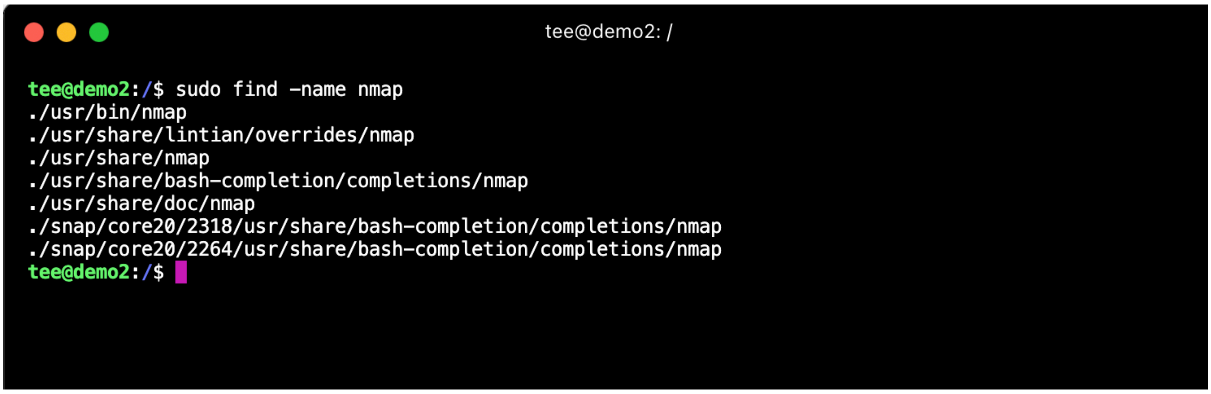
Vulnerability Scanning Using Nmap

To complete this vulnerability scanning exercise, the first step is to download the nmap application via the Linux CLI. To achieve this , enter the following command: sudo apt install nmap.

The GIT software is also needed to complete this exercise. To install this software via the CLI, enter the following command: sudo apt install git.

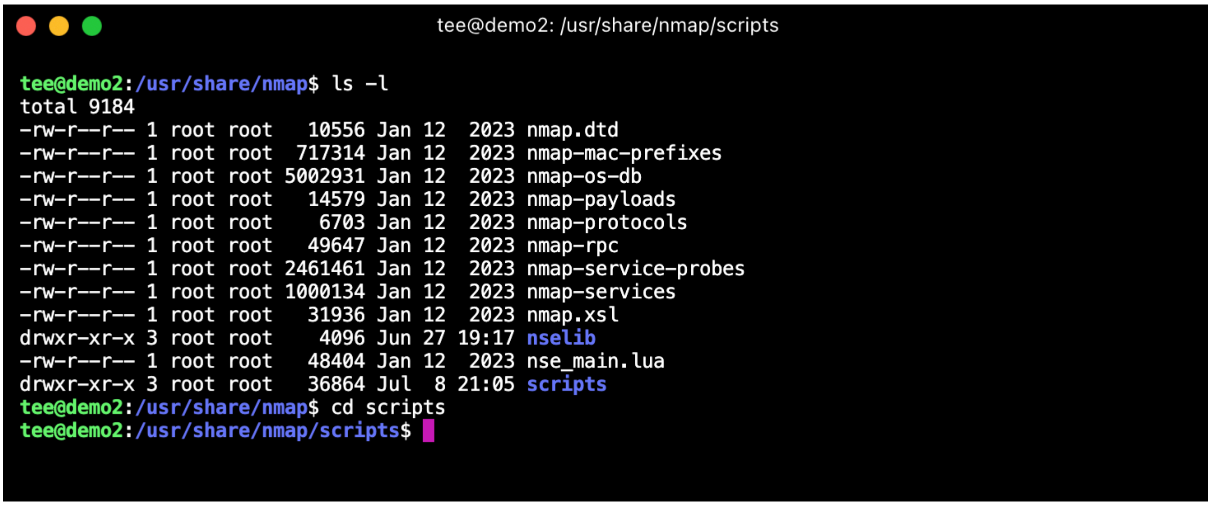
Since I have both GIT and nmap installed, I'll move on to the next step.

The next step is to identify what folder nmap is in. To do this, enter the following command in the CLI: sudo find -name nmap. This is also illustrated below:



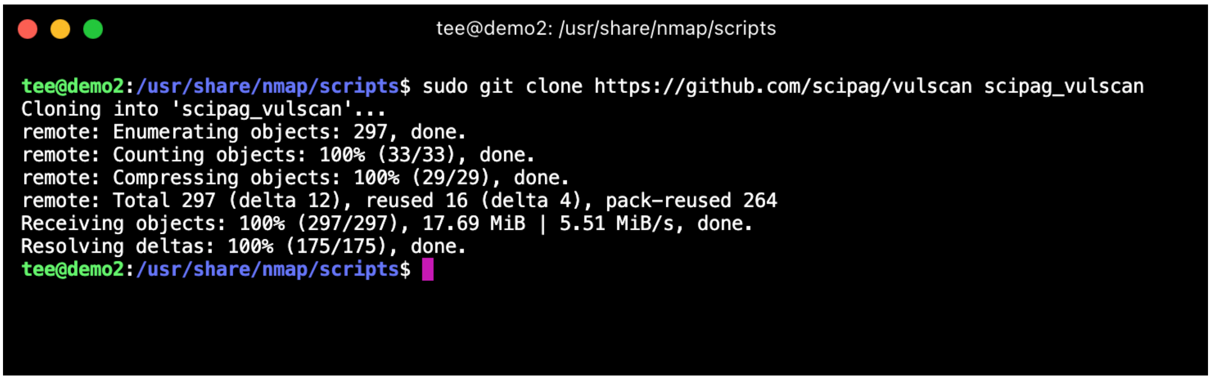
```
tee@demo2:/$ sudo find -name nmap
./usr/bin/nmap
./usr/share/lintian/overrides/nmap
./usr/share/nmap
./usr/share/bash-completion/completions/nmap
./usr/share/doc/nmap
./snap/core20/2318/usr/share/bash-completion/completions/nmap
./snap/core20/2264/usr/share/bash-completion/completions/nmap
tee@demo2:/$
```

This indicates that nmap is in the usr/share/nmap folder. The next step is to locate and clone the github repository into the scripts folder. To do this, use the ls -l command to list the contents of the usr/share/nmap folder. Once the scripts directory is located, navigate into it using the cd command.



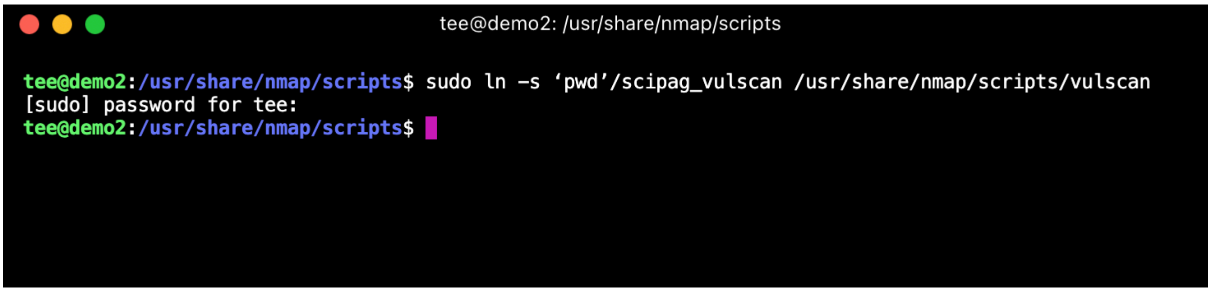
```
tee@demo2:/usr/share/nmap$ ls -l
total 9184
-rw-r--r-- 1 root root   10556 Jan 12  2023 nmap.dtd
-rw-r--r-- 1 root root  717314 Jan 12  2023 nmap-mac-prefixes
-rw-r--r-- 1 root root 5002931 Jan 12  2023 nmap-os-db
-rw-r--r-- 1 root root   14579 Jan 12  2023 nmap-payloads
-rw-r--r-- 1 root root    6703 Jan 12  2023 nmap-protocols
-rw-r--r-- 1 root root   49647 Jan 12  2023 nmap-rpc
-rw-r--r-- 1 root root 2461461 Jan 12  2023 nmap-service-probes
-rw-r--r-- 1 root root 1000134 Jan 12  2023 nmap-services
-rw-r--r-- 1 root root   31936 Jan 12  2023 nmap.xsl
drwxr-xr-x 3 root root    4096 Jun 27 19:17 nselib
-rw-r--r-- 1 root root   48404 Jan 12  2023 nse_main.lua
drwxr-xr-x 3 root root   36864 Jul  8 21:05 scripts
tee@demo2:/usr/share/nmap$ cd scripts
tee@demo2:/usr/share/nmap/scripts$
```

When in the scripts directory, clone the GITHub repository using the 'sudo git clone <github url> <name of destination folder>' command. This is illustrated below:



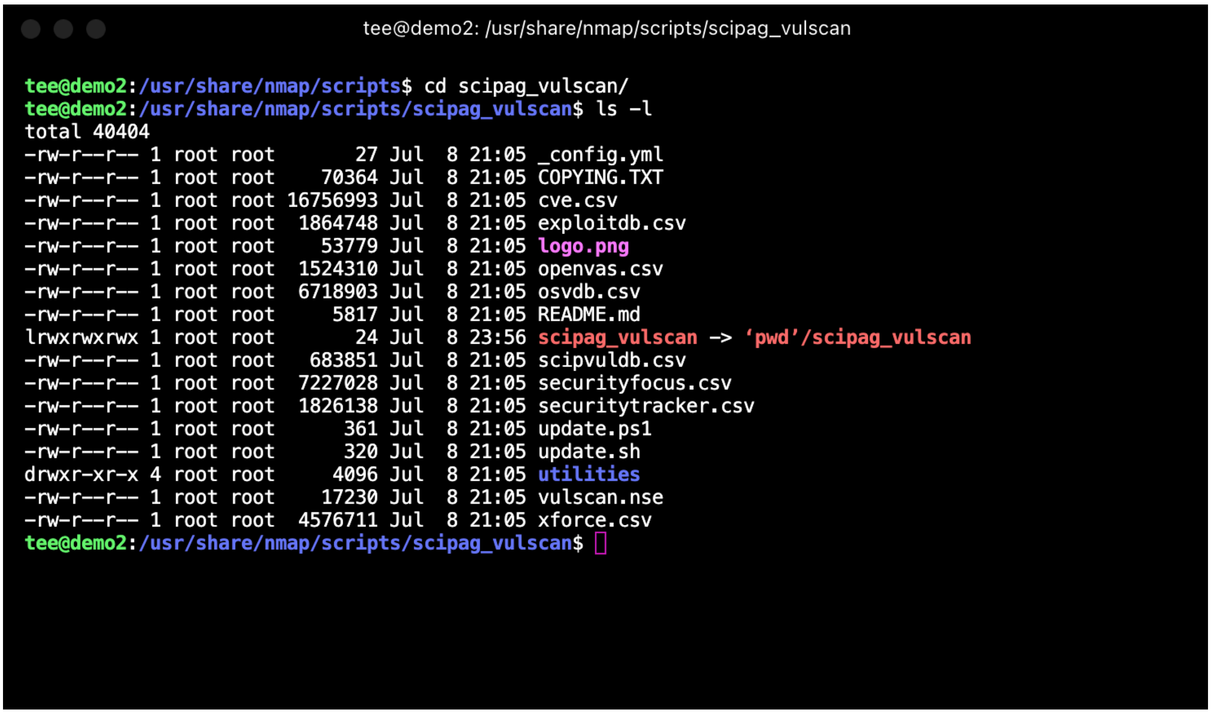
```
tee@demo2:/usr/share/nmap/scripts$ sudo git clone https://github.com/scipag/vulscan scipag_vulscan
Cloning into 'scipag_vulscan'...
remote: Enumerating objects: 297, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (29/29), done.
remote: Total 297 (delta 12), reused 16 (delta 4), pack-reused 264
Receiving objects: 100% (297/297), 17.69 MiB | 5.51 MiB/s, done.
Resolving deltas: 100% (175/175), done.
tee@demo2:/usr/share/nmap/scripts$
```

After successfully cloning the git repo, the next step is to generate a symbolic link in order to facilitate running the downloaded script from anywhere. The command to execute this is: sudo ln -s 'pwd'/scipag_vulscan /usr/share/nmap/scripts/vulscan. The command execution is illustrated below:



```
tee@demo2:/usr/share/nmap/scripts$ sudo ln -s 'pwd'/scipag_vulscan /usr/share/nmap/scripts/vulscan
[sudo] password for tee:
tee@demo2:/usr/share/nmap/scripts$
```

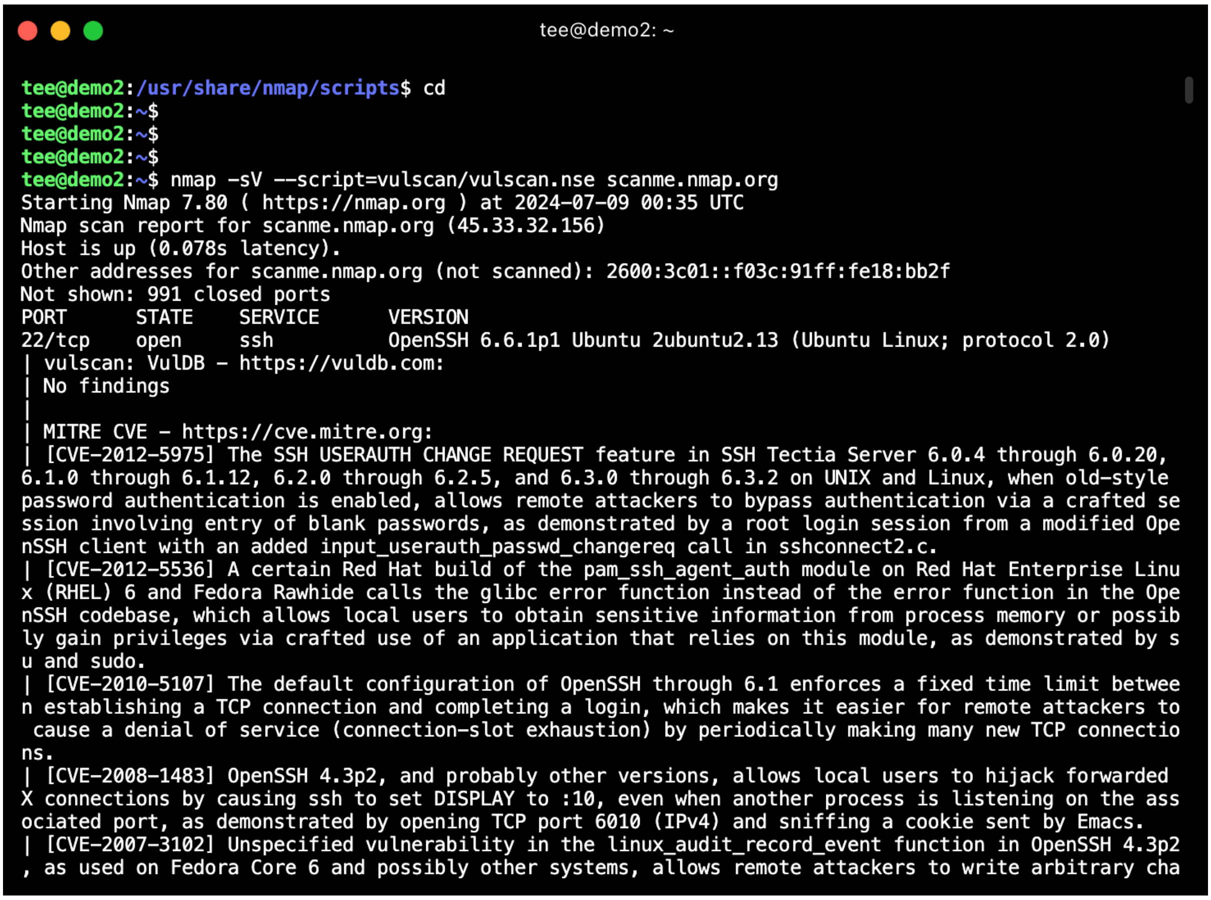
It is good practice to navigate into the destination folder and verify that all the required data is in it. To do this, navigate into the scipag_vulscan folder and list its content using the following commands: 'cd scipag_vulscan', followed by the 'ls -l' command. This is illustrated below:



```
tee@demo2:/usr/share/nmap/scripts$ cd scipag_vulscan/
tee@demo2:/usr/share/nmap/scripts/scipag_vulscan$ ls -l
total 40404
-rw-r--r-- 1 root root       27 Jul  8 21:05 _config.yml
-rw-r--r-- 1 root root    70364 Jul  8 21:05 COPYING.TXT
-rw-r--r-- 1 root root 16756993 Jul  8 21:05 cve.csv
-rw-r--r-- 1 root root  1864748 Jul  8 21:05 exploitdb.csv
-rw-r--r-- 1 root root    53779 Jul  8 21:05 logo.png
-rw-r--r-- 1 root root  1524310 Jul  8 21:05 openvas.csv
-rw-r--r-- 1 root root  6718903 Jul  8 21:05 osvdb.csv
-rw-r--r-- 1 root root     5817 Jul  8 21:05 README.md
lrwxrwxrwx 1 root root       24 Jul  8 23:56 scipag_vulscan -> 'pwd'/scipag_vulscan
-rw-r--r-- 1 root root   683851 Jul  8 21:05 scipvuldb.csv
-rw-r--r-- 1 root root  7227028 Jul  8 21:05 securityfocus.csv
-rw-r--r-- 1 root root  1826138 Jul  8 21:05 securitytracker.csv
-rw-r--r-- 1 root root      361 Jul  8 21:05 update.ps1
-rw-r--r-- 1 root root      320 Jul  8 21:05 update.sh
drwxr-xr-x 4 root root     4096 Jul  8 21:05 utilities
-rw-r--r-- 1 root root    17230 Jul  8 21:05 vulscan.nse
-rw-r--r-- 1 root root  4576711 Jul  8 21:05 xforce.csv
tee@demo2:/usr/share/nmap/scripts/scipag_vulscan$
```

Upon confirmation that the destination folder carries the required data, we can proceed with the vulnerability scanning.

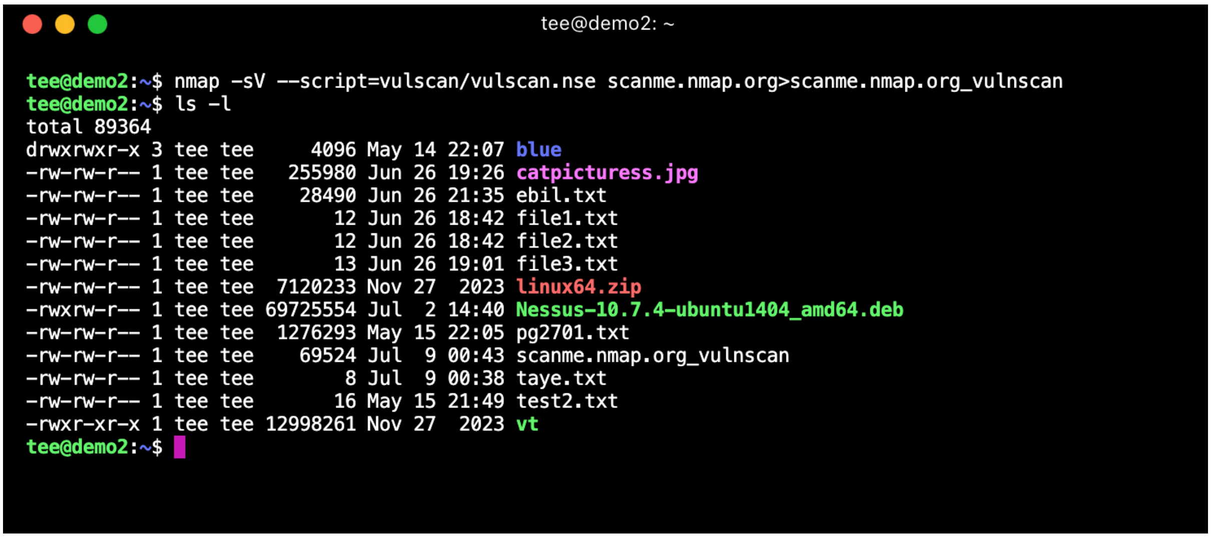
The first step in doing this is navigating back to the home folder using the ‘cd’ command. Once this is done, we can proceed with the scanning using the following command: nmap -sV —script=vulscan/vulscan.nse <desired location>. The first location to be scanned will be scanme.nmap.org. This is illustrated below:



tee@demo2: ~

```
tee@demo2:/usr/share/nmap/scripts$ cd
tee@demo2:~$
tee@demo2:~$
tee@demo2:~$
tee@demo2:~$ nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-09 00:35 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.078s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2012-5975] The SSH USERAUTH CHANGE REQUEST feature in SSH Tectia Server 6.0.4 through 6.0.20,
6.1.0 through 6.1.12, 6.2.0 through 6.2.5, and 6.3.0 through 6.3.2 on UNIX and Linux, when old-style
password authentication is enabled, allows remote attackers to bypass authentication via a crafted se
ssion involving entry of blank passwords, as demonstrated by a root login session from a modified Ope
nSSH client with an added input_userauth_passwd_changereq call in sshconnect2.c.
| [CVE-2012-5536] A certain Red Hat build of the pam_ssh_agent_auth module on Red Hat Enterprise Linu
x (RHEL) 6 and Fedora Rawhide calls the glibc error function instead of the error function in the Ope
nSSH codebase, which allows local users to obtain sensitive information from process memory or possib
ly gain privileges via crafted use of an application that relies on this module, as demonstrated by s
u and sudo.
| [CVE-2010-5107] The default configuration of OpenSSH through 6.1 enforces a fixed time limit betwee
n establishing a TCP connection and completing a login, which makes it easier for remote attackers to
 cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connectio
ns.
| [CVE-2008-1483] OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded
X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the ass
ociated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.
| [CVE-2007-3102] Unspecified vulnerability in the linux_audit_record_event function in OpenSSH 4.3p2
, as used on Fedora Core 6 and possibly other systems, allows remote attackers to write arbitrary cha
```

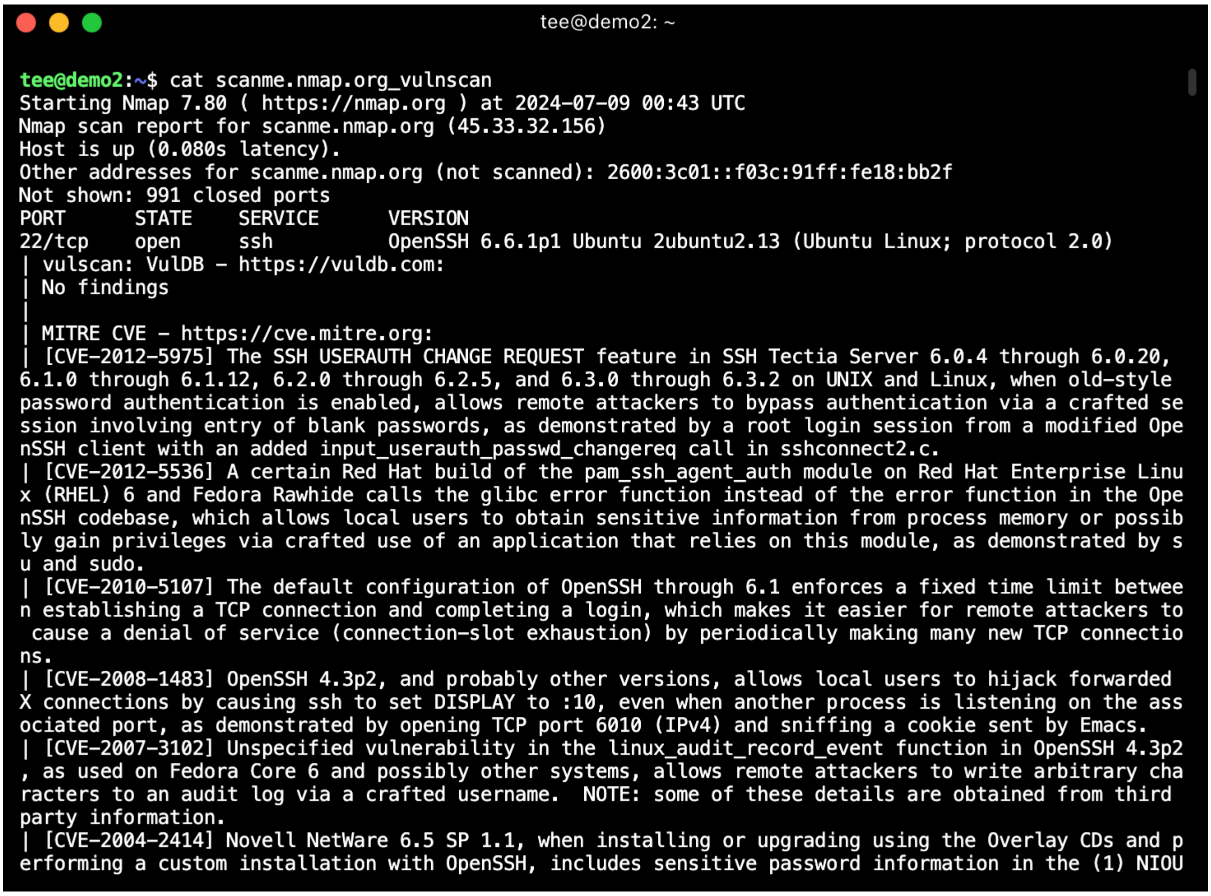
The output of this scan is quite voluminous, so it is best to direct it into a file by using the Linux redirection command; >. The command will read as follows: nmap -sV —script=vulscan/vulscan.nse <desired location> > <name of file to redirect output to>. This is illustrated below using the command: nmap -sV -–script=vulscan/vulscan.nse scanme.nmap.org>scanme.nmap.org_vulnscan.



tee@demo2: ~

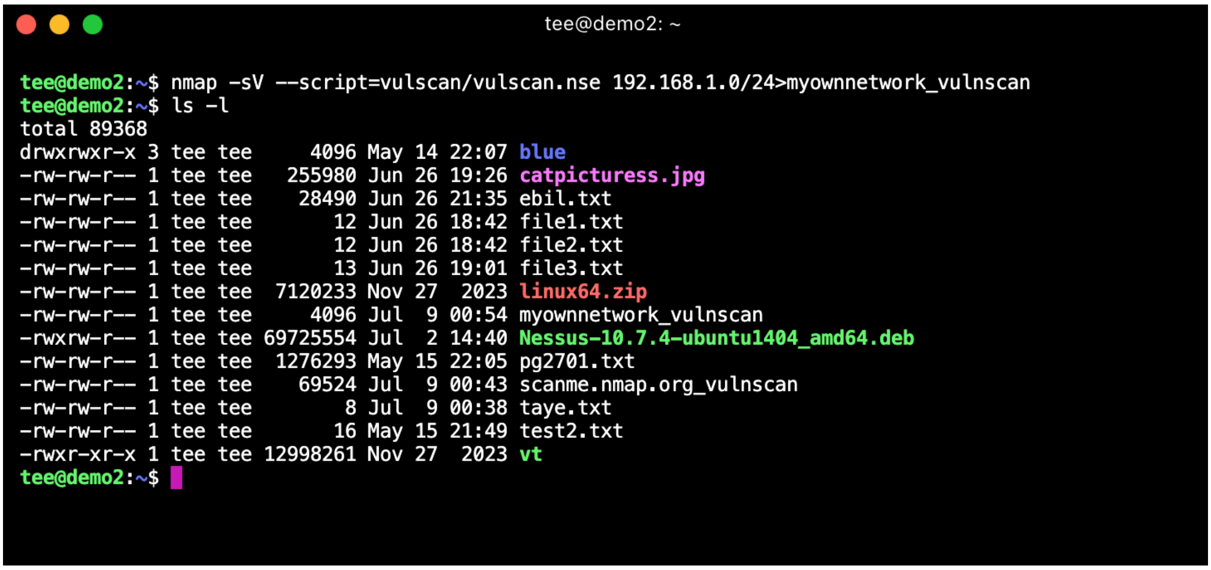
```
tee@demo2:~$ nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org>scanme.nmap.org_vulnscan
tee@demo2:~$ ls -l
total 89364
drwxrwxr-x 3 tee tee     4096 May 14 22:07 blue
-rw-rw-r-- 1 tee tee   255980 Jun 26 19:26 catpicturess.jpg
-rw-rw-r-- 1 tee tee    28490 Jun 26 21:35 ebil.txt
-rw-rw-r-- 1 tee tee       12 Jun 26 18:42 file1.txt
-rw-rw-r-- 1 tee tee       12 Jun 26 18:42 file2.txt
-rw-rw-r-- 1 tee tee       13 Jun 26 19:01 file3.txt
-rw-rw-r-- 1 tee tee  7120233 Nov 27  2023 linux64.zip
-rwxrw-r-- 1 tee tee 69725554 Jul  2 14:40 Nessus-10.7.4-ubuntu1404_amd64.deb
-rw-rw-r-- 1 tee tee  1276293 May 15 22:05 pg2701.txt
-rw-rw-r-- 1 tee tee    69524 Jul  9 00:43 scanme.nmap.org_vulnscan
-rw-rw-r-- 1 tee tee        8 Jul  9 00:38 taye.txt
-rw-rw-r-- 1 tee tee       16 May 15 21:49 test2.txt
-rwxr-xr-x 1 tee tee 12998261 Nov 27  2023 vt
tee@demo2:~$ 
```

To view the result of the scan contained in the newly created scanme.nmap.org_vulnscan file, use the 'cat' command as illustrated below:



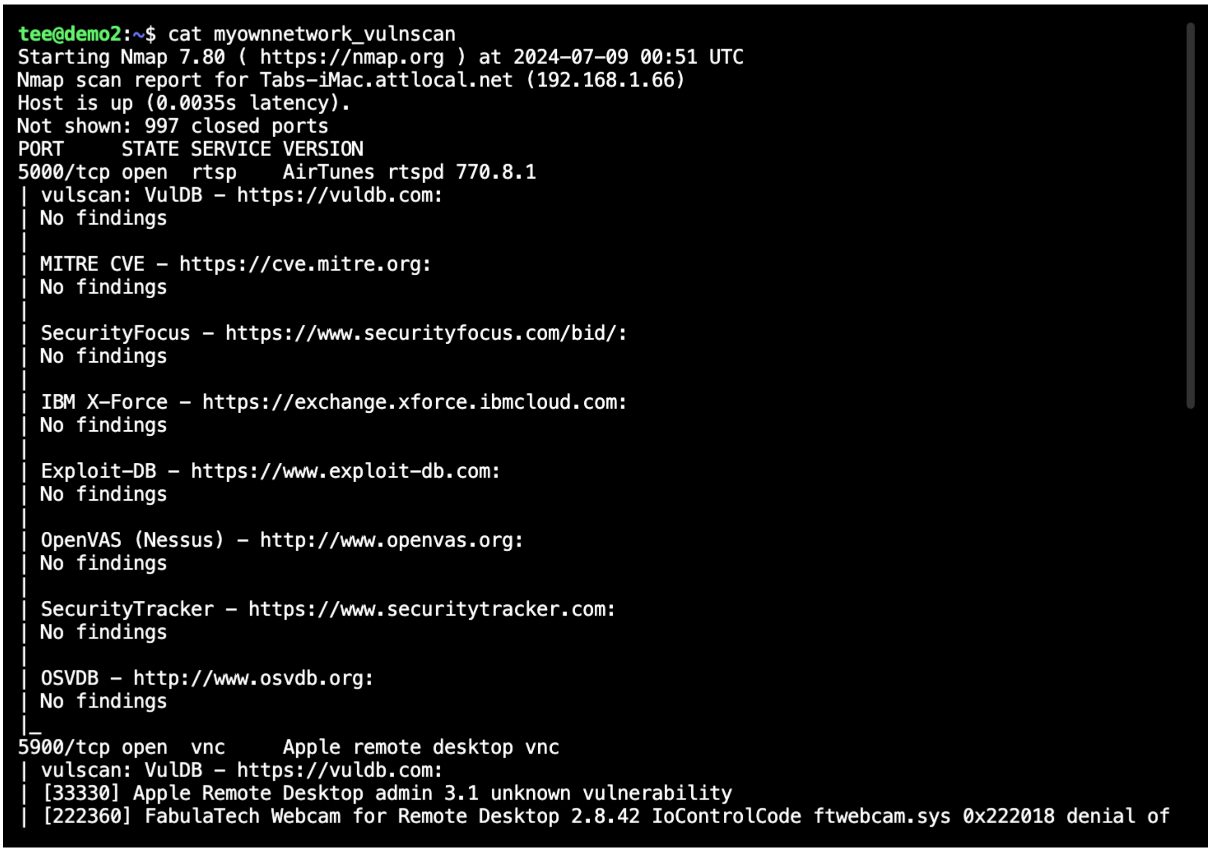
```
tee@demo2:~$ cat scanme.nmap.org_vulnscan
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-09 00:43 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.080s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2012-5975] The SSH USERAUTH CHANGE REQUEST feature in SSH Tectia Server 6.0.4 through 6.0.20,
6.1.0 through 6.1.12, 6.2.0 through 6.2.5, and 6.3.0 through 6.3.2 on UNIX and Linux, when old-style
password authentication is enabled, allows remote attackers to bypass authentication via a crafted se
ssion involving entry of blank passwords, as demonstrated by a root login session from a modified Ope
nSSH client with an added input_userauth_passwd_changereq call in sshconnect2.c.
| [CVE-2012-5536] A certain Red Hat build of the pam_ssh_agent_auth module on Red Hat Enterprise Linu
x (RHEL) 6 and Fedora Rawhide calls the glibc error function instead of the error function in the Ope
nSSH codebase, which allows local users to obtain sensitive information from process memory or possib
ly gain privileges via crafted use of an application that relies on this module, as demonstrated by s
u and sudo.
| [CVE-2010-5107] The default configuration of OpenSSH through 6.1 enforces a fixed time limit betwee
n establishing a TCP connection and completing a login, which makes it easier for remote attackers to
 cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connectio
ns.
| [CVE-2008-1483] OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded
X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the ass
ociated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.
| [CVE-2007-3102] Unspecified vulnerability in the linux_audit_record_event function in OpenSSH 4.3p2
, as used on Fedora Core 6 and possibly other systems, allows remote attackers to write arbitrary cha
racters to an audit log via a crafted username.  NOTE: some of these details are obtained from third
party information.
| [CVE-2004-2414] Novell NetWare 6.5 SP 1.1, when installing or upgrading using the Overlay CDs and p
erforming a custom installation with OpenSSH, includes sensitive password information in the (1) NIOU
```

Redirecting the results of a vulnerability scan helps with reading, editing, and processing the output generated. The just scanned network was created for educational purposes. In task 2, I will be scanning my home network for vulnerabilities and will redirect the output to a file named 'myownnetwork_vulnscan. This is illustrated below:



```
tee@demo2:~$ nmap -sV --script=vulscan/vulscan.nse 192.168.1.0/24>myownnetwork_vulnscan
tee@demo2:~$ ls -l
total 89368
drwxrwxr-x 3 tee tee     4096 May 14 22:07 blue
-rw-rw-r-- 1 tee tee   255980 Jun 26 19:26 catpicturess.jpg
-rw-rw-r-- 1 tee tee    28490 Jun 26 21:35 ebil.txt
-rw-rw-r-- 1 tee tee       12 Jun 26 18:42 file1.txt
-rw-rw-r-- 1 tee tee       12 Jun 26 18:42 file2.txt
-rw-rw-r-- 1 tee tee       13 Jun 26 19:01 file3.txt
-rw-rw-r-- 1 tee tee  7120233 Nov 27  2023 linux64.zip
-rw-rw-r-- 1 tee tee     4096 Jul  9 00:54 myownnetwork_vulnscan
-rwxrw-r-- 1 tee tee 69725554 Jul  2 14:40 Nessus-10.7.4-ubuntu1404_amd64.deb
-rw-rw-r-- 1 tee tee  1276293 May 15 22:05 pg2701.txt
-rw-rw-r-- 1 tee tee    69524 Jul  9 00:43 scanme.nmap.org_vulnscan
-rw-rw-r-- 1 tee tee        8 Jul  9 00:38 taye.txt
-rw-rw-r-- 1 tee tee       16 May 15 21:49 test2.txt
-rwxr-xr-x 1 tee tee 12998261 Nov 27  2023 vt
tee@demo2:~$
```

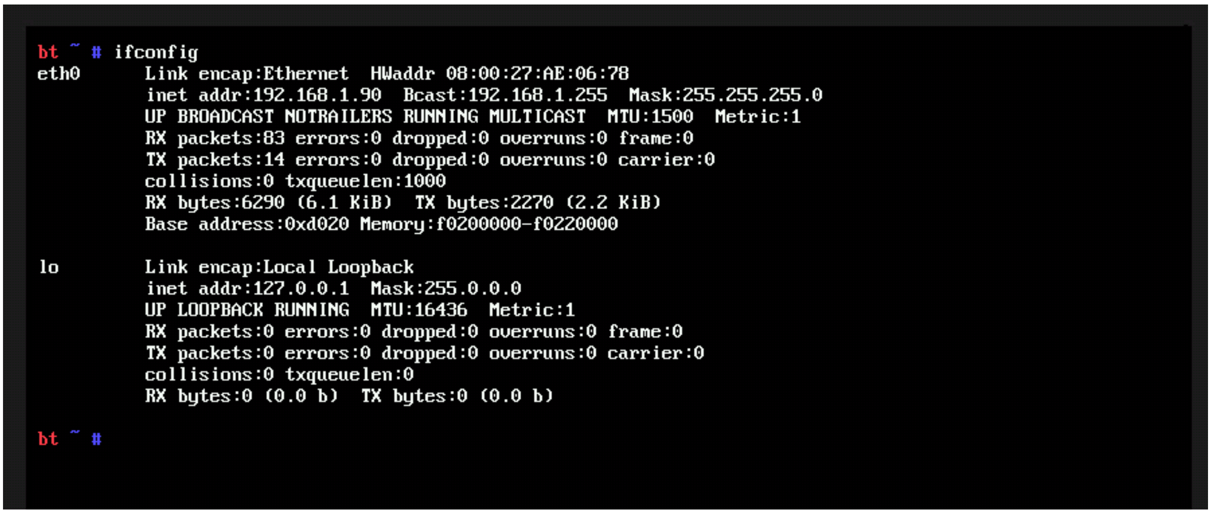
‘Catting’ the file ‘myownnetwork_vulnscan’ will reveal the results of the vulnerability scan I just carried out on my home network. This is shown below:



```
tee@demo2:~$ cat myownnetwork_vulnscan
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-09 00:51 UTC
Nmap scan report for Tabs-iMac.attlocal.net (192.168.1.66)
Host is up (0.0035s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
5000/tcp open  rtsp    AirTunes rtspd 770.8.1
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| No findings
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| No findings
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| No findings
|
| Exploit-DB - https://www.exploit-db.com:
| No findings
|
| OpenVAS (Nessus) - http://www.openvas.org:
| No findings
|
| SecurityTracker - https://www.securitytracker.com:
| No findings
|
| OSVDB - http://www.osvdb.org:
| No findings
|_
5900/tcp open  vnc     Apple remote desktop vnc
| vulscan: VulDB - https://vuldb.com:
| [33330] Apple Remote Desktop admin 3.1 unknown vulnerability
| [222360] FabulaTech Webcam for Remote Desktop 2.8.42 IoControlCode ftwebcam.sys 0x222018 denial of
```

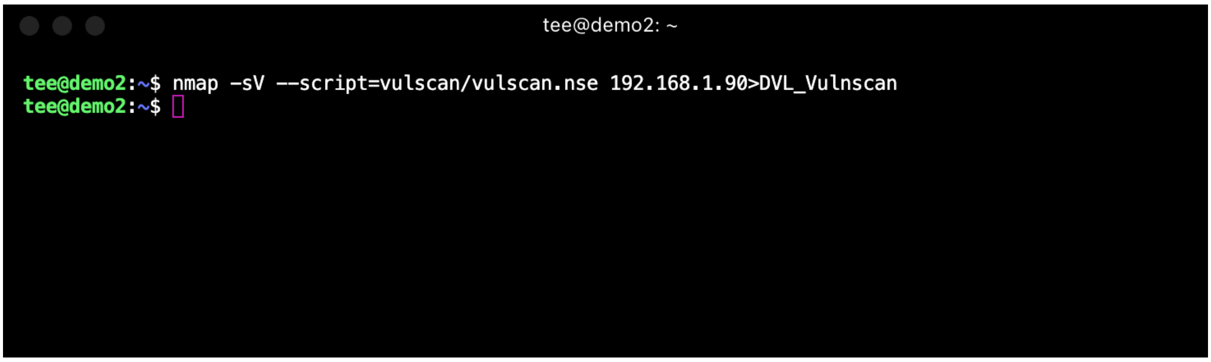
The result of this scan is very voluminous and can be seen by scrolling down the catted file.

Lastly, we will be downloading and installing a version of Linux called DamnVulnerable Linux. Once this download and install is completed, we’ll obtain the IP address using the ‘ifconfig’ command. This is illustrated below:



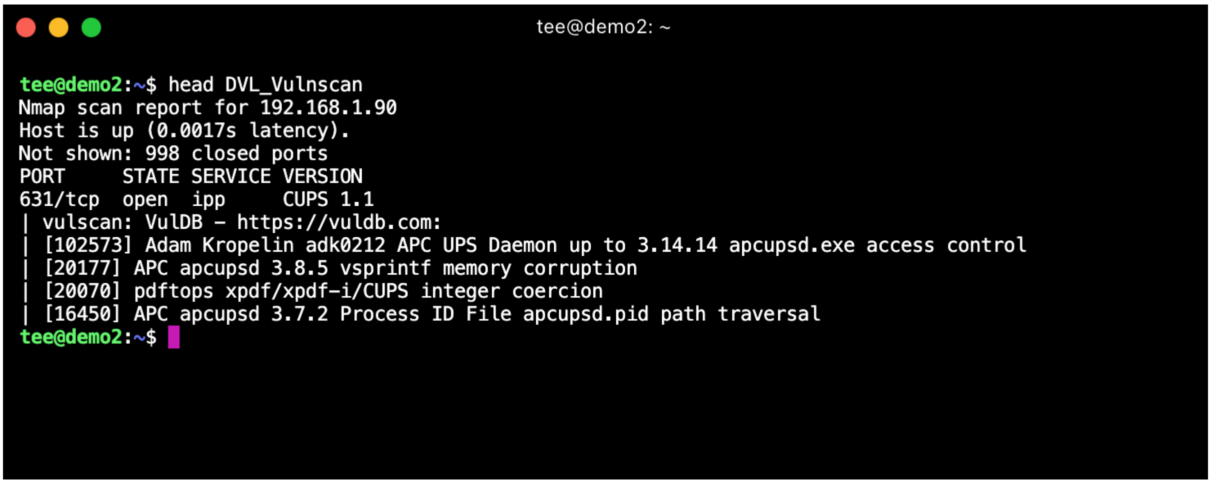
```
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:AE:06:78
          inet addr:192.168.1.90  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:83 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6290 (6.1 KiB)  TX bytes:2270 (2.2 KiB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

bt ~ #
```

Then, we will scan this IP address (192.168.1.90) for vulnerabilities. Note that this server was specifically loaded with vulnerabilities for training purposes. The result of the vulnerability scan has been directed to a file named DVL_Vulnscan as illustrated below:



```
tee@demo2:~$ nmap -sV --script=vulscan/vulscan.nse 192.168.1.90>DVL_Vulnscan
tee@demo2:~$ 
```

Catting this file will display the output of this scan. However, due to the magnanimous data output obtained from this scan, I'll use the 'head' command to display the first 10 lines of the file holding the output of the scan. The command is as follows; head DVL_Vulnscan. The result is illustrated below:



```
tee@demo2:~$ head DVL_Vulnscan
Nmap scan report for 192.168.1.90
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
631/tcp  open  ipp     CUPS 1.1
| vulscan: VulDB - https://vuldb.com:
| [102573] Adam Kropelin adk0212 APC UPS Daemon up to 3.14.14 apcupsd.exe access control
| [20177] APC apcupsd 3.8.5 vsprintf memory corruption
| [20070] pdftops xpdf/xpdf-i/CUPS integer coercion
| [16450] APC apcupsd 3.7.2 Process ID File apcupsd.pid path traversal
tee@demo2:~$ 
```