



**VIT**<sup>®</sup>  
**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

***SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING***

***DIGITAL ASSIGNMENT 3 - WINTER SEMESTER 2023-24***

***Course : Information Security Management***

***Lab Marks : 10***

***Course Code : BCSE354E***

***Slot : L33+L34***

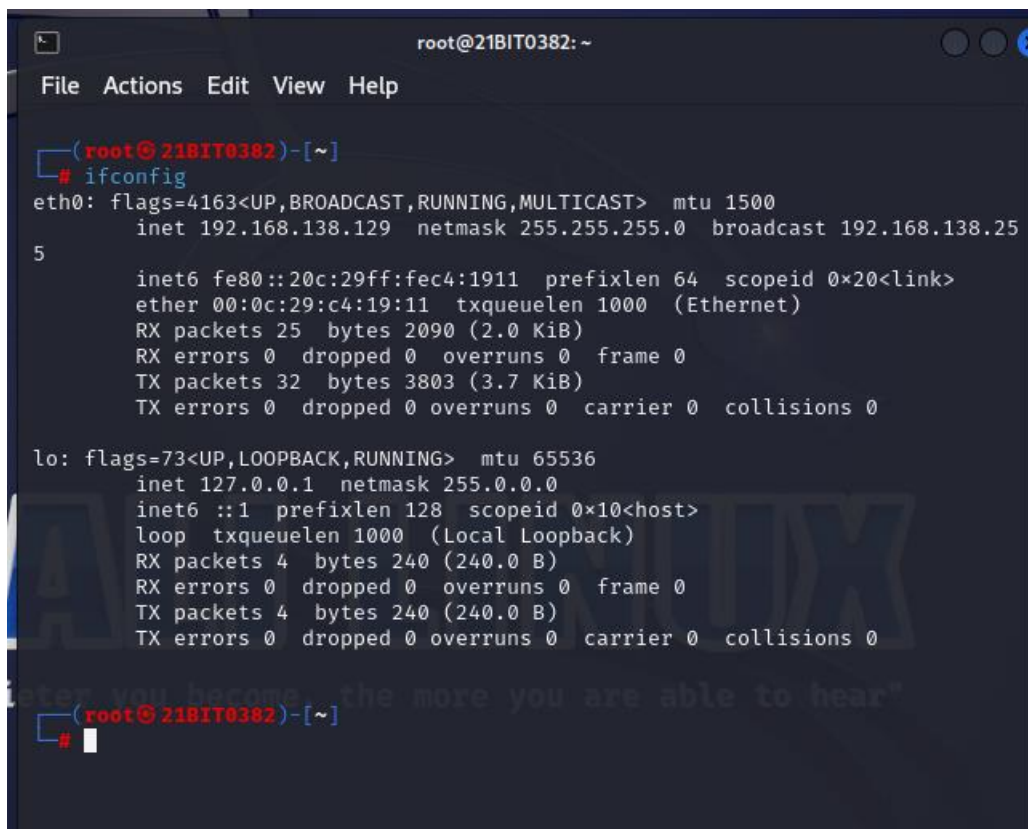
***Give screenshot of System IP, Kali Linux IP and Metasploitable IP***

***EACH QUESTION CARRIES 5 MARKS***

***NAME: POLI VARDHINI REDDY***

***REGISTER NUMBER: 21BIT0382***

1. Using OWASP-ZAP perform penetration testing on the website <http://googlegruyere.appspot.com/start> . You can start an instance of Gruyere with a unique ID. Click Agree & Start.
  - Identify hidden, potentially forgotten, or unsecured pages
  - Identify the attack which gives high-risk alert



```
root@21BIT0382: ~  
File Actions Edit View Help  
  
(root@21BIT0382)-[~]  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.138.129 netmask 255.255.255.0 broadcast 192.168.138.255  
    ether 00:0c:29:c4:19:11 txqueuelen 1000 (Ethernet)  
    RX packets 25 bytes 2090 (2.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 32 bytes 3803 (3.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(root@21BIT0382)-[~]  
#
```



## Command Prompt



Microsoft Windows [Version 10.0.22631.3155]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\Lenovo>ipconfig

### Windows IP Configuration

#### Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :

#### Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::b7d0:3ced:7c85:3bc%5  
IPv4 Address. . . . . : 192.168.56.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :

#### Wireless LAN adapter Local Area Connection\* 1:

Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :

#### Wireless LAN adapter Local Area Connection\* 2:

Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :

#### Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::7f5b:a4d6:5ca5:30ef%16  
IPv4 Address. . . . . : 192.168.220.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :

#### Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::dbf5:7dce:10ec:1bff%13  
IPv4 Address. . . . . : 192.168.138.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :

#### Wireless LAN adapter WiFi:

Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::73ef:2ae5:4ebd:e461%9  
IPv4 Address. . . . . : 172.17.70.157  
Subnet Mask . . . . . : 255.255.248.0  
Default Gateway . . . . . : 172.17.64.1

#### Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :

C:\Users\Lenovo>|

```
polivardhinireddy@21BIT0382: ~/Downloads
File Actions Edit View Help

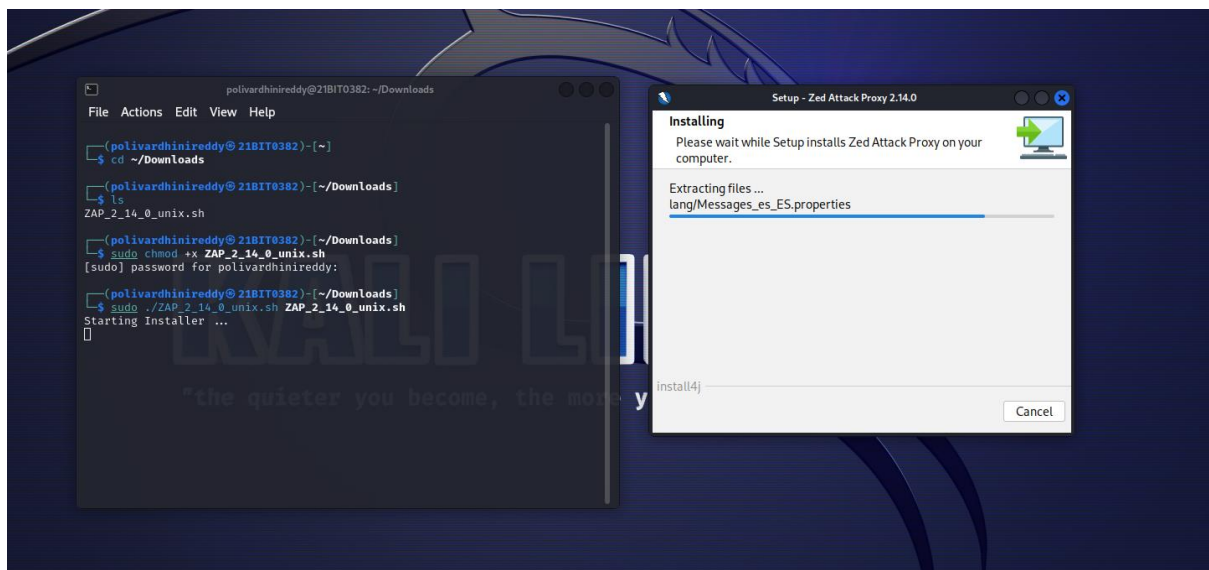
(polivardhinireddy@21BIT0382)-[~]
$ cd ~/Downloads

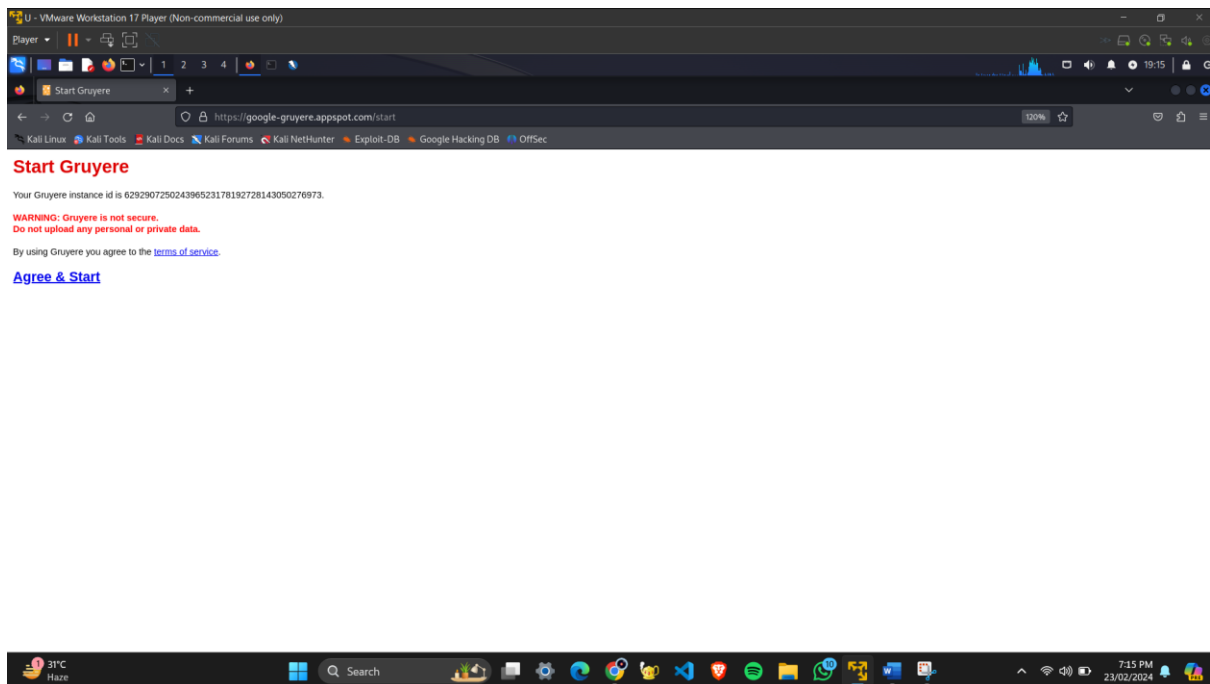
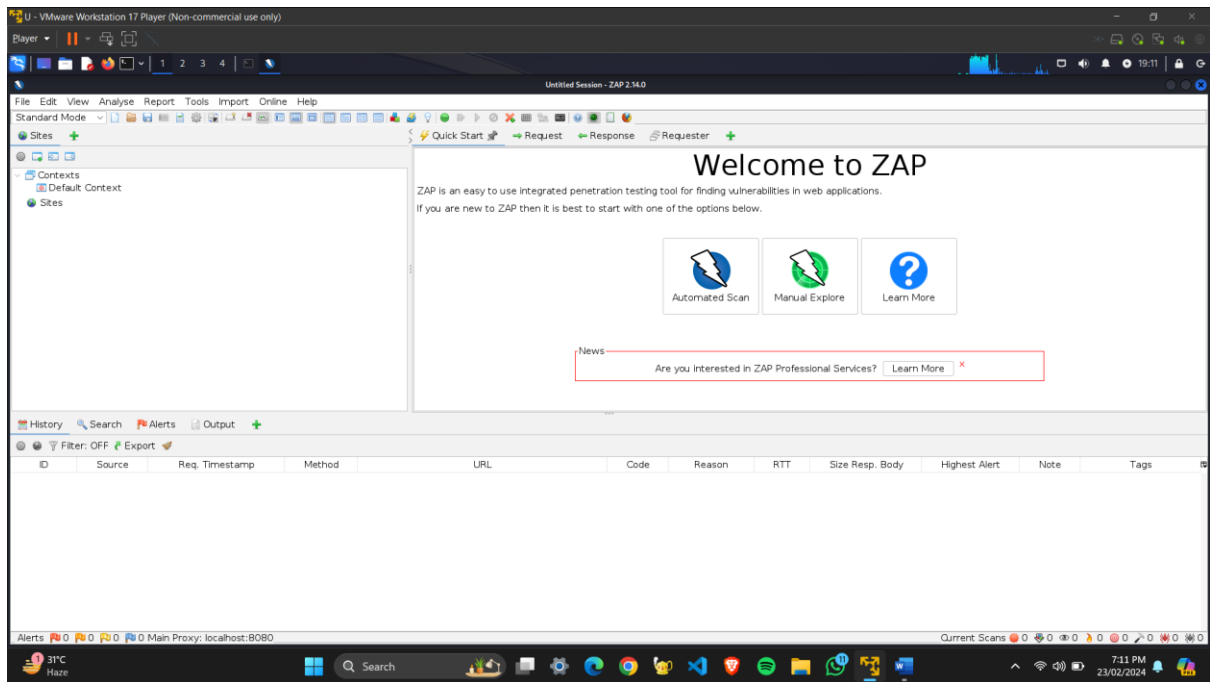
(polivardhinireddy@21BIT0382)-[~/Downloads]
$ ls
ZAP_2_14_0_unix.sh

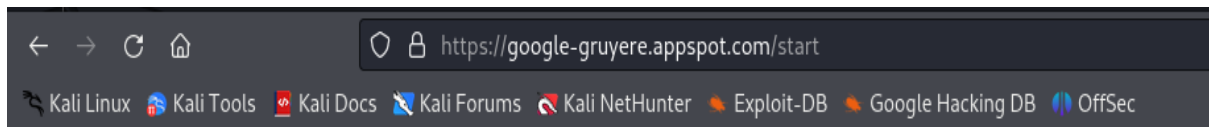
(polivardhinireddy@21BIT0382)-[~/Downloads]
$ sudo chmod +x ZAP_2_14_0_unix.sh
[sudo] password for polivardhinireddy:

(polivardhinireddy@21BIT0382)-[~/Downloads]
$ sudo ./ZAP_2_14_0_unix.sh ZAP_2_14_0_unix.sh
Starting Installer ...

(polivardhinireddy@21BIT0382)-[~/Downloads]
$
```







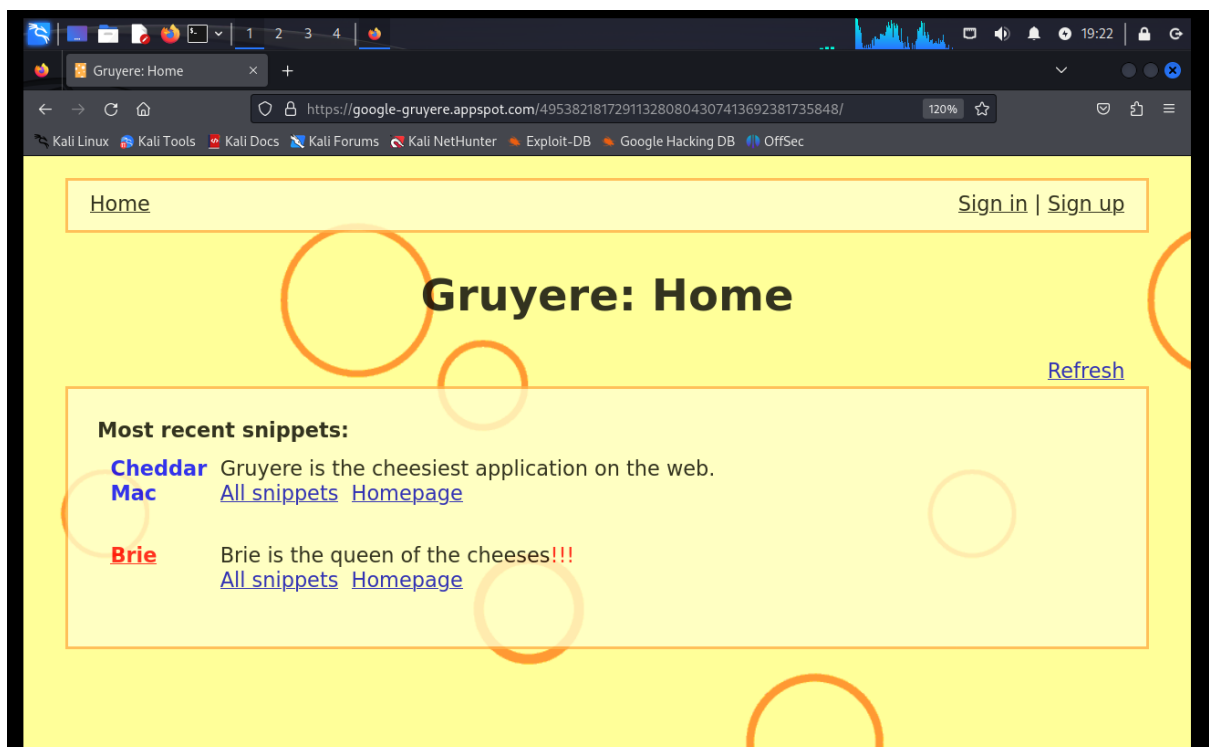
## Start Gruyere

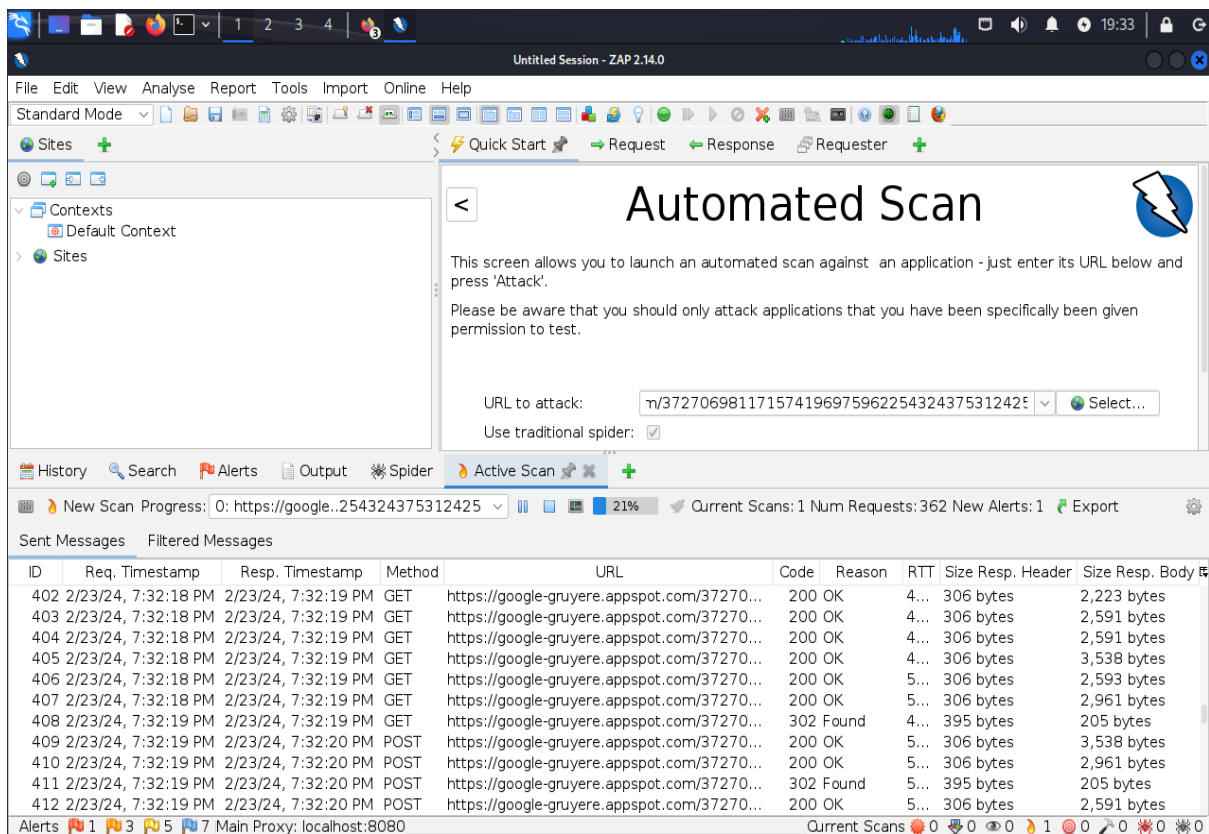
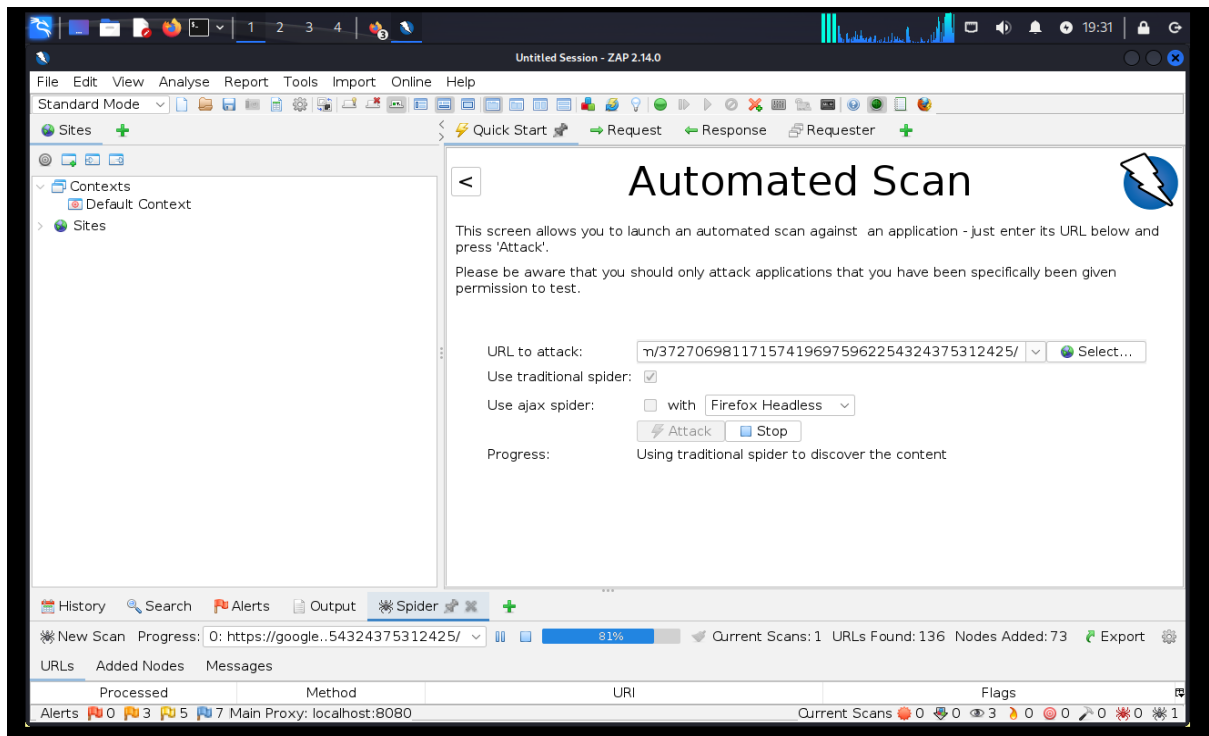
Your Gruyere instance id is 629290725024396523178192728143050276973.

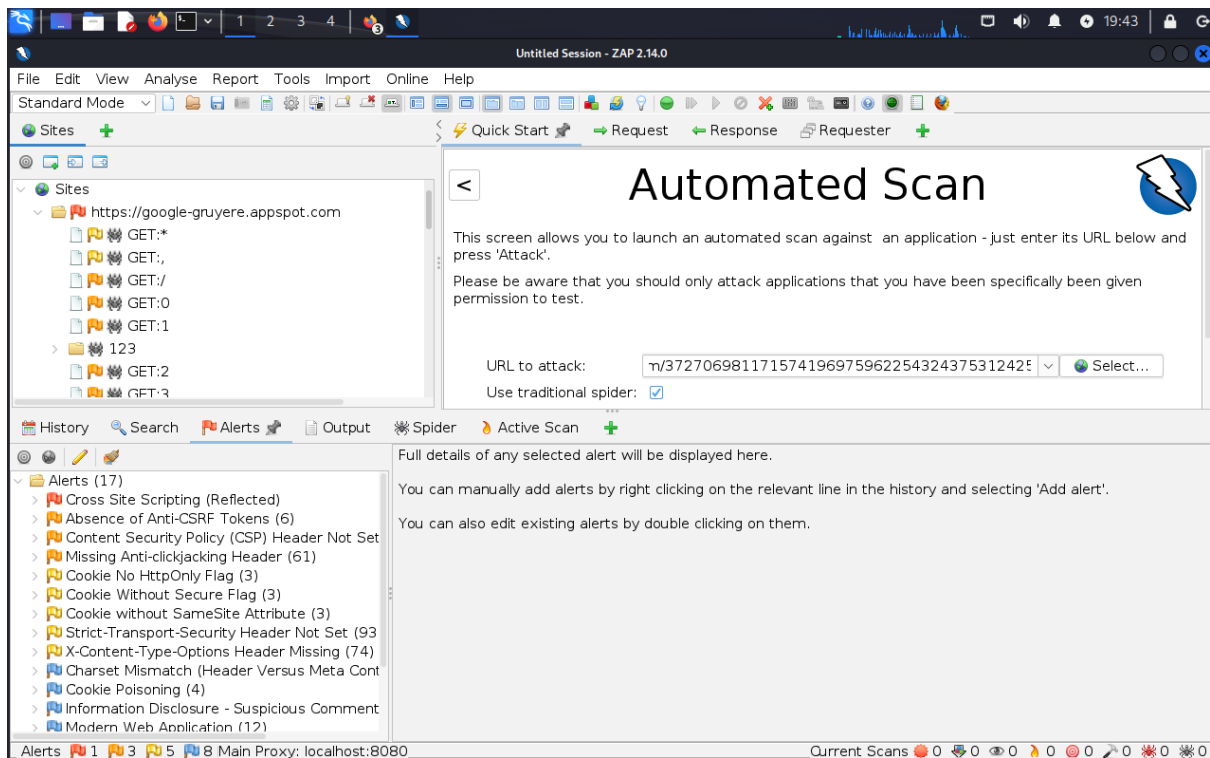
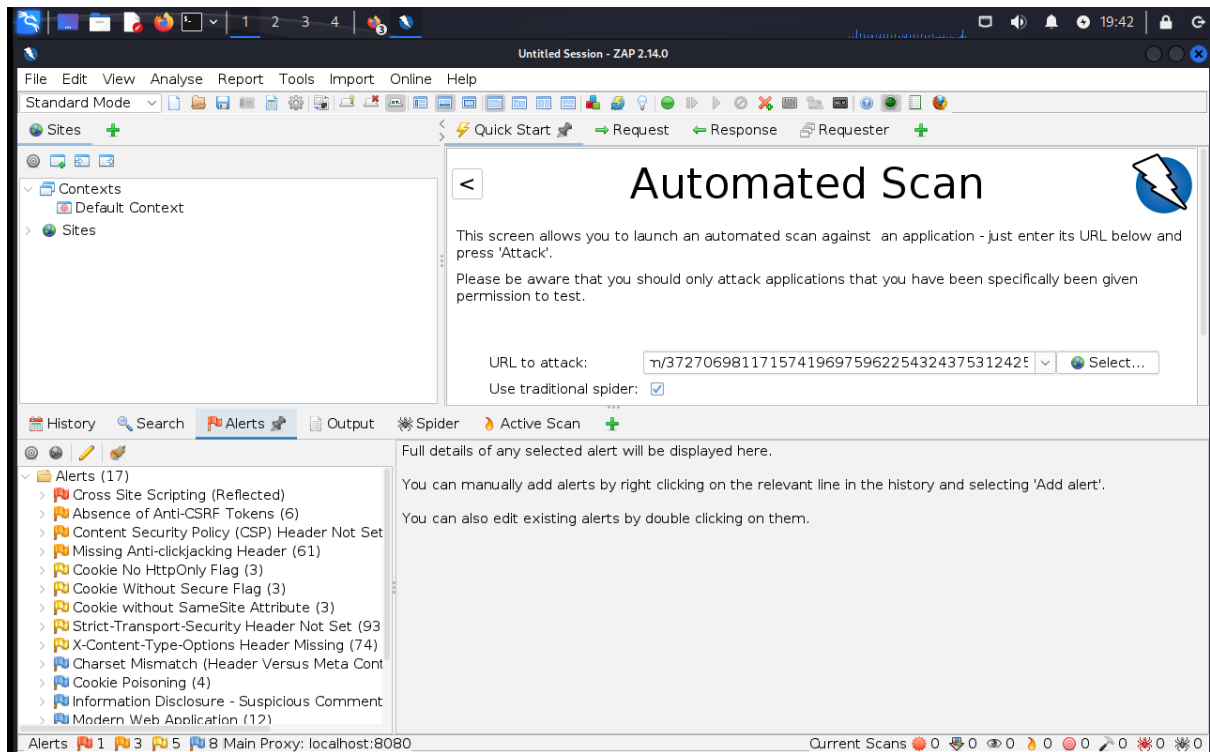
**WARNING: Gruyere is not secure.**  
**Do not upload any personal or private data.**

By using Gruyere you agree to the [terms of service](#).

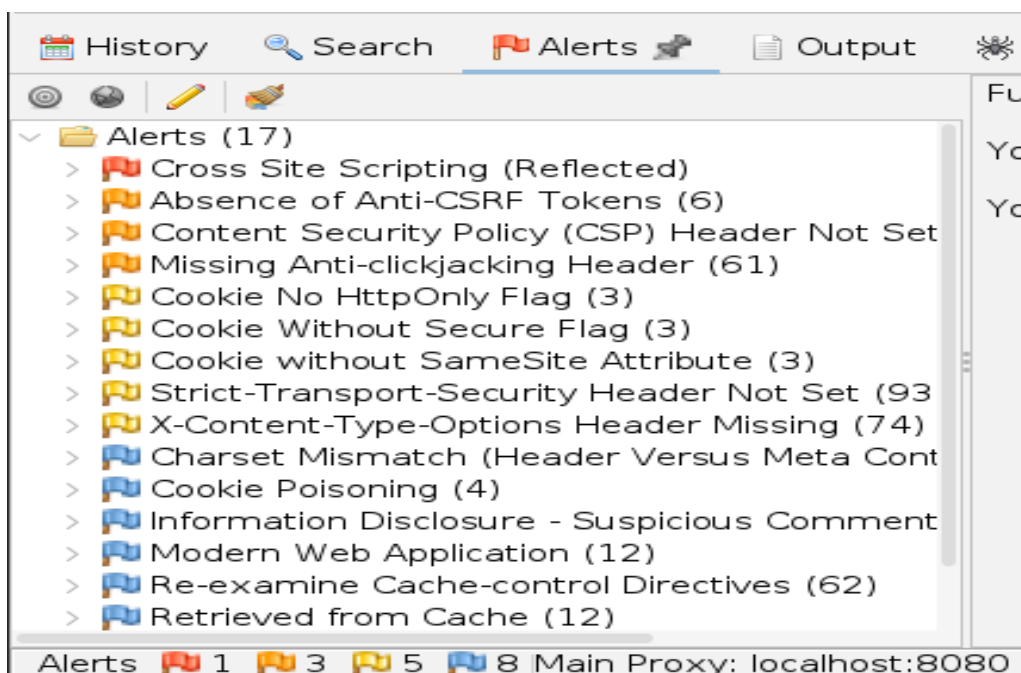
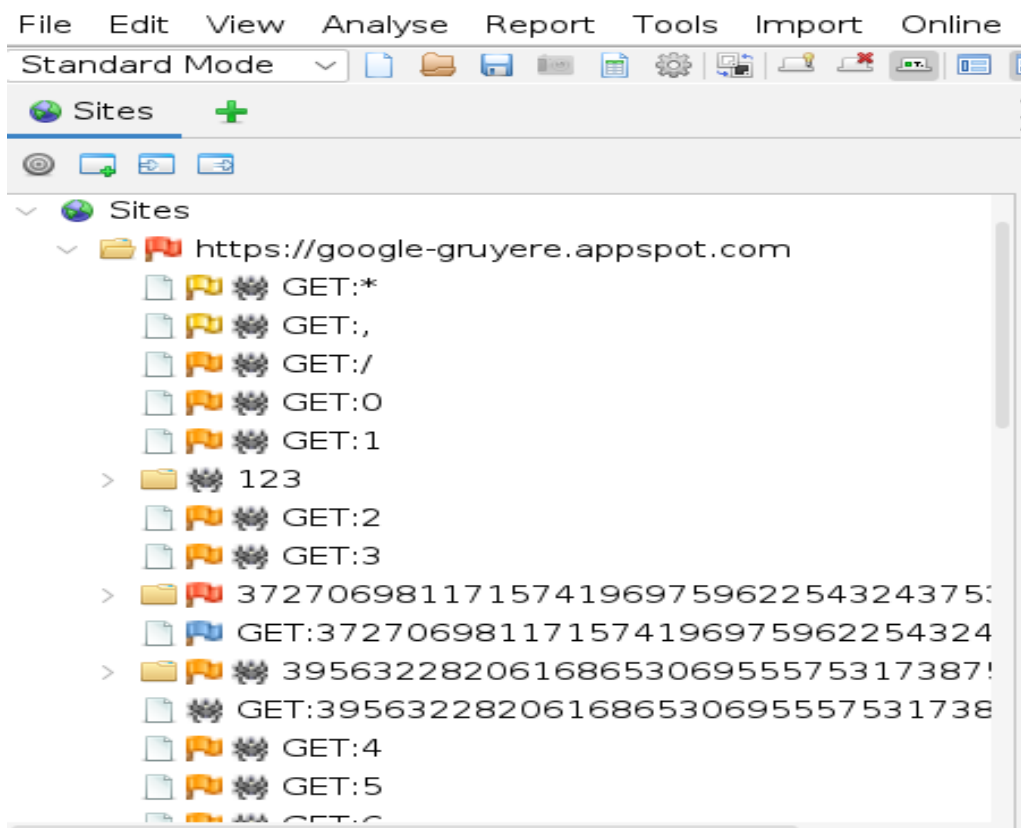
[Agree & Start](#)















History Search Alerts Output Spider Active Scan +

Alerts (17)

- Cross Site Scripting (Reflected)
- GET: https://google-gruyere.appspot.com/3727069
- Absence of Anti-CSRF Tokens (6)
- Content Security Policy (CSP) Header Not Set (62)
- Missing Anti-clickjacking Header (61)
- Cookie No HttpOnly Flag (3)
- Cookie Without Secure Flag (3)
- Cookie without SameSite Attribute (3)
- Strict-Transport-Security Header Not Set (93)
- X-Content-Type-Options Header Missing (74)
- Charset Mismatch (Header Versus Meta Content-Type)
- Cookie Poisoning (4)
- Information Disclosure - Suspicious Comments (2)
- Modern Web Application (12)
- Re-examine Cache-control Directives (62)

### Cross Site Scripting (Reflected)

URL: https://google-gruyere.appspot.com/372706981171574196975962254324375312425/snippets.gtl?uid=%3C%2Fh2%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Ch2%3E

Risk: High

Confidence: Medium

Parameter: uid

Attack: </h2><script>alert(1);</script><h2>

Evidence: </h2><script>alert(1);</script><h2>

CWE ID: 79

WASC ID: 8

Source: Active (40012 - Cross Site Scripting (Reflected))

Input Vector: URL Query String

Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an

Other Info:

Alerts 1 3 5 8 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

History Search Alerts Output Spider Active Scan +

Alerts (17)

- Cross Site Scripting (Reflected)
- GET: https://google-gruyere.appspot.com/3727069
- Absence of Anti-CSRF Tokens (6)
- Content Security Policy (CSP) Header Not Set (62)
- Missing Anti-clickjacking Header (61)
- Cookie No HttpOnly Flag (3)
- Cookie Without Secure Flag (3)
- Cookie without SameSite Attribute (3)
- Strict-Transport-Security Header Not Set (93)
- X-Content-Type-Options Header Missing (74)
- Charset Mismatch (Header Versus Meta Content-Type)
- Cookie Poisoning (4)
- Information Disclosure - Suspicious Comments (2)
- Modern Web Application (12)
- Re-examine Cache-control Directives (62)

### Cross Site Scripting (Reflected)

URL: https://google-gruyere.appspot.com/372706981171574196975962254324375312425/snippets.gtl?uid=%3C%2Fh2%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Ch2%3E

Risk: High

Confidence: Medium

Parameter: uid

Attack: </h2><script>alert(1);</script><h2>

Evidence: </h2><script>alert(1);</script><h2>

CWE ID: 79

WASC ID: 8

Source: Active (40012 - Cross Site Scripting (Reflected))

Input Vector: URL Query String

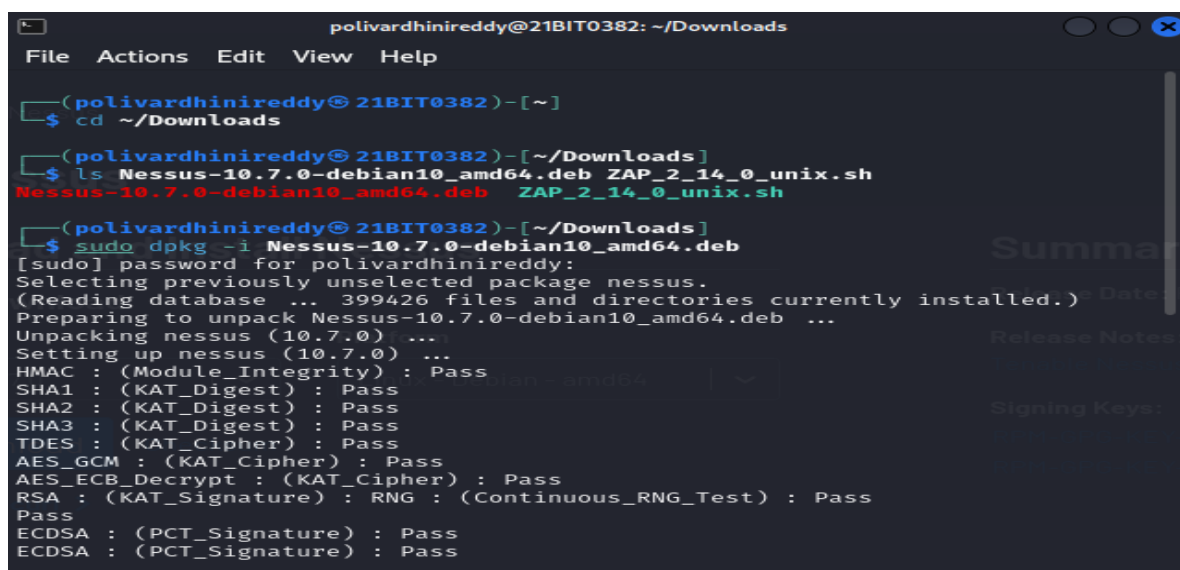
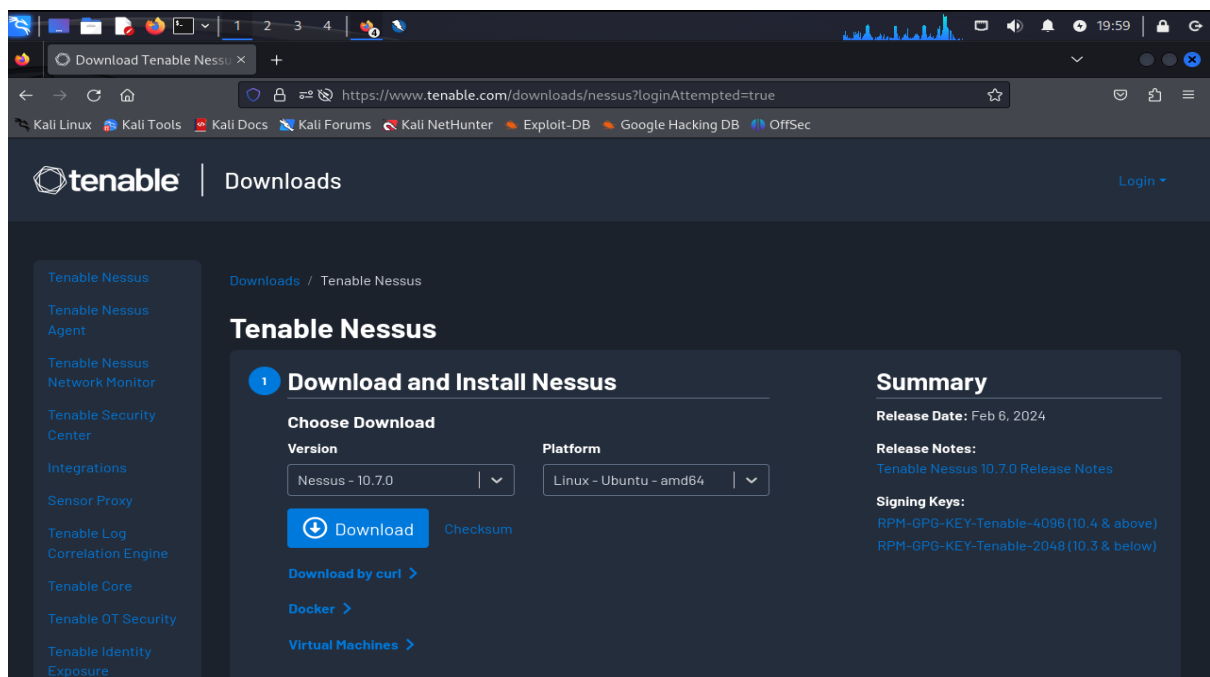
Description: Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported

Other Info:

Alerts 1 3 5 8 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

2. Perform a Nessus scan on your metasploitable IP. (5 Marks) List the vulnerabilities/ alerts identified in the scan. Export all the vulnerability report and put the file in a google drive link Give the following snapshots

- Sign in snapshot of your user details
- Date and time of scan started and completed
- For any one vulnerability, show the CVSS score



```
polivardhiniireddy@21BIT0382: ~/Downloads
File Actions Edit View Help
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://21BIT0382:8834/ to configure your scanner

(polivardhiniireddy@ 21BIT0382)-[~/Downloads]
$
```

```
polivardhiniireddy@21BIT0382: ~/Downloads
File Actions Edit View Help
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://21BIT0382:8834/ to configure your scanner

(polivardhiniireddy@ 21BIT0382)-[~/Downloads]
$ sudo systemctl status nessusd
o nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: enabled)
   Active: inactive (dead)
 ... skipping ...
o nessusd.service - The Nessus Vulnerability Scanner
```



```
polivardhinireddy@21BIT0382: ~/Downloads
File Actions Edit View Help

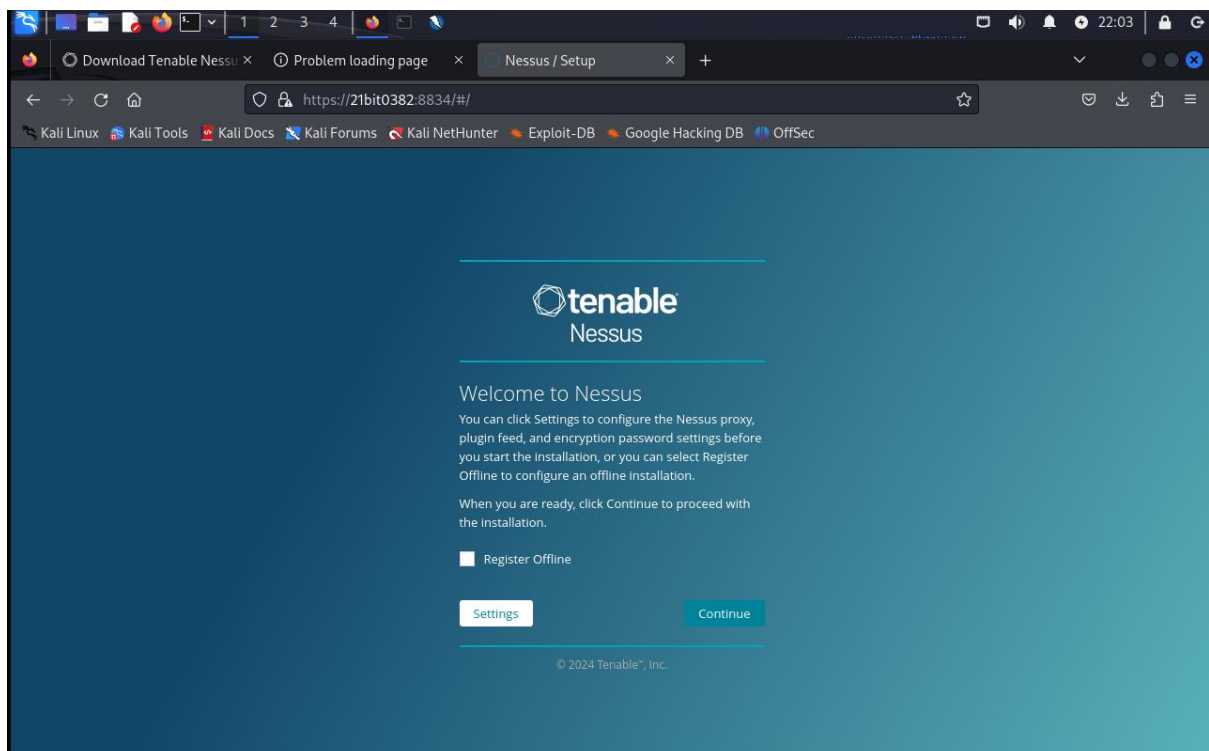
(polivardhinireddy@21BIT0382)-[~/Downloads]
$ sudo systemctl start nessusd

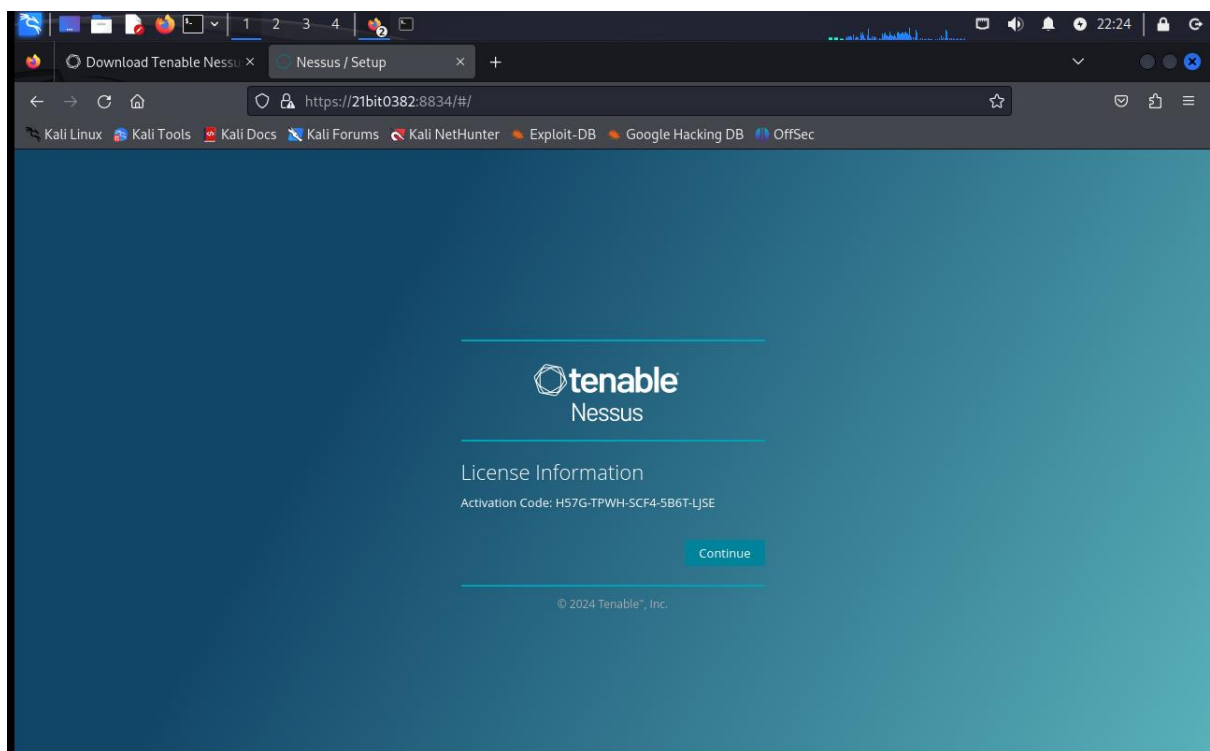
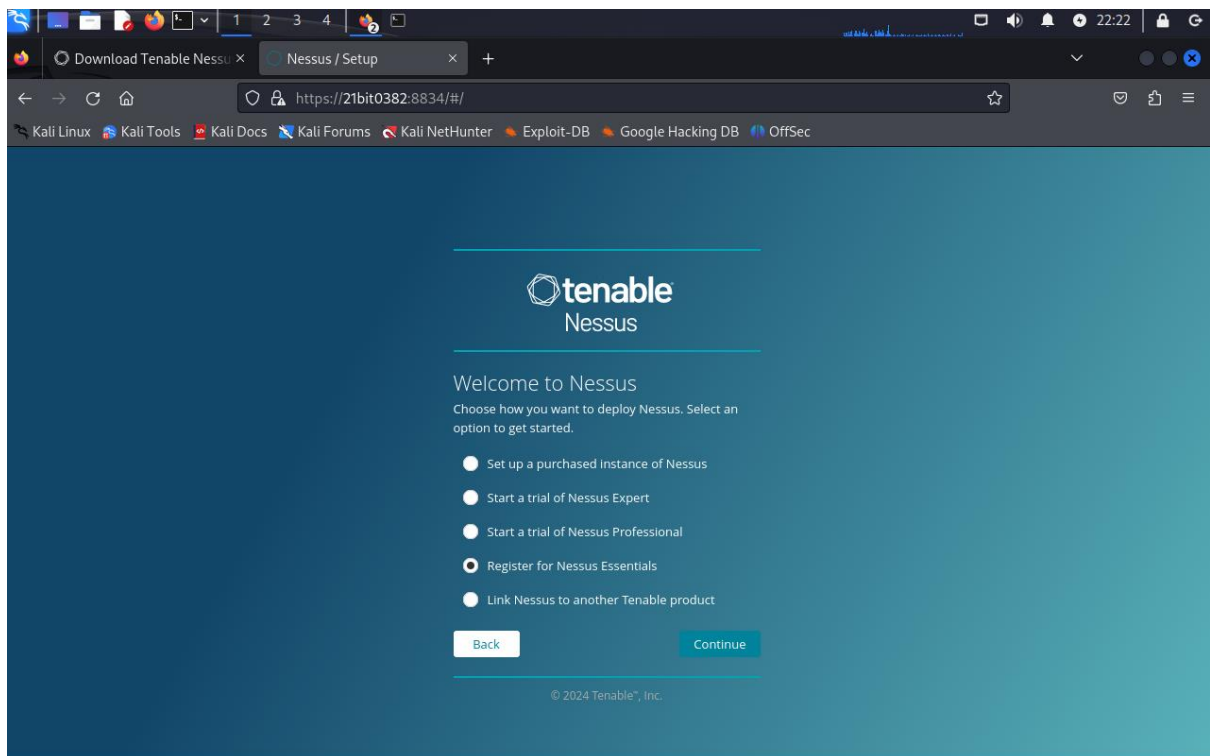
(polivardhinireddy@21BIT0382)-[~/Downloads]
$ sudo systemctl start nessusd

(polivardhinireddy@21BIT0382)-[~/Downloads]
$ sudo system status nessusd
sudo: system: command not found

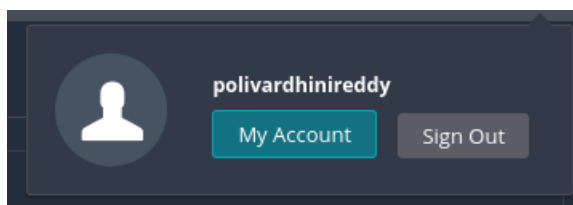
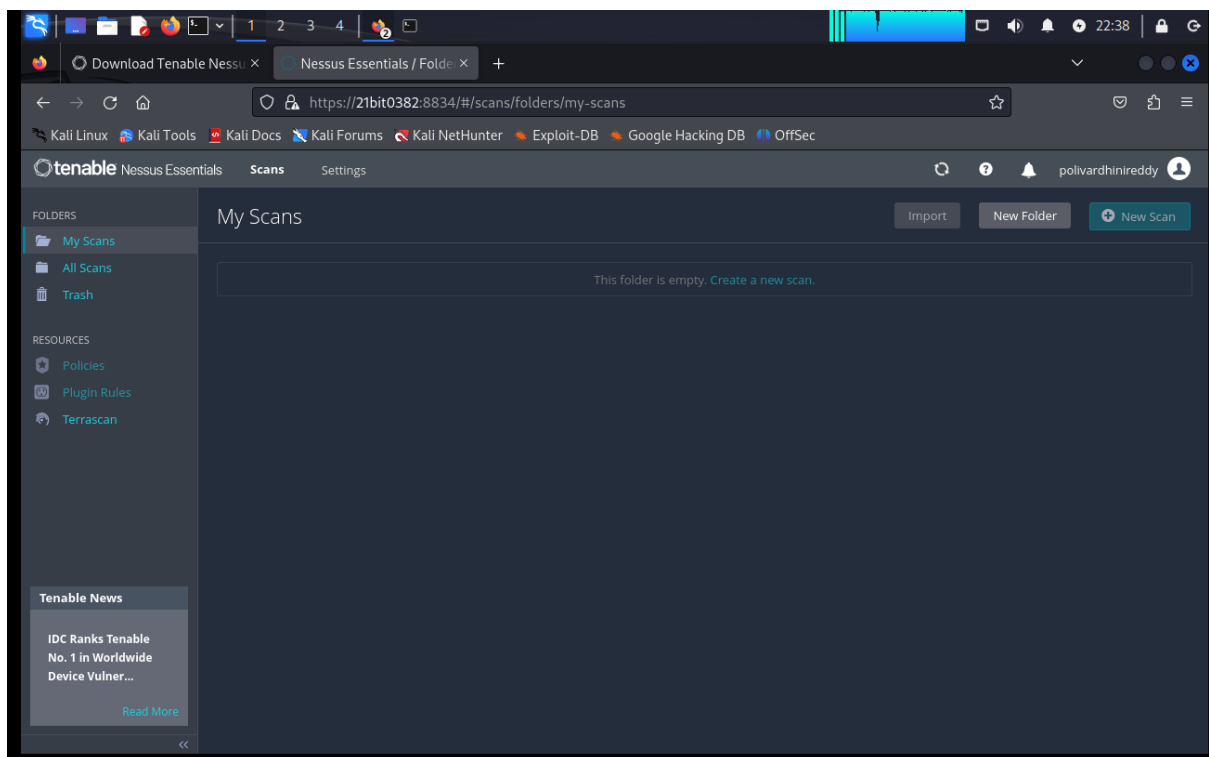
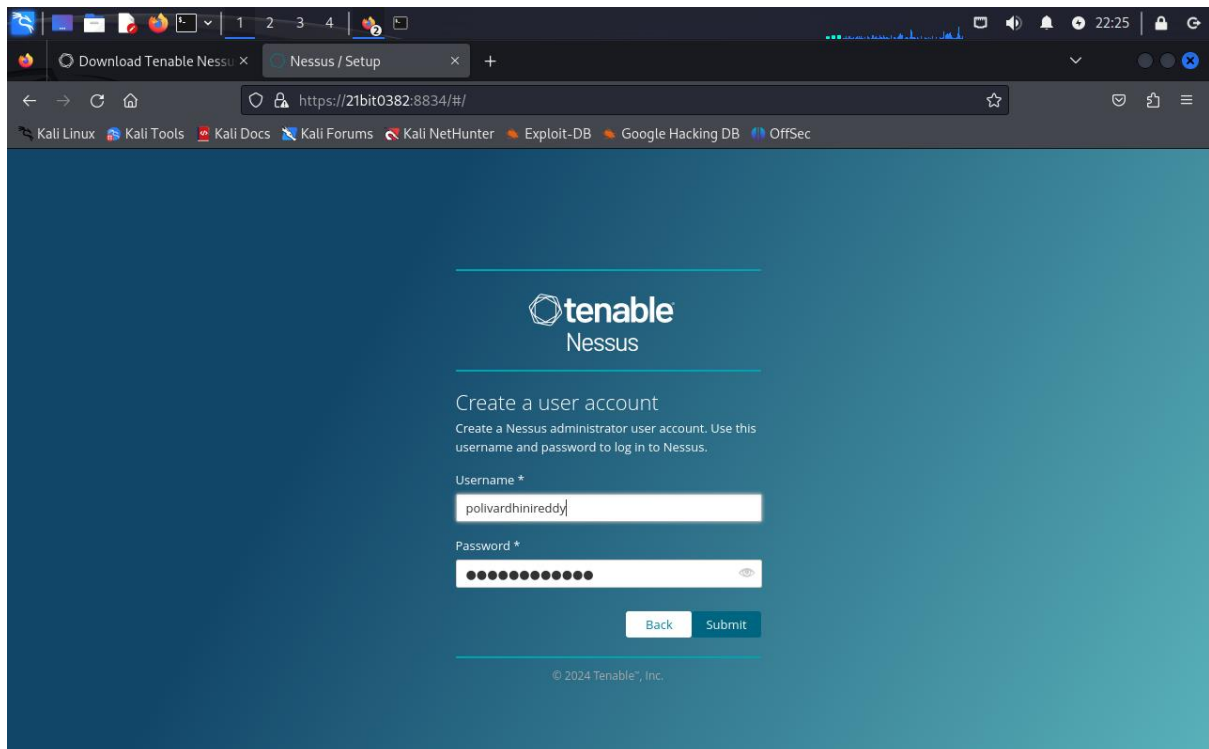
(polivardhinireddy@21BIT0382)-[~/Downloads]
$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset:
   Active: active (running) since Fri 2024-02-23 21:59:59 IST; 53s ago
     Main PID: 17954 (nessus-service)
        Tasks: 15 (limit: 4554)
      Memory: 125.3M
         CPU: 35.771s
       CGroup: /system.slice/nessusd.service
               └─17954 /opt/nessus/sbin/nessus-service -q
                 17956 nessusd -q

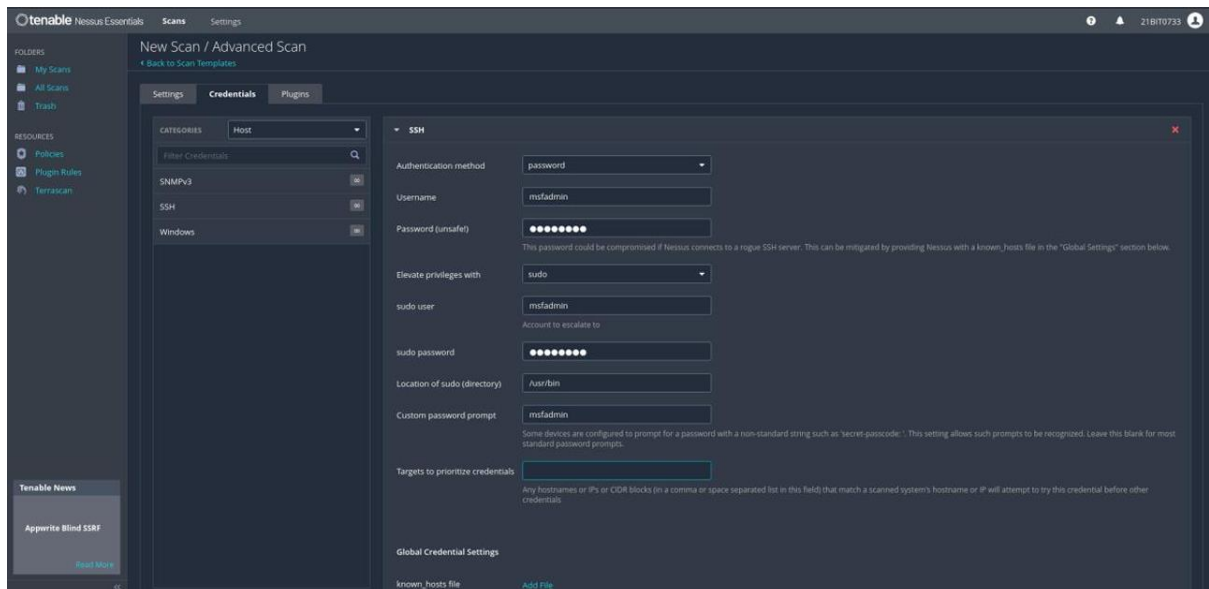
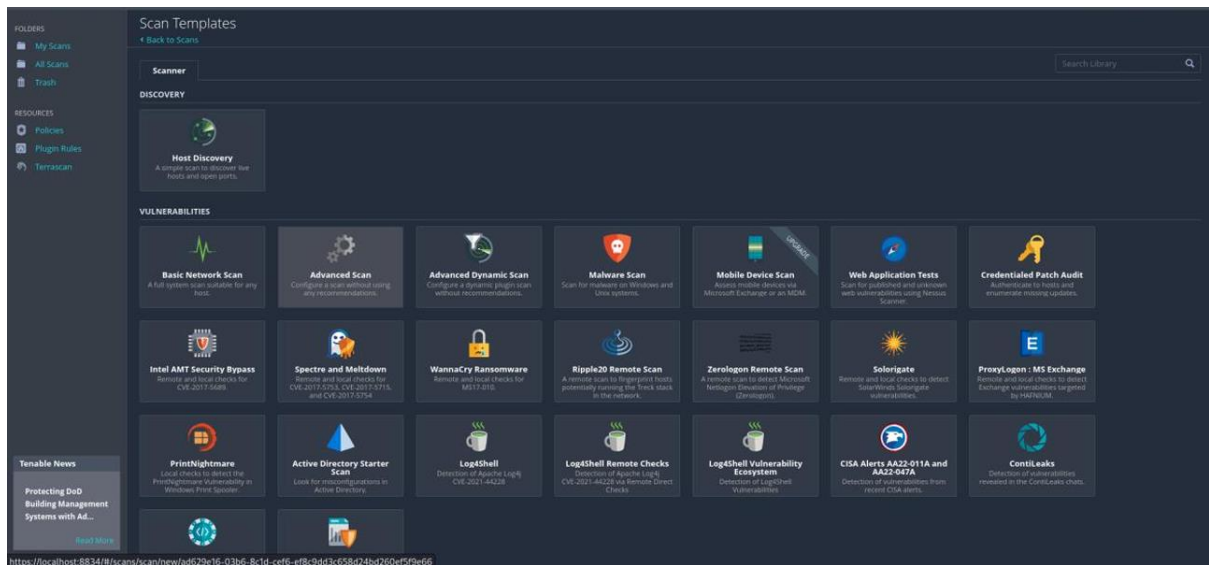
Feb 23 21:59:59 21BIT0382 systemd[1]: Started nessusd.service - The Nessus V
Feb 23 22:00:00 21BIT0382 nessus-service[17956]: Cached 0 plugin libs in 0ms>
Feb 23 22:00:00 21BIT0382 nessus-service[17956]: Cached 0 plugin libs in 0ms>
lines 1-14/14 (END)
```











Tenable

Hessus Essentials

Scans

Settings

21819733

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

Managed Kubernetes: Is It Right for My Organization...

Elevate privileges with

sudo

sudo user

msfadmin

sudo password

Account to escalate to

Location of sudo (directory)

/usr/bin

Custom password prompt

msfadmin

Targets to prioritize credentials

Any hostnames or IPs or CIDR blocks in a comma or space separated list in this field that match a scanned system's hostname or IP will attempt to try this credential before other credentials

Global Credential Settings

known\_hosts file

Add File

Preferred port

22

Client version

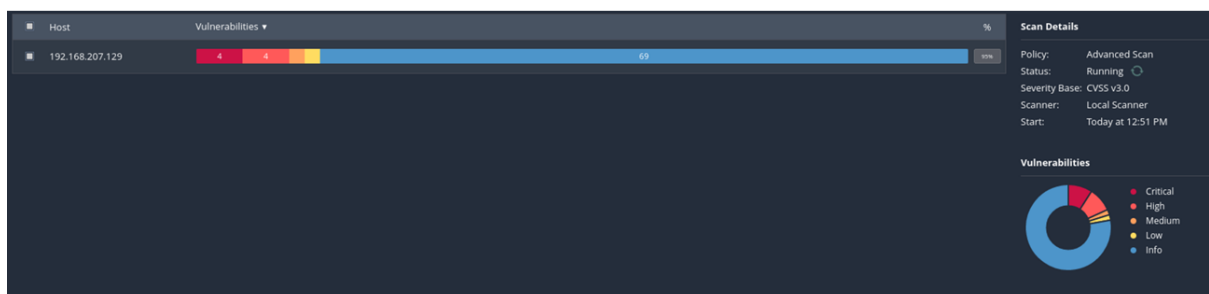
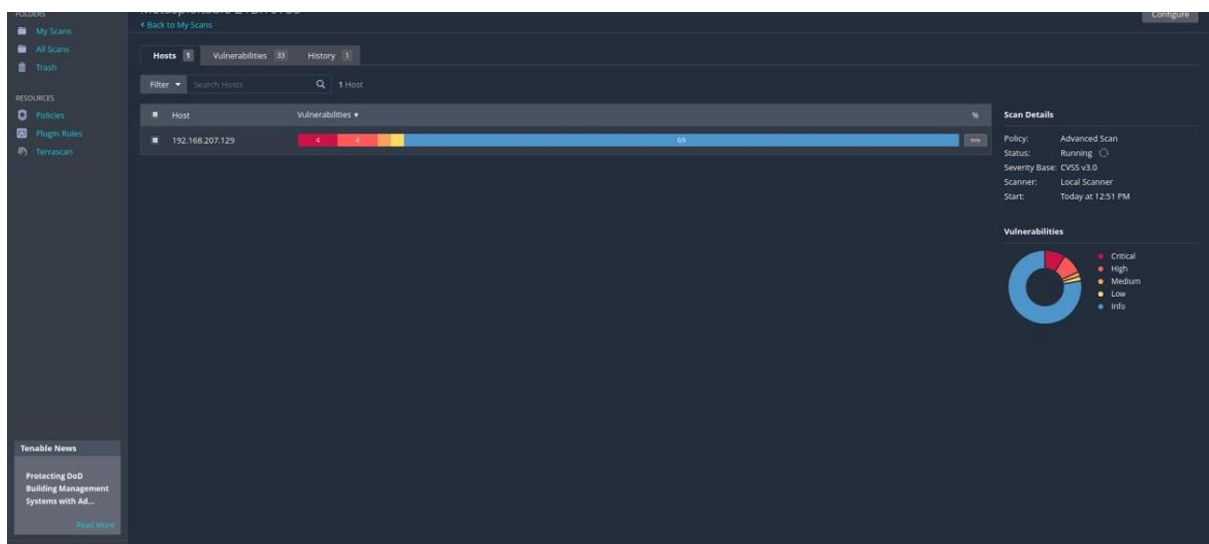
OpenSSH\_5.0

Attempt least privilege

Enable dynamic privilege escalation. If the working credentials for the target include privilege escalation, commands will first be attempted without privilege escalation. Commands will be run again with privilege escalation only if needed.

Save

Cancel



## Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 12:51 PM  
End: Today at 12:53 PM  
Elapsed: 3 minutes

## Vulnerabilities



My Scans

All Scans

Scans

RESULTS

Policies

Plugin Rules

Services

Retirable Issues

Missing Authentication for Critical Function in Ad...

Read More

1 Scan in Progress

Vulnerabilities 38

Filter Search vulnerabilities 38 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
Critical	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
Critical	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1	
Critical	10.0 *		VNC Server password Password	Gain a shell remotely	1	
Critical	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Gh0st0ut)	Web Servers	1	
High	7.5 *	5.9	High Service Detection	Service detection	1	
High	7.5 *	5.9	rdp Service Detection	Service detection	1	
High	7.5	5.9	Samba Badlock Vulnerability	General	1	
High	7.5		NFS Shares World Readable	RPC	1	
Medium	4.9 *	6.3	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1	
Info			SMB (Multiple Issues)	Misc.	2	
Info	2.8 *		S Server Detection	Service detection	1	
Info			SMB (Multiple Issues)	Windows	7	
Info			Apache HTTP Server (Multiple Issues)	Web Servers	2	
Info			FTP (Multiple Issues)	Service detection	3	

Host Details

IP: 192.168.207.129

OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Start: Today at 12:51 PM

End: Today at 12:53 PM

Elapsed: 3 minutes

KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

Back to Vulnerabilities

Vulnerabilities38

CriticalUnrealIRCd Backdoor Detection

Description

Solution

See Also

Output

The remote IRC server is running as:  
c:\windows\system32\cmd.exe /c whoami

To see debug logs, please visit individual host

PortHosts

6667/tcp192.168.207.129

Plugin Details

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

Vulnerability Priority Rating (VPR): 7.4  
Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Temporal Score: 8.3  
CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:C/I:C/A:C  
CVSS v2.0 Temporal Vector: CVSS2:RE:K/RL:OF/RC:C

Vulnerability Information

### Plugin Details



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

Vulnerability Priority Rating (VPR): 7.4  
Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Temporal Score: 8.3  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C  
/I:C/A:C  
CVSS v2.0 Temporal Vector:  
CVSS2#E:F/RL:OF/RC:C

```
Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player
- - - - -

-bash: msfadmin: command not found
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ac:ec:ff
          inet addr:192.168.138.128  Bcast:192.168.138.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feac:ecff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:202 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14963 (14.6 KB)  TX bytes:11580 (11.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:46333 (45.2 KB)  TX bytes:46333 (45.2 KB)

msfadmin@metasploitable:~$

-bash: msfadmin: command not found
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ac:ec:ff
          inet addr:192.168.138.128  Bcast:192.168.138.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feac:ecff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:202 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14963 (14.6 KB)  TX bytes:11580 (11.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:148 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:46333 (45.2 KB)  TX bytes:46333 (45.2 KB)

msfadmin@metasploitable:~$ _
```