In **Phase 2** of the penetration test, we will use enumeration and host discovery tools to be able to establish an active connection to the target hosts which will allow us to discover potential attack vectors in the system. These attack vectors will then be used for exploitation of the system. Enumeration is used to collect the following attributes about the targets:

Usernames and group names
Hostnames
Network shares and services
IP tables and routing tables
Service setting and audit configurations
Application and banners
SNMP and DNS details

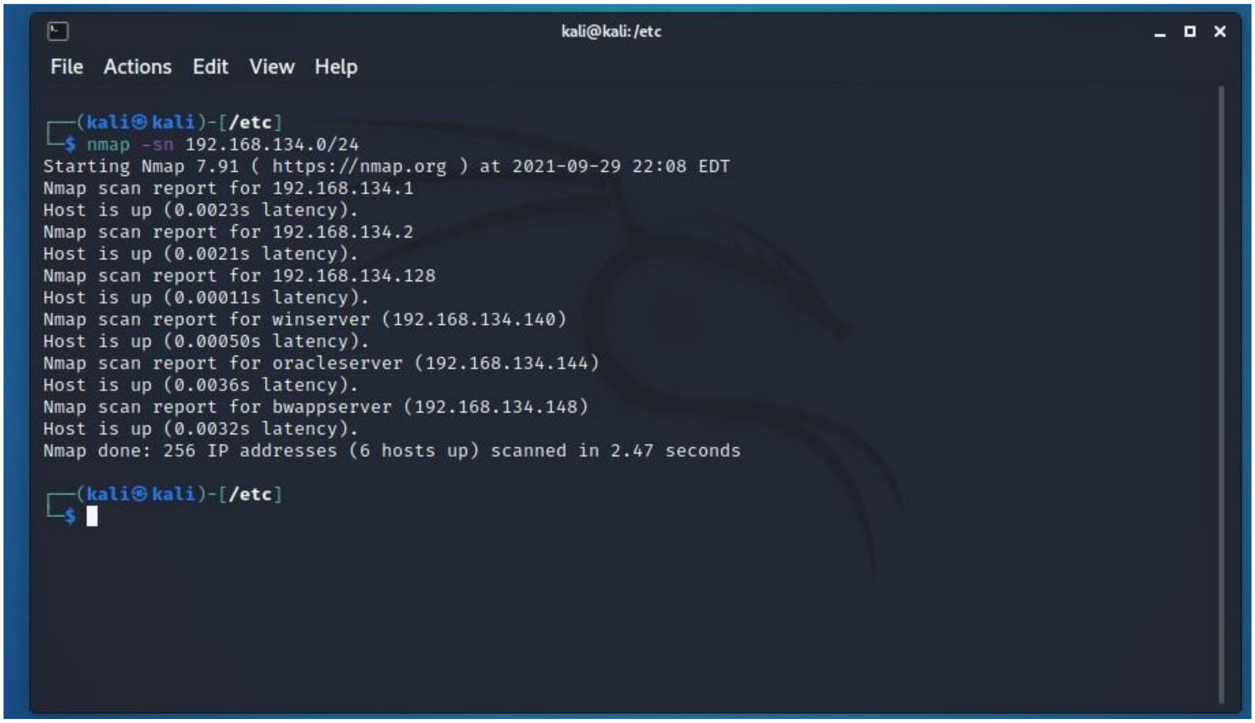
The lab environment will be used to test the enumeration tools used at the Artemis Company before the actual penetration test. The tools are as follows:

Tool 1: Nmap is one of the most widely used enumeration tools. The diagrams are the result of running the following commands:

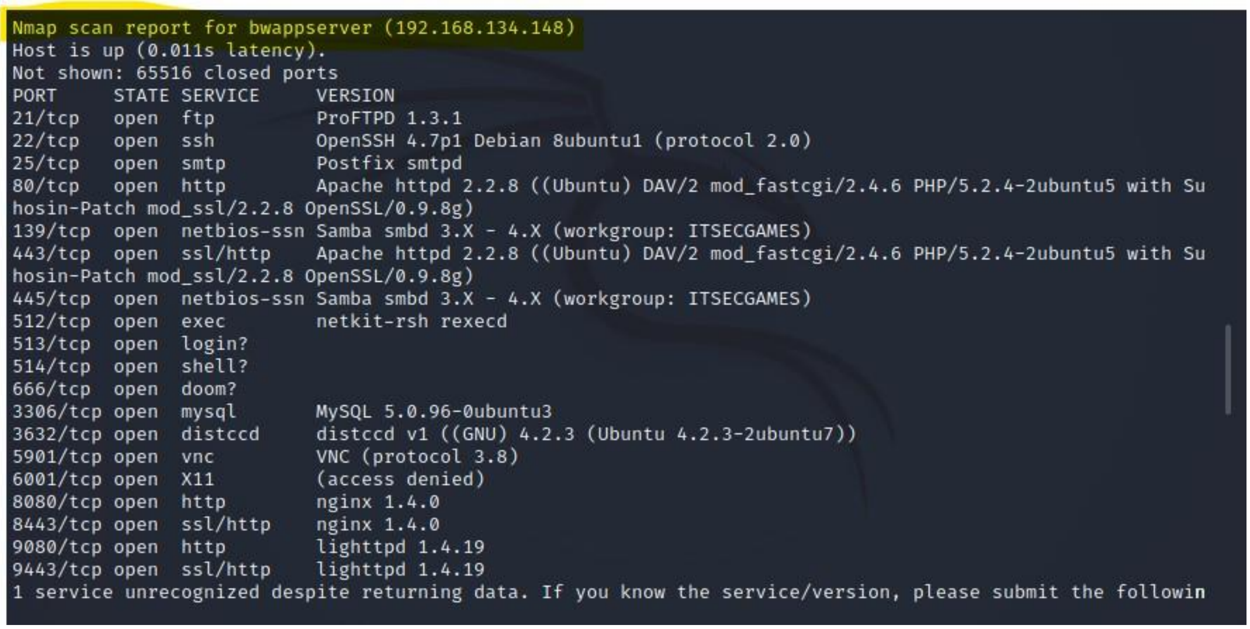
-> nmap -sn 192.168.134.0/24
Ping sweep the network (pinging range of IP addresses)

-> nmap -p -sV 192.168.134.0/24
Full TCP port scan with service version detection

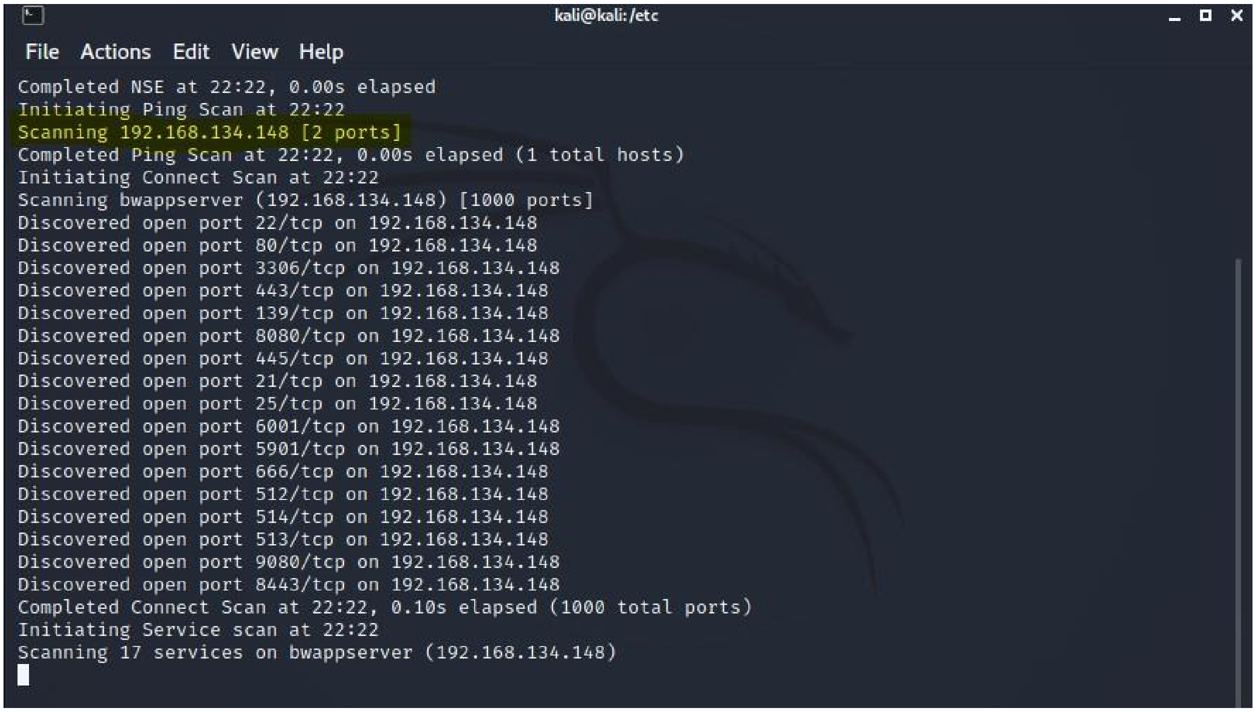
-> nmap -v -A -T4 192.168.134.0/24
Aggressive scan (-A) with faster speed (-T4). Aggressive scan is a combination of OS detection -O), version scanning (-sV) and script scanning (-sC). The Nmap Scripting Engine (NSE) scripts have associated categories (safe, intrusive, malware, backdoor, version, discovery, and vulnerability).



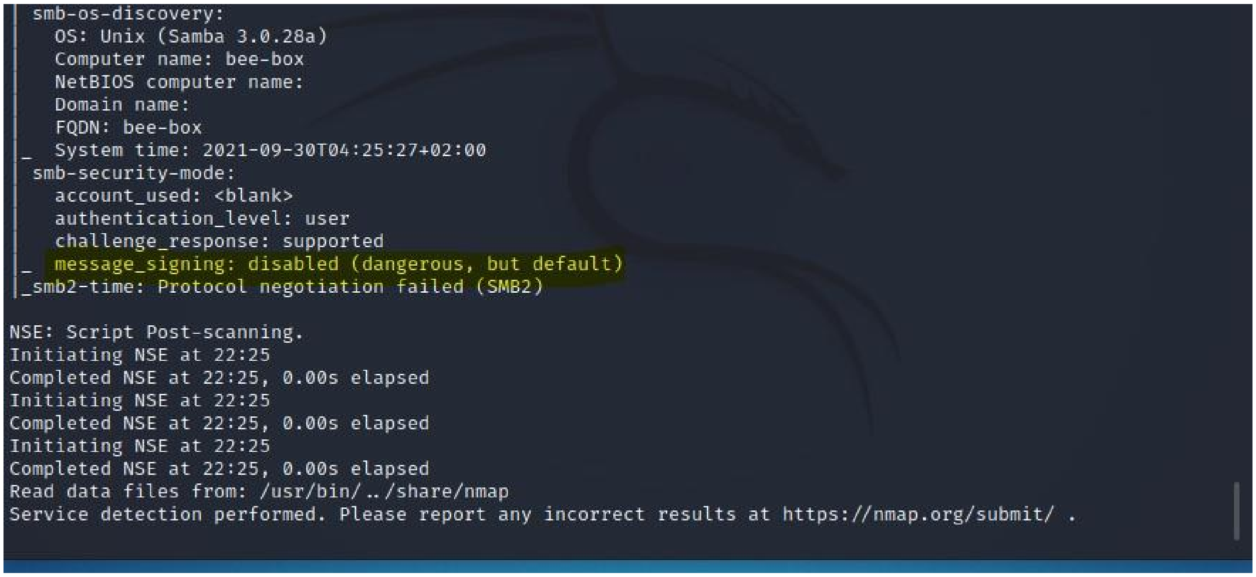
```
┌──(kali㉿kali)-[/etc]
└─$ nmap -sn 192.168.134.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 22:08 EDT
Nmap scan report for 192.168.134.1
Host is up (0.0023s latency).
Nmap scan report for 192.168.134.2
Host is up (0.0021s latency).
Nmap scan report for 192.168.134.128
Host is up (0.00011s latency).
Nmap scan report for winserver (192.168.134.140)
Host is up (0.00050s latency).
Nmap scan report for oracleserver (192.168.134.144)
Host is up (0.0036s latency).
Nmap scan report for bwappserver (192.168.134.148)
Host is up (0.0032s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.47 seconds

┌──(kali㉿kali)-[/etc]
└─$ 
```



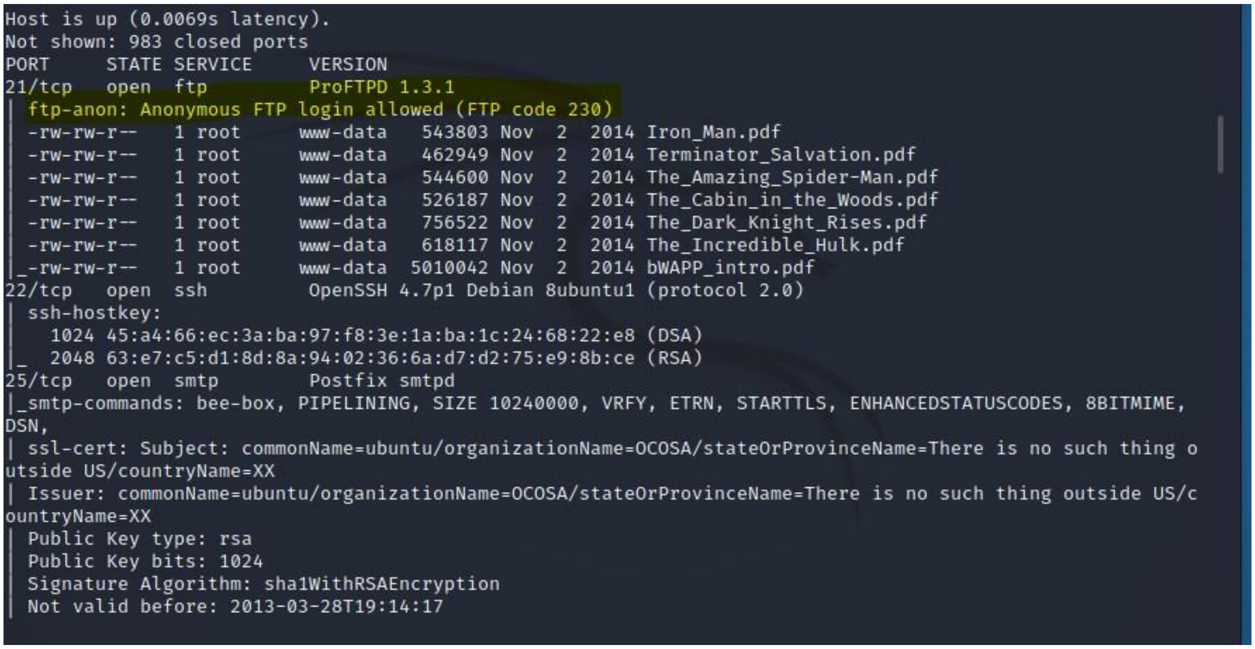
```
Nmap scan report for bwappserver (192.168.134.148)
Host is up (0.011s latency).
Not shown: 65516 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Su
hosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Su
hosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3-2ubuntu7))
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
9443/tcp open  ssl/http    lighttpd 1.4.19
1 service unrecognized despite returning data. If you know the service/version, please submit the followin
```



```
Completed NSE at 22:22, 0.00s elapsed
Initiating Ping Scan at 22:22
Scanning 192.168.134.148 [2 ports]
Completed Ping Scan at 22:22, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 22:22
Scanning bwappserver (192.168.134.148) [1000 ports]
Discovered open port 22/tcp on 192.168.134.148
Discovered open port 80/tcp on 192.168.134.148
Discovered open port 3306/tcp on 192.168.134.148
Discovered open port 443/tcp on 192.168.134.148
Discovered open port 139/tcp on 192.168.134.148
Discovered open port 8080/tcp on 192.168.134.148
Discovered open port 445/tcp on 192.168.134.148
Discovered open port 21/tcp on 192.168.134.148
Discovered open port 25/tcp on 192.168.134.148
Discovered open port 6001/tcp on 192.168.134.148
Discovered open port 5901/tcp on 192.168.134.148
Discovered open port 666/tcp on 192.168.134.148
Discovered open port 512/tcp on 192.168.134.148
Discovered open port 514/tcp on 192.168.134.148
Discovered open port 513/tcp on 192.168.134.148
Discovered open port 9080/tcp on 192.168.134.148
Discovered open port 8443/tcp on 192.168.134.148
Completed Connect Scan at 22:22, 0.10s elapsed (1000 total ports)
Initiating Service scan at 22:22
Scanning 17 services on bwappserver (192.168.134.148)
```

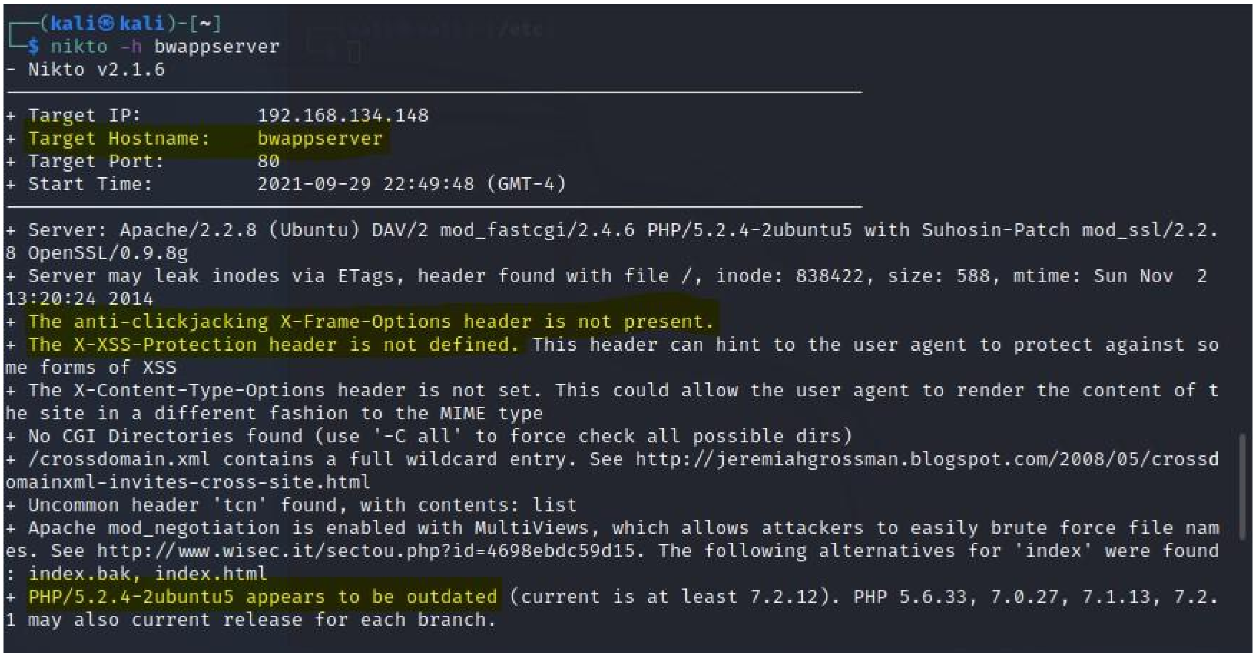


```
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: bee-box
|   NetBIOS computer name:
|   Domain name:
|   FQDN: bee-box
|_  System time: 2021-09-30T04:25:27+02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

NSE: Script Post-scanning.
Initiating NSE at 22:25
Completed NSE at 22:25, 0.00s elapsed
Initiating NSE at 22:25
Completed NSE at 22:25, 0.00s elapsed
Initiating NSE at 22:25
Completed NSE at 22:25, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

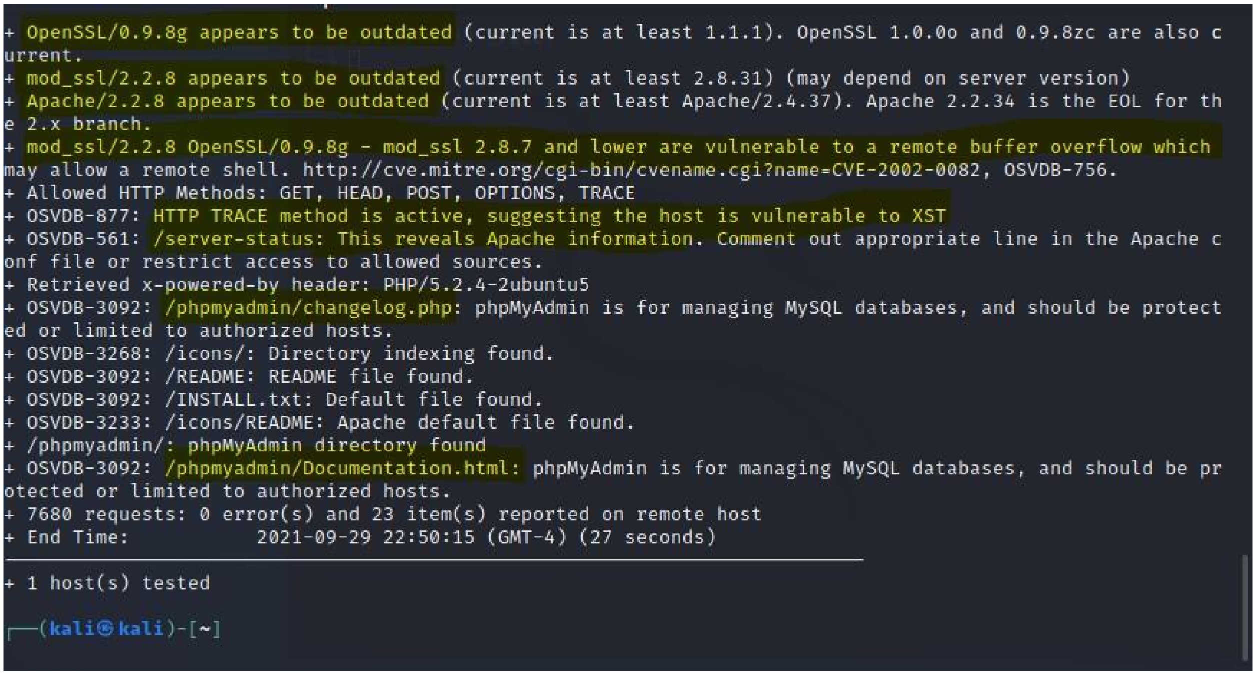


```
Host is up (0.0069s latency).
Not shown: 983 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--   1 root     www-data   543803 Nov  2  2014 Iron_Man.pdf
| -rw-rw-r--   1 root     www-data   462949 Nov  2  2014 Terminator_Salvation.pdf
| -rw-rw-r--   1 root     www-data   544600 Nov  2  2014 The_Amazing_Spider-Man.pdf
| -rw-rw-r--   1 root     www-data   526187 Nov  2  2014 The_Cabin_in_the_Woods.pdf
| -rw-rw-r--   1 root     www-data   756522 Nov  2  2014 The_Dark_Knight_Rises.pdf
| -rw-rw-r--   1 root     www-data   618117 Nov  2  2014 The_Incredible_Hulk.pdf
|_-rw-rw-r--   1 root     www-data  5010042 Nov  2  2014 bWAPP_intro.pdf
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 45:a4:66:ec:3a:ba:97:f8:3e:1a:ba:1c:24:68:22:e8 (DSA)
|_  2048 63:e7:c5:d1:8d:8a:94:02:36:6a:d7:d2:75:e9:8b:ce (RSA)
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: bee-box, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,
| ssl-cert: Subject: commonName=ubuntu/organizationName=OCOSA/stateOrProvinceName=There is no such thing o
utside US/countryName=XX
| Issuer: commonName=ubuntu/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/c
ountryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2013-03-28T19:14:17
```

Tool 2: Nikto is a web server scanner which performs complete tests against web servers for numerous items such as dangerous fies/programs, checks for outdated versions of servers, and version specific problems on many servers. In the example below, **bwappserver** contains the following protocols and applications on Ubuntu: PHP/5.2.4, Apache, MySQL, and OpenSSL. The scan discovered the server-status directory which contains the Apache config file. In addition, the /phpmyadmin/changelog.php and /phpmyadmin/Documentation.html files contain information an attacker can use and should be protected by authorized hosts.

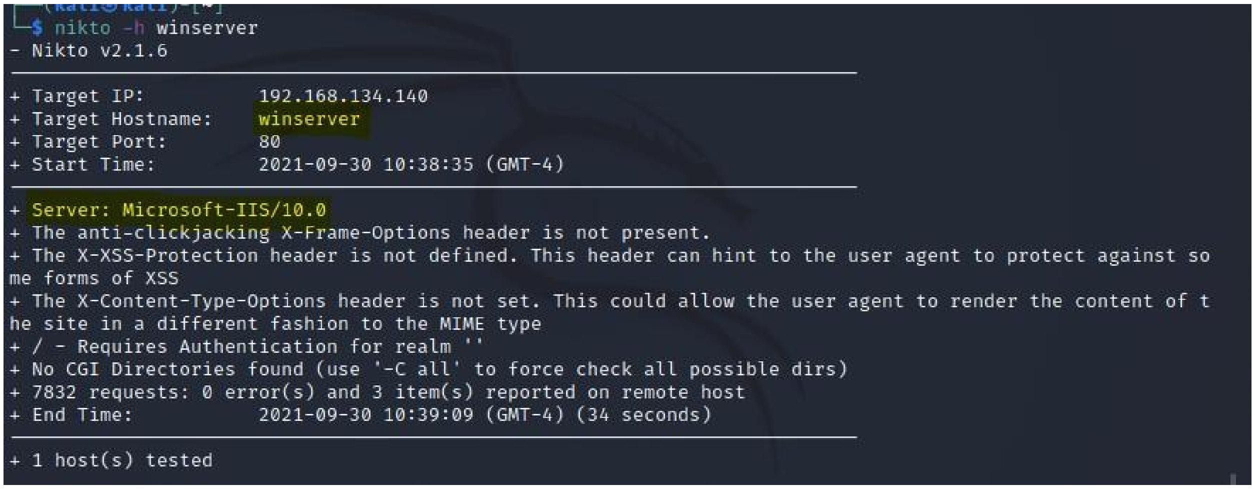


```
┌──(kali㉿kali)-[~]
└─$ nikto -h bwappserver
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.134.148
+ Target Hostname:    bwappserver
+ Target Port:        80
+ Start Time:         2021-09-29 22:49:48 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.
8 OpenSSL/0.9.8g
+ Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov  2
13:20:24 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against so
me forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
he site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossd
omainxml-invites-cross-site.html
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file nam
es. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found
: index.bak, index.html
+ PHP/5.2.4-2ubuntu5 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.
1 may also current release for each branch.
```



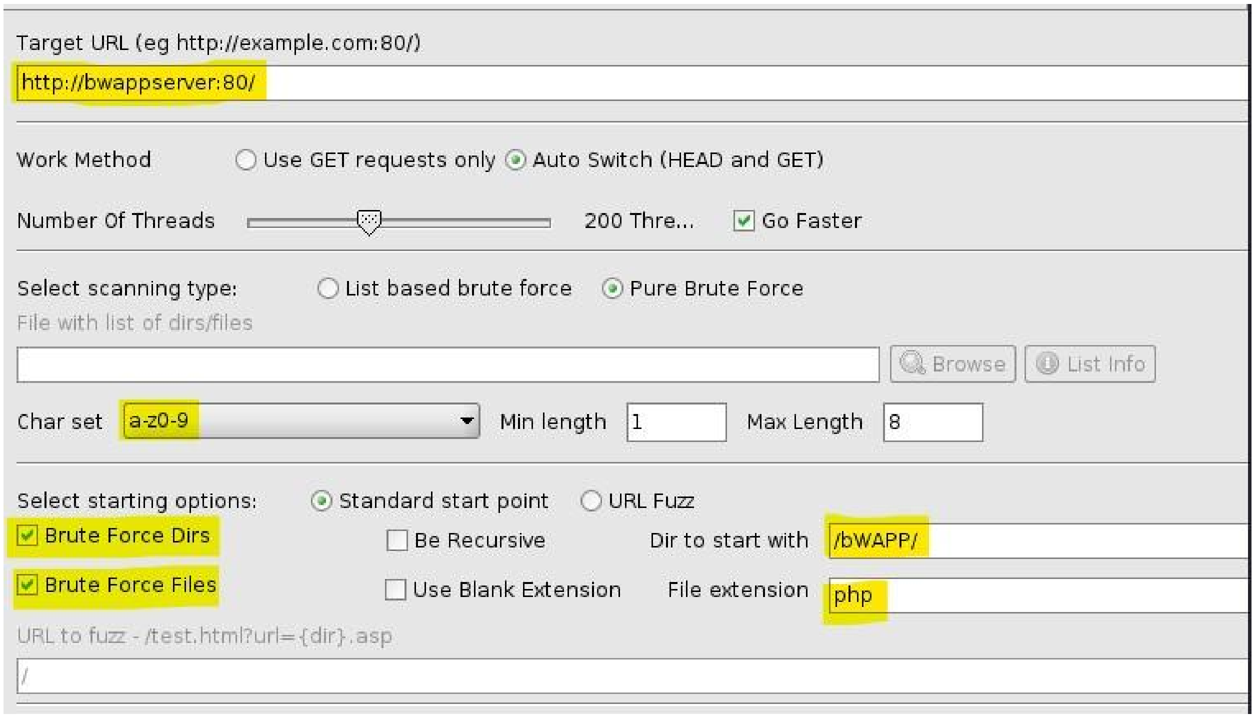
```
+ OpenSSL/0.9.8g appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also c
urrent.
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for th
e 2.x branch.
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which
may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in the Apache c
onf file or restrict access to allowed sources.
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protect
ed or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /README: README file found.
+ OSVDB-3092: /INSTALL.txt: Default file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be pr
otected or limited to authorized hosts.
+ 7680 requests: 0 error(s) and 23 item(s) reported on remote host
+ End Time:           2021-09-29 22:50:15 (GMT-4) (27 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
```

Another example is the winserver shown below where nikto discovered the IP address, the operating system, and that it is a web server using IIS.



```
┌──(kali㉿kali)-[~]
└─$ nikto -h winserver
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.134.140
+ Target Hostname:    winserver
+ Target Port:        80
+ Start Time:         2021-09-30 10:38:35 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against so
me forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
he site in a different fashion to the MIME type
+ / - Requires Authentication for realm ''
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7832 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2021-09-30 10:39:09 (GMT-4) (34 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Tool 3: DirBuster is a multithreaded java application pre-installed on Kali Linux that uses brute force to enumerate directories and file names on web/application servers. It will pick up on hidden files on a web server in a state of default installation. The example below shows the discovery of files and directory in the **/bWAPP/** directory of the **bwappserver** with URL of http://bwappserver:80/ DirBuster has discovered the database file **bwapp.sqlite**.



Target URL (eg http://example.com:80/)

http://bwappserver:80/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ○ List based brute force ● Pure Brute Force

File with list of dirs/files

Char set a-z0-9 Min length 1 Max Length 8

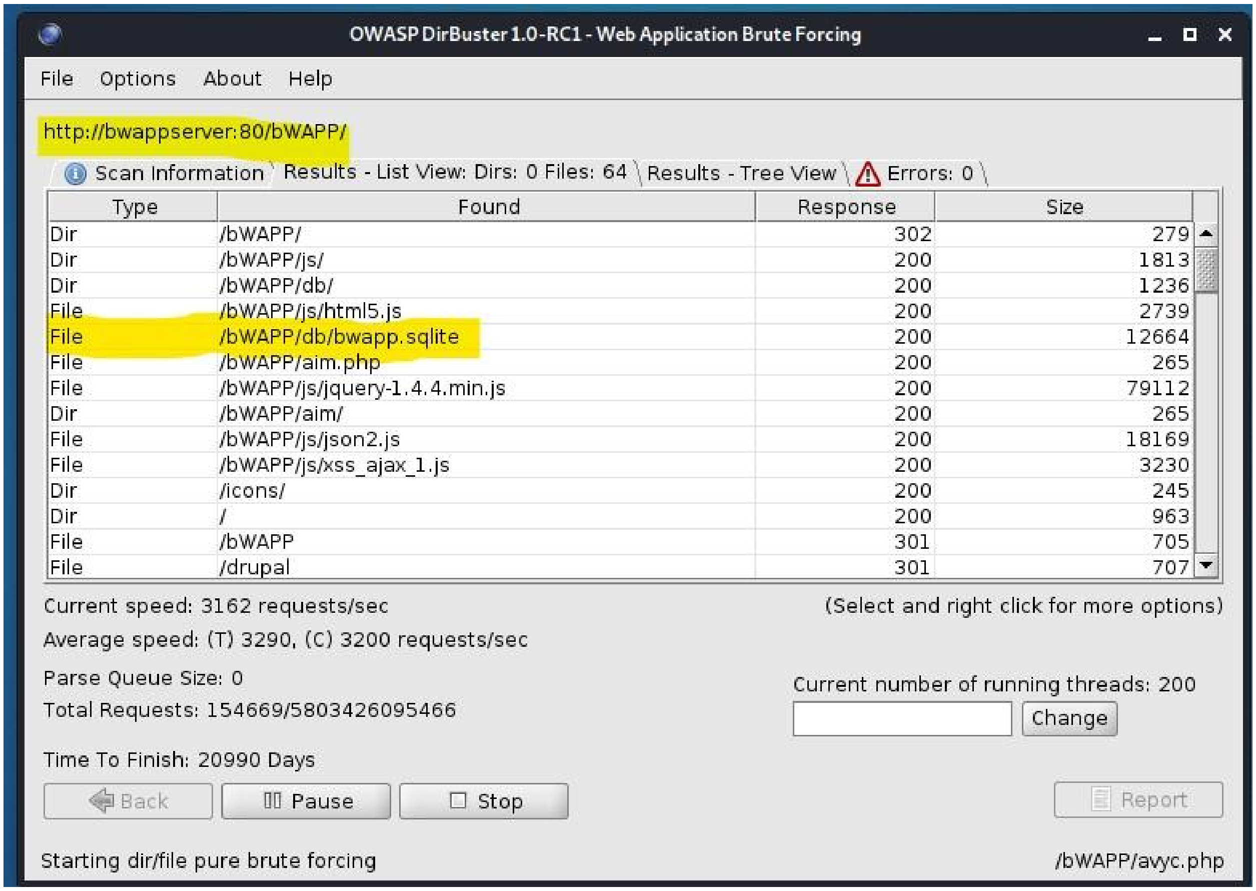
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs □ Be Recursive Dir to start with /bWAPP/

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

/



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://bwappserver:80/bWAPP/

Type	Found	Response	Size
Dir	/bWAPP/	302	279
Dir	/bWAPP/js/	200	1813
Dir	/bWAPP/db/	200	1236
File	/bWAPP/js/html5.js	200	2739
File	/bWAPP/db/bwapp.sqlite	200	12664
File	/bWAPP/aim.php	200	265
File	/bWAPP/js/jquery-1.4.4.min.js	200	79112
Dir	/bWAPP/aim/	200	265
File	/bWAPP/js/json2.js	200	18169
File	/bWAPP/js/xss_ajax_1.js	200	3230
Dir	/icons/	200	245
Dir	/	200	963
File	/bWAPP	301	705
File	/drupal	301	707

Current speed: 3162 requests/sec (Select and right click for more options)

Average speed: (T) 3290, (C) 3200 requests/sec

Parse Queue Size: 0

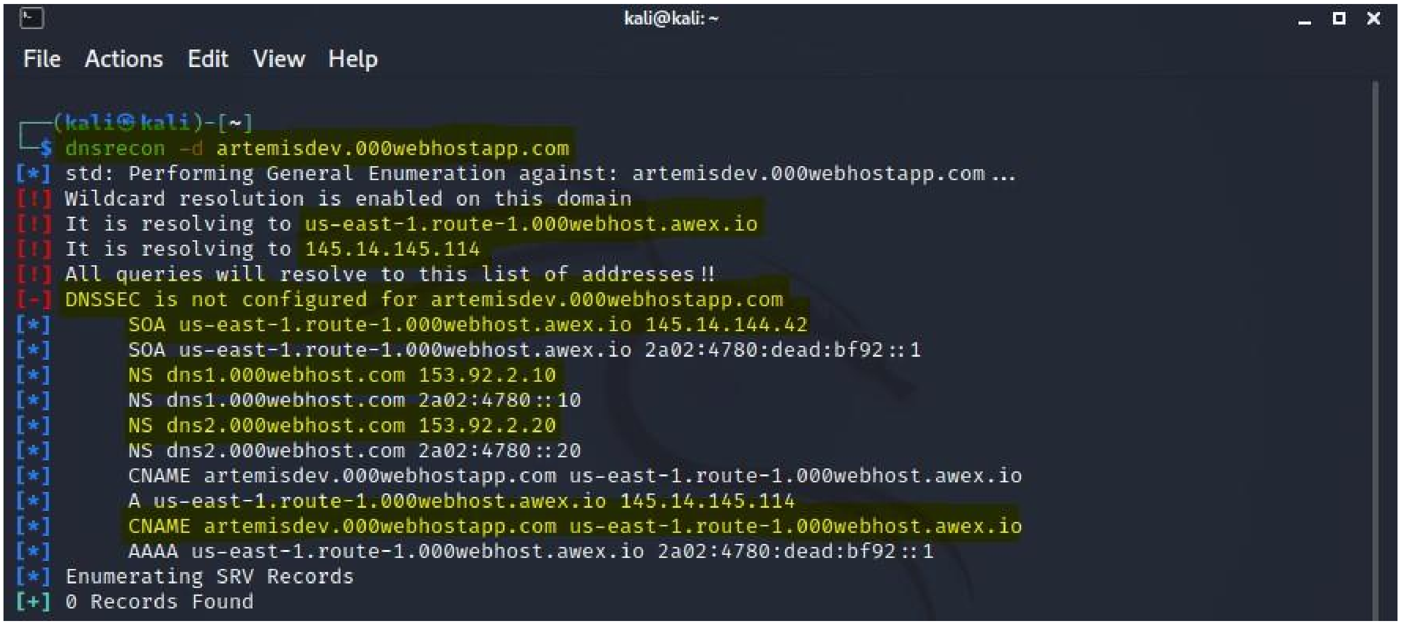
Total Requests: 154669/5803426095466

Current number of running threads: 200

Time To Finish: 20990 Days

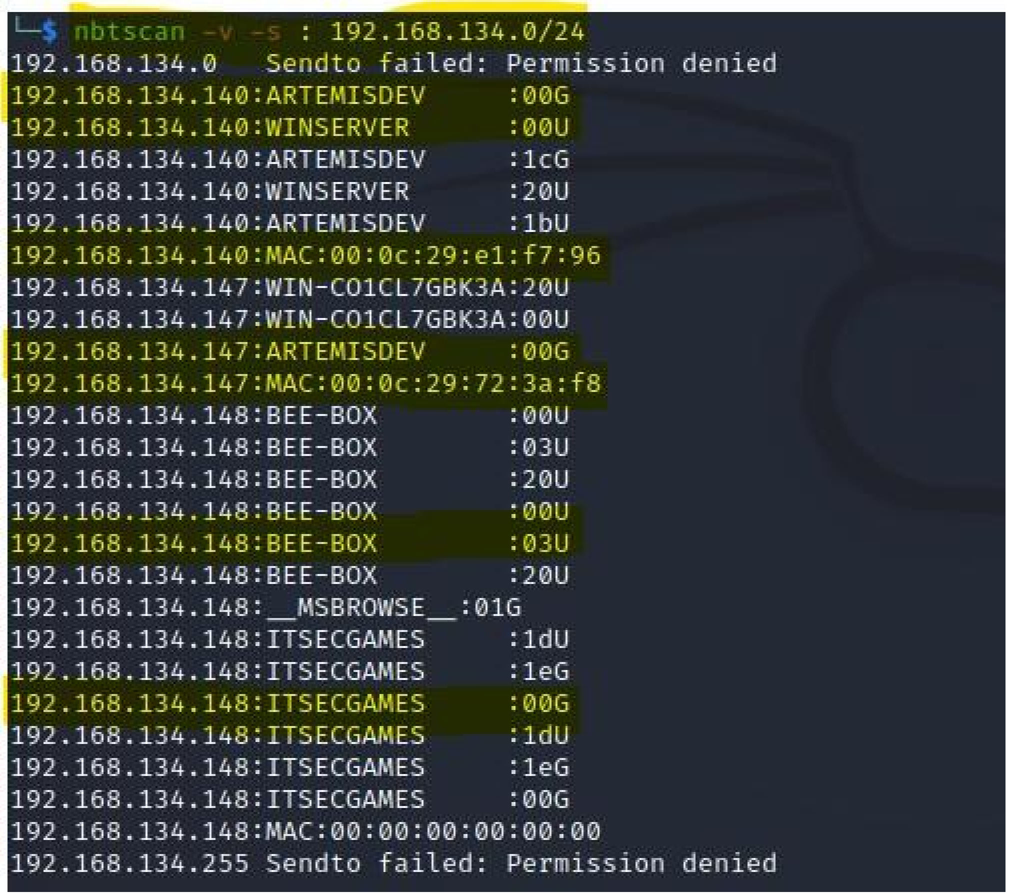
Starting dir/file pure brute forcing /bWAPP/avyc.php

Tool 4: DNS (Domain Name Service) is mainly designed as hierarchical decentralized distributed naming systems for any resource connected to the network with the primary function of linking IP addresses to hostnames. Some of the record types that DNS enumeration reveals are:
Start of Authority (SOA) records which contain important information about a domain
A records which contain IP addresses
Nameserver (NS) records which contain information about the nameservers
SMTP mail exchanger (MX) records.
The process of DNS enumeration involves the process of sending zone transfer requests to the DNS primary server pretending to be a client. The pentester can use DNS enumeration to evaluate the results of the requests which will reveal confidential domain records. DNS enumeration was performed using **dnsrecon** on the private network in the lab. Dnsrecon was used on the http://winserver.artemisdev.com which is redirected to https://artemisdev.000webhostapp.com . The diagrams below show **SOA** records, the **NS** records, and the **CNAME records** and the corresponding IP address.



```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d artemisdev.000webhostapp.com
[*] std: Performing General Enumeration against: artemisdev.000webhostapp.com ...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to us-east-1.route-1.000webhost.awex.io
[!] It is resolving to 145.14.145.114
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for artemisdev.000webhostapp.com
[*]      SOA us-east-1.route-1.000webhost.awex.io 145.14.144.42
[*]      SOA us-east-1.route-1.000webhost.awex.io 2a02:4780:dead:bf92::1
[*]      NS dns1.000webhost.com 153.92.2.10
[*]      NS dns1.000webhost.com 2a02:4780::10
[*]      NS dns2.000webhost.com 153.92.2.20
[*]      NS dns2.000webhost.com 2a02:4780::20
[*]      CNAME artemisdev.000webhostapp.com us-east-1.route-1.000webhost.awex.io
[*]      A us-east-1.route-1.000webhost.awex.io 145.14.145.114
[*]      CNAME artemisdev.000webhostapp.com us-east-1.route-1.000webhost.awex.io
[*]      AAAA us-east-1.route-1.000webhost.awex.io 2a02:4780:dead:bf92::1
[*] Enumerating SRV Records
[+] 0 Records Found
```

Tool 5: Nbtscan pre-installed on Kali Linux is used to discover Network Basic Input Output System (NetBIOS) software which runs on port 139. **NetBIOS** is a session layer 5 protocol and service that permits applications on computers to interconnect with one another over a LAN and access resources from a server. Attack vectors consist of reading and writing to a remote machine, Denial of Service (DoS) and discovering password policies on remote machines. In the example below, Nbtscan discovered the hostnames **winserver, winclient (WIN-C01CL7GBK3A), and bee-box** that have NetBIOS installed. The domains discovered are **artemisdev** and **itsecgames**.



```
└─$ nbtscan -v -s : 192.168.134.0/24
192.168.134.0   Sendto failed: Permission denied
192.168.134.140:ARTEMISDEV     :00G
192.168.134.140:WINSERVER      :00U
192.168.134.140:ARTEMISDEV     :1cG
192.168.134.140:WINSERVER      :20U
192.168.134.140:ARTEMISDEV     :1bU
192.168.134.140:MAC:00:0c:29:e1:f7:96
192.168.134.147:WIN-CO1CL7GBK3A:20U
192.168.134.147:WIN-CO1CL7GBK3A:00U
192.168.134.147:ARTEMISDEV     :00G
192.168.134.147:MAC:00:0c:29:72:3a:f8
192.168.134.148:BEE-BOX        :00U
192.168.134.148:BEE-BOX        :03U
192.168.134.148:BEE-BOX        :20U
192.168.134.148:BEE-BOX        :00U
192.168.134.148:BEE-BOX        :03U
192.168.134.148:BEE-BOX        :20U
192.168.134.148:__MSBROWSE__:01G
192.168.134.148:ITSECGAMES     :1dU
192.168.134.148:ITSECGAMES     :1eG
192.168.134.148:ITSECGAMES     :00G
192.168.134.148:ITSECGAMES     :1dU
192.168.134.148:ITSECGAMES     :1eG
192.168.134.148:ITSECGAMES     :00G
192.168.134.148:MAC:00:00:00:00:00:00
192.168.134.255 Sendto failed: Permission denied
```