire247hacker.com web page opens up as shown in the screenshot below and you will see that the site belongs to professional hackers who operate underground. This information related to professional hackers and hacking services can be used to build effective threat intelligence.



27. A dark web search for security professionals does not stop with hire247hacker.com. You can collect large amounts of threat information through multiple dark web searches.

28. This concludes the demonstration showing how to gather open-source intelligence by searching over deep and dark web searching using Tor Browser.

29. Close all open windows.

EXERCISE 2: GATHER THREAT INTELLIGENCE FEED USING THREATFEEDS.IO

Threat intelligence feeds (TI feeds) are continuous streams of packaged data related to potential or current threats to the organization.

LAB SCENARIO

A security professional must have the required knowledge about gathering threat intelligence feeds from the open-source platforms such as threatfeeds.io. Threat feeds can assist security professionals in blocking bad IP addresses, blacklisting malicious or phishing websites, etc, in order to prevent the organizational network from outside threats.

OBJECTIVE

The objective of this lab is to learn how to collect TI feeds using online tools such as threatfeeds.io.

OVERVIEW OF THREAT INTELLIGENCE FEED

Threat intelligence feeds (TI feeds) feature a packaged collection of data taken from different sources related to potential or current threats in an organization. Most feeds concentrate on domains, malicious IP addresses, or botnet activity. These comprise actionable information and are implemented along with technical controls to prevent cyber-attacks.

threatfeeds.io is a free and open-source threat intelligence provider of popular free and open-source TI feeds and sources. It also lists links for direct downloads and live summaries.

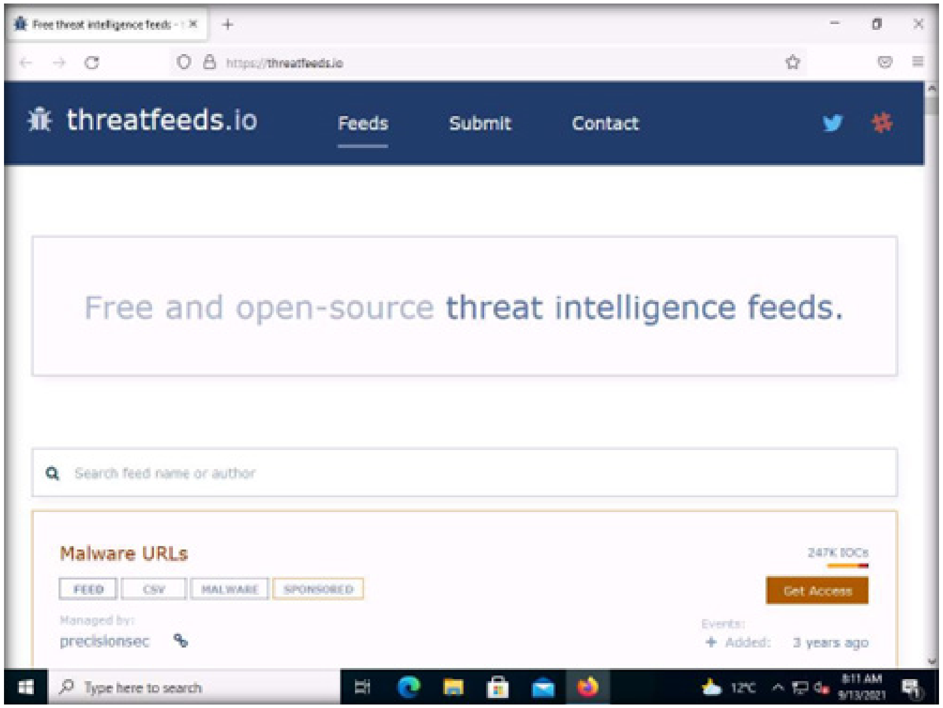
Security professional can use the online tool threatfeeds.io, as a proof of concept to gather threat intelligence feeds.

EXERCISE 2: GATHER THREAT INTELLIGENCE FEED USING THREATFEEDS.IO

Note: Ensure that the Admin Machine-1 and PfSense Firewall virtual machines are running.

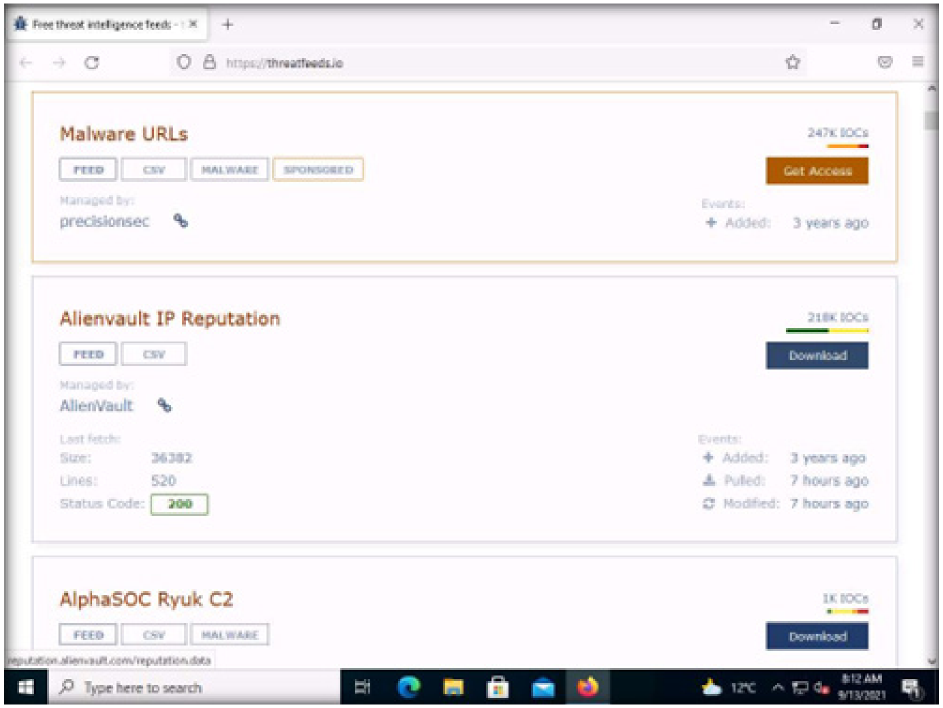
1. In the Admin Machine-1 virtual machine, launch any browser, in this lab, we are using the Mozilla Firefox browser. Double-click Firefox shortcut icon on the desktop.

2. In the address bar of the browser type https://threatfeeds.io and press Enter. threatfeeds.io page appears.



Free and open-source threat intelligence feeds.

3. You can observe that threat feeds from different online resources are displayed. Scroll-down to Alienvault IP Reputation feed and click Download button to download the file.



Malware URLs

247K IOCs

FEED CSV MALWARE SPONSORED

Get Access

Managed by:
precisionsec

Events:
Added: 3 years ago

Alienvault IP Reputation

218K IOCs

FEED CSV

Download

Managed by:
AlienVault

Last fetch:
Size: 36382
Lines: 520
Status Code: 200

Events:
Added: 3 years ago
Pulled: 7 hours ago
Modified: 7 hours ago

AlphaSOC Ryuk C2

1K IOCs

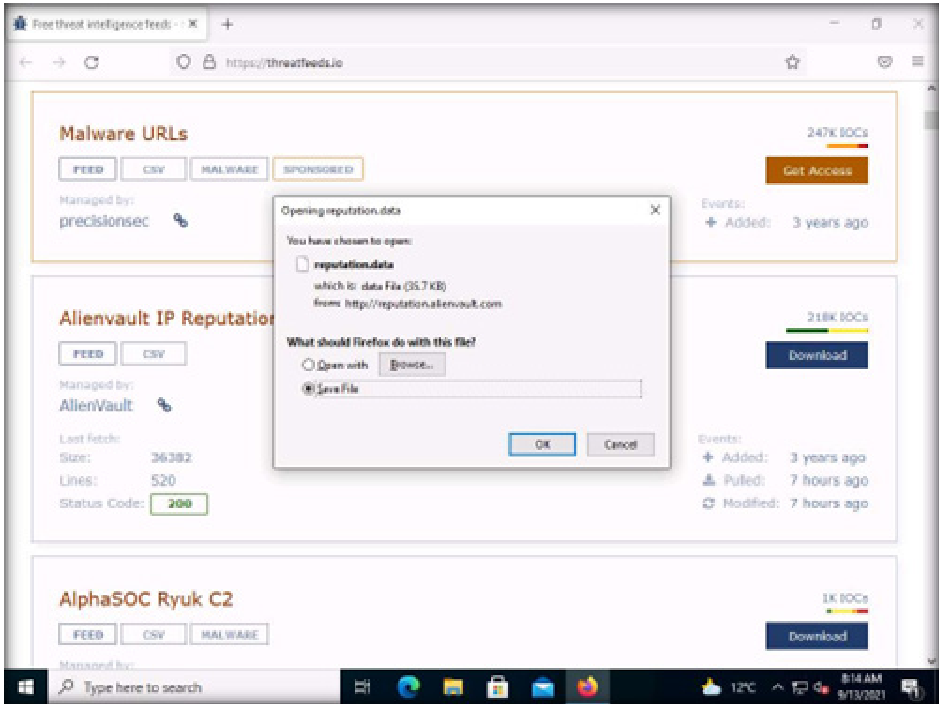
FEED CSV MALWARE

Download

reputation.alienvault.com/reputation.data

4. Opening reputation.data window appears, select Save File radio button and click OK.

EXERCISE 2:
GATHER THREAT
INTELLIGENC
FEED USING
THREATFEEDS.IO



Opening reputation.data

You have chosen to open:

reputation.data

which is: data File (35.7 KB)

from: http://reputation.alienvault.com

What should Firefox do with this file?

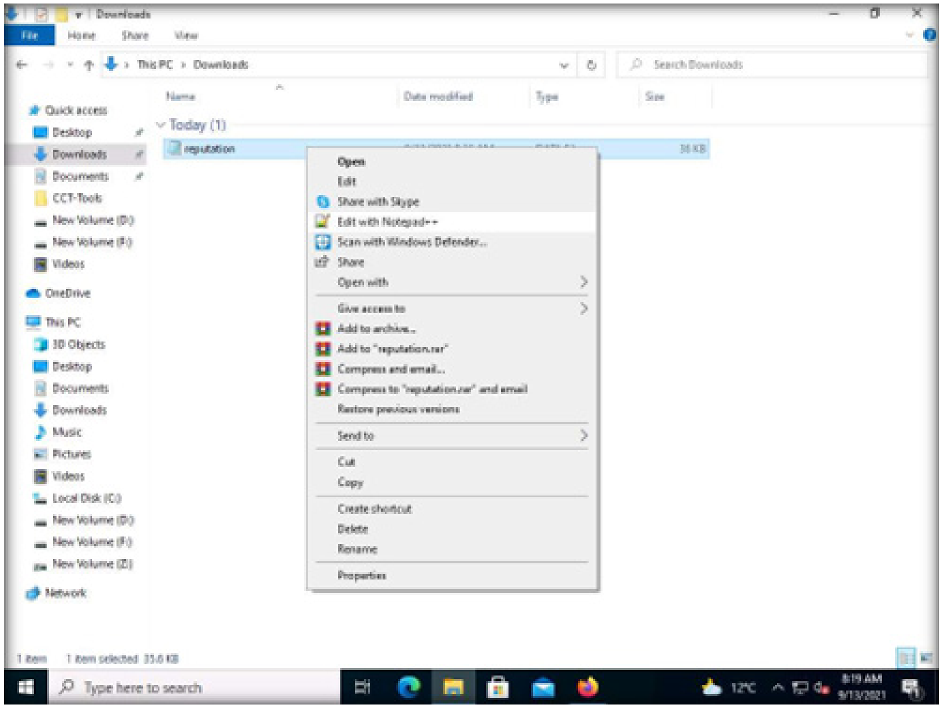
○ Open with [Browse...]

● Save File

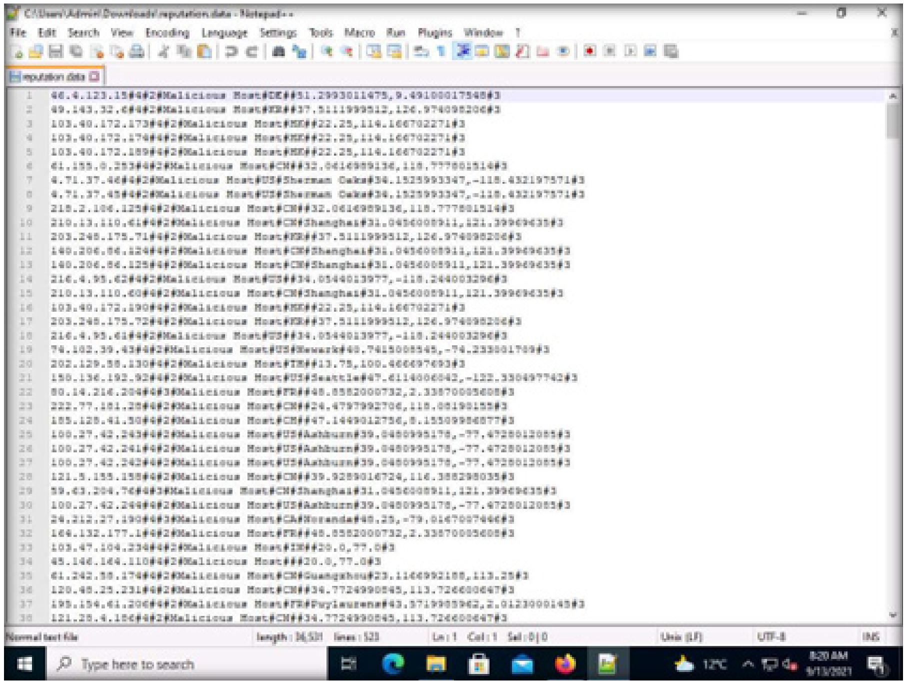
[OK] [Cancel]

5. After the completion of download, navigate to the download location (here, Downloads).

6. Click to select the file reputation.data. Right-click on it and select Edit with Notepad++ from the options.



7. A Notepad++ window appears, displaying the file content. This file contains a list of malicious IP addresses, as shown in the screenshot below.
Note: If update notepad++ pop-up appears, click on No.



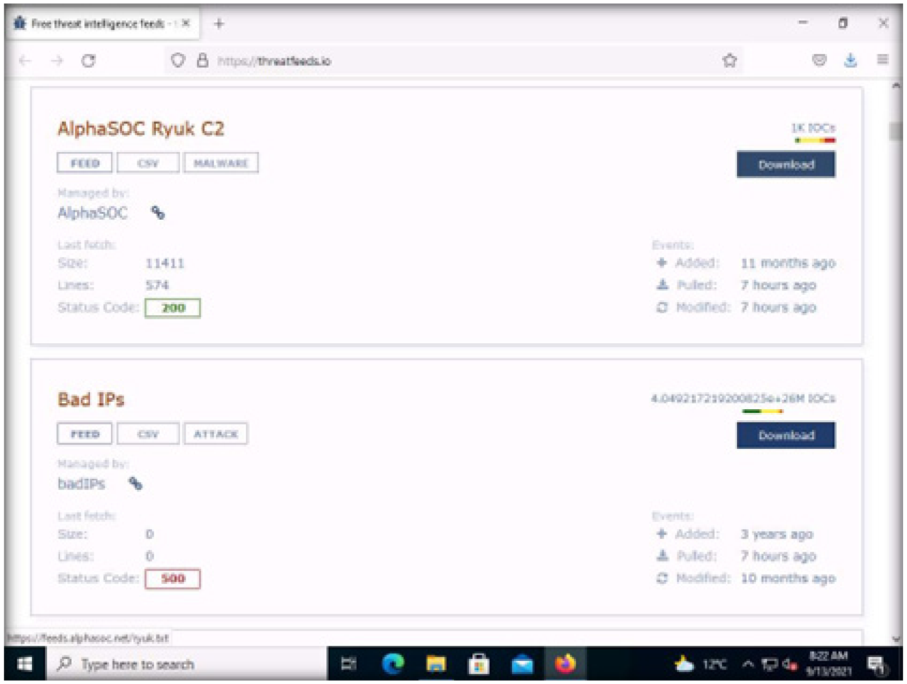
```
46.4.123.15#4#2#Malicious Host#DE##51.2993011475,9.4910001754#3
49.143.32.6#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
103.40.172.173#4#2#Malicious Host#HK##22.25,114.166702271#3
103.40.172.174#4#2#Malicious Host#HK##22.25,114.166702271#3
103.40.172.189#4#2#Malicious Host#HK##22.25,114.166702271#3
61.155.0.253#4#2#Malicious Host#CN##32.0616989136,118.777801514#3
4.71.37.46#4#2#Malicious Host#US#Sherman Oaks#34.1525993347,-118.432197571#3
4.71.37.45#4#2#Malicious Host#US#Sherman Oaks#34.1525993347,-118.432197571#3
218.2.106.125#4#2#Malicious Host#CN##32.0616989136,118.777801514#3
210.13.110.61#4#2#Malicious Host#CN#Shanghai#31.0456008911,121.39969635#3
203.248.175.71#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
140.206.86.124#4#2#Malicious Host#CN#Shanghai#31.0456008911,121.39969635#3
140.206.86.125#4#2#Malicious Host#CN#Shanghai#31.0456008911,121.39969635#3
216.4.95.62#4#2#Malicious Host#US##34.0544013977,-118.244003296#3
210.13.110.60#4#2#Malicious Host#CN#Shanghai#31.0456008911,121.39969635#3
103.40.172.190#4#2#Malicious Host#HK##22.25,114.166702271#3
203.248.175.72#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
216.4.95.61#4#2#Malicious Host#US##34.0544013977,-118.244003296#3
74.102.39.43#4#2#Malicious Host#US#Newark#40.7415008545,-74.233001709#3
202.129.58.130#4#2#Malicious Host#TH##13.75,100.466697693#3
150.136.192.92#4#2#Malicious Host#US#Seattle#47.6114006042,-122.330497742#3
80.14.216.204#4#3#Malicious Host#FR##48.8582000732,2.33870005608#3
222.77.181.28#4#2#Malicious Host#CN##24.4797992706,118.08190155#3
185.128.41.50#4#2#Malicious Host#CH##47.1449012756,8.15509986877#3
100.27.42.243#4#2#Malicious Host#US#Ashburn#39.0480995178,-77.4728012085#3
100.27.42.241#4#2#Malicious Host#US#Ashburn#39.0480995178,-77.4728012085#3
100.27.42.242#4#2#Malicious Host#US#Ashburn#39.0480995178,-77.4728012085#3
121.5.155.158#4#2#Malicious Host#CN##39.9289016724,116.388298035#3
59.63.204.76#4#3#Malicious Host#CN#Shanghai#31.0456008911,121.39969635#3
100.27.42.244#4#2#Malicious Host#US#Ashburn#39.0480995178,-77.4728012085#3
24.212.27.190#4#3#Malicious Host#CA#Noranda#48.25,-79.0167007446#3
164.132.177.1#4#2#Malicious Host#FR##48.8582000732,2.33870005608#3
103.47.104.234#4#2#Malicious Host#IN##20.0,77.0#3
45.146.164.110#4#2#Malicious Host###20.0,77.0#3
61.242.58.174#4#2#Malicious Host#CN#Guangzhou#23.1166992188,113.25#3
120.48.25.231#4#2#Malicious Host#CN##34.7724990845,113.726600647#3
195.154.41.206#4#2#Malicious Host#FR#Puylaurens#43.5719985962,2.0123000145#3
121.28.4.186#4#2#Malicious Host#CN##34.7724990845,113.726600647#3
```

Normal text file length : 36,531 lines : 523 Ln : 1 Col : 1 Sel : 0 | 0 Unix (LF) UTF-8 INS

8. Close the Notepad++ window and navigate back to the browser window.

9. Now, click Download button in the AlphaSOC Ryuk C2 feed.

EXERCISE 2: GATHER THREAT INTELLIGENC FEED USING THREATFEEDS.IO



AlphaSOC Ryuk C2

1K IOCs

FEED | CSV | MALWARE

Download

Managed by:
AlphaSOC

Last fetch:
Size: 11411
Lines: 574
Status Code: 200

Events:
Added: 11 months ago
Pulled: 7 hours ago
Modified: 7 hours ago

Bad IPs

4.0492172192008250+26M IOCs

FEED | CSV | ATTACK

Download

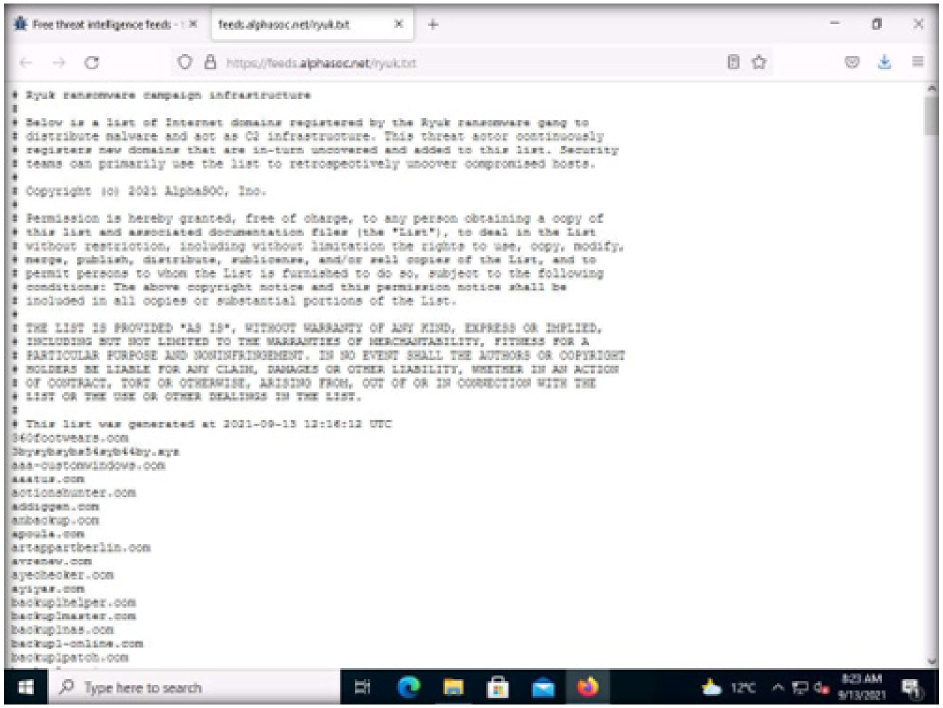
Managed by:
badIPs

Last fetch:
Size: 0
Lines: 0
Status Code: 500

Events:
Added: 3 years ago
Pulled: 7 hours ago
Modified: 10 months ago

https://feeds.alphasoc.net/ryuk.txt

10. The file content appears in a new tab. This file contains a list of Internet domains that are used to distribute malware and act as C2 infrastructure, as shown in the screenshot below.


Free threat intelligence feeds
feeds.alphasoc.net/ryuk.txt
https://feeds.alphasoc.net/ryuk.txt
Type here to search
12°C
8:23 AM
9/13/2021

```
# Ryuk ransomware campaign infrastructure
#
# Below is a list of Internet domains registered by the Ryuk ransomware gang to
# distribute malware and act as C2 infrastructure. This threat actor continuously
# registers new domains that are in-turn uncovered and added to this list. Security
# teams can primarily use the list to retrospectively uncover compromised hosts.
#
# Copyright (c) 2021 AlphaSOC, Inc.
#
# Permission is hereby granted, free of charge, to any person obtaining a copy of
# this list and associated documentation files (the "List"), to deal in the List
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the List, and to
# permit persons to whom the List is furnished to do so, subject to the following
# conditions: The above copyright notice and this permission notice shall be
# included in all copies or substantial portions of the List.
#
# THE LIST IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# LIST OR THE USE OR OTHER DEALINGS IN THE LIST.
#
# This list was generated at 2021-09-13 12:16:12 UTC
360footwears.com
3byeybeyba54eyb44by.xyz
aaa-customwindows.com
aaatus.com
actionshunter.com
addiggen.com
anbackup.com
apoula.com
artappartberlin.com
avrenew.com
ayechecker.com
ayiyas.com
backup1helper.com
backup1master.com
backup1nas.com
backup1-online.com
backup1patch.com
```

11. Close the current tab to navigate back to the tab where threatfeeds.io is opened.

12. Similarly, you can browse through other threat feeds from different online resources. These TI feeds can be used to enhance security infrastructure to thwart cyber-attacks on local network and systems.

13. This concludes the demonstration of showing how to gather threat intelligence feeds using threatfeeds.io.

14. Close all open windows.

EXERCISE 2:
GATHER THREAT
INTELLIGENC
FEED USING
THREATFEEDS.IO

EXERCISE 3: PERFORM VULNERABILITY RESEARCH IN COMMON WEAKNESS ENUMERATION (CWE)

Vulnerability Research discovers the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

LAB SCENARIO

A security professional must keep up with the most recently discovered vulnerabilities and exploits to stay one step ahead of attackers through vulnerability research.

OBJECTIVE

The objective of this lab is to learn how to perform vulnerability research using online resources such as Common Weakness Enumeration (CWE).

OVERVIEW OF THREAT INTELLIGENCE FEED

Vulnerability Research is performed, due to following reasons:

- To gather information about security trends, newly discovered threats, attack surfaces, attack vectors and techniques
- To find weaknesses in the OS and applications and alert the network administrator before a network attack
- To understand information that helps prevent security problems
- To know how to recover from a network attack

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

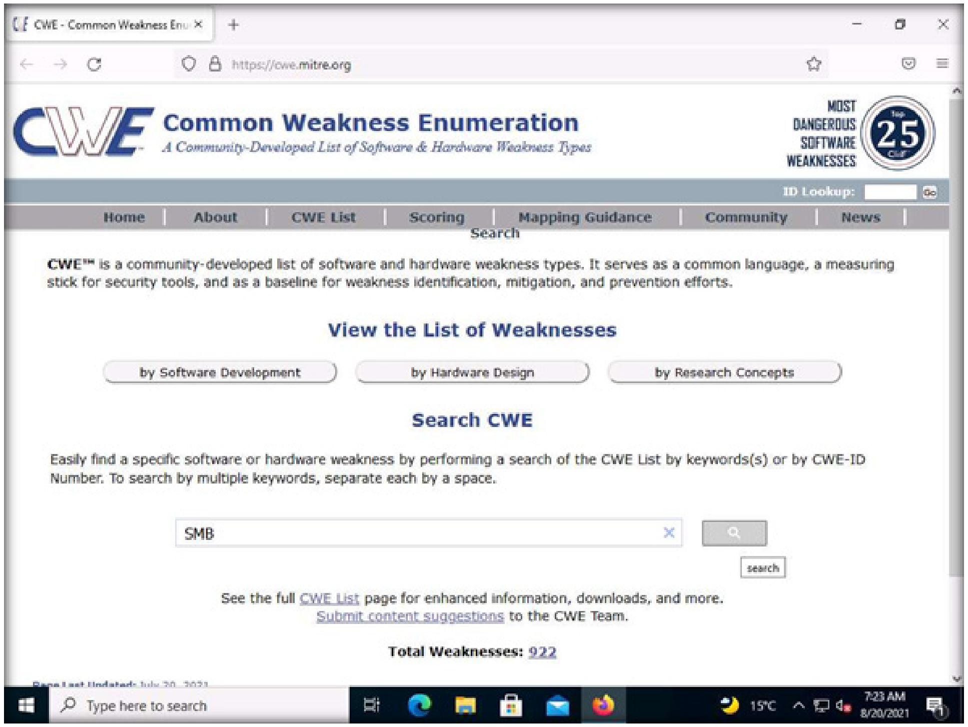
Security professional can use CWE to view the latest underlying system vulnerabilities.

EXERCISE 3: PERFORM VULNERABILITY RESEARCH IN COMMON WEAKNESS ENUMERATION (CWE)

Note: Ensure that the Admin Machine-1 and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, launch any browser, here, we are using Mozilla Firefox. In the address bar of the browser place your mouse cursor and type https://cwe.mitre.org/ and press Enter
Note: - If the Default Browser pop-up window appears, uncheck the Always perform this check when starting Firefox checkbox and click the Not now button.
Note: - If New in Firefox: Content Blocking pop-up window appears, follow the step and click Got it to finish viewing the information.
Note: If an Update available pop-up appears, click on Dismiss.

2. CWE website appears. In the Google Custom Search under Search CWE section, type SMB and click the search icon.



Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

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.

View the List of Weaknesses

Search CWE

Easily find a specific software or hardware weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

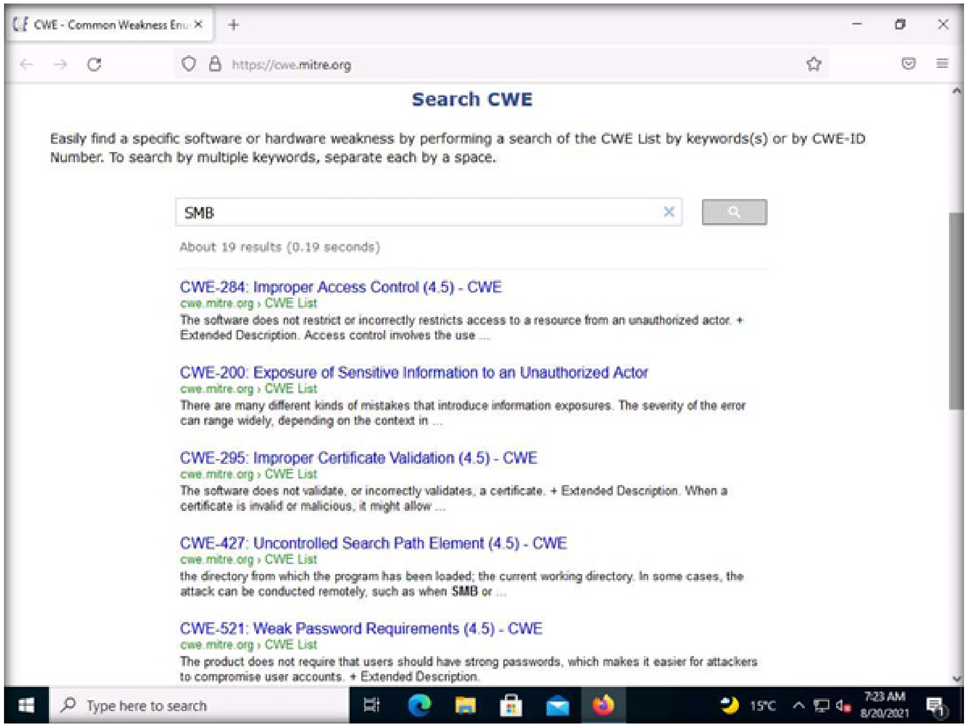
SMB

See the full CWE List page for enhanced information, downloads, and more.
Submit content suggestions to the CWE Team.

Total Weaknesses: 922

Page Last Updated: July 20, 2021

3. The search results appear, displaying the underlying vulnerabilities in the target service (here, SMB). You can click any link to view detailed information on the vulnerability.
Note: The search results might differ when you perform this lab.



Search CWE

Easily find a specific software or hardware weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

SMB

About 19 results (0.19 seconds)

CWE-284: Improper Access Control (4.5) - CWE
cwe.mitre.org › CWE List
The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor. + Extended Description. Access control involves the use ...

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
cwe.mitre.org › CWE List
There are many different kinds of mistakes that introduce information exposures. The severity of the error can range widely, depending on the context in ...

CWE-295: Improper Certificate Validation (4.5) - CWE
cwe.mitre.org › CWE List
The software does not validate, or incorrectly validates, a certificate. + Extended Description. When a certificate is invalid or malicious, it might allow ...

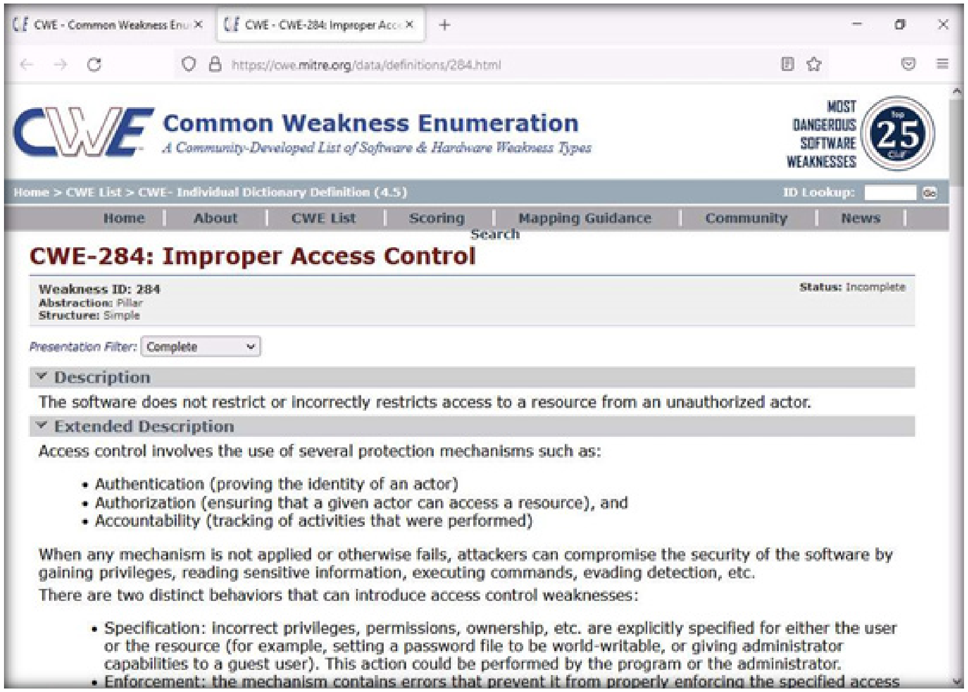
CWE-427: Uncontrolled Search Path Element (4.5) - CWE
cwe.mitre.org › CWE List
the directory from which the program has been loaded; the current working directory. In some cases, the attack can be conducted remotely, such as when SMB or ...

CWE-521: Weak Password Requirements (4.5) - CWE
cwe.mitre.org › CWE List
The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts. + Extended Description.

EXERCISE 3: PERFORM VULNERABILITY RESEARCH IN COMMON WEAKNESS ENUMERATION (CWE)

4. Now, click any link (here, CWE-284) to view detailed information about the vulnerability.

5. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.


CWE - Common Weakness Enu
CWE - CWE-284: Improper Acc
https://cwe.mitre.org/data/definitions/284.html
CWE
Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types
MOST DANGEROUS SOFTWARE WEAKNESSES
Top 25 CWE
Home > CWE List > CWE- Individual Dictionary Definition (4.5)
ID Lookup:
Go
Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

CWE-284: Improper Access Control

Weakness ID: 284
Abstraction: Pillar
Structure: Simple
Status: Incomplete

Presentation Filter: Complete

▾ Description

The software 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)

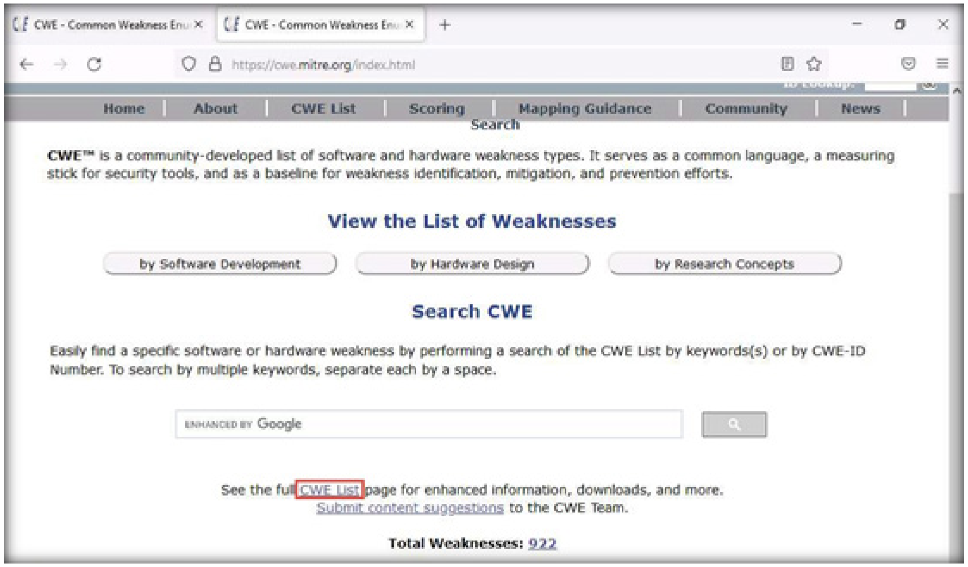
When any mechanism is not applied or otherwise fails, attackers can compromise the security of the software by gaining privileges, reading sensitive information, executing commands, evading detection, etc.

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

6. Similarly, you can click on other vulnerabilities and view detailed information.

7. Now, click on Home to navigate back to the CWE website, scroll down, and click the CWE List link present below the searched results.


CWE - Common Weakness Enu ×
CWE - Common Weakness Enu ×
https://cwe.mitre.org/index.html
Home
About
CWE List
Scoring
Mapping Guidance
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.

View the List of Weaknesses

Search CWE

Easily find a specific software or hardware weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

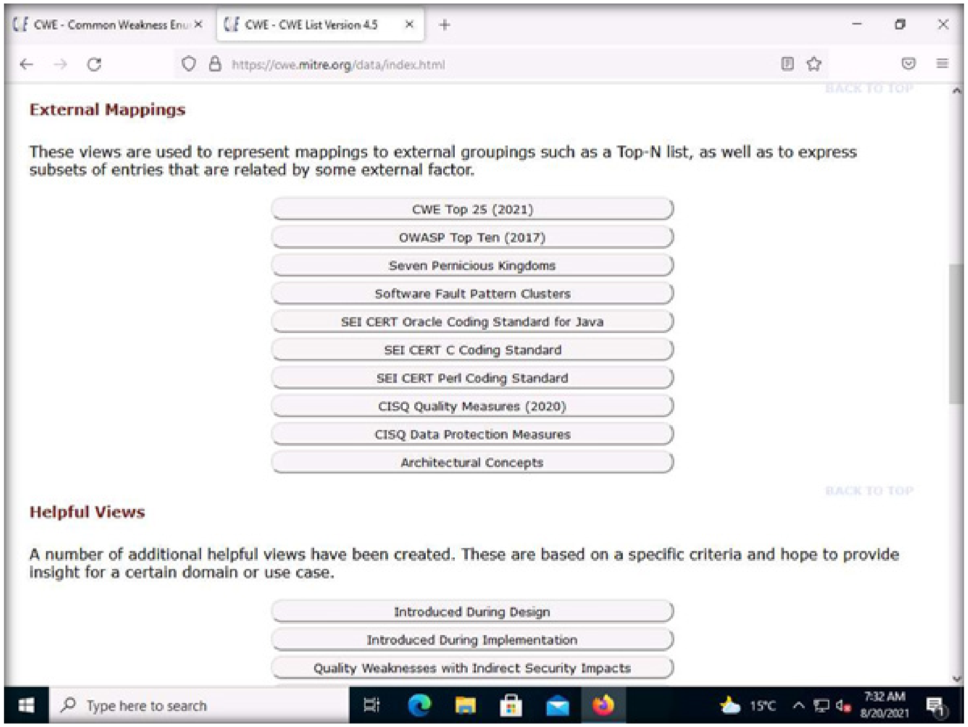
See the full CWE List page for enhanced information, downloads, and more.
Submit content suggestions to the CWE Team.

Total Weaknesses: 922

EXERCISE 3: PERFORM VULNERABILITY RESEARCH IN COMMON WEAKNESS ENUMERATION (CWE)

8. A new webpage appears, displaying CWE List Version. Scroll down, and under the External Mappings section, click CWE Top 25 (2021).
Note: The results might differ when you perform this lab.

EXERCISE 3: PERFORM VULNERABILITY RESEARCH IN COMMON WEAKNESS ENUMERATION (CWE)


CWE - Common Weakness Enu
CWE - CWE List Version 4.5
https://cwe.mitre.org/data/index.html
BACK TO TOP

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 (2021)
OWASP Top Ten (2017)
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
Architectural Concepts
BACK TO TOP

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.

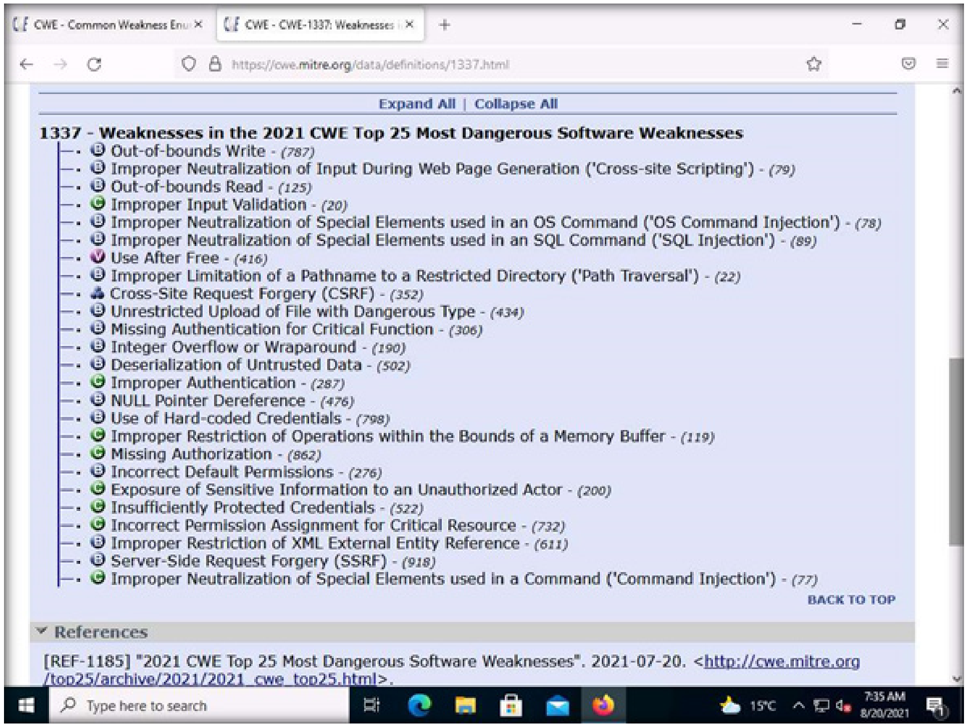
Introduced During Design
Introduced During Implementation
Quality Weaknesses with Indirect Security Impacts
Type here to search
15°C
7:32 AM
8/20/2021

9. A webpage appears, displaying CWE VIEW: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses. Scroll down and view a list of Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses under the Relationships section. You can click on each weakness to view detailed information on it.

Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

Note: The result publishing year be might different when you perform this lab.

EXERCISE 3: PERFORM VULNERABILITY RESEARCH IN COMMON WEAKNESS ENUMERATION (CWE)


CWE - Common Weakness Enu
CWE - CWE-1337: Weaknesses i
https://cwe.mitre.org/data/definitions/1337.html
Expand All | Collapse All
BACK TO TOP
Type here to search
15°C
7:35 AM
8/20/2021

1337 - Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses

- Out-of-bounds Write - *(787)*
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - *(79)*
- Out-of-bounds Read - *(125)*
- Improper Input Validation - *(20)*
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - *(78)*
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - *(89)*
- Use After Free - *(416)*
- 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 Authentication for Critical Function - *(306)*
- Integer Overflow or Wraparound - *(190)*
- Deserialization of Untrusted Data - *(502)*
- Improper Authentication - *(287)*
- NULL Pointer Dereference - *(476)*
- Use of Hard-coded Credentials - *(798)*
- Improper Restriction of Operations within the Bounds of a Memory Buffer - *(119)*
- Missing Authorization - *(862)*
- Incorrect Default Permissions - *(276)*
- Exposure of Sensitive Information to an Unauthorized Actor - *(200)*
- Insufficiently Protected Credentials - *(522)*
- Incorrect Permission Assignment for Critical Resource - *(732)*
- Improper Restriction of XML External Entity Reference - *(611)*
- Server-Side Request Forgery (SSRF) - *(918)*
- Improper Neutralization of Special Elements used in a Command ('Command Injection') - *(77)*

References

[REF-1185] "2021 CWE Top 25 Most Dangerous Software Weaknesses". 2021-07-20. <http://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html>.

10. Similarly, you can go back to the CWE website and explore other options, as well.

11. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).

12. Close all open windows and document all the acquired information.

13. Turn off the Admin Machine-1 virtual machine.

EXERCISE 3: PERFORM VULNERABILITY RESEARCH IN COMMON WEAKNESS ENUMERATION (CWE)

EXERCISE 4: **PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK**

A vulnerability assessment is the process of identifying vulnerabilities in network components, including the OS, web applications, and web servers.

LAB SCENARIO

A security professional requires knowledge to perform vulnerability assessment in order to address the issues identified in the system and avoid serious damage to an organization's assets.

OBJECTIVE

The objective of this lab is to learn how to perform vulnerability assessment to determine system vulnerabilities using OpenVAS.

OVERVIEW OF VULNERABILITY ASSESSMENT

Vulnerability assessment helps identify the category and criticality of the vulnerability in an organization. An organization rates the vulnerabilities and prioritizes them, and design methods to remedy the situation accordingly. The assessment method helps measure the effectiveness of those remedies. The goal of the vulnerability assessment includes scanning, examining, evaluating, and reporting the vulnerabilities in a network to, thus, minimize the levels of risks to an organization.

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Security professional can use the OpenVAS Tool as a proof of concept to identify system vulnerabilities in an organization.

Note: In this task, we will use the Attacker Machine-2 (10.10.1.13) machine as a host machine and the Web Server (10.10.1.16) machine as a target machine.

Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on Attacker Machine-2 and Web Server virtual machines.

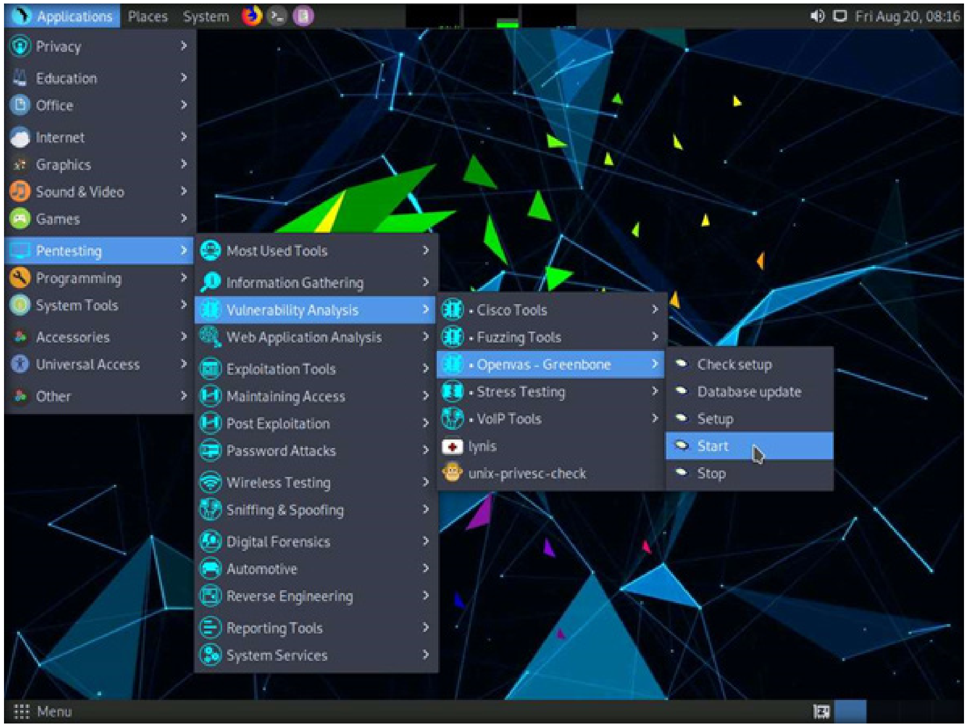
2. In the Attacker Machine-2 login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.

Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

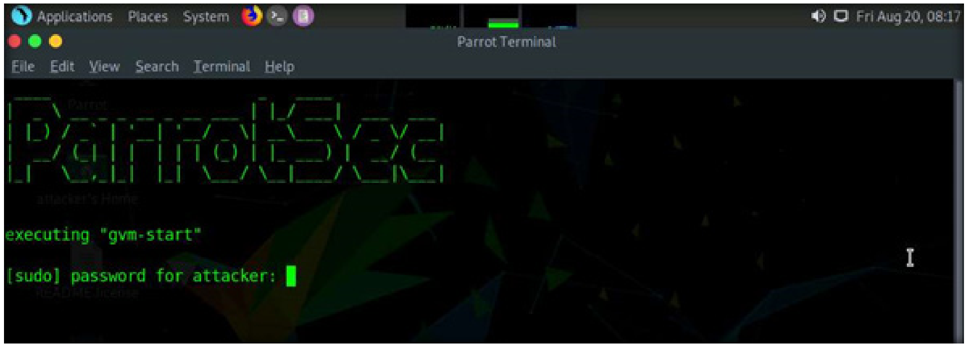
Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

3. Click Applications at the top of the Desktop window and navigate to Pentesting → Vulnerability Analysis → Openvas - Greenbone → Start to launch OpenVAS tool.

EXERCISE 4: PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK

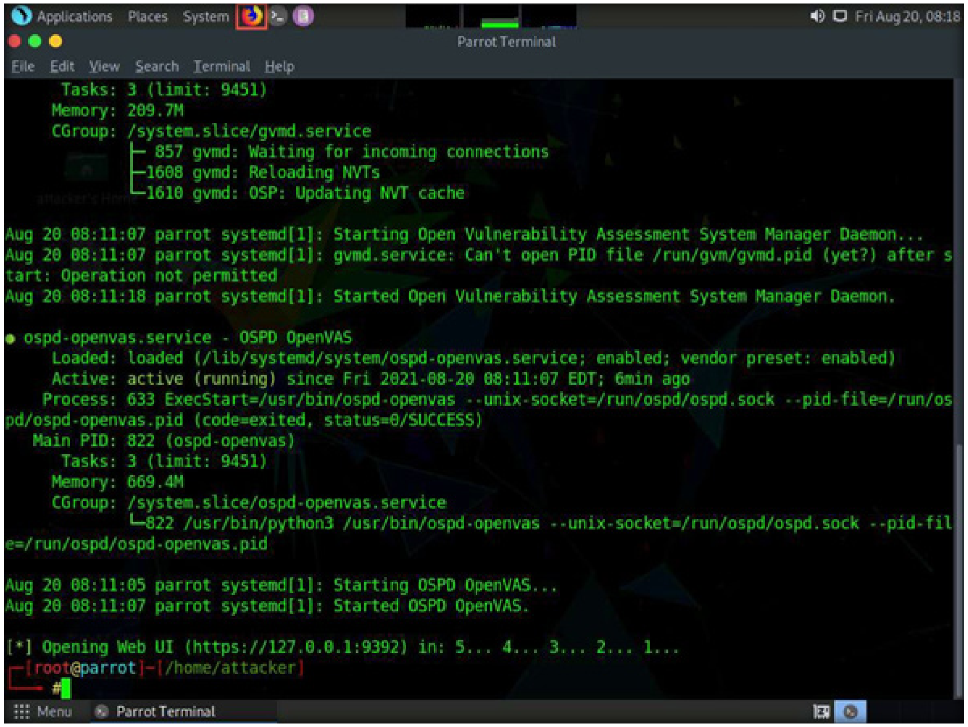


4. A terminal window appears, in the [sudo] password for attacker field, type toor as a password and press Enter. OpenVAS initializes.
Note: The password that you type will not be visible.


Applications Places System
Fri Aug 20, 08:17
Parrot Terminal
File Edit View Search Terminal Help
ParrotSec

```
executing "gvm-start"

[sudo] password for attacker:
```

5. After the tool initializes, click Firefox icon from the top-section of the Desktop.



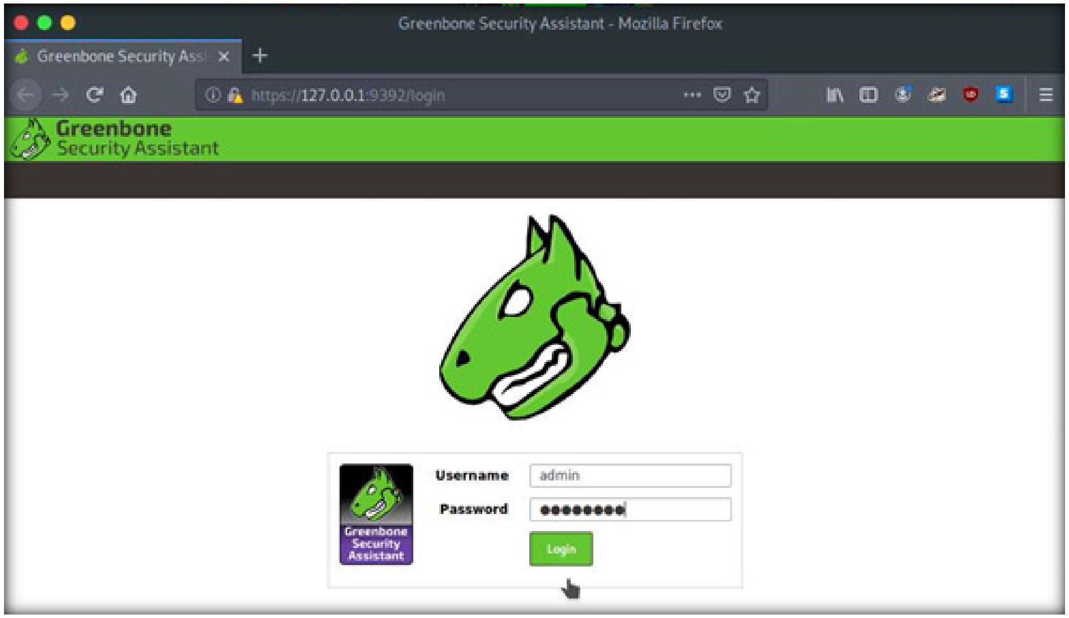
```
      Tasks: 3 (limit: 9451)
     Memory: 209.7M
     CGroup: /system.slice/gvmd.service
             ├─ 857 gvmd: Waiting for incoming connections
             ├─1608 gvmd: Reloading NVTs
             └─1610 gvmd: OSP: Updating NVT cache

Aug 20 08:11:07 parrot systemd[1]: Starting Open Vulnerability Assessment System Manager Daemon...
Aug 20 08:11:07 parrot systemd[1]: gvmd.service: Can't open PID file /run/gvm/gvmd.pid (yet?) after s
tart: Operation not permitted
Aug 20 08:11:18 parrot systemd[1]: Started Open Vulnerability Assessment System Manager Daemon.

● ospd-openvas.service - OSPD OpenVAS
     Loaded: loaded (/lib/systemd/system/ospd-openvas.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2021-08-20 08:11:07 EDT; 6min ago
    Process: 633 ExecStart=/usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-file=/run/os
pd/ospd-openvas.pid (code=exited, status=0/SUCCESS)
   Main PID: 822 (ospd-openvas)
      Tasks: 3 (limit: 9451)
     Memory: 669.4M
     CGroup: /system.slice/ospd-openvas.service
             └─822 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket=/run/ospd/ospd.sock --pid-fil
e=/run/ospd/ospd-openvas.pid

Aug 20 08:11:05 parrot systemd[1]: Starting OSPD OpenVAS...
Aug 20 08:11:07 parrot systemd[1]: Started OSPD OpenVAS.

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

EXERCISE 4: PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK

6. The Firefox browser appears, in the address bar, type https://127.0.0.1:9392 and press Enter.

7. OpenVAS login page appears, log in with Username and Password as admin and password and click the Login button.
Note: If Would you like Firefox to save login pop-up appears, click on Don’t Save.

EXERCISE 4: PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK



Greenbone Security Assistant - Mozilla Firefox

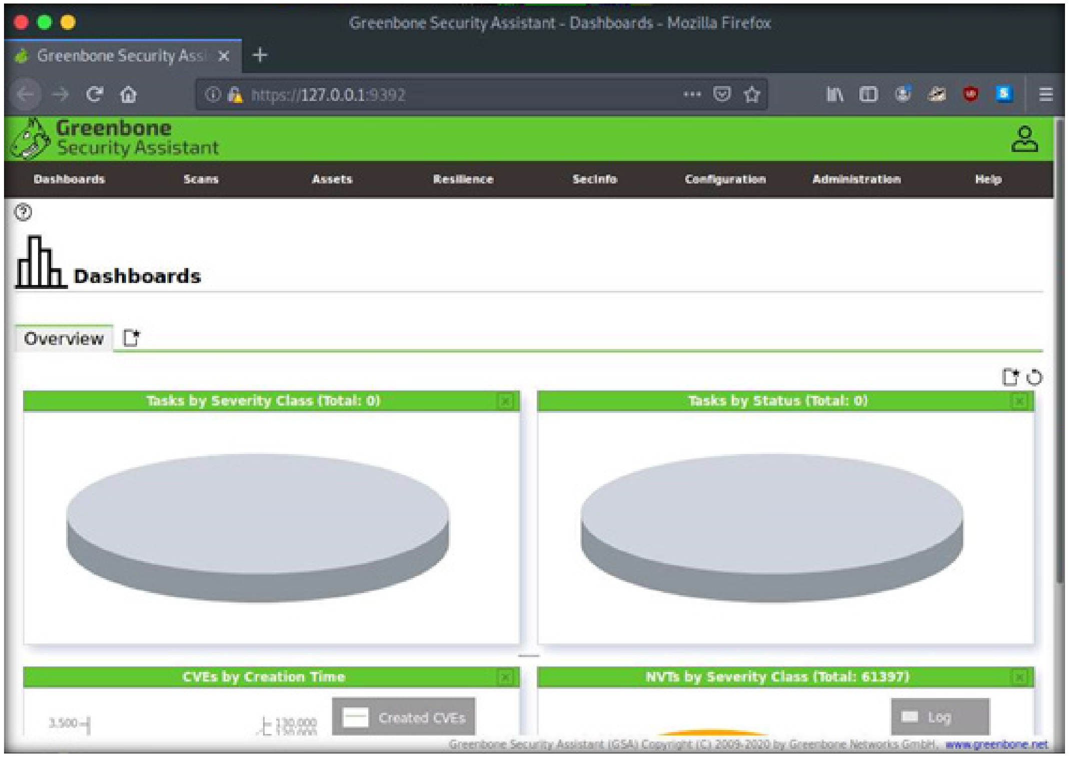
https://127.0.0.1:9392/login

Username: admin

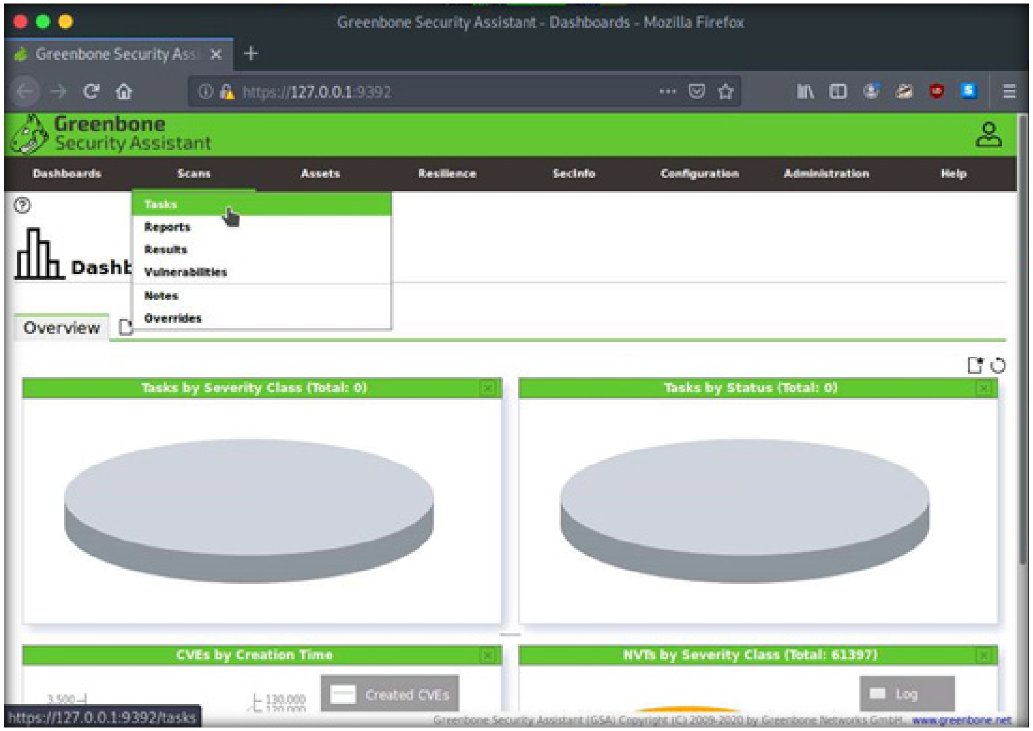
Password: ●●●●●●●●●

8. OpenVAS Dashboards appears, as shown in the screenshot below.

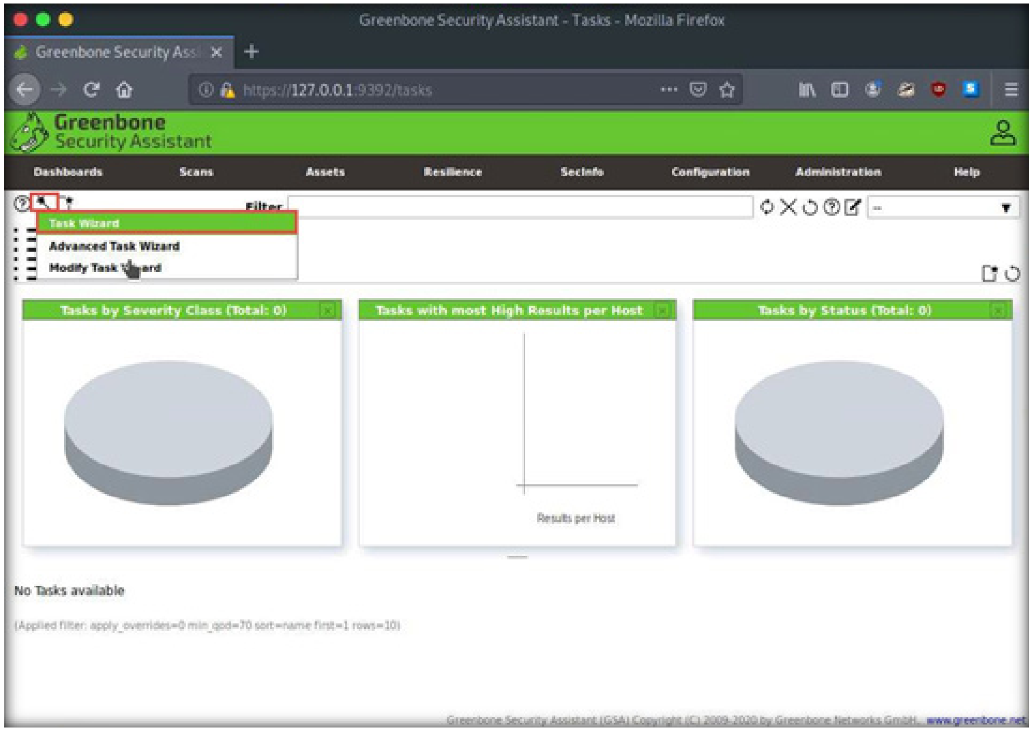
EXERCISE 4: PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK


Greenbone Security Assistant - Dashboards - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Dashboards
Overview
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
CVEs by Creation Time
NVTs by Severity Class (Total: 61397)
3,500
Created CVEs
Log
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

9. Navigate to Scans → Tasks from the Menu bar.
Note: If a Welcome to the scan management! pop-up appears, close it.


Greenbone Security Assistant - Dashboards - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392
Greenbone
Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Tasks
Reports
Results
Vulnerabilities
Notes
Overrides
Dashb
Overview
Tasks by Severity Class (Total: 0)
Tasks by Status (Total: 0)
CVEs by Creation Time
NVTs by Severity Class (Total: 61397)
Created CVEs
Log
https://127.0.0.1:9392/tasks
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

10. Hover over wand icon and click the Task Wizard option.



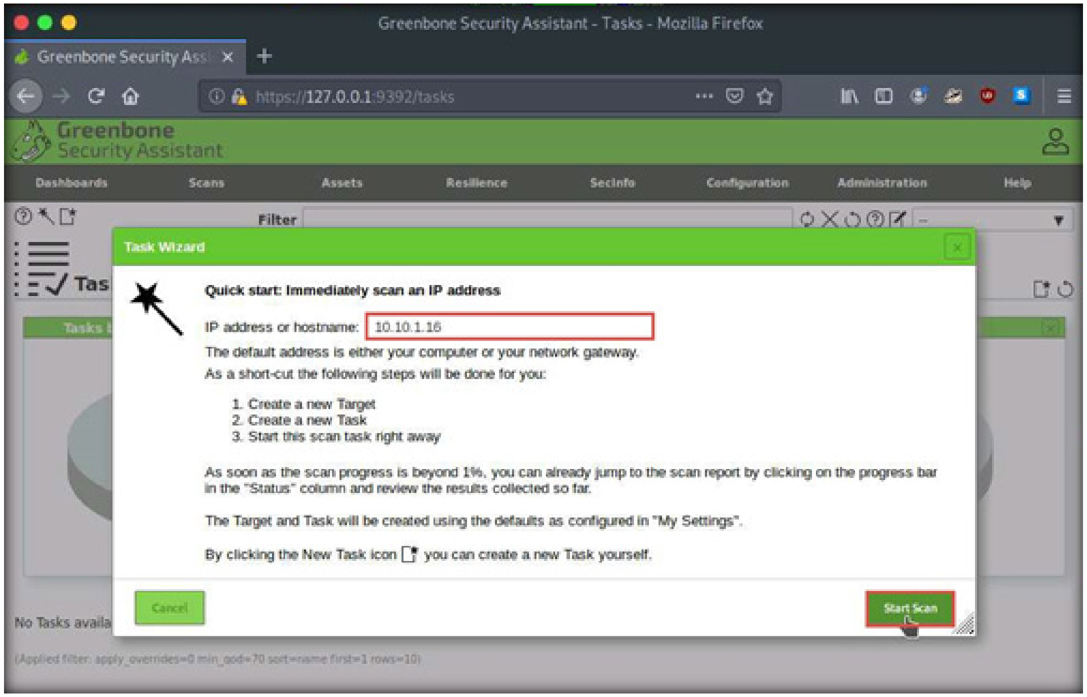
No Tasks available

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

11. The Task Wizard window appears; enter the target IP address in the IP address or hostname field (here, the target system is Web Server [10.10.1.16]) and click the Start Scan button.

EXERCISE 4: PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK


Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Assi
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tas
Tasks
No Tasks availa
(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)
Task Wizard
Cancel
Start Scan

Quick start: Immediately scan an IP address

IP address or hostname: 10.10.1.16

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

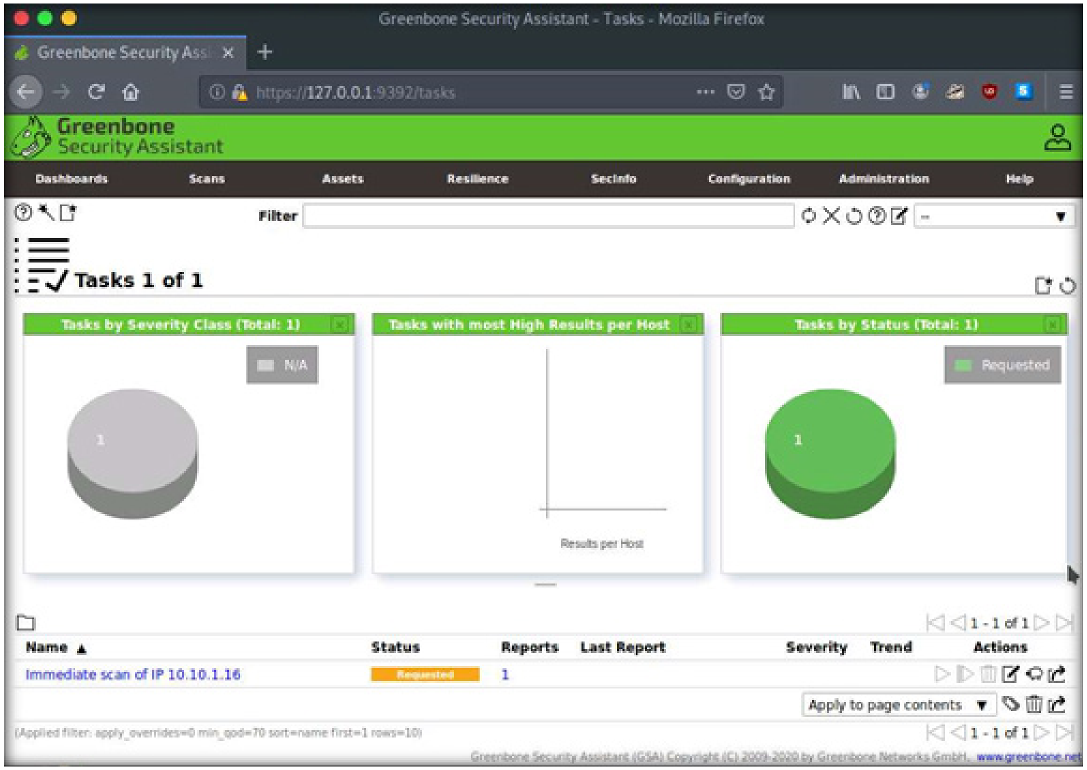
As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

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.

EXERCISE 4: PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK

12. The task appears under the Tasks section; OpenVAS starts scanning the target IP address.



Greenbone Security Assistant - Tasks - Mozilla Firefox

https://127.0.0.1:9392/tasks

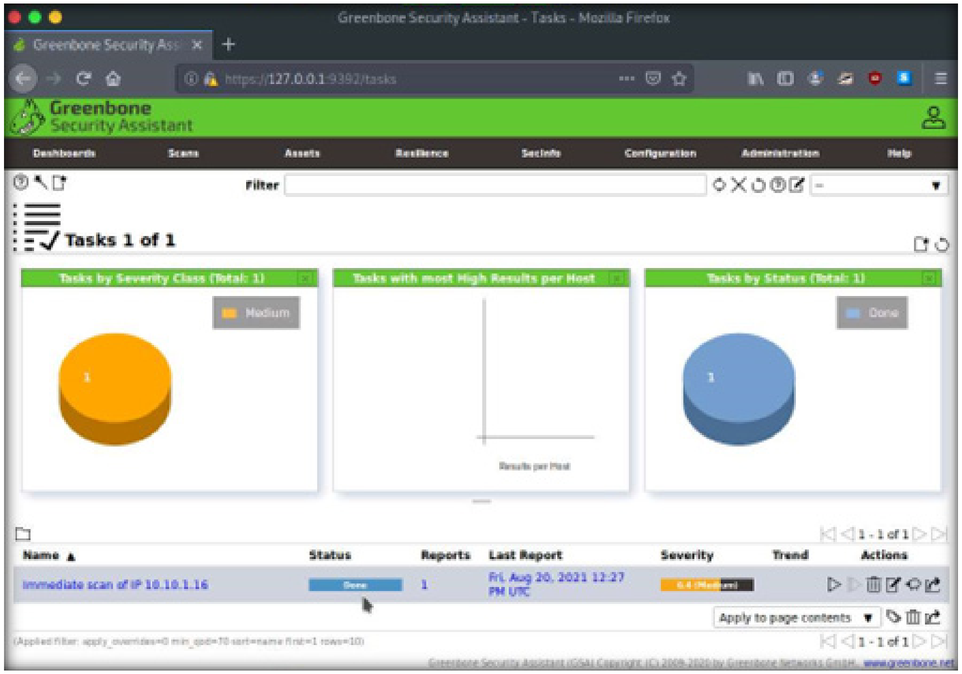
Tasks 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.10.1.16	Requested	1				

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

13. Wait for the Status to change from Requested to Done. Once it is completed, click the Done button under the Status column to view the vulnerabilities found in the target system.
Note: If you are logged out of the session, login again using credentials admin/password.

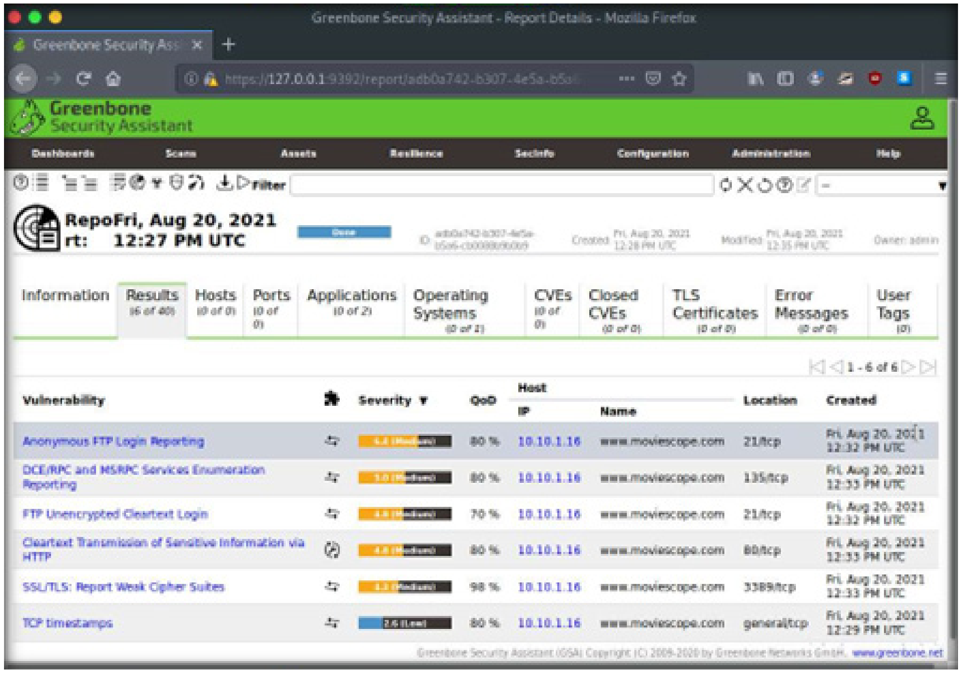

Greenbone Security Assistant - Tasks - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/tasks
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Tasks 1 of 1
Tasks by Severity Class (Total: 1)
Medium
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 1)
Done
1
1 - 1 of 1
Apply to page contents
Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.10.1.16	Done	1	Fri, Aug 20, 2021 12:27 PM UTC	6.4 (Medium)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

EXERCISE 4: PERFORM VULNERABILITY ASSESSMENT TO IDENTIFY SECURITY VULNERABILITIES IN THE TARGET SYSTEM OR NETWORK

14. Report: Information appears, click Results tab to view the discovered vulnerabilities along with their severity and the port numbers on which they are running.



Report: Fri, Aug 20, 2021 12:27 PM UTC

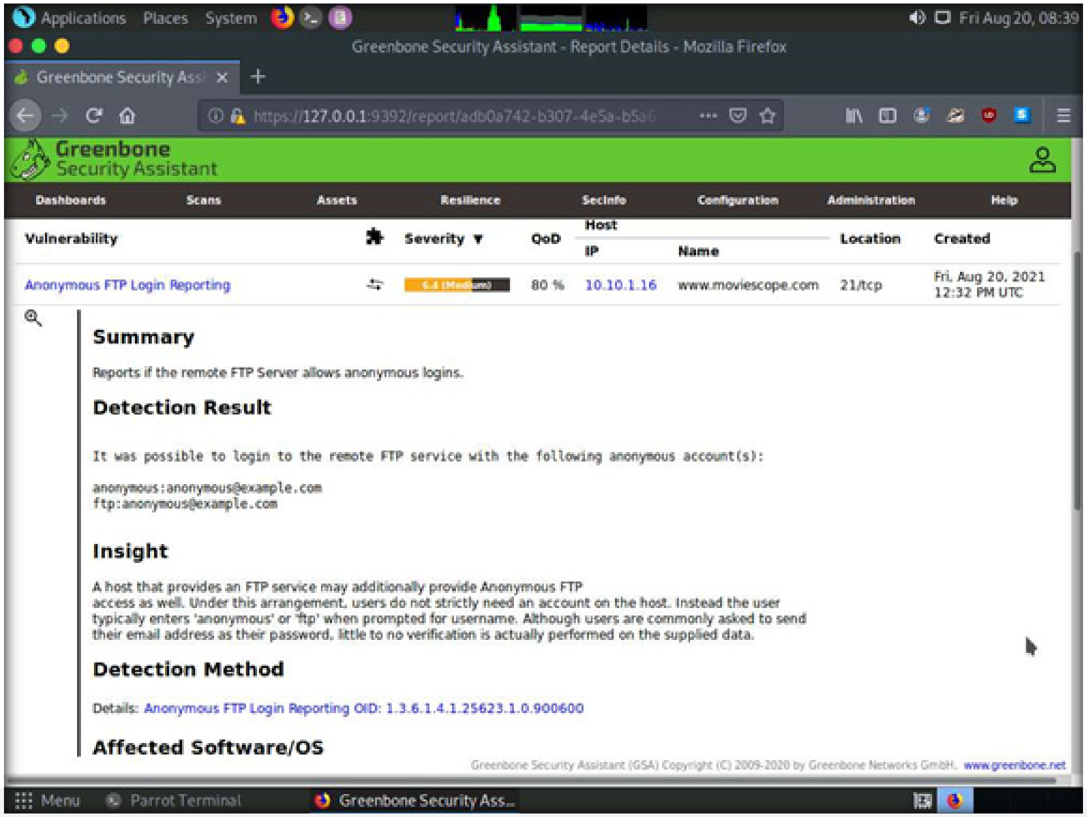
ID: adb0a742-b307-4e5a-b5a6-c000080f6069 Created: Fri, Aug 20, 2021 12:28 PM UTC Modified: Fri, Aug 20, 2021 12:35 PM UTC Owner: admin

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Anonymous FTP Login Reporting		6.4 (Medium)	80 %	10.10.1.16	www.moviescope.com	21/tcp	Fri, Aug 20, 2021 12:32 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80 %	10.10.1.16	www.moviescope.com	135/tcp	Fri, Aug 20, 2021 12:33 PM UTC
FTP Unencrypted Cleartext Login		4.8 (Medium)	70 %	10.10.1.16	www.moviescope.com	21/tcp	Fri, Aug 20, 2021 12:32 PM UTC
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80 %	10.10.1.16	www.moviescope.com	80/tcp	Fri, Aug 20, 2021 12:33 PM UTC
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98 %	10.10.1.16	www.moviescope.com	3389/tcp	Fri, Aug 20, 2021 12:33 PM UTC
TCP timestamps		2.6 (Low)	80 %	10.10.1.16	www.moviescope.com	general/tcp	Fri, Aug 20, 2021 12:29 PM UTC

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

15. Click on any vulnerability under the Vulnerability column (here, Anonymous FTP Login Reporting to view its detailed information.

16. Detailed information regarding selected vulnerability appears, as shown in the screenshot below.


Applications Places System
Fri Aug 20, 08:39
Greenbone Security Assistant - Report Details - Mozilla Firefox
Greenbone Security Ass
https://127.0.0.1:9392/report/adb0a742-b307-4e5a-b5a
Greenbone Security Assistant
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Anonymous FTP Login Reporting		6.4 (Medium)	80 %	10.10.1.16	www.moviescope.com	21/tcp	Fri, Aug 20, 2021 12:32 PM UTC

Summary

Reports if the remote FTP Server allows anonymous logins.

Detection Result

```
It was possible to login to the remote FTP service with the following anonymous account(s):

anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Insight

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Detection Method

Details: Anonymous FTP Login Reporting OID: 1.3.6.1.4.1.25623.1.0.900600

Affected Software/OS

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net
Menu
Parrot Terminal
Greenbone Security Ass...

17. Similarly, you can click other discovered vulnerabilities under the Report: Results section to view detailed information regarding the vulnerabilities in the target system.

18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known.

19. This concludes the demonstration showing how to perform vulnerabilities analysis using OpenVAS.

20. Close all open windows and document all the acquired information.

21. Turn off Attacker Machine-2, Web Server, and PfSense Firewall virtual machines.

EXERCISE 4:
PERFORM
VULNERABILITY
ASSESSMENT TO
IDENTIFY SECURITY
VULNERABILITIES IN
THE TARGET SYSTEM
OR NETWORK

EC-Council