10.15.42.36

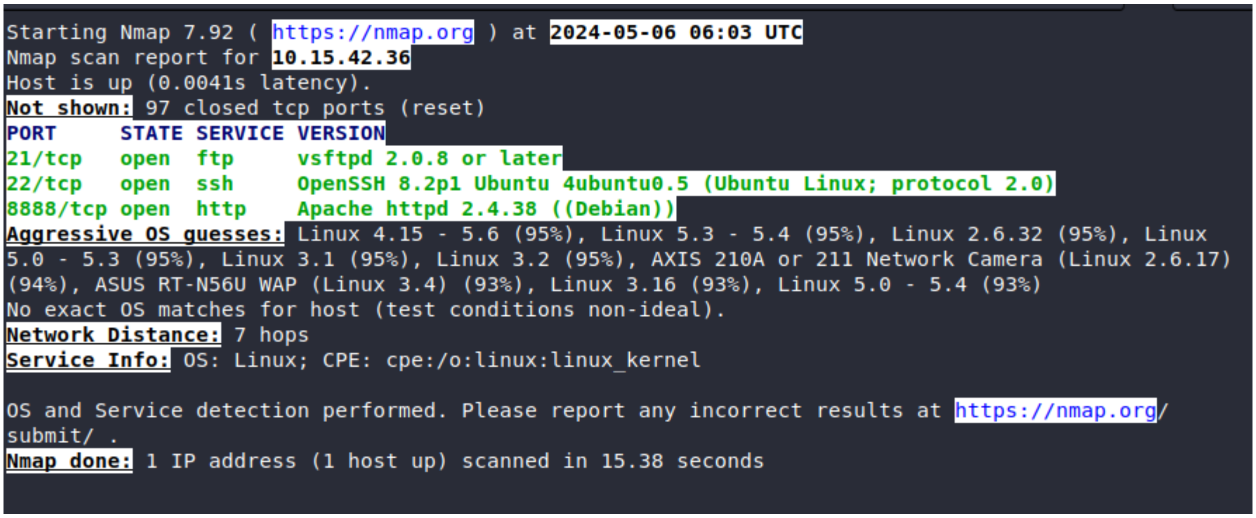
Intense Scan All Ports TCP

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-06 06:07 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating Ping Scan at 06:07
Scanning 10.15.42.36 [4 ports]
Completed Ping Scan at 06:07, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:07
Completed Parallel DNS resolution of 1 host. at 06:07, 0.01s elapsed
Initiating SYN Stealth Scan at 06:07
Scanning 10.15.42.36 [65535 ports]
Discovered open port 21/tcp on 10.15.42.36
Discovered open port 22/tcp on 10.15.42.36
Discovered open port 8888/tcp on 10.15.42.36
Completed SYN Stealth Scan at 06:07, 5.35s elapsed (65535 total ports)
Initiating Service scan at 06:07
Scanning 3 services on 10.15.42.36
Completed Service scan at 06:07, 11.04s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.15.42.36
Retrying OS detection (try #2) against 10.15.42.36
Initiating Traceroute at 06:07
```

```
Completed Traceroute at 06:07, 0.01s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 06:07
Completed Parallel DNS resolution of 7 hosts. at 06:07, 0.01s
elapsed
NSE: Script scanning 10.15.42.36.
Initiating NSE at 06:07
Completed NSE at 06:07, 0.34s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.05s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Nmap scan report for 10.15.42.36
Host is up (0.0042s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 172.18.0.3 is not the
same as 10.15.42.36
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.33.4.148
|      Logged in as ftp
|      TYPE: ASCII
|      Session bandwidth limit in byte/s is 6250000
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubunt
u Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ca:12:a1:08:41:b8:5b:01:b2:2b:c6:64:9d:01:ce:e0 (RS
A)
|   256 df:e6:37:47:be:43:54:96:1f:40:43:9b:d7:ac:78:ad (ECDS
A)
|_  256 b5:74:86:8d:ee:74:51:2a:38:09:67:38:7d:a0:e6:c0 (ED25
519)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Login Page
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.
4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.3 (95%), Linux 3.1
(95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linu
x 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.
16 (93%), Linux 5.0 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 34.844 days (since Mon Apr  1 09:52:27 2024)
Network Distance: 7 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT     ADDRESS
1   5.98 ms 10.33.0.1
2   9.89 ms 10.11.2.81
3   6.68 ms 10.11.5.5
4   9.48 ms 10.0.15.250
5   5.97 ms 10.0.1.46
6   6.73 ms 10.15.47.250
7   5.74 ms 10.15.42.36

NSE: Script Post-scanning.
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
```

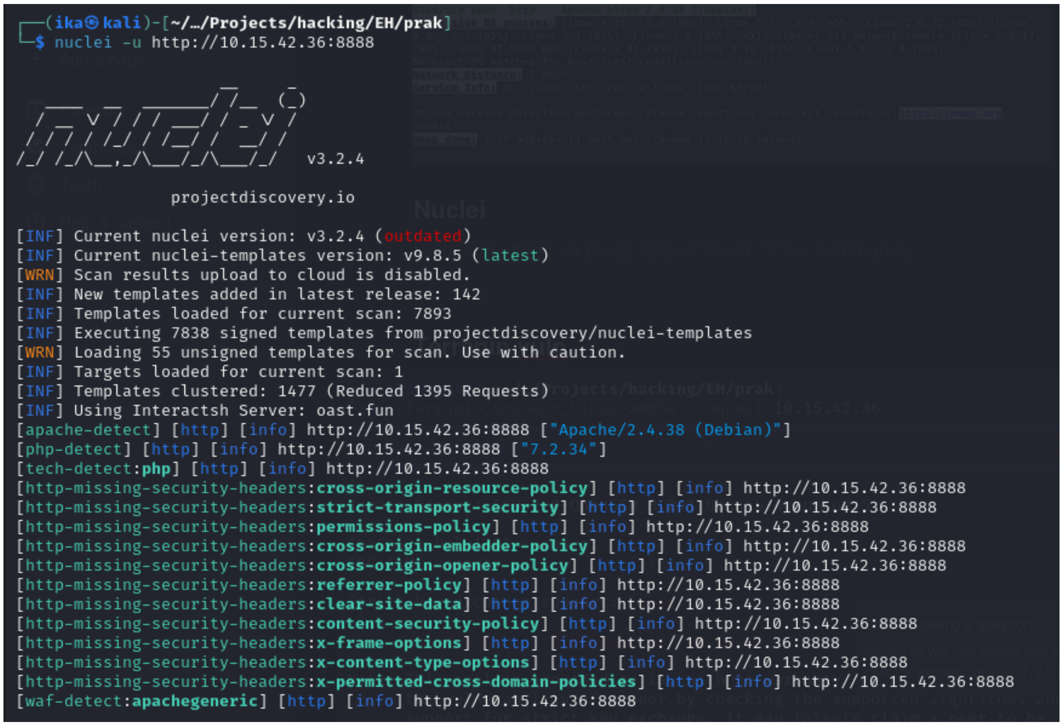
```
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorre
ct results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.91 seconds
           Raw packets sent: 65593 (2.888MB) | Rcvd: 65574
(2.624MB)
```

Quick Scan Plus



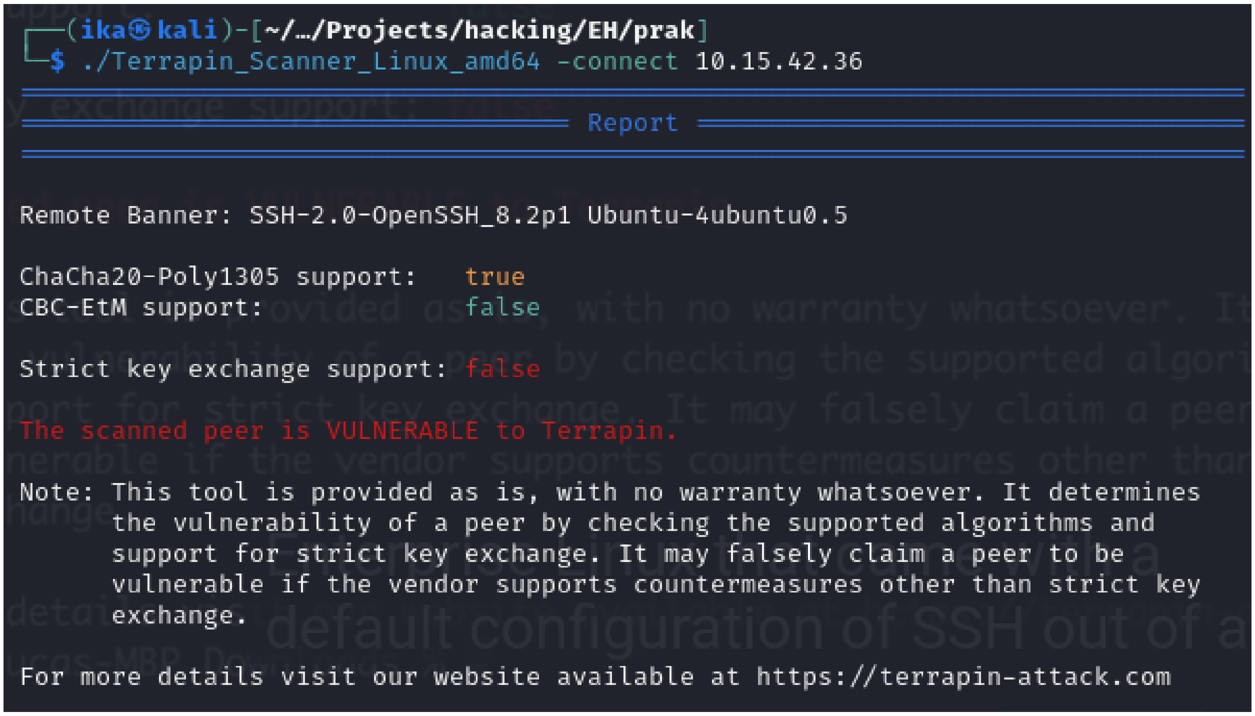
```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-06 06:03 UTC
Nmap scan report for 10.15.42.36
Host is up (0.0041s latency).
Not shown: 97 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux
5.0 - 5.3 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17)
(94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 5.0 - 5.4 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.38 seconds
```

Nuclei



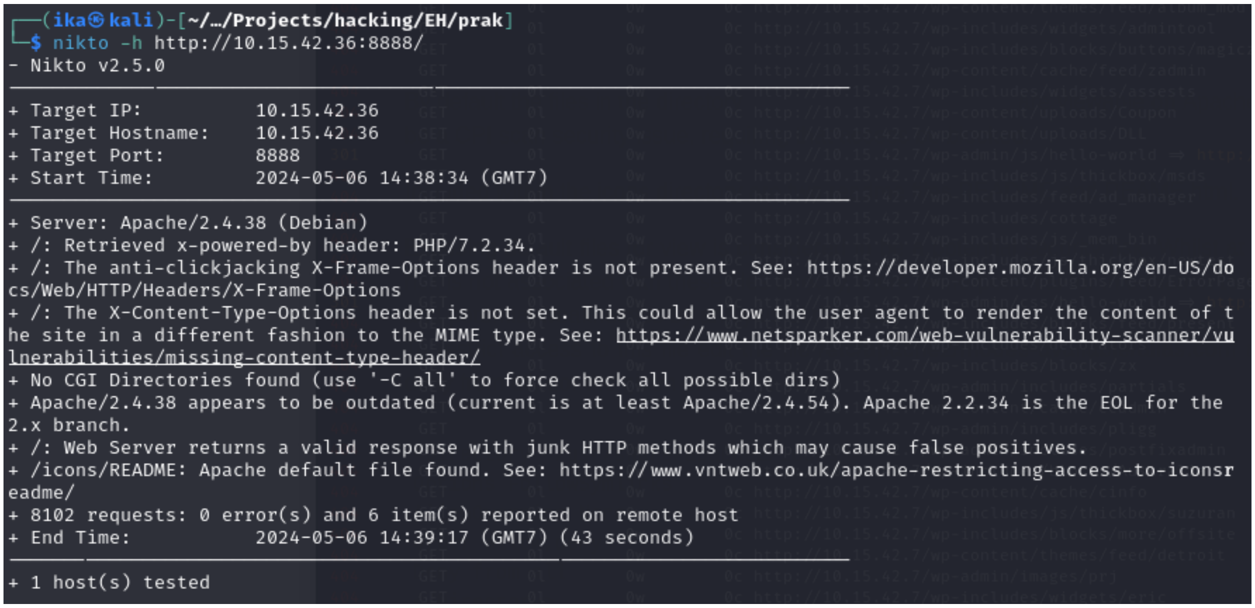
```
┌──(ika㉿kali)-[~/…/Projects/hacking/EH/prak]
└─$ nuclei -u http://10.15.42.36:8888

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.4

                projectdiscovery.io

[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[INF] Using Interactsh Server: oast.fun
[apache-detect] [http] [info] http://10.15.42.36:8888 ["Apache/2.4.38 (Debian)"]
[php-detect] [http] [info] http://10.15.42.36:8888 ["7.2.34"]
[tech-detect:php] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.36:8888
[waf-detect:apachegeneric] [http] [info] http://10.15.42.36:8888
```

Terrapin vuln



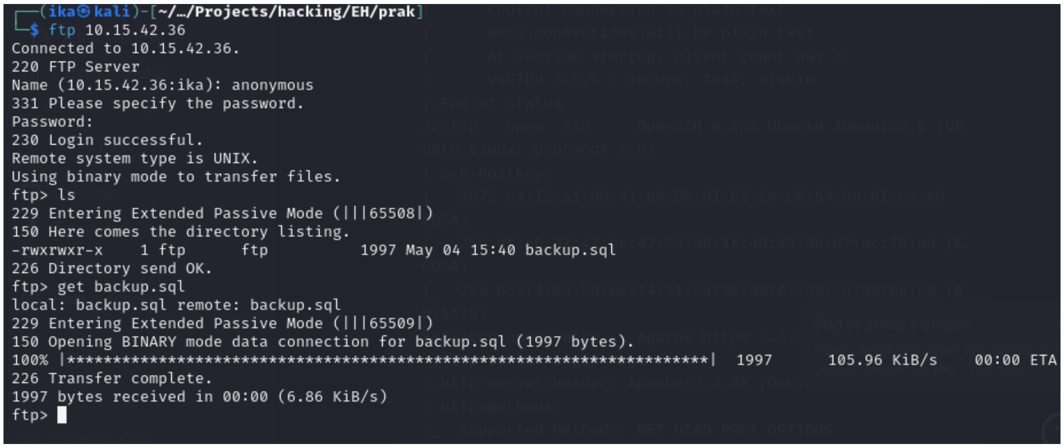
```
┌──(ika㉿kali)-[~/…/Projects/hacking/EH/prak]
└─$ ./Terrapin_Scanner_Linux_amd64 -connect 10.15.42.36
================================================================================
==================================== Report ====================================
================================================================================

Remote Banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5

ChaCha20-Poly1305 support:   true
CBC-EtM support:             false

Strict key exchange support: false

The scanned peer is VULNERABLE to Terrapin.

Note: This tool is provided as is, with no warranty whatsoever. It determines
      the vulnerability of a peer by checking the supported algorithms and
      support for strict key exchange. It may falsely claim a peer to be
      vulnerable if the vendor supports countermeasures other than strict key
      exchange.

For more details visit our website available at https://terrapin-attack.com
```

Nikto



```
┌──(ika㉿kali)-[~/…/Projects/hacking/EH/prak]
└─$ nikto -h http://10.15.42.36:8888/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.15.42.36
+ Target Hostname:    10.15.42.36
+ Target Port:        8888
+ Start Time:         2024-05-06 14:38:34 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: Retrieved x-powered-by header: PHP/7.2.34.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/do
cs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
he site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vu
lnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the
2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsr
eadme/
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-05-06 14:39:17 (GMT7) (43 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

FTP access



```
┌──(ika㉿kali)-[~/…/Projects/hacking/EH/prak]
└─$ ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:ika): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65508|)
150 Here comes the directory listing.
-rwxrwxr-x    1 ftp      ftp          1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> get backup.sql
local: backup.sql remote: backup.sql
229 Entering Extended Passive Mode (|||65509|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |***********************************************************************|  1997      105.96 KiB/s    00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (6.86 KiB/s)
ftp> █
```