

Nessus

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks.

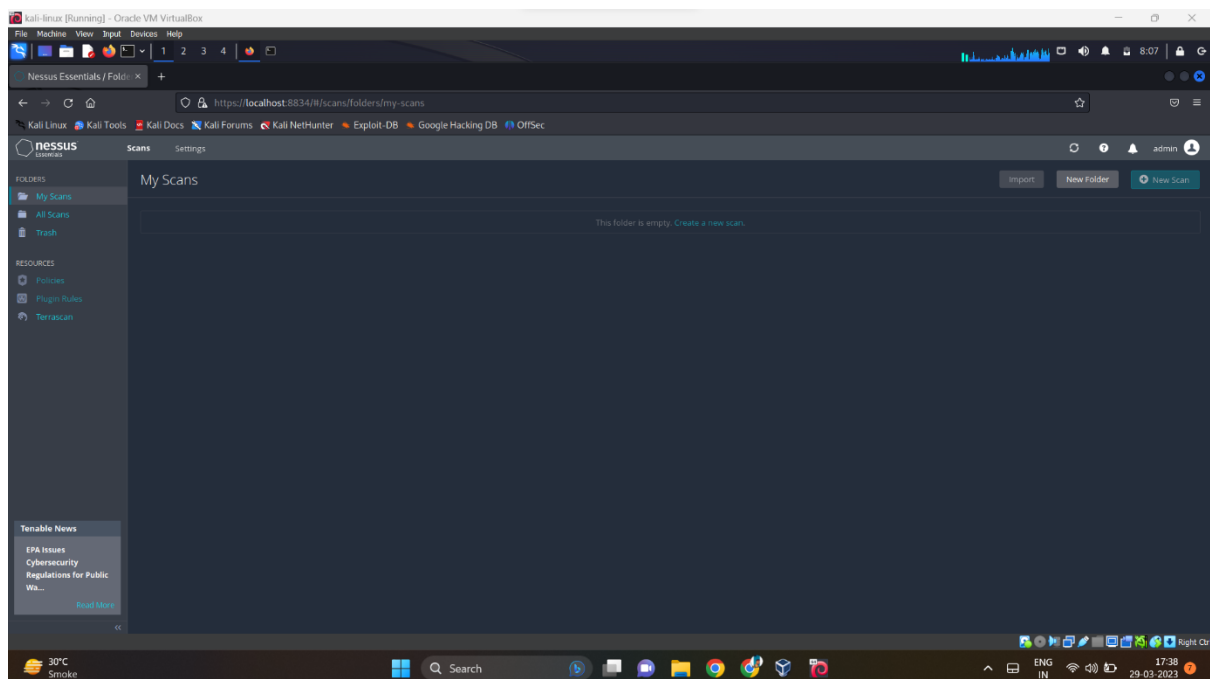
Nessus has a modular architecture consisting of centralized servers that conduct scanning, and remote clients that allow for administrator interaction. Administrators can include NASL descriptions of all suspected vulnerabilities to develop customized scans. Significant capabilities of Nessus include:

- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment.
- Scheduled security audits.

I will target 'skullcandy.com' and my MS2 with IP Address 192.168.0.5

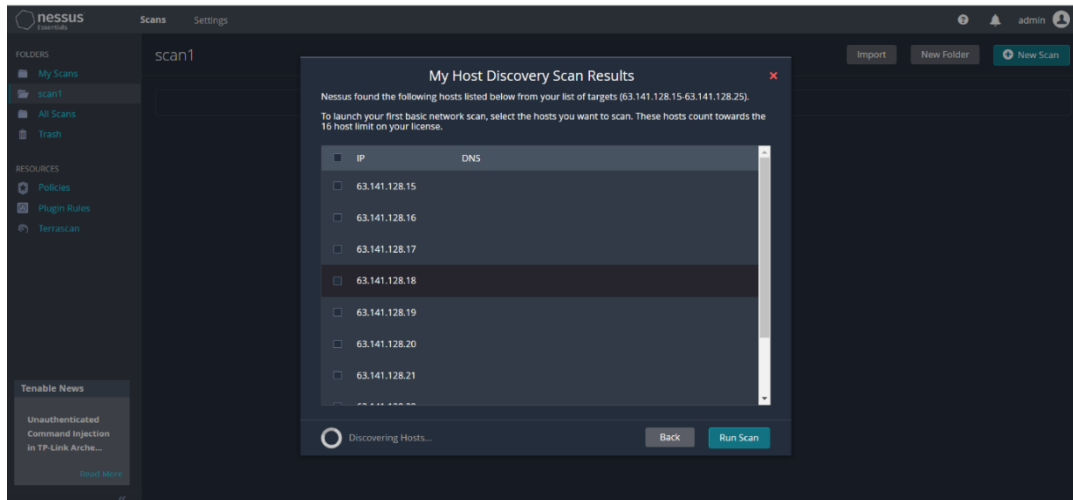
First, we have to install Nessus. Go to 'localhost:8834' and the Nessus will start. It will take time to download plugins. After it's done login using username= 'admin' and password= 'admin'.

You will come to this screen.

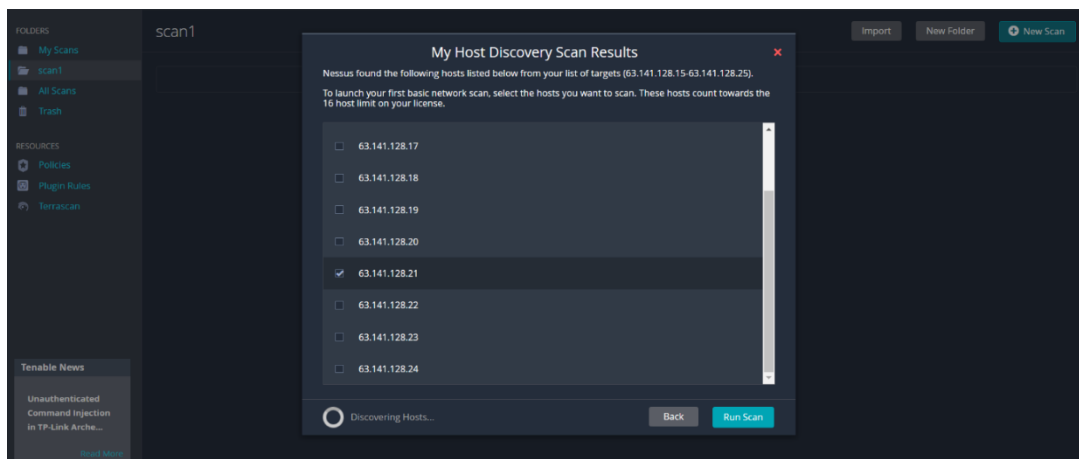


Then you scan multiple server or host and you can even scan single host.

I'll scan multiple host ranges from IP Address = 63.141.128.15 – 63.128.141.25



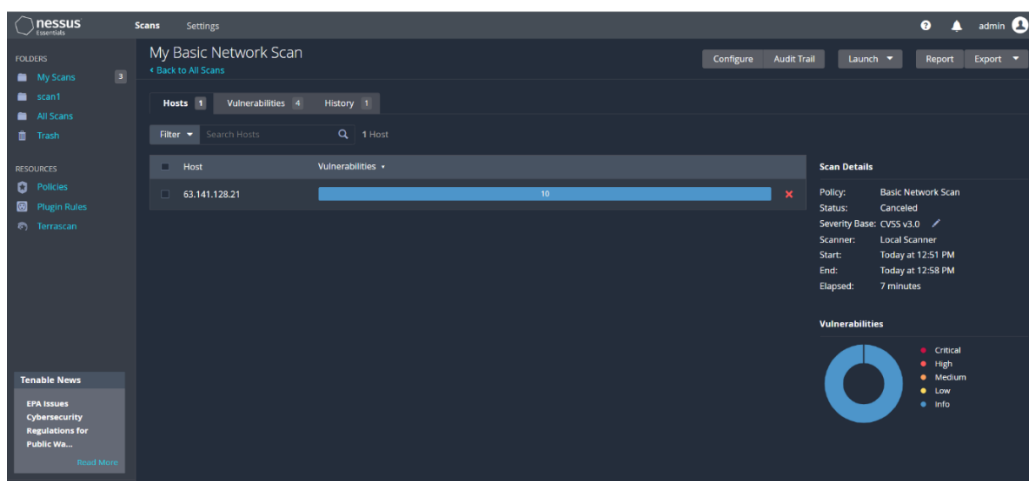
You can select a single server too.



Now it will run a basic scan on the selected host.

I stopped the scan after a while and 4 very very low level vulnerability were found.

They are not vulnerability but they can be.



The 4 vulnerabilities were as follow:

My Basic Network Scan

Configure Audit Trail Launch Report Export

Hosts: 1 Vulnerabilities: 4 History: 1

Filter Search Vulnerabilities 4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
Info			Nessus SYN scanner	Port scanners	4
Info			Service Detection	Service detection	4
Info			TCP/IP Timestamps Supported	General	1
Info			Traceroute Information	General	1

Scan Details

Policy: Basic Network Scan
 Status: Canceled
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 12:51 PM
 End: Today at 12:58 PM
 Elapsed: 7 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (0), High (0), Medium (0), Low (0), Info (4).

The first vulnerability was Nessus SYN scanner.

Nessus SYN scanner

INFO

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

Port 80/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
80 / tcp / www	63.141.128.21

Plugin Details

Severity: Info
 ID: 11219
 Version: 1.51
 Type: remote
 Family: Port scanners
 Published: February 4, 2009
 Modified: March 8, 2023

Risk Information

Risk Factor: None

Nessus SYN scanner

INFO

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

Port 443/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	63.141.128.21

Port 2083/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
2083 / tcp / www	63.141.128.21

Port 8080/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
8080 / tcp / www	63.141.128.21

The second vulnerability was Service Detection.

The screenshot shows the Nessus Essentials interface for a scan titled "My Basic Network Scan / Plugin #22964". The left sidebar contains folders like "My Scans", "scan1", "All Scans", and "Trash", along with resources like "Policies", "Plugin Rules", and "TerraScan". The main panel displays the "Service Detection" results for Plugin #22964. The "Description" states: "Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request." The "Output" section shows a table of detected services:

Port	Hosts
443 / tcp / www	63.141.128.21
80 / tcp / www	63.141.128.21
8080 / tcp / www	63.141.128.21
2083 / tcp / www	63.141.128.21

The "Plugin Details" sidebar on the right shows the following information:

- Severity: Info
- ID: 22964
- Version: 1.191
- Type: remote
- Family: Service detection
- Published: August 19, 2007
- Modified: March 21, 2023
- Risk Information: Risk Factor: None

The third vulnerability was TCP/IP Timestamps supported.

The fourth vulnerability was Traceroute information.

The screenshot shows the Nessus Essentials interface for a scan titled "My Basic Network Scan / Plugin #10287". The left sidebar is the same as the previous screenshot. The main panel displays the "Traceroute Information" results for Plugin #10287. The "Description" states: "Makes a traceroute to the remote host." The "Output" section shows the traceroute results:

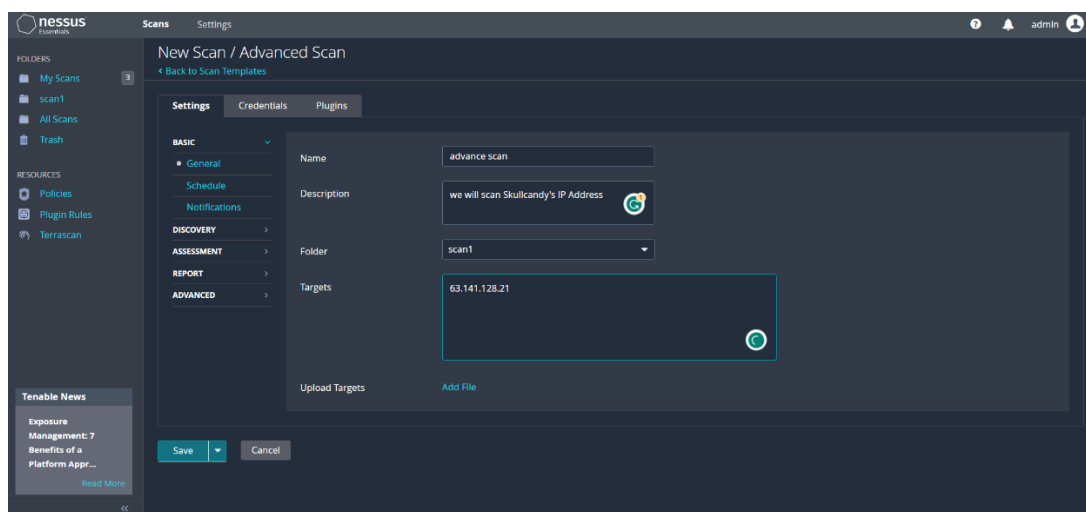
```
For your information, here is the traceroute from 192.168.0.6 to 63.141.128.21 :
192.168.0.6
192.168.0.1
103.250.39.43
103.250.39.33
?
103.27.170.48
172.71.200.2
63.141.128.21
Hop Count: 7
```

The "Plugin Details" sidebar on the right shows the following information:

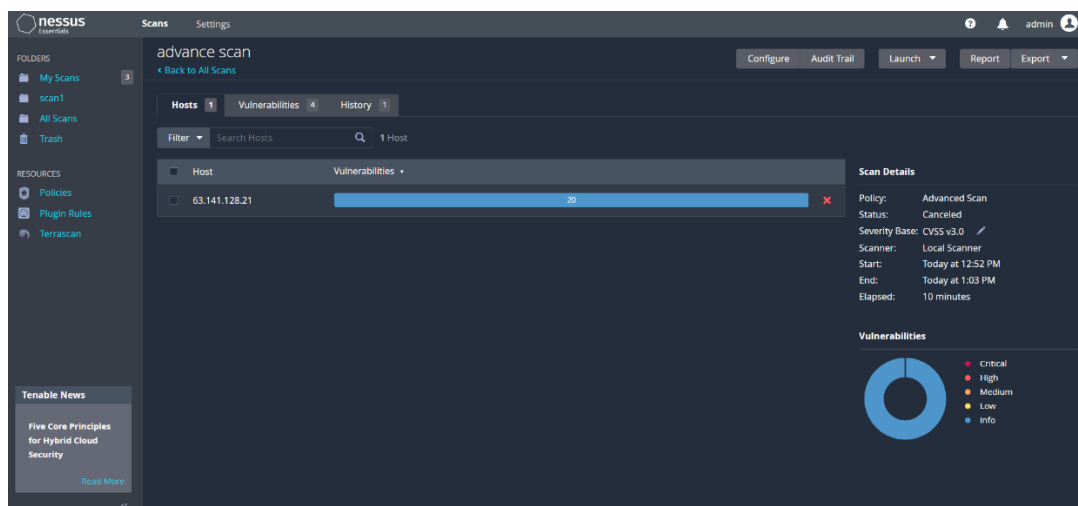
- Severity: Info
- ID: 10287
- Version: 1.67
- Type: remote
- Family: General
- Published: November 27, 1999
- Modified: August 20, 2020
- Risk Information: Risk Factor: None

It gives us the route it followed to reach the target IP Address. And it also gives the number of hop count. i.e., the no. of network in between.

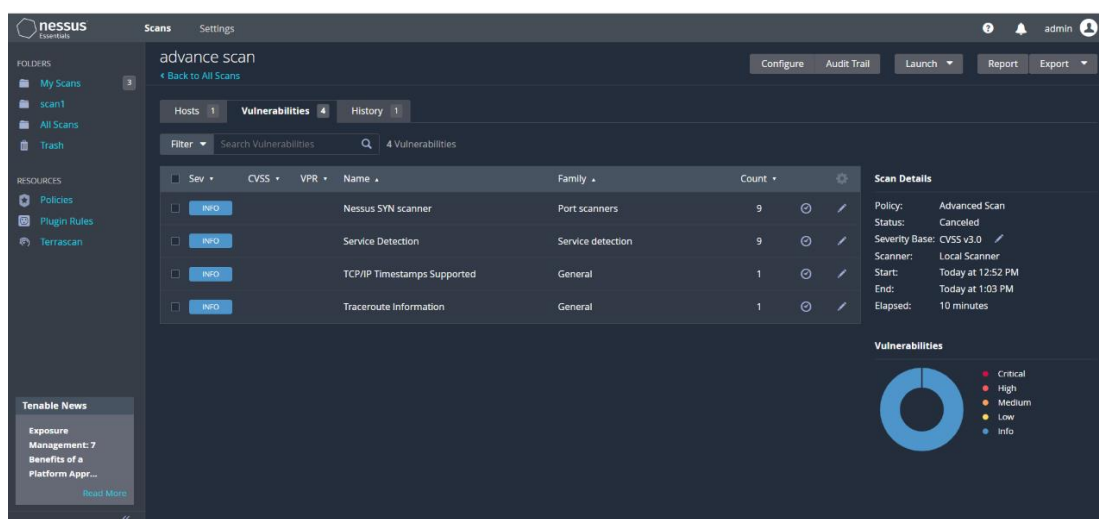
Now I'll create a advance scan on the same port.



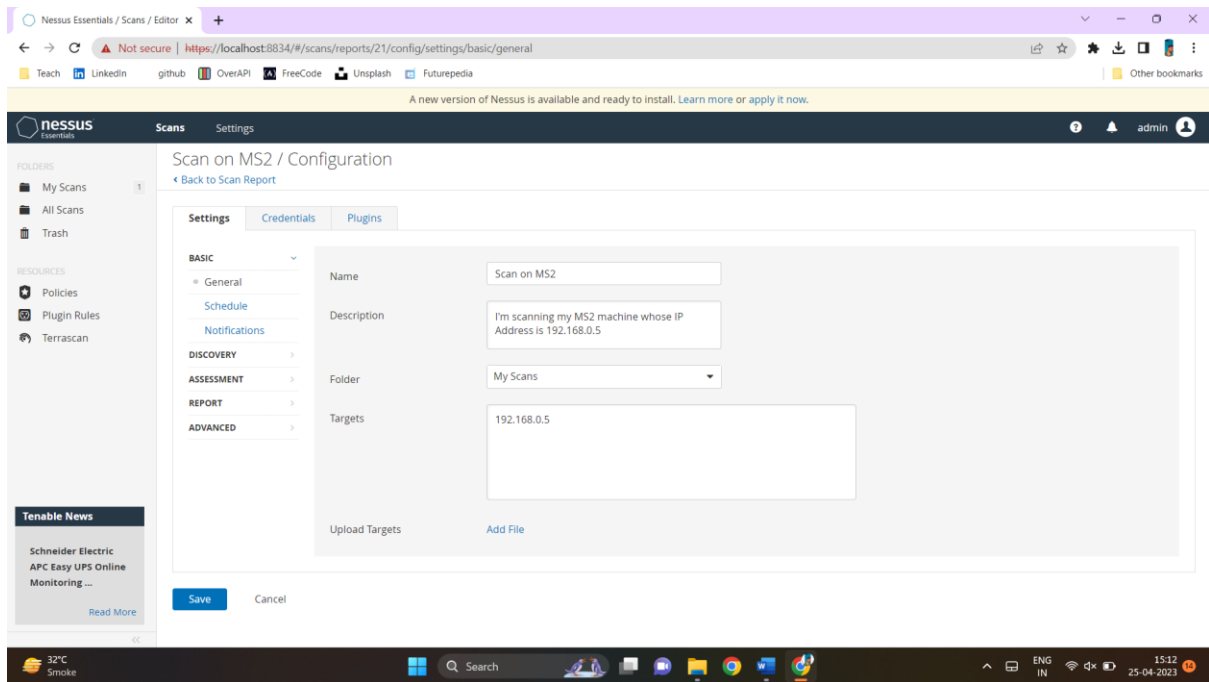
The results were same for both basic and advance scan.



The 4 same vulnerabilities were found.



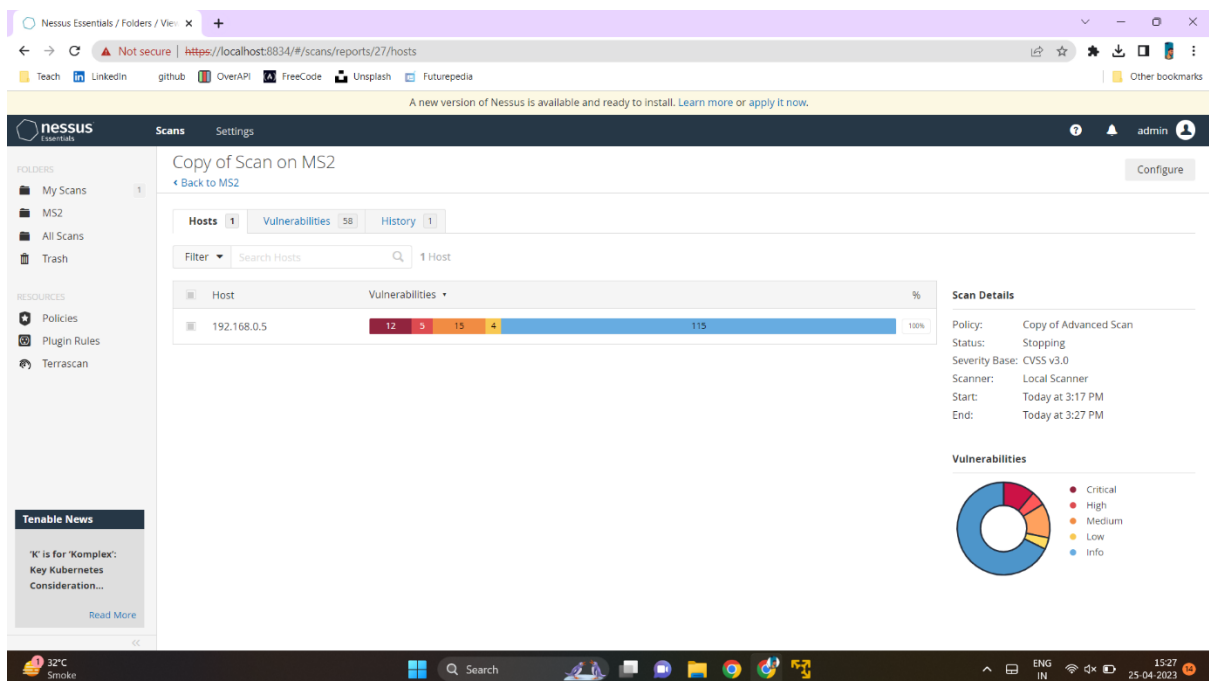
Now we will do an Advance Scan on MS2 machine:



After creating a scan, I launched.

As metasploitable is purposely made vulnerability we got a lot of vulnerabilities and I had to stop the scan because it will take a lot of time.

12 Critical, 5 High, 15 Medium, 4 Low, 115 Info, Vulnerabilities were found.



Nessus Essentials Folders / View: x

Not secure | https://localhost:8834/#/scans/reports/27/hosts/2/vulnerabilities

Teach | LinkedIn | github | OverAPI | FreeCode | Unsplash | Futurepedia

A new version of Nessus is available and ready to install. [Learn more](#) or [apply it now](#).

nessus Essentials

Scans Settings

FOLDERS

- My Scans
- M52
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

ETHOS: Bringing the OT Security Community Together...

Read More

Filter Search Vulnerabilities 58 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclos...	RPC	1	
CRITICAL	10.0 *	6.7	rexecd Service Detection	Service detection	1	
CRITICAL	10.0		Unix Operating System Unsupported Ver...	General	1	
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
MIXED	DNS (Multiple Issues)	Apache Tomcat (Multiple Issues)	6	
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5		NFS Shares World Readable	RPC	1	
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	

Host Details

IP: 192.168.0.5
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 3:17 PM
End: Today at 3:27 PM
Elapsed: 9 minutes
KB: [Download](#)

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (light blue), Info (dark blue).

With the vulnerability name, the solution is also given for that vulnerability.

Copy of Scan on MS2 / Plugin #11356

[Configure](#)
[Audit Trail](#)
[Launch](#)
[Report](#)
[Export](#)

Vulnerabilities

58

CRITICAL

NFS Exported Share Information Disclosure

[<](#)
[>](#)

Plugin Details

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```

The following NFS shares could be mounted :

+ /
+ Contents of / :
+ ..
+ bin
+ boot
+ ...

```

To see debug logs, please visit individual host

Port

Hosts

Severity: Critical

ID: 11356

Version: 1.20

Type: remote

Family: RPC

Published: March 12, 2003

Modified: September 17, 2018

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: 5.9

Threat Sources: No recorded events

Risk Information

Copy of Scan on MS2 / Plugin #46882

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities

58

CRITICAL

UnrealIRCd Backdoor Detection

< >

Plugin Details

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

The remote IRC server is running as :

uid=0(root) gid=0(root)

To see debug logs, please visit individual host

Port - Hosts

Severity: Critical

ID: 46882

Version: 1.16

Type: remote

Family: Backdoors

Published: June 14, 2010

Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Functional

Age of Vuln: 730 days +

Product Coverage: Low

CVSSV3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Copy of Scan on MS2 / Plugin #10407

Configure Audit Trail Launch Report Export

Vulnerabilities 58

LOW X Server Detection

Description
The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution
Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Output
X11 Version : 11.0

To see debug logs, please visit individual host

Port	Hosts
6000 / tcp / x11	192.168.0.5

Plugin Details

Severity: Low
ID: 10407
Version: 1.38
Type: remote
Family: Service detection
Published: May 12, 2000
Modified: March 5, 2019

Risk Information

Risk Factor: Low
CVSS v2.0 Base Score: 2.6
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

It will also group vulnerabilities together.

Copy of Scan on MS2 / 192.168.0.5 / Apache Tomcat (Multiple Issues)

Configure Audit Trail Launch Report Export

Vulnerabilities 58

Search Vulnerabilities 4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Apache Tomcat Web Server SEoL (<= 5.5.x)	Web Servers	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injec...	Web Servers	1
MEDIUM	5.3		Apache Tomcat Default Files	Web Servers	1
INFO			Apache Tomcat Detection	Web Servers	1

Scan Details

Policy: Copy of Advanced Scan
Status: Canceled
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:17 PM
End: Today at 3:27 PM
Elapsed: 9 minutes

Vulnerabilities

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

Here, all these vulnerabilities are of Apache Tomcat server, so they are group together.