

NMAP FOR PENTESTER

VULNERABILITY SCAN

Contents

Introduction.....	3
ms17-010 Vulnerability	5
Vsftpd backdoor	5
SSL-Poodle Vulnerability	6
Rmi classloader Vulnerability	7
HTTP Slowloris Vulnerability	7
SSL-CCS-Injection	8
Nmap-Vulners.....	9
Conclusion	11

Introduction

The Nmap Scripting Engine (NSE) has been one of the most efficient features of Nmap, letting users prepare and share their scripts to automate the numerous tasks that are involved in networking. As we know about the Nmap's speed and competence, it allows executing these scripts side-by-side. According to the needs of the users, they can pick from the range of available scripts or create their own scripts as per the requirements.

So, let's get started by listing all the scripts that are available for discovering the vulnerability. Here we see that a list of scripts is available to detect the vulnerabilities. One by one, we will run these scripts and check for vulnerabilities.

```
cd /usr/share/nmap/scripts/  
ls -al *vulns*
```

```
root@kali:~# cd /usr/share/nmap/scripts/
root@kali:/usr/share/nmap/scripts# ls -al *vuln*
-rw-r--r-- 1 root root 7001 Oct 12 09:29 afp-path-vuln.nse
-rw-r--r-- 1 root root 5923 Oct 12 09:29 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root 6973 Oct 12 09:29 http-huawei-hg5xx-vuln.nse
-rw-r--r-- 1 root root 7921 Oct 12 09:29 http-iis-webdav-vuln.nse
-rw-r--r-- 1 root root 4111 Oct 12 09:29 http-vmware-path-vuln.nse
-rw-r--r-- 1 root root 3273 Oct 12 09:29 http-vuln-cve2006-3392.nse
-rw-r--r-- 1 root root 6610 Oct 12 09:29 http-vuln-cve2009-3960.nse
-rw-r--r-- 1 root root 2957 Oct 12 09:29 http-vuln-cve2010-0738.nse
-rw-r--r-- 1 root root 5607 Oct 12 09:29 http-vuln-cve2010-2861.nse
-rw-r--r-- 1 root root 4527 Oct 12 09:29 http-vuln-cve2011-3192.nse
-rw-r--r-- 1 root root 5851 Oct 12 09:29 http-vuln-cve2011-3368.nse
-rw-r--r-- 1 root root 4403 Oct 12 09:29 http-vuln-cve2012-1823.nse
-rw-r--r-- 1 root root 4831 Oct 12 09:29 http-vuln-cve2013-0156.nse
-rw-r--r-- 1 root root 2853 Oct 12 09:29 http-vuln-cve2013-6786.nse
-rw-r--r-- 1 root root 5009 Oct 12 09:29 http-vuln-cve2013-7091.nse
-rw-r--r-- 1 root root 2945 Oct 12 09:29 http-vuln-cve2014-2126.nse
-rw-r--r-- 1 root root 3334 Oct 12 09:29 http-vuln-cve2014-2127.nse
-rw-r--r-- 1 root root 3193 Oct 12 09:29 http-vuln-cve2014-2128.nse
-rw-r--r-- 1 root root 2979 Oct 12 09:29 http-vuln-cve2014-2129.nse
-rw-r--r-- 1 root root 14018 Oct 12 09:29 http-vuln-cve2014-3704.nse
-rw-r--r-- 1 root root 4523 Oct 12 09:29 http-vuln-cve2014-8877.nse
-rw-r--r-- 1 root root 7774 Oct 12 09:29 http-vuln-cve2015-1427.nse
-rw-r--r-- 1 root root 3443 Oct 12 09:29 http-vuln-cve2015-1635.nse
-rw-r--r-- 1 root root 4372 Oct 12 09:29 http-vuln-cve2017-1001000.nse
-rw-r--r-- 1 root root 2594 Oct 12 09:29 http-vuln-cve2017-5638.nse
-rw-r--r-- 1 root root 5480 Oct 12 09:29 http-vuln-cve2017-5689.nse
-rw-r--r-- 1 root root 5187 Oct 12 09:29 http-vuln-cve2017-8917.nse
-rw-r--r-- 1 root root 2699 Oct 12 09:29 http-vuln-misfortune-cookie.nse
-rw-r--r-- 1 root root 4225 Oct 12 09:29 http-vuln-wnr1000-creds.nse
-rw-r--r-- 1 root root 6977 Oct 12 09:29 mysql-vuln-cve2012-2122.nse
-rw-r--r-- 1 root root 8904 Oct 12 09:29 rdp-vuln-ms12-020.nse
-rw-r--r-- 1 root root 4011 Oct 12 09:29 rmi-vuln-classloader.nse
-rw-r--r-- 1 root root 6528 Oct 12 09:29 rsa-vuln-roca.nse
-rw-r--r-- 1 root root 4148 Oct 12 09:29 samba-vuln-cve-2012-1182.nse
-rw-r--r-- 1 root root 5238 Oct 12 09:29 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root 7524 Oct 12 09:29 smb-vuln-conficker.nse
-rw-r--r-- 1 root root 6402 Oct 12 09:29 smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 23154 Oct 12 09:29 smb-vuln-cve-2017-7494.nse
-rw-r--r-- 1 root root 6545 Oct 12 09:29 smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root 5386 Oct 12 09:29 smb-vuln-ms07-029.nse
-rw-r--r-- 1 root root 5688 Oct 12 09:29 smb-vuln-ms08-067.nse
-rw-r--r-- 1 root root 5647 Oct 12 09:29 smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root 7214 Oct 12 09:29 smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root 7344 Oct 12 09:29 smb-vuln-ms17-010.nse
-rw-r--r-- 1 root root 4400 Oct 12 09:29 smb-vuln-regsvc-dos.nse
-rw-r--r-- 1 root root 6586 Oct 12 09:29 smb-vuln-webexec.nse
-rw-r--r-- 1 root root 14781 Oct 12 09:29 smtp-vuln-cve2010-4344.nse
-rw-r--r-- 1 root root 7719 Oct 12 09:29 smtp-vuln-cve2011-1720.nse
-rw-r--r-- 1 root root 7603 Oct 12 09:29 smtp-vuln-cve2011-1764.nse
-rw-r--r-- 1 root root 7058 Oct 12 09:29 vulners.nse
root@kali:/usr/share/nmap/scripts#
```

ms17-010 Vulnerability

This script detects whether an SMBv1 server in Microsoft systems is vulnerable to the remote code execution which is commonly known as the **EternalBlue vulnerability**. This vulnerability had been vastly exploited by ransomware like WannaCry. This works on Windows XP, 2003, 7, 8, 8.1, 10, and server 2008, 2012 and 2016.

You see that on executing this script, you see that the system is susceptible to a vulnerability that is at high risk in nature.

```
nmap --script smb-vuln-ms17-010.nse 192.168.1.16
```

```
root@kali:~# nmap --script smb-vuln-ms17-010.nse 192.168.1.16
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:49 EST
Nmap scan report for 192.168.1.16
Host is up (0.00068s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 00:0C:29:5C:69:16 (VMware)

Host script results:
smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMBv1
    servers (ms17-010).

    Disclosure date: 2017-03-14
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-
```

Vsftpd backdoor

This script checks for the presence of the **vsFTPd 2.3.4 backdoor vulnerability** by attempting to exploit the backdoor using a harmful command.

```
nmap --script ftp-vsftpd-backdoor -p21 192.168.1.12
```



```

root@kali:~# nmap --script ftp-vsftpd-backdoor -p21 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:15 EST
Nmap scan report for 192.168.1.12
Host is up (0.00026s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
ftp-vsftpd-backdoor:
  VULNERABLE:
    vsFTPD version 2.3.4 backdoor
    State: VULNERABLE (Exploitable)
    IDs: CVE:CVE-2011-2523 BID:48539
    vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
    Disclosure date: 2011-07-03
    Exploit results:
      Shell command: id
      Results: uid=0(root) gid=0(root)
    References:
      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
      https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:78:20:90 (VMware)

```

SSL-Poodle Vulnerability

The SSL Poodle is a man-in-the-middle exploit whose purpose is to take advantage of the security software running on SSL. Running this script, you see that the system is vulnerable.

```
nmap --script ssl-poodle 192.168.1.12
```

```

root@kali:~# nmap --script ssl-poodle 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:18 EST
Nmap scan report for 192.168.1.12
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  rsh
25/tcp    open  smtp
ssl-poodle:
  VULNERABLE:
    SSL POODLE information leak
    State: VULNERABLE
    IDs: CVE:CVE-2014-3566 BID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
    products, uses nondeterministic CBC padding, which makes it easier
    for man-in-the-middle attackers to obtain cleartext data via a
    padding-oracle attack, aka the "POODLE" issue.
    Disclosure date: 2014-10-14
    Check results:
      TLS_RSA_WITH_AES_128_CBC_SHA
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
      https://www.openssl.org/~bodo/ssl-poodle.pdf
      https://www.securityfocus.com/bid/70574
      https://www.imperialviolet.org/2014/10/14/poodle.html

```

Rmi classloader Vulnerability

This script checks whether Java rmiregistry allows class loads or not. The rmiregistry has a default configuration that allows the class to load from remote URLs, which may lead to remote code execution.

```
nmap --script=rmi-vuln-classloader.nse -p1099 192.168.1.12
```

```
root@kali:~# nmap --script rmi-vuln-classloader.nse -p1099 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:20 EST
Nmap scan report for 192.168.1.12
Host is up (0.00028s latency).

PORT      STATE SERVICE
1099/tcp  open  rmiregistry
rmi-vuln-classloader:
  VULNERABLE:
    RMI registry default configuration remote code execution vulnerability
    State: VULNERABLE
    Default configuration of RMI registry allows loading classes from remote URL

    References:
    - https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/
MAC Address: 00:0C:29:78:20:90 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

HTTP Slowloris Vulnerability

It checks for the vulnerability in the web server's Slowloris DoS attack, but does not launch an actual DoS attack. This script will open 2 separate connections to the server and then request the URL in the base configuration.

```
nmap --script http-slowloris-check 192.168.1.12
```

```
root@kali:~# nmap --script http-slowloris-check 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:22 EST
Nmap scan report for 192.168.1.12
Host is up (0.0029s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  nmap
25/tcp    open  smtp
27/tcp    open  rdp
54/tcp    open  irc
80/tcp    open  http

http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE:CVE-2007-6750
Slowloris tries to keep many connections to the target web server open and
them open as long as possible. It accomplishes this by opening connection
the target web server and sending a partial request. By doing so, it starv
the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
http://ha.ckers.org/slowloris/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

SSL-CCS-Injection

When run, this script determines whether a server is vulnerable to the SSL/TLS "CCS Injection" vulnerability. To exploit this vulnerability using MITM (Man in the Middle Attack), the attacker will then wait for a new TLS connection, which will be followed by Client-Sever 'Hello' handshake messages.

```
nmap --script ssl-ccs-injection -p 5432 192.168.1.12
```



```

root@kali:~# nmap --script ssl-ccs-injection -p 5432 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:29 EST
Nmap scan report for 192.168.1.12
Host is up (0.00033s latency).

PORT      STATE SERVICE
5432/tcp  open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|   State: VULNERABLE
|   Risk factor: High
|   OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|   does not properly restrict processing of ChangeCipherSpec messages,
|   which allows man-in-the-middle attackers to trigger use of a zero
|   length master key in certain OpenSSL-to-OpenSSL communications, and
|   consequently hijack sessions or obtain sensitive information, via
|   a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|     http://www.cvedetails.com/cve/2014-0224
|     http://www.openssl.org/news/secadv_20140605.txt
|_
MAC Address: 00:0C:29:78:20:90 (VMware)

```

Nmap-Vulners

Nmap -Vulners is a NSE script that uses some well-known services to provide info on vulnerabilities. This script completely depends on having information on software versions and therefore works with the **-sV** flag.

You can install it using the github code. Then update the scripts in the NSE database.

```

git clone https://github.com/vulnersCom/nmap-vulners /usr/share/nmap/scripts/vulners
nmap --scripts-updatedb

```

```

root@kali:~# git clone https://github.com/vulnersCom/nmap-vulners /usr/share/nmap/scripts/vulners
Cloning into '/usr/share/nmap/scripts/vulners' ...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 73 (delta 2), reused 4 (delta 1), pack-reused 62
Unpacking objects: 100% (73/73), 433.57 KiB | 622.00 KiB/s, done.
root@kali:~# nmap --script-updatedb
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:42 EST
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.32 seconds

```

Let us load the scripts and check the service versions available on the target machine using nmap vulners. Here we see that all the scripts are loaded, which can be used for vulnerability detection based on a particular service version.

```

nmap -sV -Pn 192.168.1.12 --script=vulners/vulners.nse

```

```

root@kali:~# nmap -sV -Pn 192.168.1.12 --script=vulners/vulners.nse
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slow
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 13:51 EST
Nmap scan report for 192.168.1.12
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     PACKETSTORM:101052 7.8 https://vulners.com/packetstorm/PACKETSTORM:101052
|     CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
|     CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
|     SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
|     CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906
|     CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
|     CVE-2010-4755 4.0 https://vulners.com/cve/CVE-2010-4755
|     CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
|     CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
|     CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
|     CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
|_
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
| vulners:
|   cpe:/a:isc:bind:9.4.2:
|     SSV:2853 10.0 https://vulners.com/seebug/SSV:2853 *EXPLOIT*
|     CVE-2008-0122 10.0 https://vulners.com/cve/CVE-2008-0122
|     SSV:60184 8.5 https://vulners.com/seebug/SSV:60184 *EXPLOIT*
|     CVE-2012-1667 8.5 https://vulners.com/cve/CVE-2012-1667
|     SSV:60292 7.8 https://vulners.com/seebug/SSV:60292 *EXPLOIT*
|     CVE-2014-8500 7.8 https://vulners.com/cve/CVE-2014-8500
|     CVE-2012-5166 7.8 https://vulners.com/cve/CVE-2012-5166
|     CVE-2012-4244 7.8 https://vulners.com/cve/CVE-2012-4244
|     CVE-2012-3817 7.8 https://vulners.com/cve/CVE-2012-3817
|     CVE-2008-4163 7.8 https://vulners.com/cve/CVE-2008-4163
|     CVE-2010-0382 7.6 https://vulners.com/cve/CVE-2010-0382
|     CVE-2015-8461 7.1 https://vulners.com/cve/CVE-2015-8461
|     CVE-2015-8704 6.8 https://vulners.com/cve/CVE-2015-8704
|     CVE-2009-0025 6.8 https://vulners.com/cve/CVE-2009-0025
|     CVE-2015-8705 6.6 https://vulners.com/cve/CVE-2015-8705
|     CVE-2010-3614 6.4 https://vulners.com/cve/CVE-2010-3614
|     SSV:30099 5.0 https://vulners.com/seebug/SSV:30099 *EXPLOIT*
|     SSV:20595 5.0 https://vulners.com/seebug/SSV:20595 *EXPLOIT*
|     CVE-2016-9444 5.0 https://vulners.com/cve/CVE-2016-9444
|     CVE-2016-2848 5.0 https://vulners.com/cve/CVE-2016-2848
|     CVE-2016-1286 5.0 https://vulners.com/cve/CVE-2016-1286
|     CVE-2015-8000 5.0 https://vulners.com/cve/CVE-2015-8000
|     CVE-2012-1033 5.0 https://vulners.com/cve/CVE-2012-1033
|     CVE-2011-4313 5.0 https://vulners.com/cve/CVE-2011-4313
|     CVE-2011-1910 5.0 https://vulners.com/cve/CVE-2011-1910
|     CVE-2009-0265 5.0 https://vulners.com/cve/CVE-2009-0265
|     SSV:11919 4.3 https://vulners.com/seebug/SSV:11919 *EXPLOIT*
|     EDB-ID:9300 4.3 https://vulners.com/exploitdb/EDB-ID:9300 *EXPLOIT*
|     CVE-2016-1285 4.3 https://vulners.com/cve/CVE-2016-1285

```

```

2121/tcp open  ftp          ProFTPD 1.3.1
vulners:
  cpe:/a:proftpd:proftpd:1.3.1:
    SSV:26016      9.0    https://vulners.com/seebug/SSV:26016    *EXPLOIT*
    SSV:24282      9.0    https://vulners.com/seebug/SSV:24282    *EXPLOIT*
    CVE-2011-4130  9.0    https://vulners.com/cve/CVE-2011-4130
    EDB-ID:8037    7.5    https://vulners.com/exploitdb/EDB-ID:8037    *EXPLOIT*
    CVE-2019-12815 7.5    https://vulners.com/cve/CVE-2019-12815
    SSV:20226      7.1    https://vulners.com/seebug/SSV:20226    *EXPLOIT*
    PACKETSTORM:95517 7.1    https://vulners.com/packetstorm/PACKETSTORM:95517
    CVE-2010-3867  7.1    https://vulners.com/cve/CVE-2010-3867
    CVE-2010-4652  6.8    https://vulners.com/cve/CVE-2010-4652
    CVE-2009-0543  6.8    https://vulners.com/cve/CVE-2009-0543
    SSV:12523      5.8    https://vulners.com/seebug/SSV:12523    *EXPLOIT*
    CVE-2009-3639  5.8    https://vulners.com/cve/CVE-2009-3639
    EDB-ID:16129   5.0    https://vulners.com/exploitdb/EDB-ID:16129    *EXPLOIT*
    CVE-2019-19272 5.0    https://vulners.com/cve/CVE-2019-19272
    CVE-2019-19271 5.0    https://vulners.com/cve/CVE-2019-19271
    CVE-2019-19270 5.0    https://vulners.com/cve/CVE-2019-19270
    CVE-2019-18217 5.0    https://vulners.com/cve/CVE-2019-18217
    CVE-2016-3125  5.0    https://vulners.com/cve/CVE-2016-3125
    CVE-2011-1137  5.0    https://vulners.com/cve/CVE-2011-1137
    CVE-2008-7265  4.0    https://vulners.com/cve/CVE-2008-7265
    CVE-2017-7418  2.1    https://vulners.com/cve/CVE-2017-7418
    CVE-2012-6095  1.2    https://vulners.com/cve/CVE-2012-6095
3306/tcp open  mysql          MySQL 5.0.51a-3ubuntu5
vulners:
  cpe:/a:mysql:mysql:5.0.51a-3ubuntu5:
    SSV:15006      6.8    https://vulners.com/seebug/SSV:15006    *EXPLOIT*
    CVE-2009-4028  6.8    https://vulners.com/cve/CVE-2009-4028
    SSV:3280       4.6    https://vulners.com/seebug/SSV:3280    *EXPLOIT*
    CVE-2008-2079  4.6    https://vulners.com/cve/CVE-2008-2079
    EDB-ID:34506   4.0    https://vulners.com/exploitdb/EDB-ID:34506    *EXPLOIT*
    CVE-2010-3682  4.0    https://vulners.com/cve/CVE-2010-3682
    CVE-2010-3677  4.0    https://vulners.com/cve/CVE-2010-3677
5432/tcp open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
vulners:
  cpe:/a:postgresql:postgresql:8.3:
    SSV:60718      10.0   https://vulners.com/seebug/SSV:60718    *EXPLOIT*
    CVE-2013-1903  10.0   https://vulners.com/cve/CVE-2013-1903
    CVE-2013-1902  10.0   https://vulners.com/cve/CVE-2013-1902
    SSV:30015      8.5    https://vulners.com/seebug/SSV:30015    *EXPLOIT*
    SSV:19652      8.5    https://vulners.com/seebug/SSV:19652    *EXPLOIT*
    CVE-2010-1447  8.5    https://vulners.com/cve/CVE-2010-1447
    CVE-2010-1169  8.5    https://vulners.com/cve/CVE-2010-1169
    SSV:30152      6.8    https://vulners.com/seebug/SSV:30152    *EXPLOIT*
    CVE-2013-0255  6.8    https://vulners.com/cve/CVE-2013-0255
    CVE-2012-0868  6.8    https://vulners.com/cve/CVE-2012-0868
    CVE-2009-3231  6.8    https://vulners.com/cve/CVE-2009-3231
    SSV:62083      6.5    https://vulners.com/seebug/SSV:62083    *EXPLOIT*
    SSV:61543      6.5    https://vulners.com/seebug/SSV:61543    *EXPLOIT*
    CVE-2014-0065  6.5    https://vulners.com/cve/CVE-2014-0065
    CVE-2014-0064  6.5    https://vulners.com/cve/CVE-2014-0064
    CVE-2014-0063  6.5    https://vulners.com/cve/CVE-2014-0063
    CVE-2014-0061  6.5    https://vulners.com/cve/CVE-2014-0061
    CVE-2012-0866  6.5    https://vulners.com/cve/CVE-2012-0866
    CVE-2010-1015  6.5    https://vulners.com/cve/CVE-2010-1015

```

Conclusion

Hence, we see that by using the nmap scripts we can detect the vulnerabilities present on the system, which can be a benefit for pen testers.

JOIN OUR TRAINING PROGRAMS

