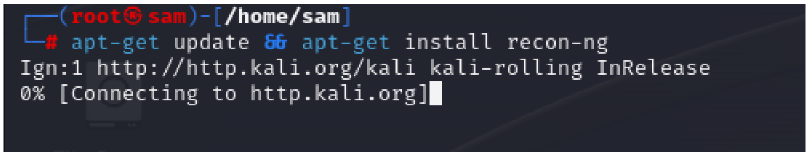
What is Recon-ng?

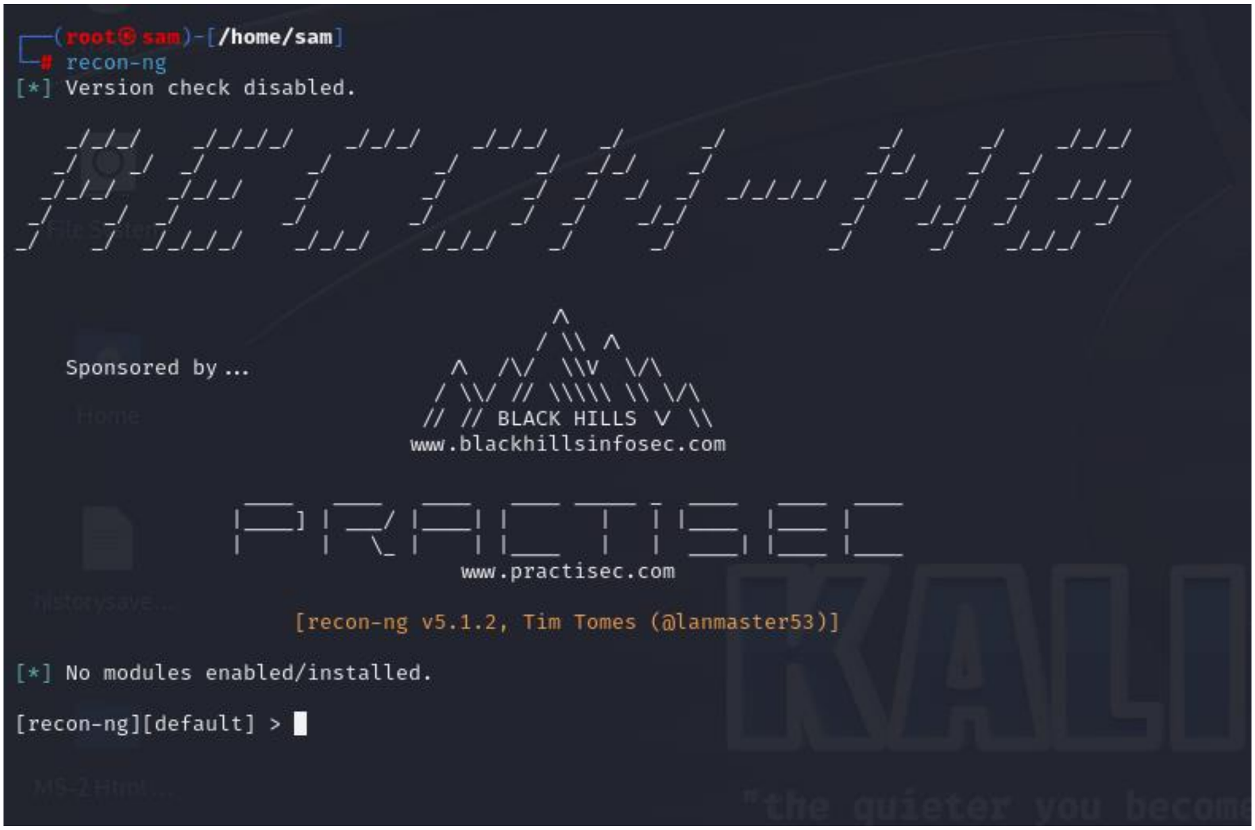
Recon-ng is a reconnaissance / OSINT tool with an interface similar to Metasploit. Running recon-ng from the command line speeds up the recon process as it automates gathering information from open sources.

Recon-ng has a variety of options to configure, perform recon, and output results to different report types.

Recon-ng Installation

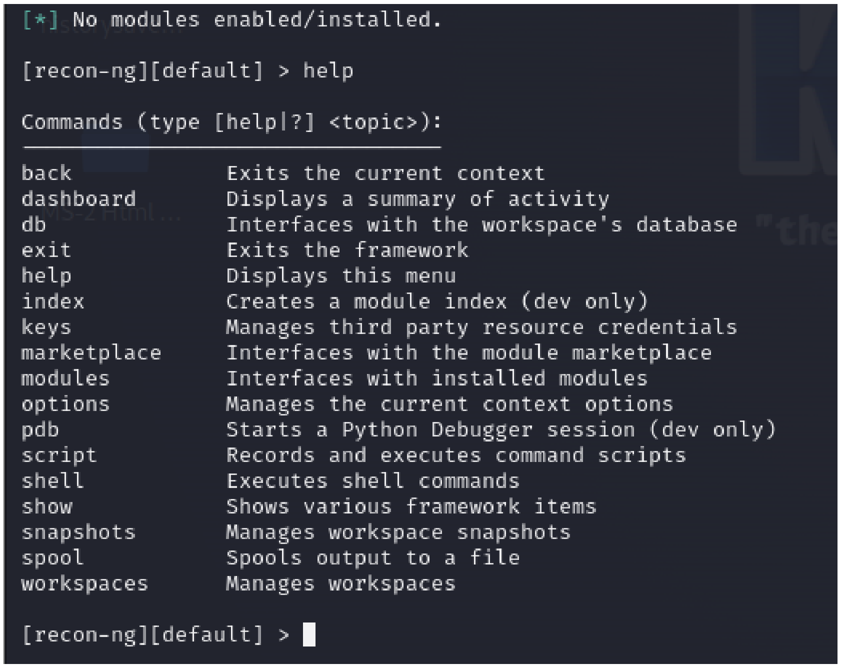


```
┌──(root㉿sam)-[/home/sam]
└─# apt-get update && apt-get install recon-ng
Ign:1 http://http.kali.org/kali kali-rolling InRelease
0% [Connecting to http.kali.org]
```



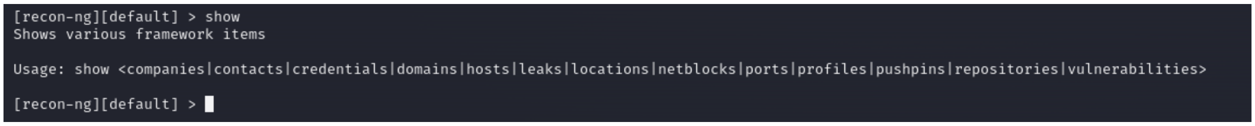
```
┌──(root㉿sam)-[/home/sam]
└─# recon-ng
[*] Version check disabled.

    Sponsored by ...
                                  BLACK HILLS
                          www.blackhillsinfosec.com

                              www.practisec.com

                 [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

[recon-ng][default] >
```

Help Command:



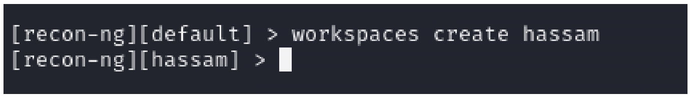
```
[*] No modules enabled/installed.

[recon-ng][default] > help

Commands (type [help|?] <topic>):
─────────────────────────────────
back             Exits the current context
dashboard        Displays a summary of activity
db               Interfaces with the workspace's database
exit             Exits the framework
help             Displays this menu
index            Creates a module index (dev only)
keys             Manages third party resource credentials
marketplace      Interfaces with the module marketplace
modules          Interfaces with installed modules
options          Manages the current context options
pdb              Starts a Python Debugger session (dev only)
script           Records and executes command scripts
shell            Executes shell commands
show             Shows various framework items
snapshots        Manages workspace snapshots
spool            Spools output to a file
workspaces       Manages workspaces

[recon-ng][default] >
```

Show cmd:



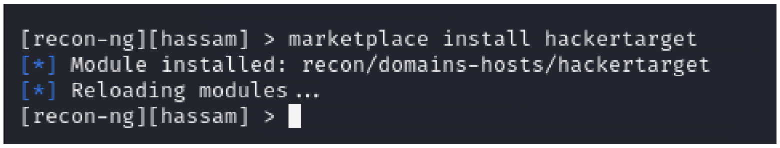
```
[recon-ng][default] > show
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] >
```

Create workspace:



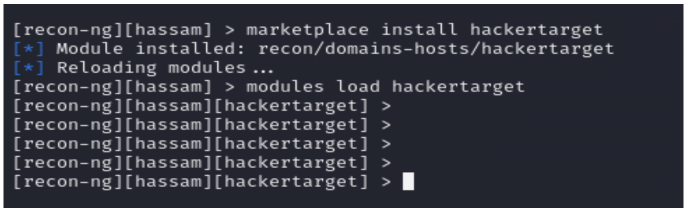
```
[recon-ng][default] > workspaces create hassam
[recon-ng][hassam] >
```

Hackertarget installation to find sub domains



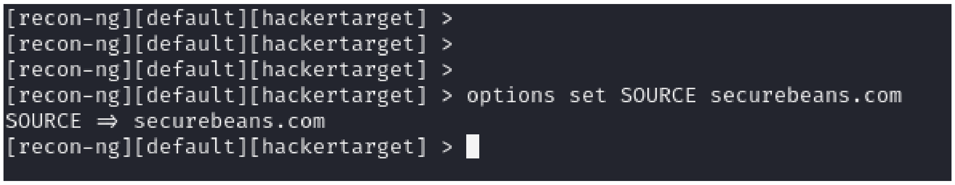
```
[recon-ng][hassam] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][hassam] >
```

Module Load hacker targert:



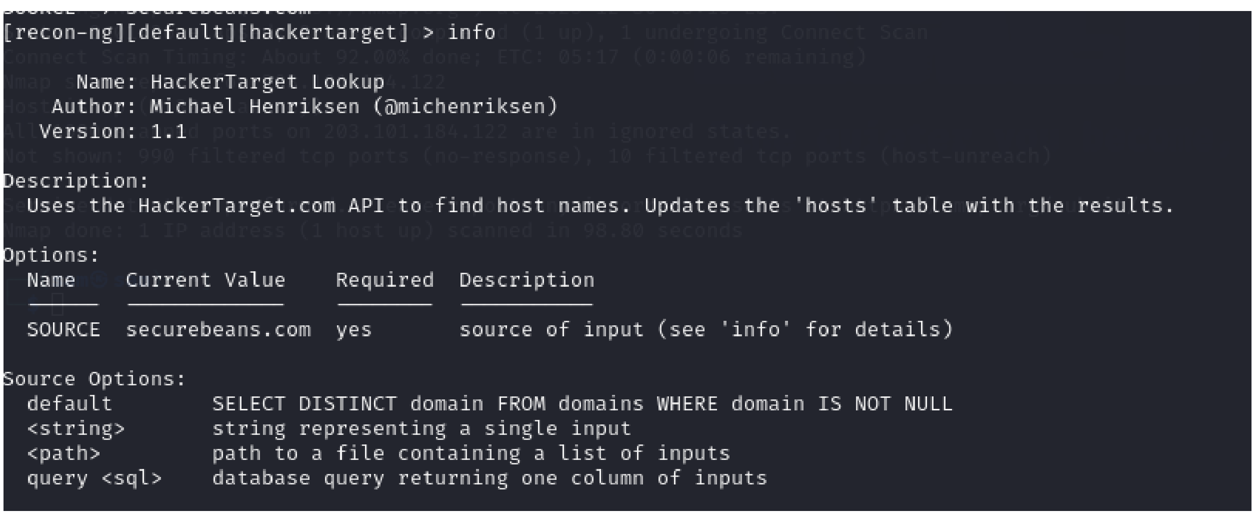
```
[recon-ng][hassam] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][hassam] > modules load hackertarget
[recon-ng][hassam][hackertarget] >
[recon-ng][hassam][hackertarget] >
[recon-ng][hassam][hackertarget] >
[recon-ng][hassam][hackertarget] >
[recon-ng][hassam][hackertarget] >
```

Add target:



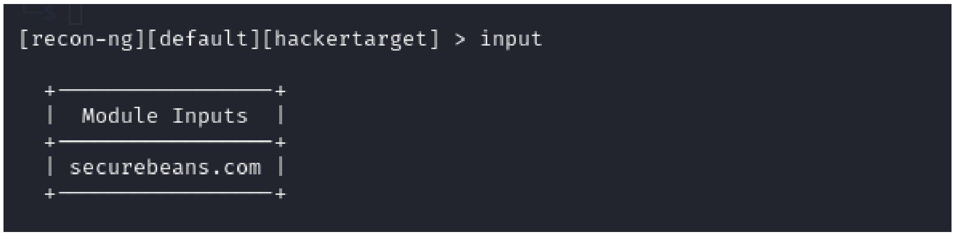
```
[recon-ng][default][hackertarget] >
[recon-ng][default][hackertarget] >
[recon-ng][default][hackertarget] >
[recon-ng][default][hackertarget] > options set SOURCE securebeans.com
SOURCE ⇒ securebeans.com
[recon-ng][default][hackertarget] > █
```

Info of hacker target source



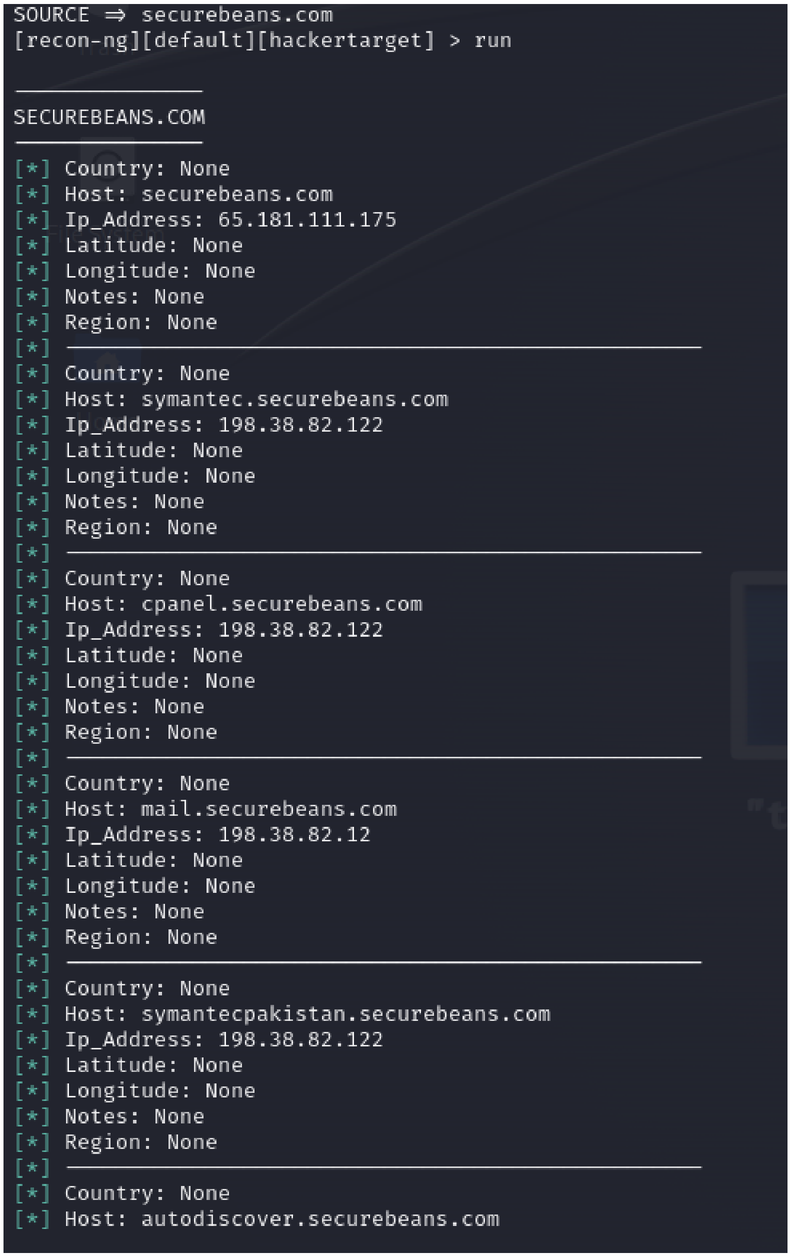
```
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value    Required  Description
  ──────  ───────────────  ────────  ───────────
  SOURCE  securebeans.com  yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
```

Check Giving input:

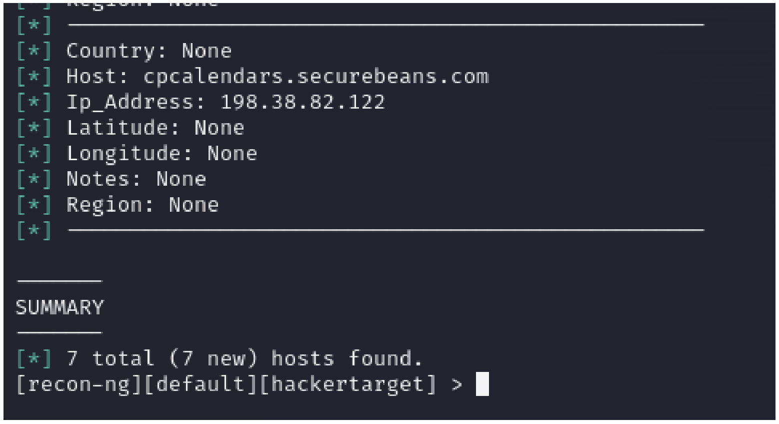


```
[recon-ng][default][hackertarget] > input

  +─────────────────+
  |  Module Inputs  |
  +─────────────────+
  | securebeans.com |
  +─────────────────+
```

Scan the target:

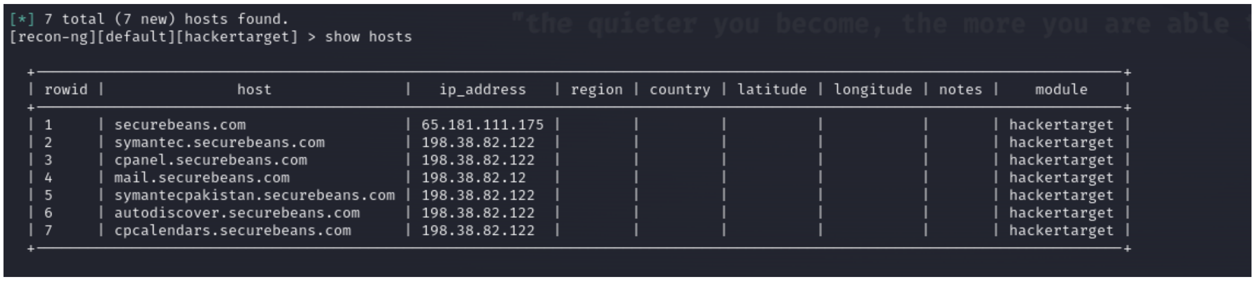


```
SOURCE ⇒ securebeans.com
[recon-ng][default][hackertarget] > run

───────────────
SECUREBEANS.COM
───────────────
[*] Country: None
[*] Host: securebeans.com
[*] Ip_Address: 65.181.111.175
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: symantec.securebeans.com
[*] Ip_Address: 198.38.82.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: cpanel.securebeans.com
[*] Ip_Address: 198.38.82.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: mail.securebeans.com
[*] Ip_Address: 198.38.82.12
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: symantecpakistan.securebeans.com
[*] Ip_Address: 198.38.82.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: autodiscover.securebeans.com
```



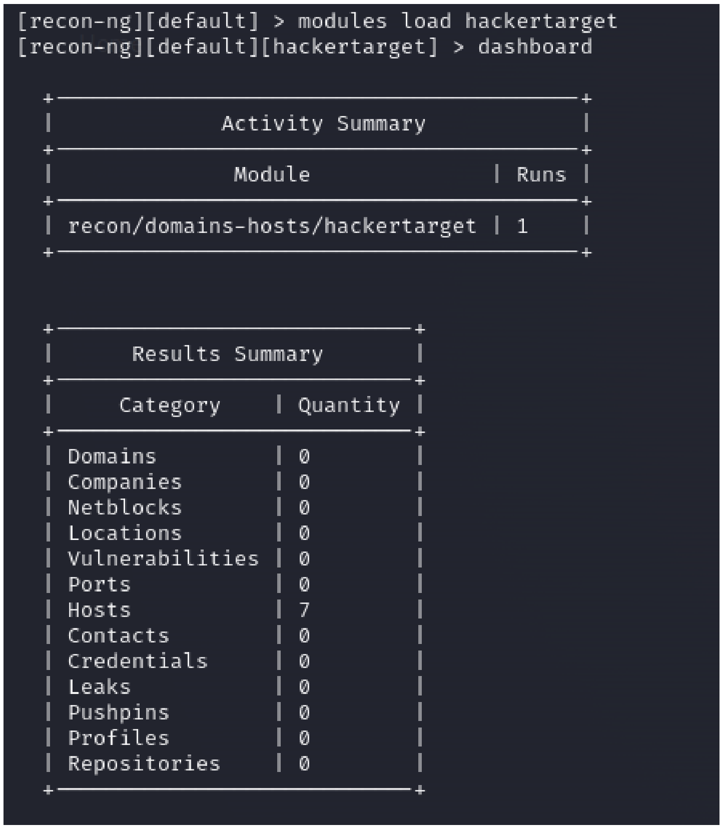
```
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: cpcalendars.securebeans.com
[*] Ip_Address: 198.38.82.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────

───────
SUMMARY
───────
[*] 7 total (7 new) hosts found.
[recon-ng][default][hackertarget] >
```

Show host:



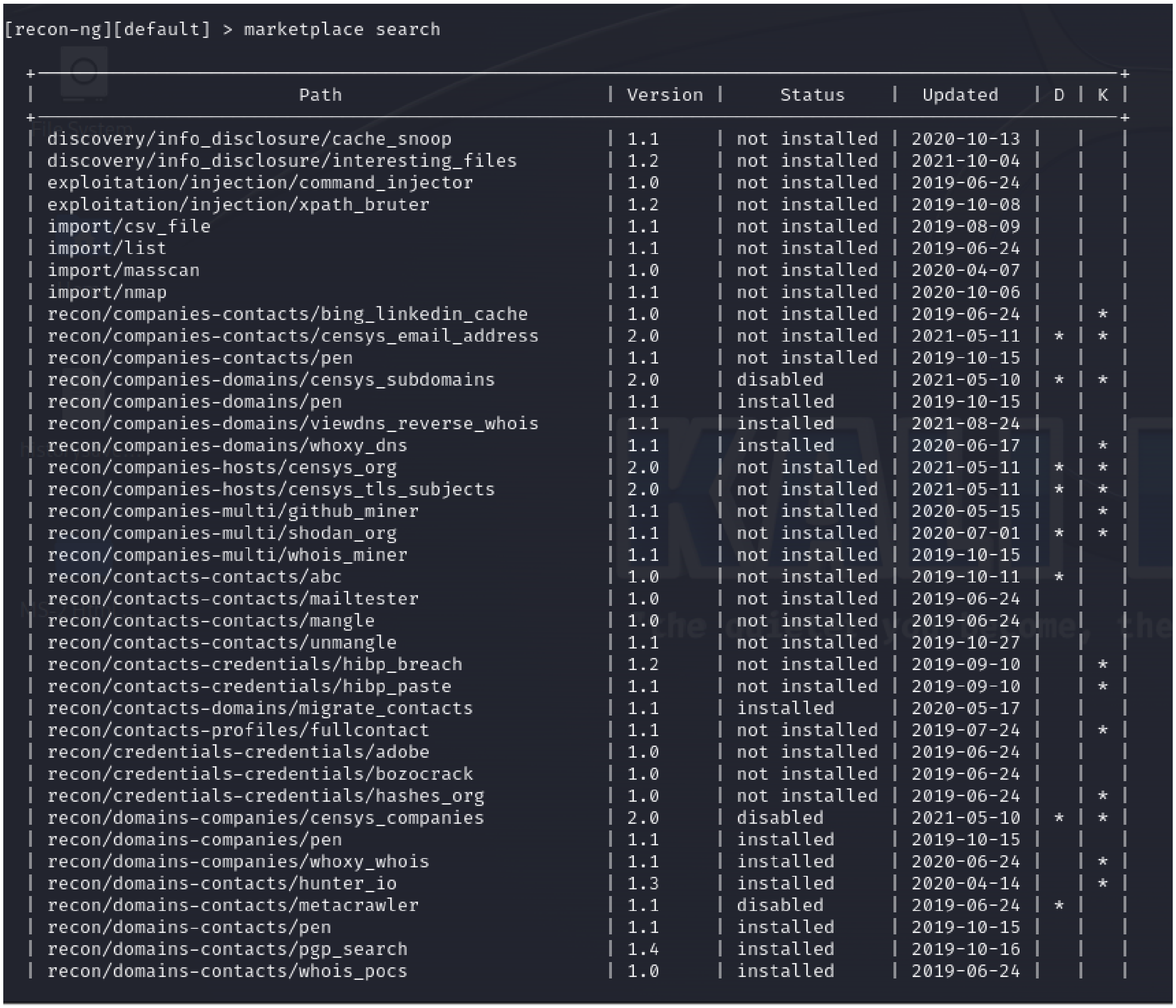
```
[*] 7 total (7 new) hosts found.
[recon-ng][default][hackertarget] > show hosts

  +----------------------------------------------------------------------------------------------------------------------------+
  | rowid |               host               |   ip_address   | region | country | latitude | longitude | notes |    module    |
  +----------------------------------------------------------------------------------------------------------------------------+
  | 1     | securebeans.com                  | 65.181.111.175 |        |         |          |           |       | hackertarget |
  | 2     | symantec.securebeans.com         | 198.38.82.122  |        |         |          |           |       | hackertarget |
  | 3     | cpanel.securebeans.com           | 198.38.82.122  |        |         |          |           |       | hackertarget |
  | 4     | mail.securebeans.com             | 198.38.82.12   |        |         |          |           |       | hackertarget |
  | 5     | symantecpakistan.securebeans.com | 198.38.82.122  |        |         |          |           |       | hackertarget |
  | 6     | autodiscover.securebeans.com     | 198.38.82.122  |        |         |          |           |       | hackertarget |
  | 7     | cpcalendars.securebeans.com      | 198.38.82.122  |        |         |          |           |       | hackertarget |
  +----------------------------------------------------------------------------------------------------------------------------+
```

Show Dashboard:



```
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > dashboard

  +-----------------------------------------+
  |             Activity Summary            |
  +-----------------------------------------+
  |              Module              | Runs |
  +-----------------------------------------+
  | recon/domains-hosts/hackertarget | 1    |
  +-----------------------------------------+


  +----------------------------+
  |       Results Summary      |
  +----------------------------+
  |     Category    | Quantity |
  +----------------------------+
  | Domains         | 0        |
  | Companies       | 0        |
  | Netblocks       | 0        |
  | Locations       | 0        |
  | Vulnerabilities | 0        |
  | Ports           | 0        |
  | Hosts           | 7        |
  | Contacts        | 0        |
  | Credentials     | 0        |
  | Leaks           | 0        |
  | Pushpins        | 0        |
  | Profiles        | 0        |
  | Repositories    | 0        |
  +----------------------------+
```

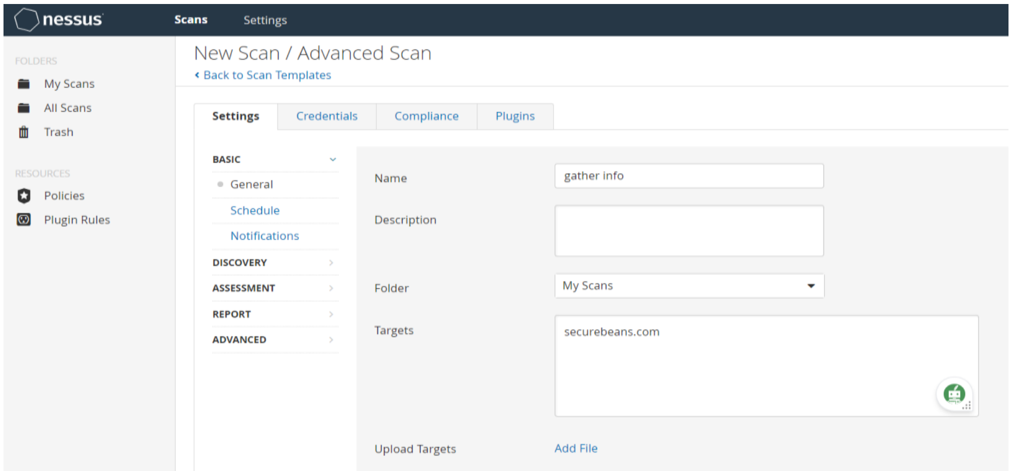
Run this cmd to install the different modules of recon –ng



```
[recon-ng][default] > marketplace search

  +-----------------------------------------------------------------------------------------------------+
  |                        Path                        | Version |     Status     |  Updated   | D | K |
  +-----------------------------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop              | 1.1     | not installed  | 2020-10-13 |   |   |
  | discovery/info_disclosure/interesting_files        | 1.2     | not installed  | 2021-10-04 |   |   |
  | exploitation/injection/command_injector            | 1.0     | not installed  | 2019-06-24 |   |   |
  | exploitation/injection/xpath_bruter                | 1.2     | not installed  | 2019-10-08 |   |   |
  | import/csv_file                                    | 1.1     | not installed  | 2019-08-09 |   |   |
  | import/list                                        | 1.1     | not installed  | 2019-06-24 |   |   |
  | import/masscan                                     | 1.0     | not installed  | 2020-04-07 |   |   |
  | import/nmap                                        | 1.1     | not installed  | 2020-10-06 |   |   |
  | recon/companies-contacts/bing_linkedin_cache       | 1.0     | not installed  | 2019-06-24 |   | * |
  | recon/companies-contacts/censys_email_address      | 2.0     | not installed  | 2021-05-11 | * | * |
  | recon/companies-contacts/pen                       | 1.1     | not installed  | 2019-10-15 |   |   |
  | recon/companies-domains/censys_subdomains          | 2.0     | disabled       | 2021-05-10 | * | * |
  | recon/companies-domains/pen                        | 1.1     | installed      | 2019-10-15 |   |   |
  | recon/companies-domains/viewdns_reverse_whois      | 1.1     | installed      | 2021-08-24 |   |   |
  | recon/companies-domains/whoxy_dns                  | 1.1     | installed      | 2020-06-17 |   | * |
  | recon/companies-hosts/censys_org                   | 2.0     | not installed  | 2021-05-11 | * | * |
  | recon/companies-hosts/censys_tls_subjects          | 2.0     | not installed  | 2021-05-11 | * | * |
  | recon/companies-multi/github_miner                 | 1.1     | not installed  | 2020-05-15 |   | * |
  | recon/companies-multi/shodan_org                   | 1.1     | not installed  | 2020-07-01 | * | * |
  | recon/companies-multi/whois_miner                  | 1.1     | not installed  | 2019-10-15 |   |   |
  | recon/contacts-contacts/abc                        | 1.0     | not installed  | 2019-10-11 | * |   |
  | recon/contacts-contacts/mailtester                 | 1.0     | not installed  | 2019-06-24 |   |   |
  | recon/contacts-contacts/mangle                     | 1.0     | not installed  | 2019-06-24 |   |   |
  | recon/contacts-contacts/unmangle                   | 1.1     | not installed  | 2019-10-27 |   |   |
  | recon/contacts-credentials/hibp_breach             | 1.2     | not installed  | 2019-09-10 |   | * |
  | recon/contacts-credentials/hibp_paste              | 1.1     | not installed  | 2019-09-10 |   | * |
  | recon/contacts-domains/migrate_contacts            | 1.1     | installed      | 2020-05-17 |   |   |
  | recon/contacts-profiles/fullcontact                | 1.1     | not installed  | 2019-07-24 |   | * |
  | recon/credentials-credentials/adobe                | 1.0     | not installed  | 2019-06-24 |   |   |
  | recon/credentials-credentials/bozocrack            | 1.0     | not installed  | 2019-06-24 |   |   |
  | recon/credentials-credentials/hashes_org           | 1.0     | not installed  | 2019-06-24 |   | * |
  | recon/domains-companies/censys_companies           | 2.0     | disabled       | 2021-05-10 | * | * |
  | recon/domains-companies/pen                        | 1.1     | installed      | 2019-10-15 |   |   |
  | recon/domains-companies/whoxy_whois                | 1.1     | installed      | 2020-06-24 |   | * |
  | recon/domains-contacts/hunter_io                   | 1.3     | installed      | 2020-04-14 |   | * |
  | recon/domains-contacts/metacrawler                 | 1.1     | disabled       | 2019-06-24 | * |   |
  | recon/domains-contacts/pen                         | 1.1     | installed      | 2019-10-15 |   |   |
  | recon/domains-contacts/pgp_search                  | 1.4     | installed      | 2019-10-16 |   |   |
  | recon/domains-contacts/whois_pocs                  | 1.0     | installed      | 2019-06-24 |   |   |
```

NESSUS:

- Create an Advance scan and enter the target



New Scan / Advanced Scan

Name: gather info

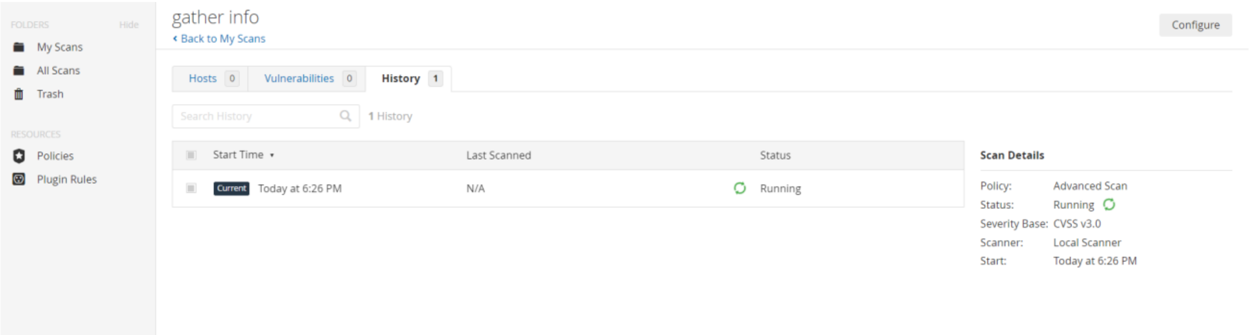
Description:

Folder: My Scans

Targets: securebeans.com

Upload Targets: Add File

- Scan is in process



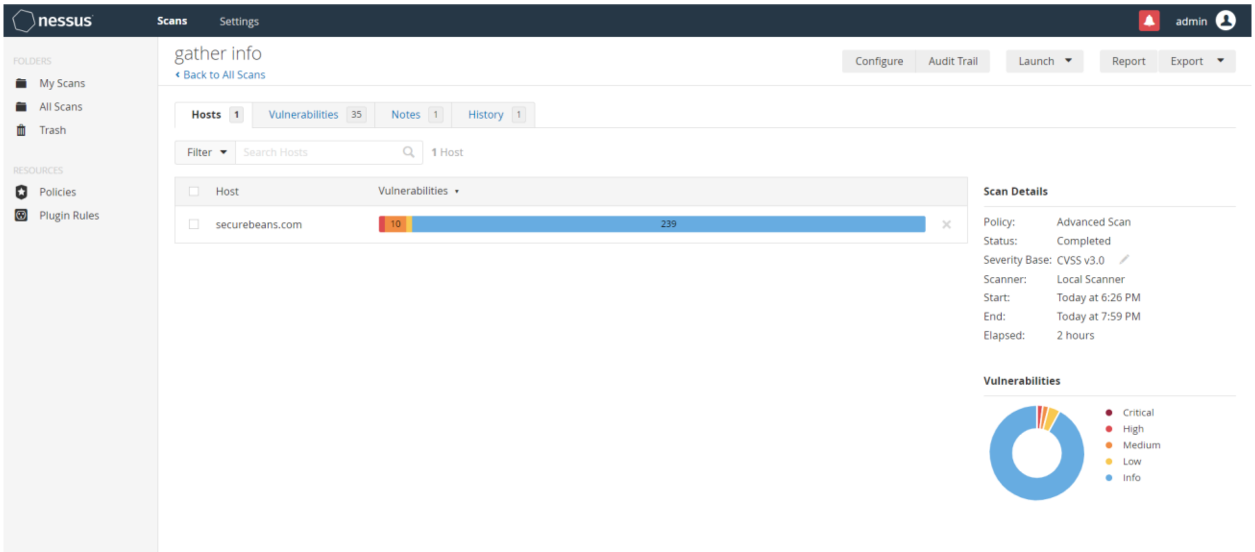
gather info

Start Time	Last Scanned	Status
Current Today at 6:26 PM	N/A	Running

Scan Details

Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:26 PM

- Scan complete:



gather info

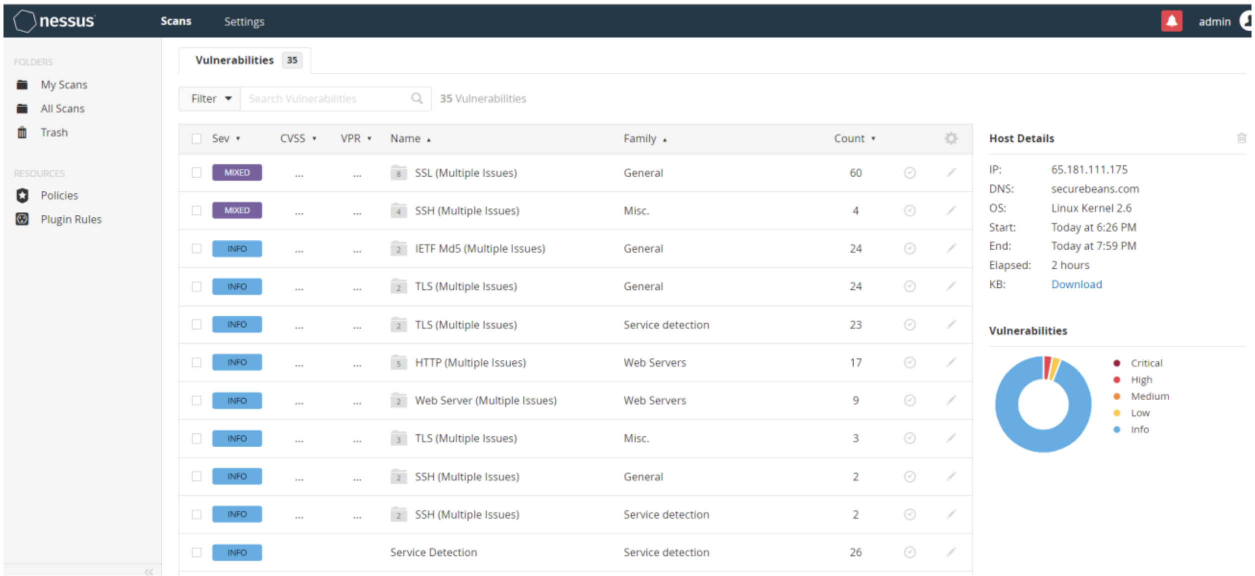
Host	Vulnerabilities
securebeans.com	10 239

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:26 PM
End: Today at 7:59 PM
Elapsed: 2 hours

Vulnerabilities

- Information of vulnerabilities:



Vulnerabilities 35

35 Vulnerabilities

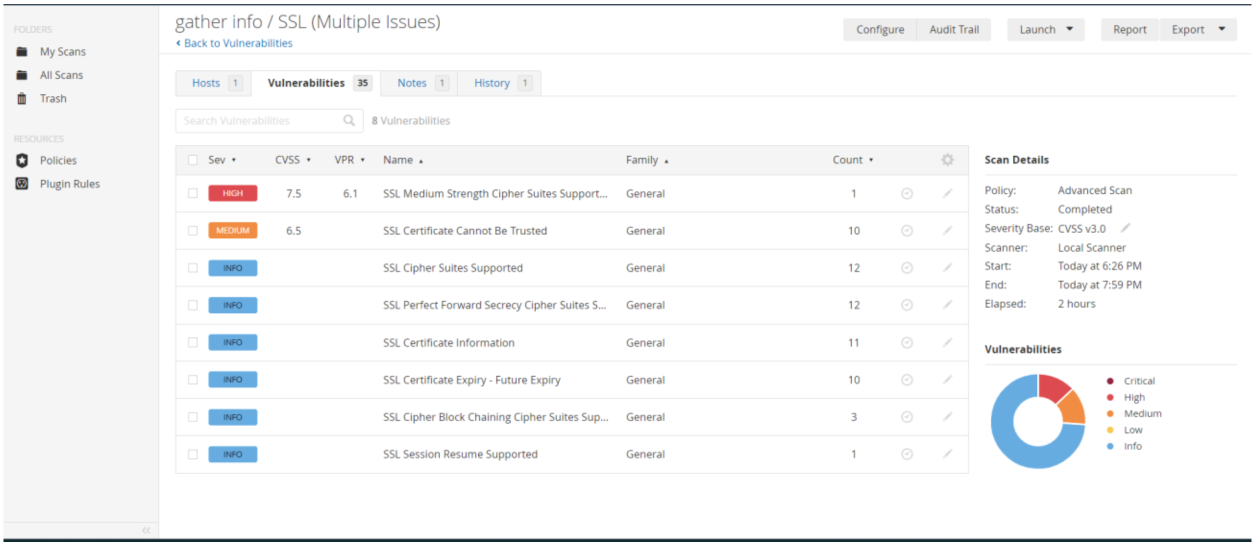
□	Sev	CVSS	VPR	Name	Family	Count
□	MIXED	...	...	8 SSL (Multiple Issues)	General	60
□	MIXED	...	...	4 SSH (Multiple Issues)	Misc.	4
□	INFO	...	...	2 IETF Md5 (Multiple Issues)	General	24
□	INFO	...	...	2 TLS (Multiple Issues)	General	24
□	INFO	...	...	2 TLS (Multiple Issues)	Service detection	23
□	INFO	...	...	5 HTTP (Multiple Issues)	Web Servers	17
□	INFO	...	...	2 Web Server (Multiple Issues)	Web Servers	9
□	INFO	...	...	3 TLS (Multiple Issues)	Misc.	3
□	INFO	...	...	2 SSH (Multiple Issues)	General	2
□	INFO	...	...	2 SSH (Multiple Issues)	Service detection	2
□	INFO			Service Detection	Service detection	26

Host Details

IP:	65.181.111.175
DNS:	securebeans.com
OS:	Linux Kernel 2.6
Start:	Today at 6:26 PM
End:	Today at 7:59 PM
Elapsed:	2 hours
KB:	Download

Vulnerabilities

- Exploitable vulnerabilities:



gather info / SSL (Multiple Issues)

‹ Back to Vulnerabilities

Hosts 1 | Vulnerabilities 35 | Notes 1 | History 1

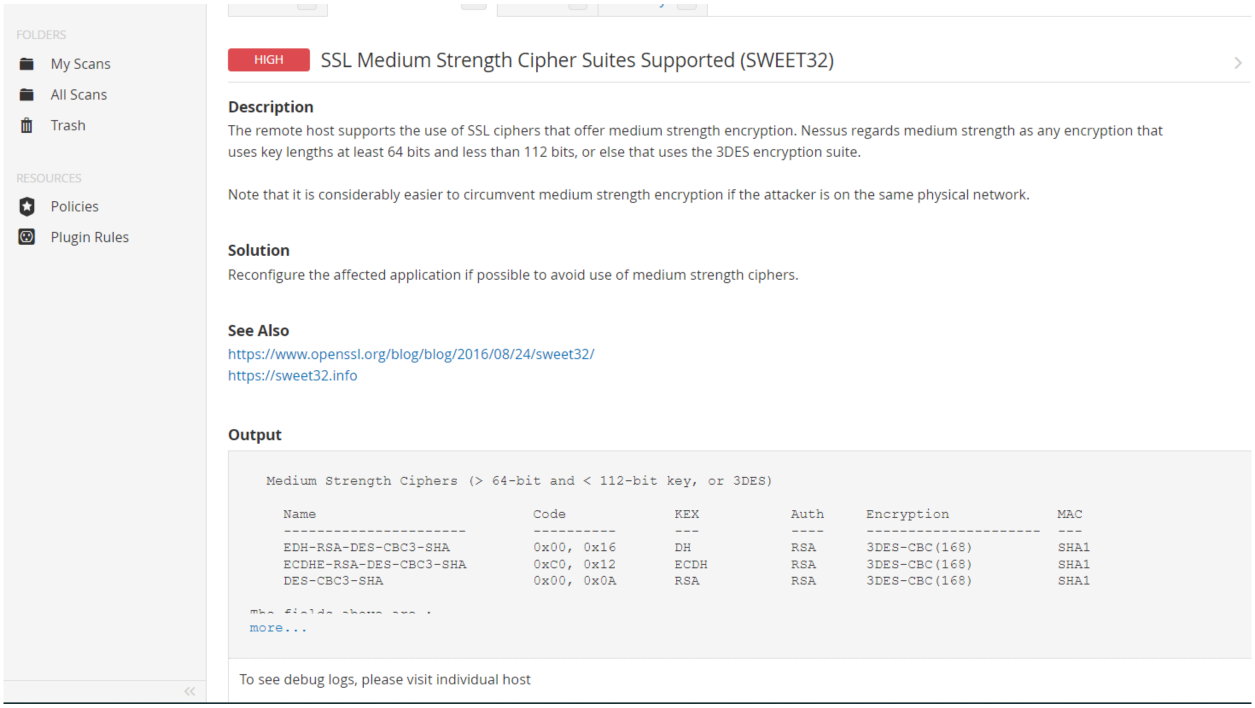
8 Vulnerabilities

□	Sev	CVSS	VPR	Name	Family	Count
□	HIGH	7.5	6.1	SSL Medium Strength Cipher Suites Support...	General	1
□	MEDIUM	6.5		SSL Certificate Cannot Be Trusted	General	10
□	INFO			SSL Cipher Suites Supported	General	12
□	INFO			SSL Perfect Forward Secrecy Cipher Suites S...	General	12
□	INFO			SSL Certificate Information	General	11
□	INFO			SSL Certificate Expiry - Future Expiry	General	10
□	INFO			SSL Cipher Block Chaining Cipher Suites Sup...	General	3
□	INFO			SSL Session Resume Supported	General	1

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:26 PM
End:	Today at 7:59 PM
Elapsed:	2 hours

Vulnerabilities



SSL Medium Strength Cipher Suites Supported (SWEET32)

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

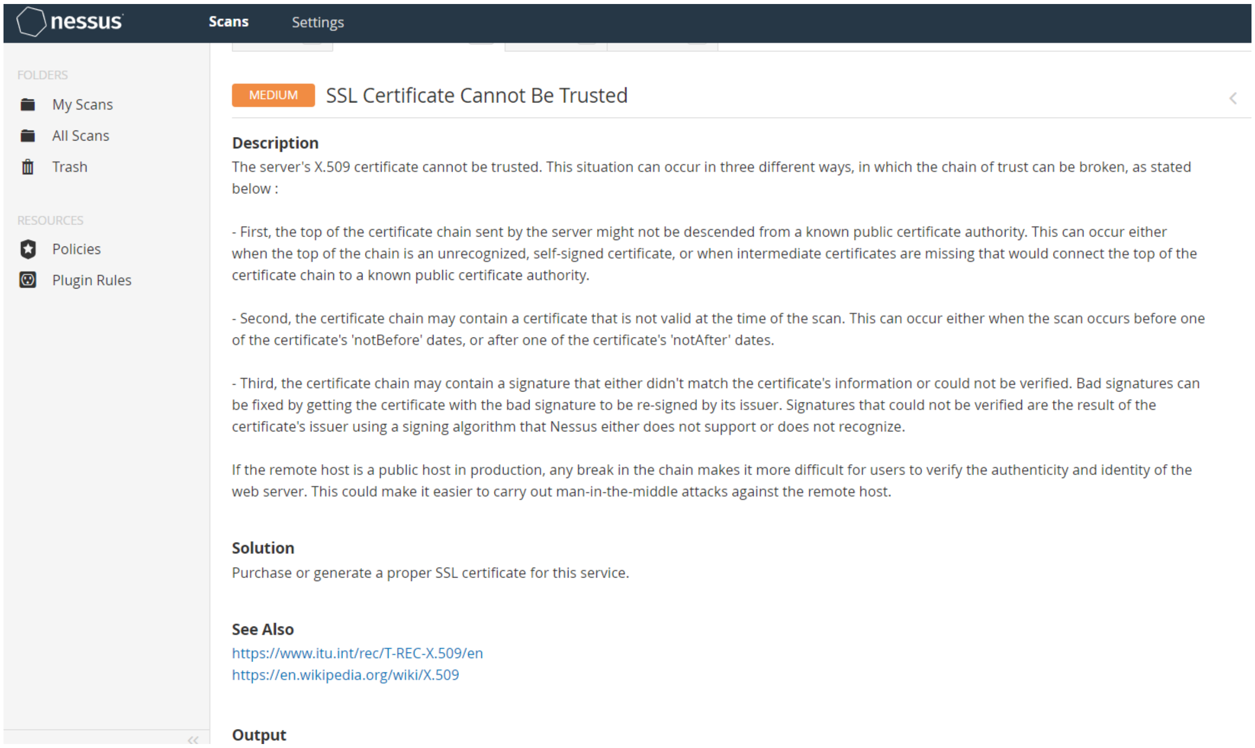
See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)          SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)          SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)          SHA1

The fields above are :
more...
```

To see debug logs, please visit individual host



SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

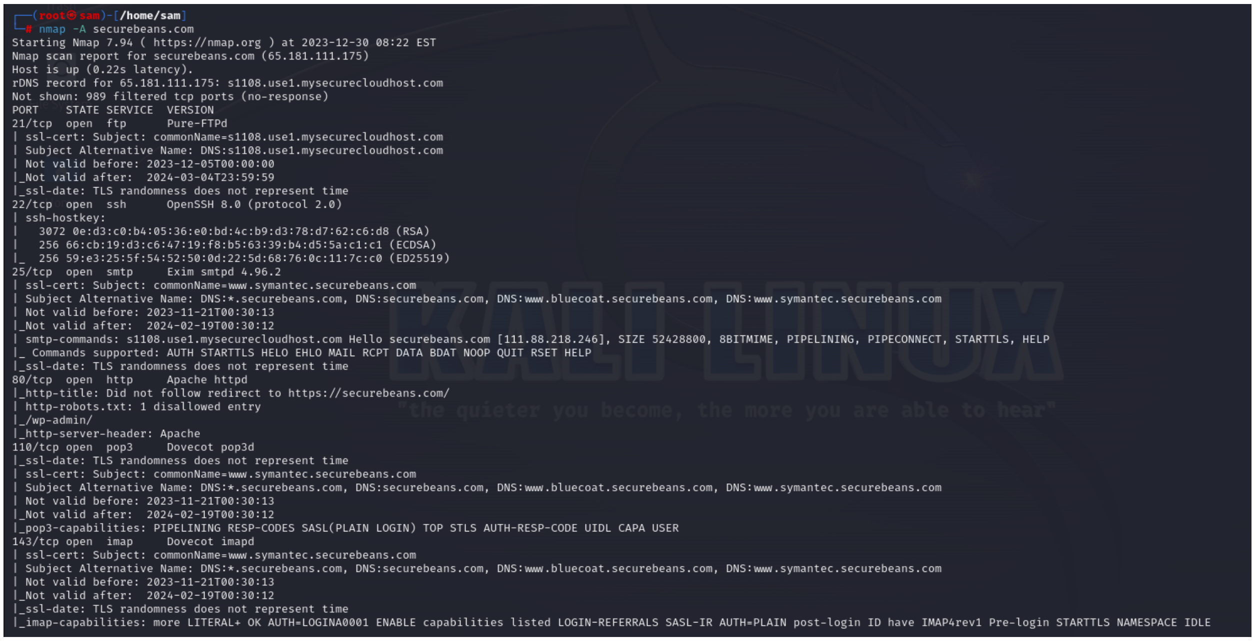
See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

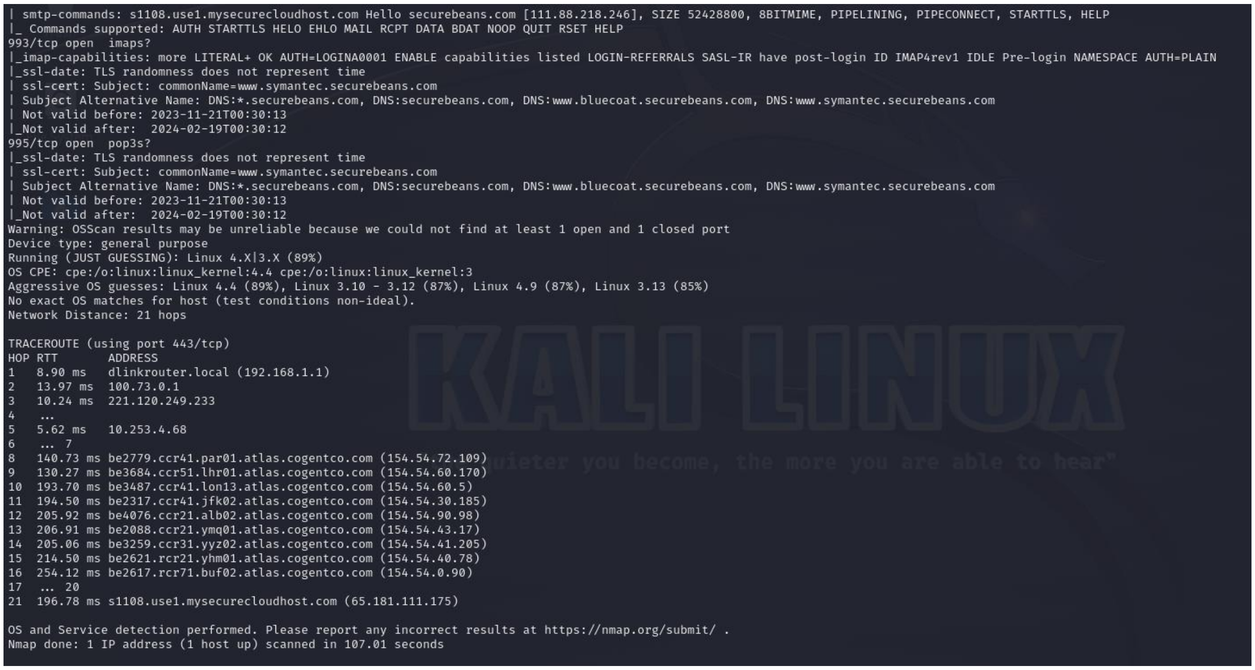
Output

NMAP:

Aggressive scan to gather more info:

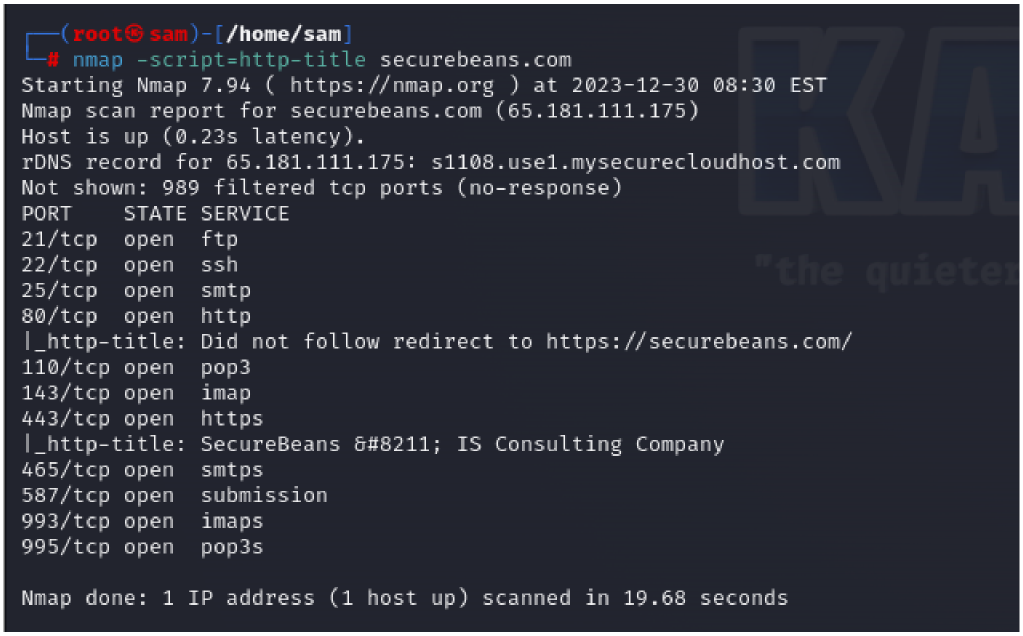


```
┌──(root㉿sam)-[/home/sam]
└─# nmap -A securebeans.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 08:22 EST
Nmap scan report for securebeans.com (65.181.111.175)
Host is up (0.22s latency).
rDNS record for 65.181.111.175: s1108.use1.mysecurecloudhost.com
Not shown: 989 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      Pure-FTPd
| ssl-cert: Subject: commonName=s1108.use1.mysecurecloudhost.com
| Subject Alternative Name: DNS:s1108.use1.mysecurecloudhost.com
| Not valid before: 2023-12-05T00:00:00
|_Not valid after:  2024-03-04T23:59:59
|_ssl-date: TLS randomness does not represent time
22/tcp  open  ssh      OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 0e:d3:c0:b4:05:36:e0:bd:4c:b9:d3:78:d7:62:c6:d8 (RSA)
|   256 66:cb:19:d3:c6:47:19:f8:b5:63:39:b4:d5:5a:c1:c1 (ECDSA)
|_  256 59:e3:25:5f:54:52:50:0d:22:5d:68:76:0c:11:7c:c0 (ED25519)
25/tcp  open  smtp     Exim smtpd 4.96.2
| ssl-cert: Subject: commonName=www.symantec.securebeans.com
| Subject Alternative Name: DNS:*.securebeans.com, DNS:securebeans.com, DNS:www.bluecoat.securebeans.com, DNS:www.symantec.securebeans.com
| Not valid before: 2023-11-21T00:30:13
|_Not valid after:  2024-02-19T00:30:12
| smtp-commands: s1108.use1.mysecurecloudhost.com Hello securebeans.com [111.88.218.246], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http     Apache httpd
|_http-title: Did not follow redirect to https://securebeans.com/
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache
110/tcp open  pop3     Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=www.symantec.securebeans.com
| Subject Alternative Name: DNS:*.securebeans.com, DNS:securebeans.com, DNS:www.bluecoat.securebeans.com, DNS:www.symantec.securebeans.com
| Not valid before: 2023-11-21T00:30:13
|_Not valid after:  2024-02-19T00:30:12
|_pop3-capabilities: PIPELINING RESP-CODES SASL(PLAIN LOGIN) TOP STLS AUTH-RESP-CODE UIDL CAPA USER
143/tcp open  imap     Dovecot imapd
| ssl-cert: Subject: commonName=www.symantec.securebeans.com
| Subject Alternative Name: DNS:*.securebeans.com, DNS:securebeans.com, DNS:www.bluecoat.securebeans.com, DNS:www.symantec.securebeans.com
| Not valid before: 2023-11-21T00:30:13
|_Not valid after:  2024-02-19T00:30:12
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: more LITERAL+ OK AUTH=LOGINA0001 ENABLE capabilities listed LOGIN-REFERRALS SASL-IR AUTH=PLAIN post-login ID have IMAP4rev1 Pre-login STARTTLS NAMESPACE IDLE
```



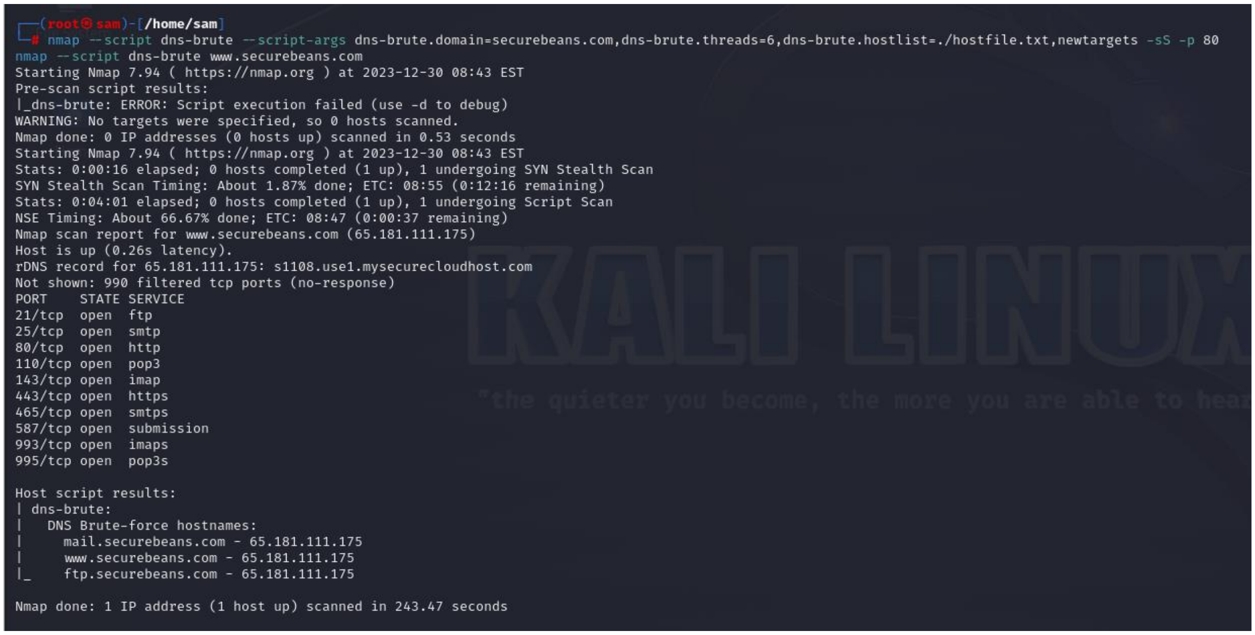
```
| smtp-commands: s1108.use1.mysecurecloudhost.com Hello securebeans.com [111.88.218.246], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
993/tcp open  imaps?
|_imap-capabilities: more LITERAL+ OK AUTH=LOGINA0001 ENABLE capabilities listed LOGIN-REFERRALS SASL-IR have post-login ID IMAP4rev1 IDLE Pre-login NAMESPACE AUTH=PLAIN
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=www.symantec.securebeans.com
| Subject Alternative Name: DNS:*.securebeans.com, DNS:securebeans.com, DNS:www.bluecoat.securebeans.com, DNS:www.symantec.securebeans.com
| Not valid before: 2023-11-21T00:30:13
|_Not valid after:  2024-02-19T00:30:12
995/tcp open  pop3s?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=www.symantec.securebeans.com
| Subject Alternative Name: DNS:*.securebeans.com, DNS:securebeans.com, DNS:www.bluecoat.securebeans.com, DNS:www.symantec.securebeans.com
| Not valid before: 2023-11-21T00:30:13
|_Not valid after:  2024-02-19T00:30:12
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|3.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 4.4 (89%), Linux 3.10 - 3.12 (87%), Linux 4.9 (87%), Linux 3.13 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 21 hops

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   8.90 ms   dlinkrouter.local (192.168.1.1)
2   13.97 ms  100.73.0.1
3   10.24 ms  221.120.249.233
4   ...
5   5.62 ms   10.253.4.68
6   ... 7
8   140.73 ms be2779.ccr41.par01.atlas.cogentco.com (154.54.72.109)
9   130.27 ms be3684.ccr51.lhr01.atlas.cogentco.com (154.54.60.170)
10  193.70 ms be3487.ccr41.lon13.atlas.cogentco.com (154.54.60.5)
11  194.50 ms be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
12  205.92 ms be4076.ccr21.alb02.atlas.cogentco.com (154.54.90.98)
13  206.91 ms be2088.ccr21.ymq01.atlas.cogentco.com (154.54.43.17)
14  205.06 ms be3259.ccr31.yyz02.atlas.cogentco.com (154.54.41.205)
15  214.50 ms be2621.rcr21.yhm01.atlas.cogentco.com (154.54.40.78)
16  254.12 ms be2617.rcr71.buf02.atlas.cogentco.com (154.54.0.90)
17  ... 20
21  196.78 ms s1108.use1.mysecurecloudhost.com (65.181.111.175)

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 107.01 seconds
```

To get the HTTP headers of web services:

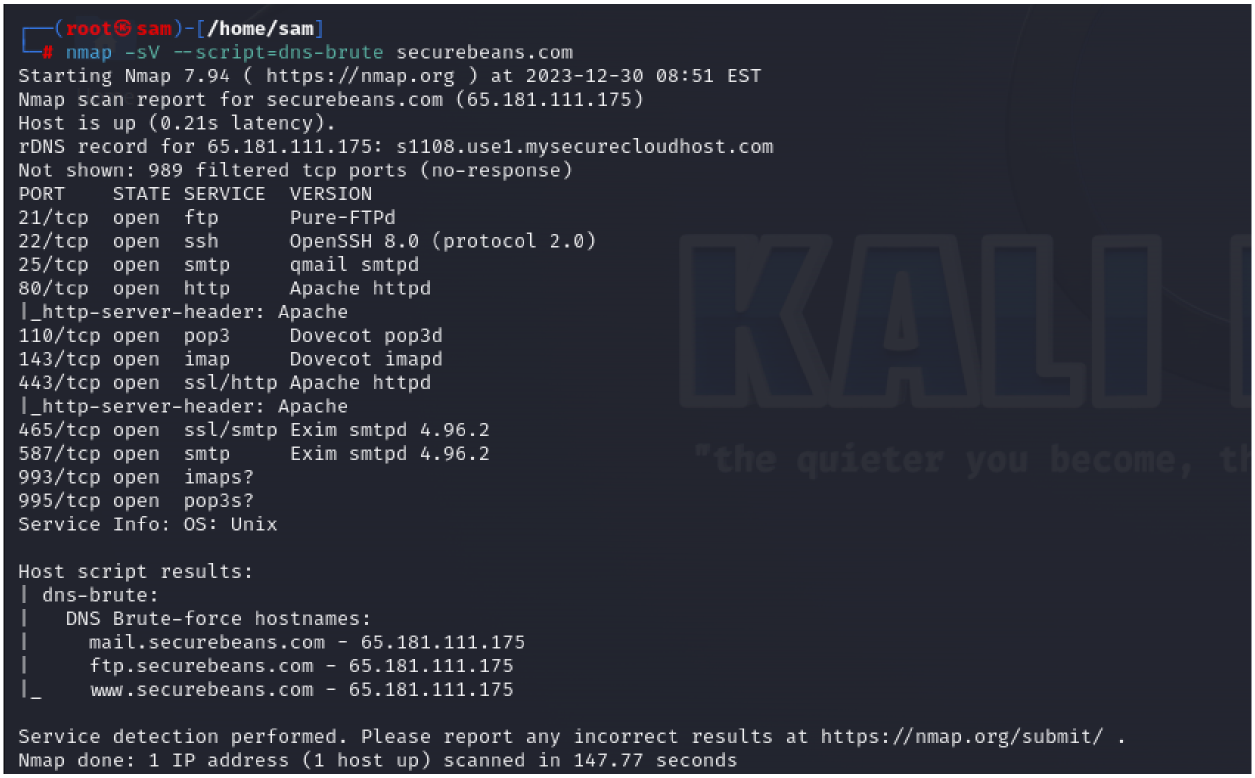


```
┌──(root㉿sam)-[/home/sam]
└─# nmap -script=http-title securebeans.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 08:30 EST
Nmap scan report for securebeans.com (65.181.111.175)
Host is up (0.23s latency).
rDNS record for 65.181.111.175: s1108.use1.mysecurecloudhost.com
Not shown: 989 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
|_http-title: Did not follow redirect to https://securebeans.com/
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
|_http-title: SecureBeans &#8211; IS Consulting Company
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 19.68 seconds
```

DNS Brute

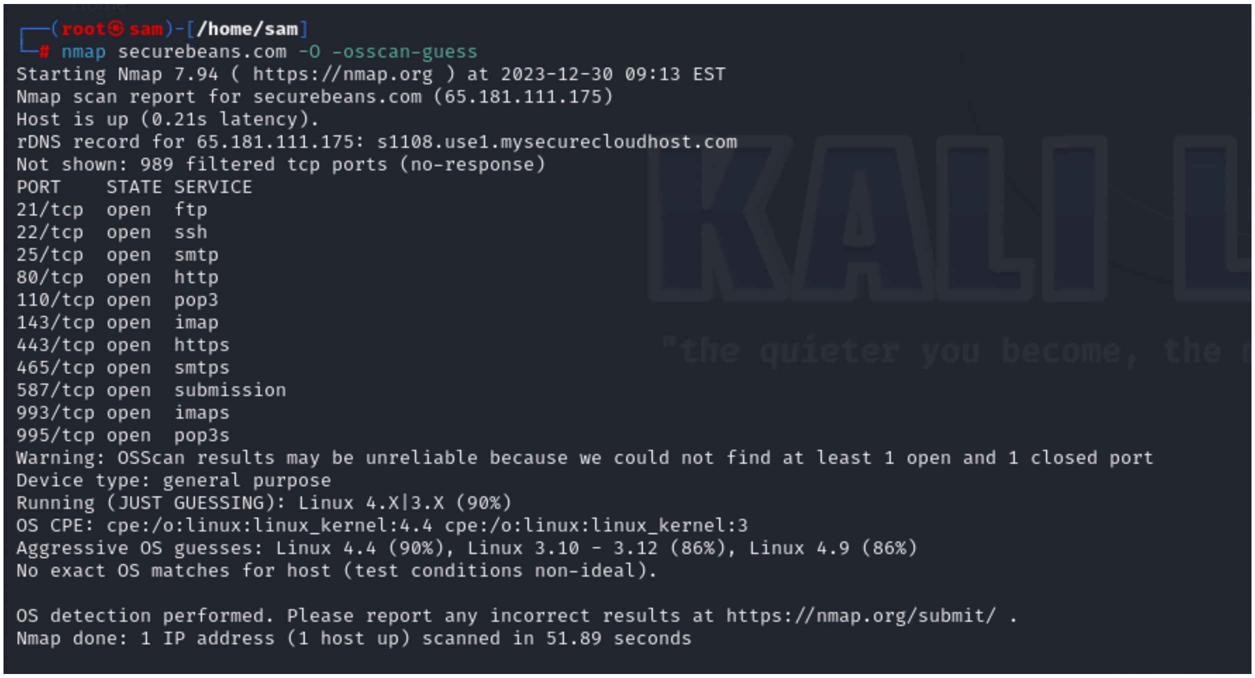


```
┌──(root㉿sam)-[/home/sam]
└─# nmap --script dns-brute --script-args dns-brute.domain=securebeans.com,dns-brute.threads=6,dns-brute.hostlist=./hostfile.txt,newtargets -sS -p 80
nmap --script dns-brute www.securebeans.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 08:43 EST
Pre-scan script results:
|_dns-brute: ERROR: Script execution failed (use -d to debug)
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.53 seconds
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 08:43 EST
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.87% done; ETC: 08:55 (0:12:16 remaining)
Stats: 0:04:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 66.67% done; ETC: 08:47 (0:00:37 remaining)
Nmap scan report for www.securebeans.com (65.181.111.175)
Host is up (0.26s latency).
rDNS record for 65.181.111.175: s1108.use1.mysecurecloudhost.com
Not shown: 990 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     mail.securebeans.com - 65.181.111.175
|     www.securebeans.com - 65.181.111.175
|_    ftp.securebeans.com - 65.181.111.175

Nmap done: 1 IP address (1 host up) scanned in 243.47 seconds
```



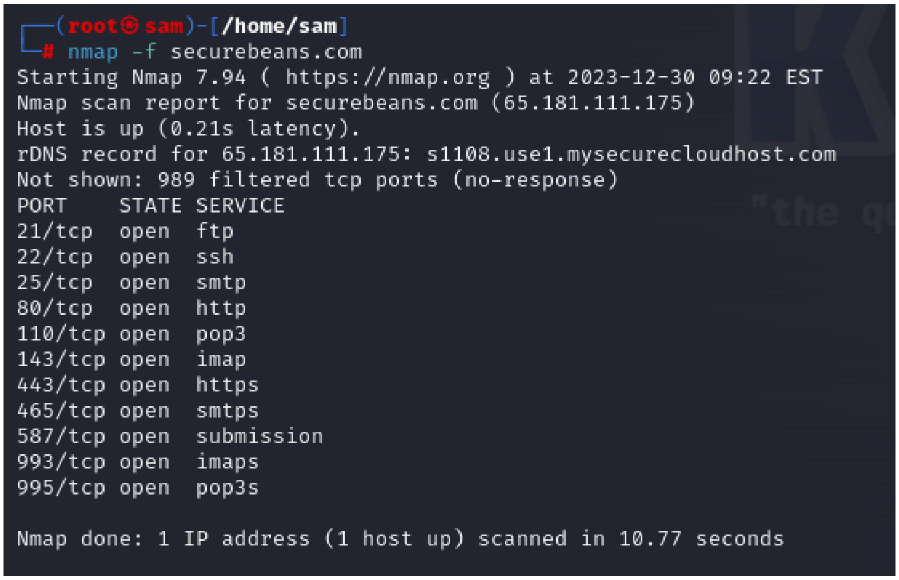
```
┌──(root㉿sam)-[/home/sam]
└─# nmap -sV --script=dns-brute securebeans.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 08:51 EST
Nmap scan report for securebeans.com (65.181.111.175)
Host is up (0.21s latency).
rDNS record for 65.181.111.175: s1108.use1.mysecurecloudhost.com
Not shown: 989 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      Pure-FTPd
22/tcp  open  ssh      OpenSSH 8.0 (protocol 2.0)
25/tcp  open  smtp     qmail smtpd
80/tcp  open  http     Apache httpd
|_http-server-header: Apache
110/tcp open  pop3     Dovecot pop3d
143/tcp open  imap     Dovecot imapd
443/tcp open  ssl/http Apache httpd
|_http-server-header: Apache
465/tcp open  ssl/smtp Exim smtpd 4.96.2
587/tcp open  smtp     Exim smtpd 4.96.2
993/tcp open  imaps?
995/tcp open  pop3s?
Service Info: OS: Unix

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     mail.securebeans.com - 65.181.111.175
|     ftp.securebeans.com - 65.181.111.175
|_    www.securebeans.com - 65.181.111.175

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.77 seconds
```

Aggressive OS detection



```
┌──(root㉿sam)-[/home/sam]
└─# nmap securebeans.com -O -osscan-guess
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 09:13 EST
Nmap scan report for securebeans.com (65.181.111.175)
Host is up (0.21s latency).
rDNS record for 65.181.111.175: s1108.use1.mysecurecloudhost.com
Not shown: 989 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|3.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 4.4 (90%), Linux 3.10 - 3.12 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.89 seconds
```

Domain Spoofing:



```
┌──(root㉿sam)-[/home/sam]
└─# nmap -f securebeans.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-30 09:22 EST
Nmap scan report for securebeans.com (65.181.111.175)
Host is up (0.21s latency).
rDNS record for 65.181.111.175: s1108.use1.mysecurecloudhost.com
Not shown: 989 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 10.77 seconds
```