ETHICAL HACKING COURSE

MINOR PROJECT

Topic:- Scanning the network and finding vulnerabilities using Nmap

Submitted by : SAGAR MAHESHWARI

Submitted to : Mr. MOHSIN QURESH

INDEX

1. Setting up the environment …….....3

2. Nmap……..8

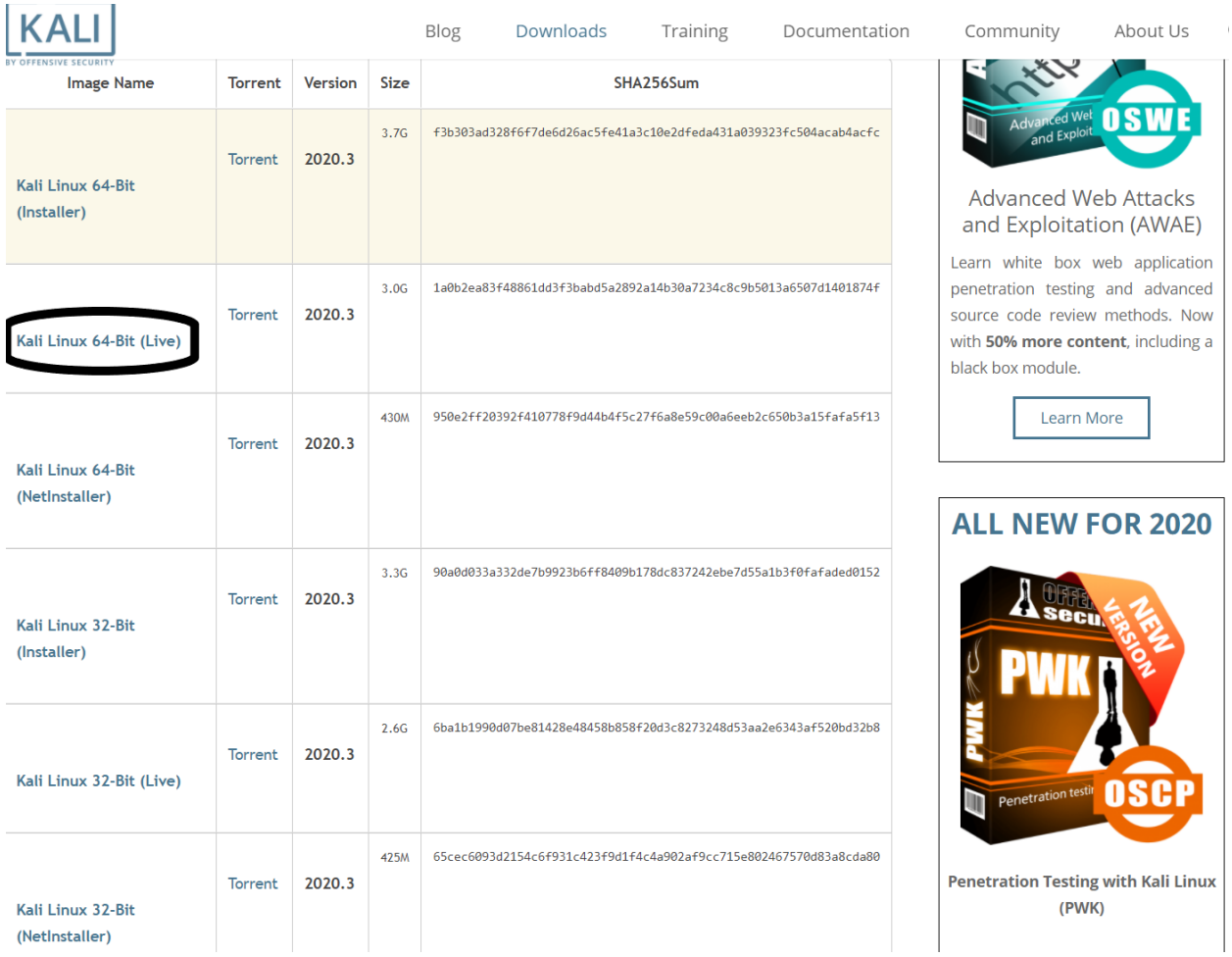
3. Installing Nmap……...11

4. USING NMAP (Practicals)……..…..13

SETTING UP THE ENVIRONMENT

1. For setting up the environment you will need the iso image of the operating system(“KALI LINUX” in our case). To download the iso image of KALI follow this link:

   https://www.kali.org/downloads/



KALI BY OFFENSIVE SECURITY

Blog | Downloads | Training | Documentation | Community | About Us

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.3	3.7G	f3b303ad328f6f7de6d26ac5fe41a3c10e2dfeda431a039323fc504acab4acfc
Kali Linux 64-Bit (Live)	Torrent	2020.3	3.0G	1a0b2ea83f48861dd3f3babd5a2892a14b30a7234c8c9b5013a6507d1401874f
Kali Linux 64-Bit (NetInstaller)	Torrent	2020.3	430M	950e2ff20392f410778f9d44b4f5c27f6a8e59c00a6eeb2c650b3a15fafa5f13
Kali Linux 32-Bit (Installer)	Torrent	2020.3	3.3G	90a0d033a332de7b9923b6ff8409b178dc837242ebe7d55a1b3f0fafaded0152
Kali Linux 32-Bit (Live)	Torrent	2020.3	2.6G	6ba1b1990d07be81428e48458b858f20d3c8273248d53aa2e6343af520bd32b8
Kali Linux 32-Bit (NetInstaller)	Torrent	2020.3	425M	65cec6093d2154c6f931c423f9d1f4c4a902af9cc715e802467570d83a8cda80

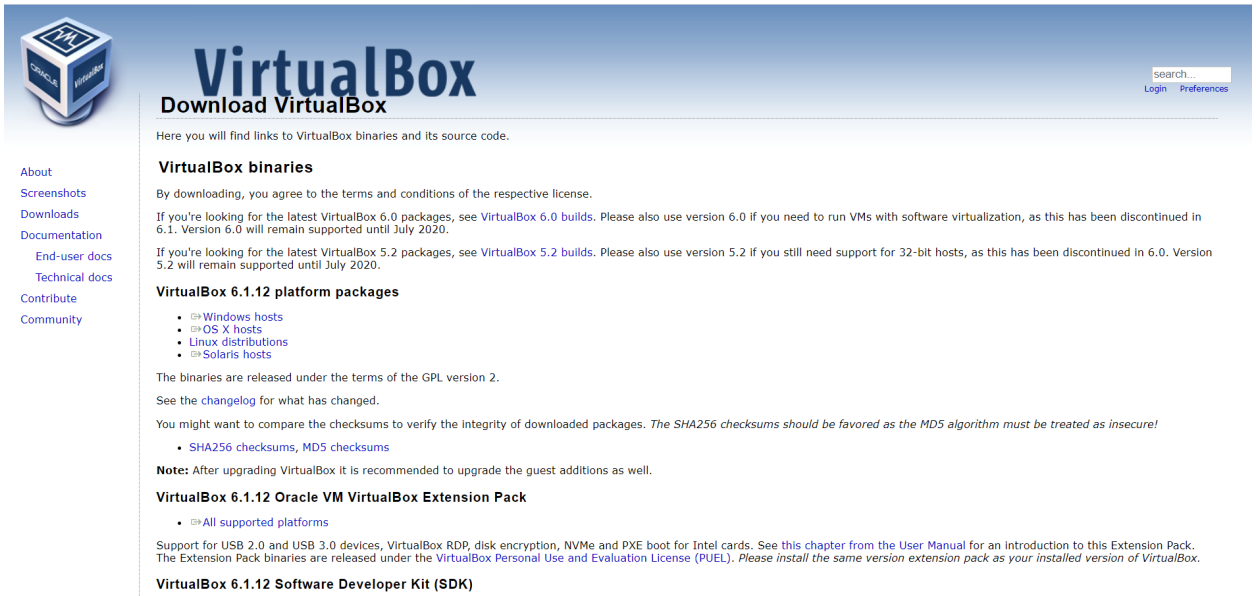
   Download the live version and depending on your pc architecture choose 64-bit or 32-bit version.

2. Now you can use one of the two options to boot KALI:
   a. LIVE

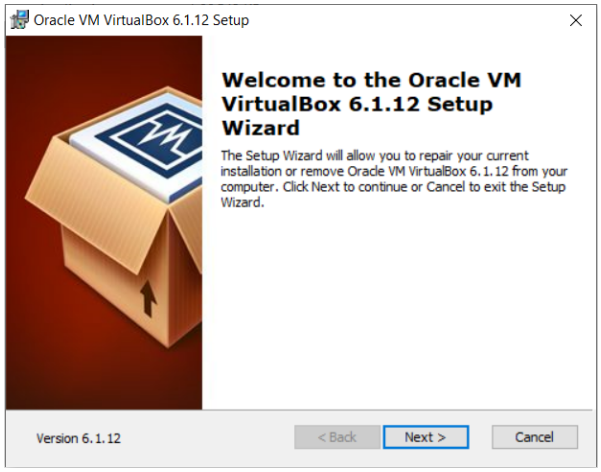
b. Virtualisation

The following steps are related to virtualisation method as i have sufficient specifications on my pc but to use live, follow this link.

For virtualisation, download Oracle VM Virtualbox from this link.

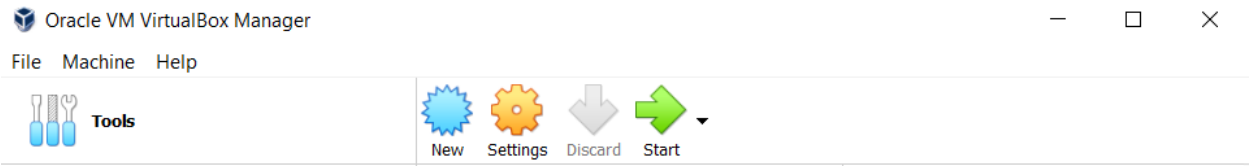


3. Now run the setup files for the virtualbox and install it.

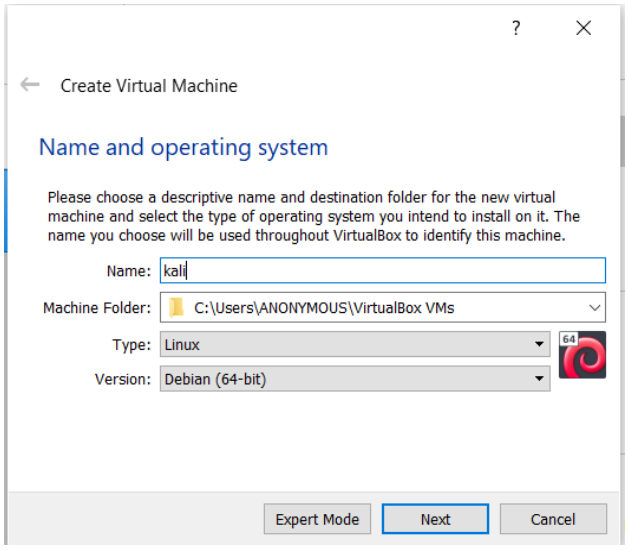


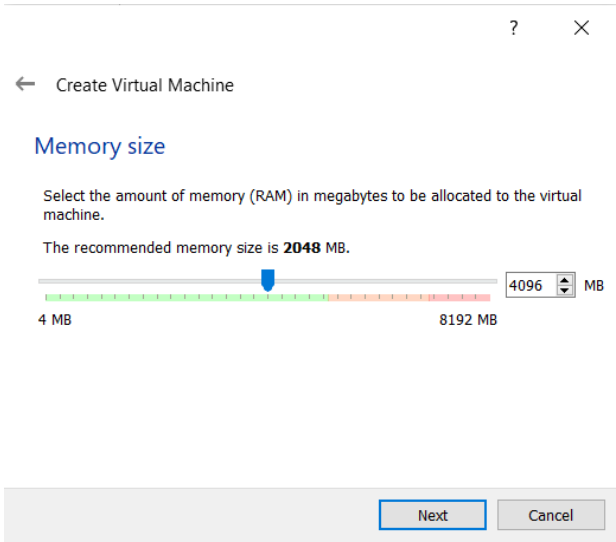
Complete the installation.

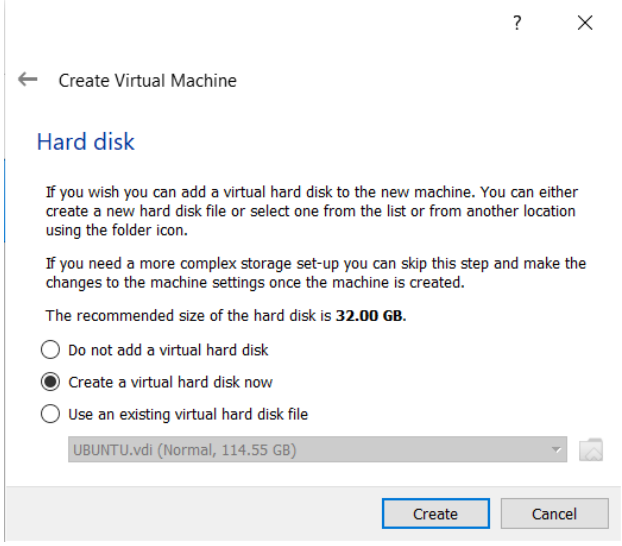
4. After the installation, open the Virtualbox and click on new machine.

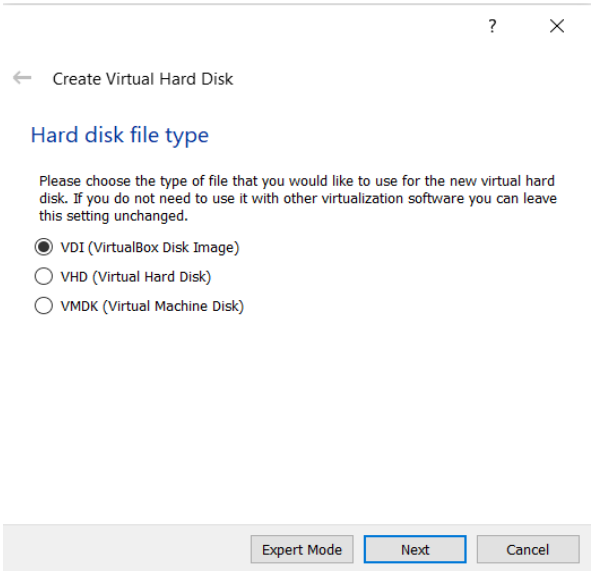


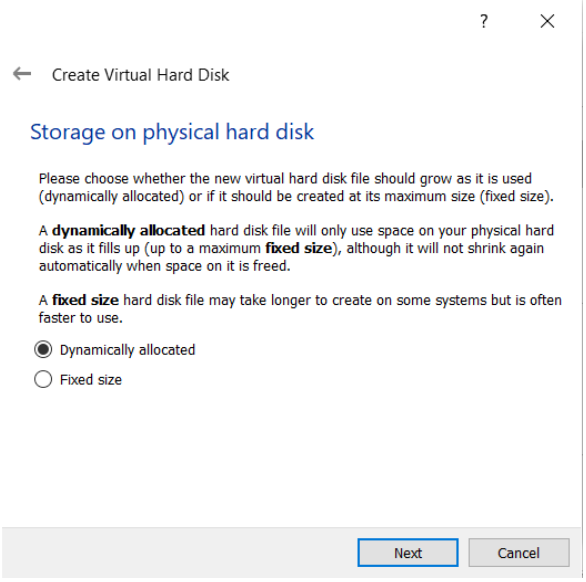
5. Name the machine and select linux from the first dropdown menu and Debian from the second(as Kali is not an option and Kali is Debian-derived Linux Distribution), allot a minimum of 4GB RAM and 100GB disk storage as Virtualbox Disk Image, dynamically allocated.

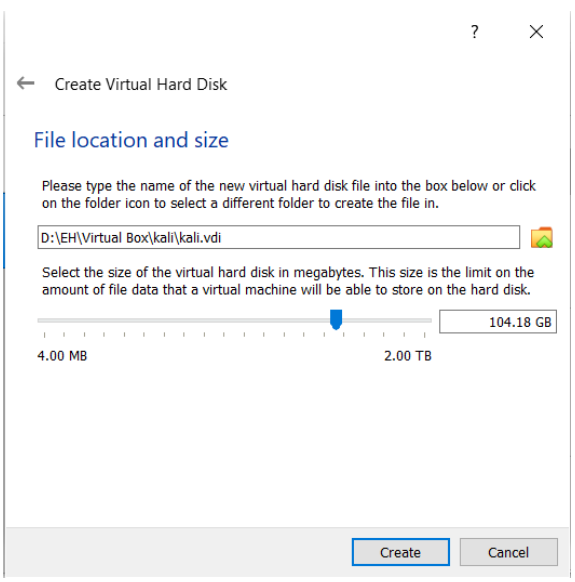




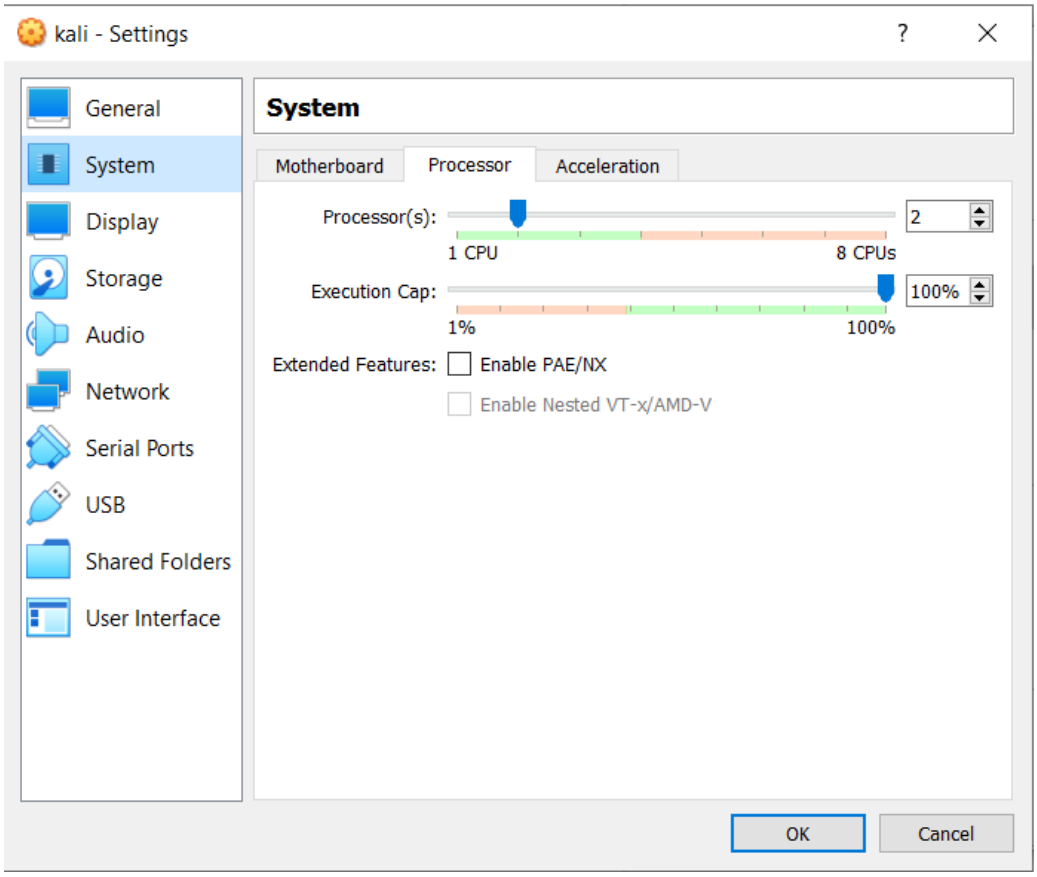


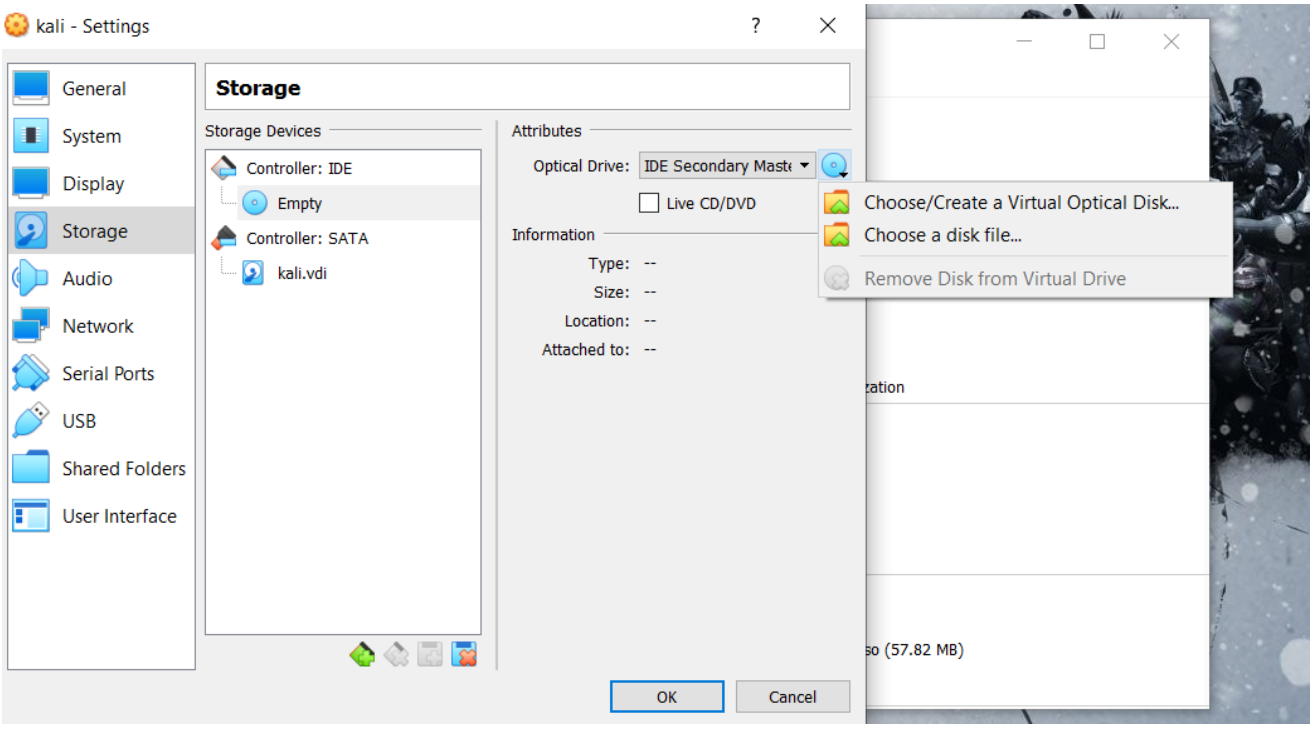






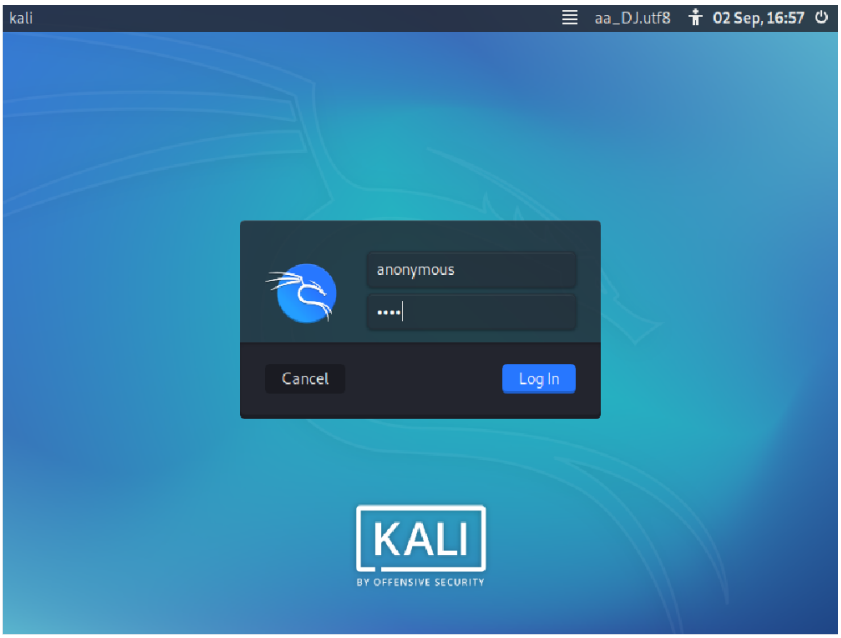
6. Now go to the settings and add the iso image file, increase the number of processors for the virtual machine and change the network adapter settings.





Browse and select the iso image of the operating system.

7. Now run the virtual machine.. After the installation is complete insert your credentials and login. Now configure your system as you want to.



NMAP

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).
Nmap was named "Security Product of the Year" by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

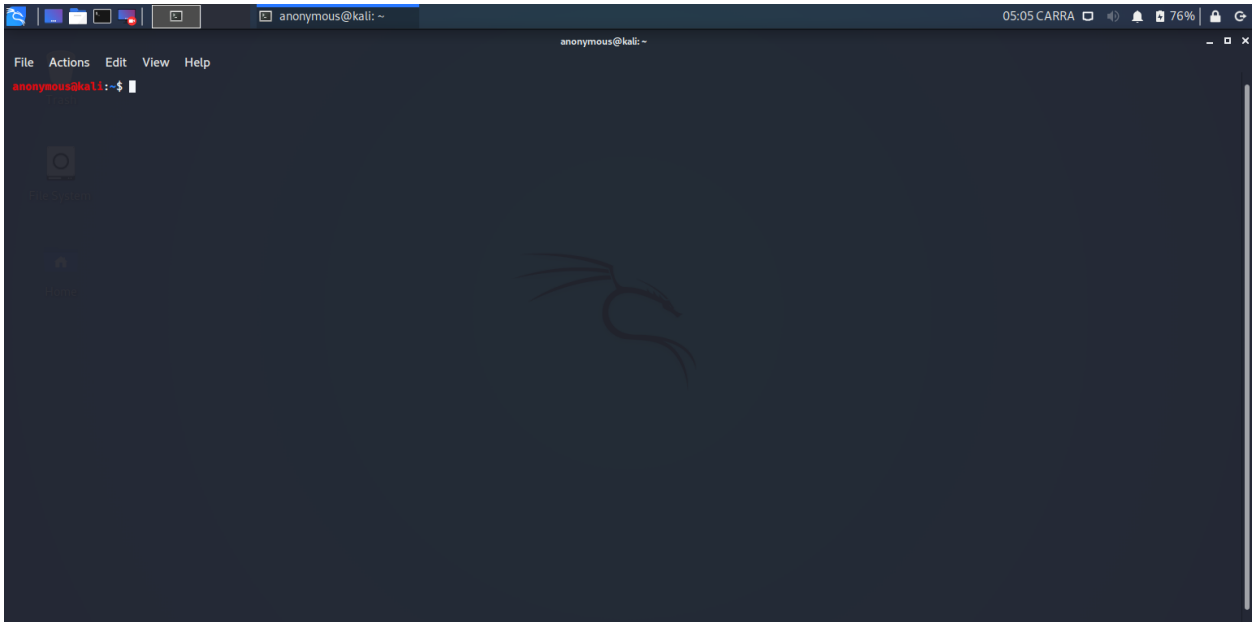
Nmap is ...

- Flexible: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.

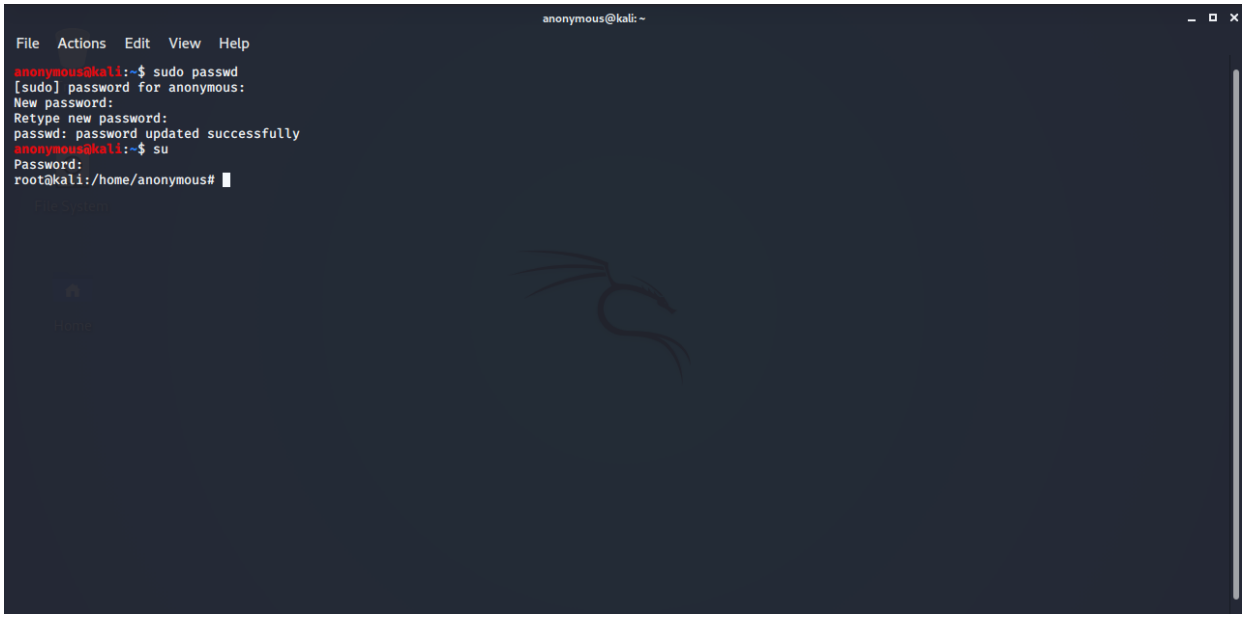
- Powerful: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- Portable: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- Easy: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A targethost". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
- Free: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.
- Well Documented: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.
- Supported: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #nmap channel on Freenode or EFNet.
- Acclaimed: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the press page for further details.

INSTALLING NMAP

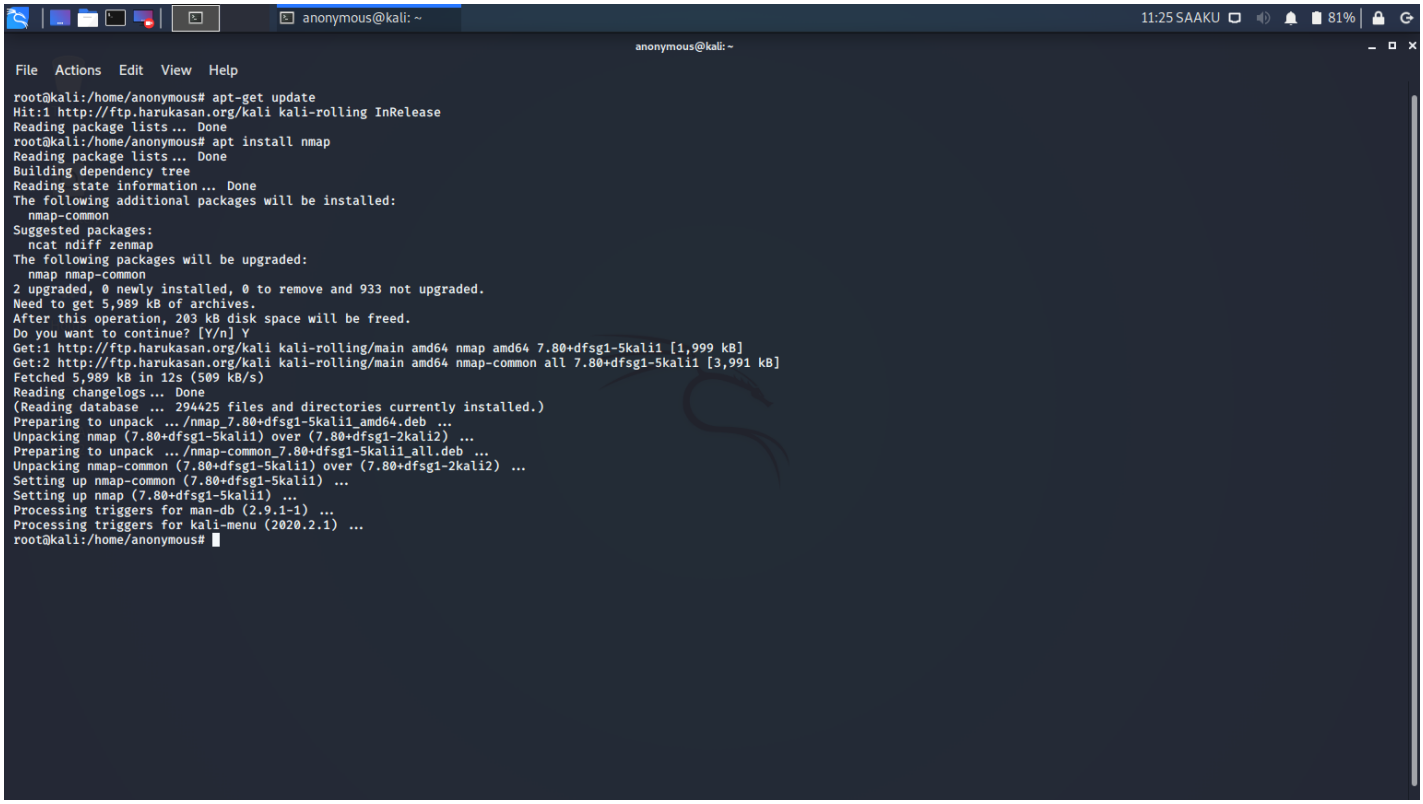
1. Open the terminal in your kali linux, it will be present on the panel.



2. Now you have to gain access as root. For this type first "sudo passwd" and then enter your password and then the password for root access. Then type "su" and then enter the password when it asks you to.



3. Now you have the root access, then type”apt-get update” to update your system software and when the update completes, type “apt install nmap”, to install nmap.



USING NMAP

1. Now type nmap in the terminal and it will show the following options for scanning and output.

```
root@kali:/home/anonymous# nmap
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
```

```
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
```

```
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND
EXAMPLES
```

2. As in the previous text the usage of nmap is ”**nmap [Scan Type(s)] [Options] {target specification}”.**
   You can use it to scan IPs, domains, etc.

Practical 1:- Domain name : lnmiit.ac.in

1. Scan:-

```
root@kali:/home/anonymous# nmap -sS lnmiit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 11:26 IST
Nmap scan report for lnmiit.ac.in (172.107.175.224)
Host is up (0.031s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
443/tcp  open  https
1092/tcp open  obrpd
1093/tcp open  proofd
9001/tcp open  tor-orport
9003/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 55.60 seconds
root@kali:/home/anonymous# nmap -sS -sV lnmiit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 11:28 IST
Nmap scan report for lnmiit.ac.in (172.107.175.224)
Host is up (0.042s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     FileZilla ftpd 0.9.45 beta
80/tcp   open  http    Microsoft IIS httpd 10.0
443/tcp  open  https?
1093/tcp open  proofd?
9003/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.81 seconds
root@kali:/home/anonymous# nmap -sS -sV -O lnmiit.ac.in -p 21,80,443,9003
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 11:31 IST
Nmap scan report for lnmiit.ac.in (172.107.175.224)
Host is up (0.0037s latency).

PORT     STATE    SERVICE VERSION
21/tcp   filtered ftp
80/tcp   filtered http
443/tcp  filtered https
9003/tcp filtered unknown
Too many fingerprints match this host to give specific OS details

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 6.07 seconds
root@kali:/home/anonymous#
```

Versions found:

OS : Windows; ftp server: FileZilla ftpd 0.9.45 beta; http server: Microsoft IIS httpd 10.0

2. Finding Vulnerabilities:-
   a. On FileZilla ftpd 0.9.45 beta: https://www.cvedetails.com/vulnerability-list/vendor_id-2889/Filezilla.html

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2009-0884	119		DoS Overflow	2009-03-12	2017-08-16	5.0	None	Remote	Low	Not required	None	None	Partial
Buffer overflow in FileZilla Server before 0.9.31 allows remote attackers to cause a denial of service via unspecified vectors related to SSL/TLS packets.														
2	CVE-2007-2318			Exec Code	2007-04-26	2008-11-13	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complete
Multiple format string vulnerabilities in FileZilla before 2.2.32 allow remote attackers to execute arbitrary code via format string specifiers in (1) FTP server responses or (2) data sent by an FTP server. NOTE: some of these details are obtained from third party information.														
3	CVE-2007-0317			DoS Exec Code	2007-01-17	2017-07-28	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
Format string vulnerability in the LogMessage function in FileZilla before 3.0.0-betaS allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted arguments. NOTE: some of these details are obtained from third party information.														
4	CVE-2007-0315	119		DoS Exec Code Overflow	2007-01-17	2017-07-28	9.3	Admin	Remote	Medium	Not required	Complete	Complete	Complete
Multiple buffer overflows in FileZilla before 2.2.30a allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors related to (1) Options.cpp when storing settings in the registry, and (2) the transfer queue (QueueCtrl.cpp). NOTE: some of these details are obtained from third party information.														
5	CVE-2006-6565			DoS	2006-12-15	2017-10-18	4.0	None	Remote	Low	Single system	None	None	Partial
FileZilla Server before 0.9.22 allows remote attackers to cause a denial of service (crash) via a wildcard argument to the (1) LIST or (2) NLST commands, which results in a NULL pointer dereference, a different set of vectors than CVE-2006-6564. NOTE: CVE analysis suggests that the problem might be due to a malformed PORT command.														
6	CVE-2006-6564			DoS	2006-12-15	2017-07-28	4.0	None	Remote	Low	Single system	None	None	Partial
FileZilla Server before 0.9.22 allows remote attackers to cause a denial of service (crash) via a malformed argument to the STOR command, which results in a NULL pointer dereference. NOTE: CVE analysis suggests that the problem might be due to a malformed PORT command.														
7	CVE-2006-2403			Exec Code Overflow	2006-05-15	2017-07-19	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
Buffer overflow in FileZilla before 2.2.23 allows remote attackers to execute arbitrary commands via unknown attack vectors.														
8	CVE-2006-2173			DoS Exec Code Overflow	2006-05-04	2017-07-19	6.4	None	Remote	Low	Not required	None	Partial	Partial
Buffer overflow in FileZilla FTP Server 2.2.22 allows remote authenticated attackers to cause a denial of service and possibly execute arbitrary code via a long (1) PORT or (2) PASS followed by the MLSD command, or (2) the remote server interface, as demonstrated by the Infigo FTPStress Fuzzer.														
9	CVE-2005-3589			DoS Overflow	2005-11-16	2018-10-19	7.8	None	Remote	Low	Not required	None	None	Complete
Buffer overflow in FileZilla Server Terminal 0.9.4d may allow remote attackers to cause a denial of service (terminal crash) via a long USER ftp command.														
10	CVE-2005-2898				2005-09-14	2017-07-11	4.6	User	Local	Low	Not required	Partial	Partial	Partial
** DISPUTED ** NOTE: this issue has been disputed by the vendor. FileZilla 2.2.14b and 2.2.15, and possibly earlier versions, when "Use secure mode" is disabled, uses a weak encryption scheme to store the user's password in the configuration settings file, which allows local users to obtain sensitive information. NOTE: the vendor has disputed the issue, stating that "the problem is not a vulnerability at all, but in fact a fundamental issue of every single program that can store passwords transparently."														
11	CVE-2005-0851			DoS	2005-05-02	2008-09-05	5.0	None	Remote	Low	Not required	None	None	Partial
FileZilla FTP server before 0.9.6, when using MODE Z (zlib compression), allows remote attackers to cause a denial of service (infinite loop) via certain file uploads or directory listings.														
12	CVE-2005-0850			DoS	2005-05-02	2008-09-05	5.0	None	Remote	Low	Not required	None	None	Partial
FileZilla FTP server before 0.9.6 allows remote attackers to cause a denial of service via a request for a filename containing an MS-DOS device name such as CON, NUL, COM1, LPT1, and others.														

Total number of vulnerabilities : 12 Page : 1 (This Page)

b. On Microsoft IIS httpd 10.0: https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-3436/Microsoft-IIS.html

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2015-2808	310			2015-03-31	2018-01-18	4.3	None	Remote	Medium	Not required	Partial	None	None
The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.														
2	CVE-2013-2566	310			2013-03-15	2018-01-18	4.3	None	Remote	Medium	Not required	Partial	None	None
The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.														
3	CVE-2011-5279	20			2014-04-23	2019-07-03	6.4	None	Remote	Low	Not required	None	Partial	Partial
CRLF injection vulnerability in the CGI implementation in Microsoft Internet Information Services (IIS) 4.x and 5.x on Windows NT and Windows 2000 allows remote attackers to modify arbitrary uppercase environment variables via a \n (newline) character in an HTTP header.														
4	CVE-2009-4444	20		Bypass	2009-12-29	2019-07-03	6.0	User	Remote	Medium	Single system	Partial	Partial	Partial
Microsoft Internet Information Services (IIS) 5.x and 6.x uses only the portion of a filename before a ; (semicolon) character to determine the file extension, which allows remote attackers to bypass intended extension restrictions of third-party upload applications via a filename with a (1) .asp, (2) .cer, or (3) .asa first extension, followed by a semicolon and a safe extension, as demonstrated by the use of asp.dll to handle a .asp;.jpg file.														
5	CVE-2009-3023	119	2	Exec Code Overflow Mem. Corr.	2009-08-31	2019-07-03	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Buffer overflow in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 6.0 allows remote authenticated users to execute arbitrary code via a crafted NLST (NAME LIST) command that uses wildcards, leading to memory corruption, aka "IIS FTP Service RCE and DoS Vulnerability."														
6	CVE-2009-2521	399		DoS	2009-09-04	2019-07-03	2.6	None	Remote	High	Not required	None	None	Partial
Stack consumption vulnerability in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows remote authenticated users to cause a denial of service (daemon crash) via a list (ls) -R command containing a wildcard that references a subdirectory, followed by a .. (dot dot), aka "IIS FTP Service DoS Vulnerability."														
7	CVE-2009-1535	287		Bypass	2009-06-10	2019-07-03	7.6	None	Remote	High	Not required	Complete	Complete	Complete
The WebDAV extension in Microsoft Internet Information Services (IIS) 5.1 and 6.0 allows remote attackers to bypass URI-based protection mechanisms, and list folders or read, create, or modify files, via a %c0%af (Unicode / character) at an arbitrary position in the URI, as demonstrated by inserting %c0%af into a "/protected/" initial pathname component to bypass the password protection on the protected\ folder, aka "IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability," a different vulnerability than CVE-2009-1122.														
8	CVE-2009-1122	287		Bypass	2009-06-10	2018-10-12	7.6	None	Remote	High	Not required	Complete	Complete	Complete
The WebDAV extension in Microsoft Internet Information Services (IIS) 5.0 on Windows 2000 SP4 does not properly decode URLs, which allows remote attackers to bypass authentication, and possibly read or create files, via a crafted HTTP request, aka "IIS 5.0 WebDAV Authentication Bypass Vulnerability," a different vulnerability than CVE-2009-1535.														
9	CVE-2008-4301	255			2008-09-29	2018-10-11	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
** DISPUTED ** A certain ActiveX control in iisext.dll in Microsoft Internet Information Services (IIS) allows remote attackers to set a password via a string argument to the SetPassword method. NOTE: this issue could not be reproduced by a reliable third party. In addition, the original researcher is unreliable. Therefore the original disclosure is probably erroneous.														
10	CVE-2008-4300	20		DoS	2008-09-29	2018-10-11	5.0	None	Remote	Low	Not required	None	None	Partial
A certain ActiveX control in adsiis.dll in Microsoft Internet Information Services (IIS) allows remote attackers to cause a denial of service (browser crash) via a long string in the second argument to the GetObject method. NOTE: this issue was disclosed by an unreliable researcher, so it might be incorrect.														
11	CVE-2008-1446	189		Exec Code Overflow	2008-10-14	2019-07-03	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
Integer overflow in the Internet Printing Protocol (IPP) ISAPI extension in Microsoft Internet Information Services (IIS) 5.0 through 7.0 on Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to execute arbitrary code via an HTTP POST request that triggers an outbound IPP connection from a web server to a machine operated by the attacker, aka "Integer Overflow in IPP Service Vulnerability."														

Total number of vulnerabilities : **11** Page : 1 (This Page)

Practical 2: IP address: 50.116.6.205

Scan:-

```
anonymous@kali: ~
File  Actions  Edit  View  Help
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 18:04 IST
Nmap scan report for ftp.rrze.uni-erlangen.de (131.188.12.211)
Host is up (0.13s latency).
Not shown: 979 closed ports
PORT      STATE    SERVICE        VERSION
19/tcp    filtered chargen
21/tcp    open     ftp            ProFTPD
23/tcp    filtered telnet
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open     http           Apache httpd 2.4
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
161/tcp   filtered snmp
443/tcp   open     ssl/http       Apache httpd 2.4
444/tcp   filtered snpp
445/tcp   filtered microsoft-ds
873/tcp   open     rsync          (protocol version 31)
1434/tcp  filtered ms-sql-m
1900/tcp  filtered upnp
9000/tcp  filtered cslistener
9100/tcp  filtered jetdirect
13782/tcp filtered netbackup
16992/tcp filtered amt-soap-http
16993/tcp filtered amt-soap-https
Aggressive OS guesses: Linux 3.10 - 4.11 (94%), Linux 3.16 - 4.6 (93%), Linux 4.4 (93%), Linux 3.13 or 4.2 (92%), Linux 4.2 (92%), Linux 3.16 (92%), Linux
3.2 - 4.9 (92%), Linux 3.13 (91%), HP P2000 G3 NAS device (90%), Linux 3.18 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 20 hops
Service Info: Host: Welcome

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 31.74 seconds
root@kali:/home/anonymous#
```

server

1. Vulnerabilities:-
    a. On Proftpd: https://www.cvedetails.com/vulnerability-list/vendor_id-9520/product_id-16873/Proftpd-Proftpd.html

1	CVE-2019-12815	284		Exec Code	2019-07-19	2019-07-23	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.														
2	CVE-2017-7418	59		Bypass	2017-04-04	2019-08-08	2.1	None	Local	Low	Not required	None	Partial	None
ProFTPD before 1.3.5e and 1.3.6 before 1.3.6rc5 controls whether the home directory of a user could contain a symbolic link through the AllowChrootSymlinks configuration option, but checks only the last path component when enforcing AllowChrootSymlinks. Attackers with local access could bypass the AllowChrootSymlinks control by replacing a path component (other than the last one) with a symbolic link. The threat model includes an attacker who is not granted full filesystem access by a hosting provider, but can reconfigure the home directory of an FTP user.														
3	CVE-2016-3125	254			2016-04-05	2018-10-30	5.0	None	Remote	Low	Not required	Partial	None	None
The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.														
4	CVE-2015-3306	284			2015-05-18	2017-01-02	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.														
5	CVE-2013-4359	189		DoS Overflow	2013-09-30	2016-12-30	5.0	None	Remote	Low	Not required	None	None	Partial
Integer overflow in kbdint.c in mod_sftp in ProFTPD 1.3.4d and 1.3.5r3 allows remote attackers to cause a denial of service (memory consumption) via a large response count value in an authentication request, which triggers a large memory allocation.														
6	CVE-2012-6095	362			2013-01-24	2013-01-25	1.2	None	Local	High	Not required	None	Partial	None
ProFTPD before 1.3.5rc1, when using the UserOwner directive, allows local users to modify the ownership of arbitrary files via a race condition and a symlink attack on the (1) MKD or (2) XMKD commands.														
7	CVE-2011-4130	399		Exec Code	2011-12-06	2011-12-08	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
Use-after-free vulnerability in the Response API in ProFTPD before 1.3.3g allows remote authenticated users to execute arbitrary code via vectors involving an error that occurs after an FTP data transfer.														
8	CVE-2011-1137	189	1	DoS Overflow	2011-03-11	2011-09-06	5.0	None	Remote	Low	Not required	None	None	Partial
Integer overflow in the mod_sftp (aka SFTP) module in ProFTPD 1.3.3d and earlier allows remote attackers to cause a denial of service (memory consumption leading to OOM kill) via a malformed SSH message.														
9	CVE-2010-4652	119		DoS Exec Code Overflow	2011-02-01	2011-03-17	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Heap-based buffer overflow in the sql_prepare_where function (contrib/mod_sql.c) in ProFTPD before 1.3.3d, when mod_sql is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted username containing substitution tags, which are not properly handled during construction of an SQL query.														
10	CVE-2010-4221	119		Exec Code Overflow	2010-11-09	2011-09-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Multiple stack-based buffer overflows in the pr_netio_telnet_gets function in netio.c in ProFTPD before 1.3.3c allow remote attackers to execute arbitrary code via vectors involving a TELNET IAC escape character to a (1) FTP or (2) FTPS server.														
11	CVE-2010-3867	22		Dir. Trav.	2010-11-09	2011-09-14	7.1	None	Remote	High	Single system	Complete	Complete	Complete
Multiple directory traversal vulnerabilities in the mod_site_misc module in ProFTPD before 1.3.3c allow remote authenticated users to create directories, delete directories, create symlinks, and modify file timestamps via directory traversal sequences in a (1) SITE MKDIR, (2) SITE RMDIR, (3) SITE SYMLINK, or (4) SITE UTIME command.														
12	CVE-2009-3639	310		Bypass	2009-10-28	2017-08-16	5.8	None	Remote	Medium	Not required	None	Partial	Partial
The mod_tls module in ProFTPD before 1.3.2b, and 1.3.3 before 1.3.3rc2, when the dNSNameRequired TLS option is enabled, does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 client certificate, which allows remote attackers to bypass intended client-hostname restrictions via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.														
13	CVE-2009-0543	89		Sql Bypass	2009-02-12	2009-06-09	6.8	User	Remote	Medium	Not required	Partial	Partial	Partial
ProFTPD Server 1.3.1, with NLS support enabled, allows remote attackers to bypass SQL injection protection mechanisms via invalid, encoded multibyte characters, which are not properly handled in (1) mod_sql_mysql and (2) mod_sql_postgres.														
14	CVE-2008-7265	399		DoS	2010-11-09	2011-03-17	4.0	None	Remote	Low	Single system	None	None	Partial
The pr_data_xfer function in ProFTPD before 1.3.2rc3 allows remote authenticated users to cause a denial of service (CPU consumption) via an ABOR command during a data transfer.														
15	CVE-2001-0136	399		DoS	2001-03-12	2018-02-07	5.0	None	Remote	Low	Not required	None	None	Partial
Memory leak in ProFTPd 1.2.0rc2 allows remote attackers to cause a denial of service via a series of USER commands, and possibly SIZE commands if the server has been improperly installed.														

Total number of vulnerabilities : **15** Page : 1 (This Page)

b.On Apache 2.4:
https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-124859/Apache-Http-Server-2.4.0.html

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-10098	601			2019-09-25	2019-10-09	5.8	None	Remote	Medium	Not required	Partial	Partial	None
In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.														
2	CVE-2019-10092	79		XSS	2019-09-26	2019-09-30	4.3	None	Remote	Medium	Not required	None	Partial	None
In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.														
3	CVE-2019-0220	399			2019-06-11	2019-06-25	5.0	None	Remote	Low	Not required	Partial	None	None
A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.														
4	CVE-2018-17199	384			2019-01-30	2019-07-23	5.0	None	Remote	Low	Not required	None	Partial	None
In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.														
5	CVE-2018-1312	287			2018-03-26	2019-07-29	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.														
6	CVE-2018-1283	20			2018-03-26	2019-08-15	3.5	None	Remote	Medium	Single system	None	Partial	None
In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.														
7	CVE-2017-15715	20			2018-03-26	2019-08-15	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.														
8	CVE-2017-9798	416			2017-09-18	2019-04-23	5.0	None	Remote	Low	Not required	Partial	None	None
Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.														
9	CVE-2017-9788	20		DoS +Info	2017-07-13	2019-08-15	6.4	None	Remote	Low	Not required	Partial	None	Partial
In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.														
10	CVE-2017-7679	119		Overflow	2017-06-19	2018-06-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.														
11	CVE-2016-8612	20			2018-03-09	2019-10-09	3.3	None	Local Network	Low	Not required	None	None	Partial
Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.														
12	CVE-2016-2161	20			2017-07-27	2018-04-24	5.0	None	Remote	Low	Not required	None	None	Partial
In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.														
12	CVE-2016-2161	20			2017-07-27	2018-04-24	5.0	None	Remote	Low	Not required	None	None	Partial
In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.														
13	CVE-2016-0736	310			2017-07-27	2018-04-24	5.0	None	Remote	Low	Not required	Partial	None	None
In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.														
14	CVE-2015-3185	264		Bypass	2015-07-20	2018-01-04	4.3	None	Remote	Medium	Not required	None	Partial	None
The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.														
15	CVE-2014-8109	264		Bypass	2014-12-29	2016-12-30	4.3	None	Remote	Medium	Not required	None	Partial	None
mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.														
16	CVE-2014-0098	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.														
17	CVE-2013-6438	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.														
18	CVE-2013-2249				2013-07-23	2017-01-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.														
19	CVE-2012-4558	79		XSS	2013-02-26	2017-09-18	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.														
20	CVE-2012-3502	200		+Info	2012-08-22	2013-04-18	4.3	None	Remote	Medium	Not required	Partial	None	None
The proxy functionality in (1) mod_proxy_ajp.c in the mod_proxy_ajp module and (2) mod_proxy_http.c in the mod_proxy_http module in the Apache HTTP Server 2.4.x before 2.4.3 does not properly determine the situations that require closing a back-end connection, which allows remote attackers to obtain sensitive information in opportunistic circumstances by reading a response that was intended for a different client.														
21	CVE-2012-3499	79		XSS	2013-02-26	2017-09-18	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.														
22	CVE-2012-2687	79		XSS	2012-08-22	2017-09-18	2.6	None	Remote	High	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.														
23	CVE-2012-0883	264		+Priv	2012-04-18	2017-12-28	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.														

Total number of vulnerabilities : **23** Page : 1 (This Page)