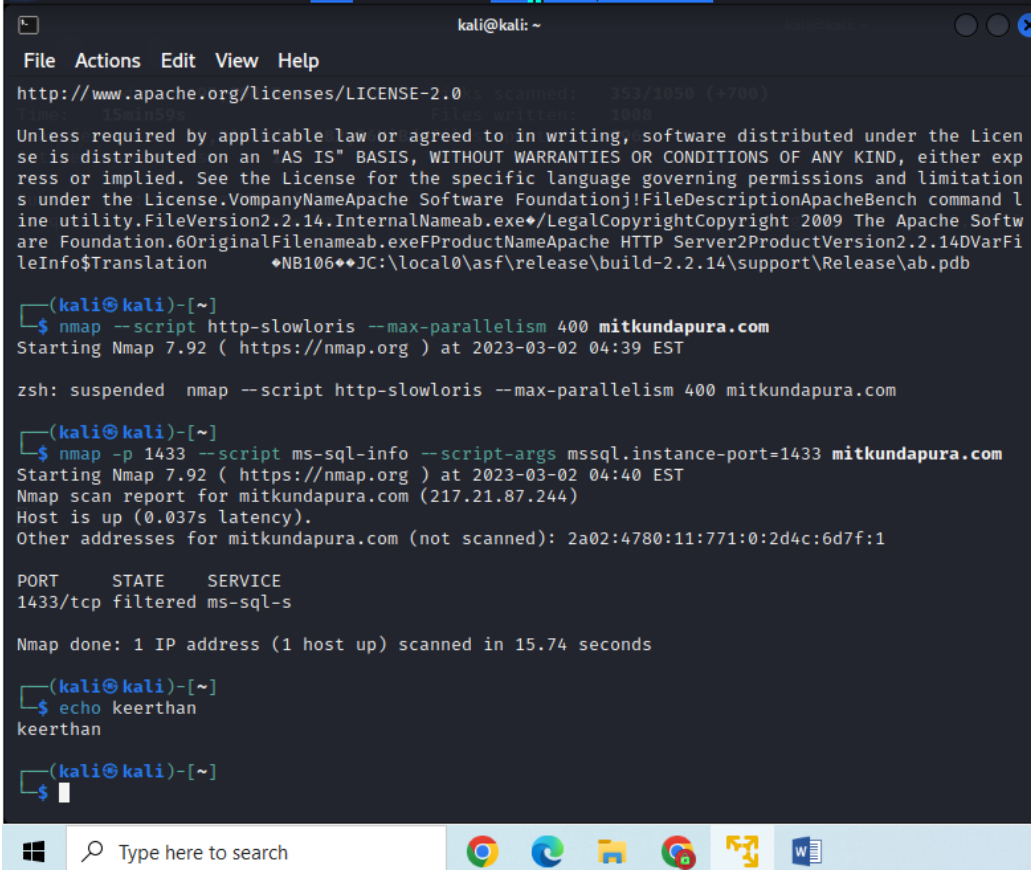


2. Sql empty password enumeration scanning using nmap:

Command:

```
$nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433
```

mitkundapura.com



```
kali@kali: ~  
File Actions Edit View Help  
http://www.apache.org/licenses/LICENSE-2.0 scanned: 353/1050 (+700)  
1501/100% 1155 ms111ms 100%  
Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either expressed or implied. See the License for the specific language governing permissions and limitations under the License.VompanyNameApache Software Foundationj!FileDescriptionApacheBench command line utility.FileVersion2.2.14.InternalNameab.exeLegalCopyrightCopyright 2009 The Apache Software Foundation.6OriginalFilenameab.exeFProductNameApache HTTP Server2ProductVersion2.2.140VarFileInfo$Translation ◆NB106◆JC:\local0\asf\release\build-2.2.14\support\Release\ab.pdb  
  
(kali@kali)-[~]  
$ nmap --script http-slowloris --max-parallelism 400 mitkundapura.com  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:39 EST  
  
zsh: suspended nmap --script http-slowloris --max-parallelism 400 mitkundapura.com  
  
(kali@kali)-[~]  
$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:40 EST  
Nmap scan report for mitkundapura.com (217.21.87.244)  
Host is up (0.037s latency).  
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1  
  
PORT      STATE      SERVICE  
1433/tcp  filtered  ms-sql-s  
  
Nmap done: 1 IP address (1 host up) scanned in 15.74 seconds  
  
(kali@kali)-[~]  
$ echo keerthan  
keerthan  
  
(kali@kali)-[~]  
$
```

3. Vulnerability scan using nmap:

Command:

```
$ nmap -sV --script vuln mitkundapura.com
```

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 03:05 EST
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 03:07 (0:00:00 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.043s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD or KnFTPD
| ssl-dh-params:
| VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|   State: VULNERABLE
|     Transport Layer Security (TLS) services that use Diffie-Hellman groups
|     of insufficient strength, especially those using one of a few commonly
|     shared groups, may be susceptible to passive eavesdropping attacks.
|   Check results:
|     WEAK DH GROUP 1
|       Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
|       Modulus Type: Safe prime
|       Modulus Source: Unknown/Custom-generated
|       Modulus Length: 1024
|       Generator Length: 8
|       Public Key Length: 1024
|   References:
|     https://weakdh.org
|_
80/tcp    open  tcpwrapped
|_ http-server-header: LiteSpeed
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.

firewall.png

kali@kali: ~
File Actions Edit View Help
SF:%;\x20">\x20\x20\x20\x20\x20<div\x20style="\text-align:\x20center;\x20
SF:width:800px;\x20margin-left:\x20-400px;\x20position:absolute;\x20top:\x
SF:2030%;\x20left:50%;"\>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20style="\
SF:margin:0;\x20font-size:150px;\x20line-height:150px;\x20font-weight:bold
SF:;\x20">\x20403</h1>\n<h2\x20style="\margin-top:20px;font-size:\x2030px;\x20">Forb
SF:idden\r\n</h2>\n<p>Access\x20to\x20this\x20resource")%r(HTTPOptions,3BD
SF:,"HTTP/1.0\x20403\x20Forbidden\r\nConnection:\x20close\r\ncache-contro
SF:l:\x20private,\x20no-cache,\x20no-store,\x20must-revalidate,\x20max-age
SF:=0\r\npragma:\x20no-cache\r\ncontent-type:\x20text/html\r\ncontent-leng
SF:th:\x20699\r\ndate:\x20Thu,\x2002\x20Mar\x202023\x2009:27:05\x20GMT\r\n
SF:server:\x20LiteSpeed\r\nplatform:\x20hostinger\r\n\r\n<!DOCTYPE\x20html
SF:>\n<html\x20style="\height:100%;"\>\n<head>\n<meta\x20name="\viewport"
SF:x20content="\width=device-width,\x20initial-scale=1,\x20shrink-to-fit=n
SF:o"\x20/>\n<title>\x20403\x20Forbidden\r\n</title></head>\n<body\x20sty
SF:le="\color:\x20#444;\x20margin:0;font:\x20normal\x2014px/20px\x20Arial,
SF:\x20Helvetica,\x20sans-serif;\x20height:100%; \x20background-color:\x20#
SF:fff;\x20">\n<div\x20style="\height:auto;\x20min-height:100%;\x20">\x20\x2
SF:0\x20\x20\x20<div\x20style="\text-align:\x20center;\x20width:800px;\x20
SF:margin-left:\x20-400px;\x20position:absolute;\x20top:\x2030%;\x20left:5
SF:0%;"\>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20style="\margin:0;\x20fon
SF:t-size:150px;\x20line-height:150px;\x20font-weight:bold;\x20">\x20403</h1>\n<h
SF:2\x20style="\margin-top:20px;font-size:\x2030px;\x20">Forbidden\r\n</h2>\n
SF:<p>Access\x20to\x20this\x20resource");
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 507.65 seconds

(kali@kali)-[~]
$ echo keerthan
keerthan
```

4. Create a password list using characters "fghy" the password should be minimum and maximum length 4 letters using tool hydra

Command:

\$crunch 4 4 fghy -o pass.txt

```
kali@kali: ~  
File Actions Edit View Help  
197.48MB Links Scanned: 360/1083 (+726)  
File Position: 1043  
(kali@kali)-[~]  
$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:40 EST  
Nmap scan report for mitkundapura.com (217.21.87.244)  
Host is up (0.037s latency).  
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1  
PORT      STATE      SERVICE  
1433/tcp  filtered  ms-sql-s  
Nmap done: 1 IP address (1 host up) scanned in 15.74 seconds  
(kali@kali)-[~]  
$ echo keerthan  
keerthan  
(kali@kali)-[~]  
$ crunch 4 4 fghy -o wordlist.txt  
Crunch will now generate the following amount of data: 1280 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 256  
crunch: 100% completed generating output  
(kali@kali)-[~]  
$ echo keerthan  
keerthan
```

5. Wordpress scan using nmap:

Command:

\$nmap -sV --script http-wordpress-enum mitkundapura.com

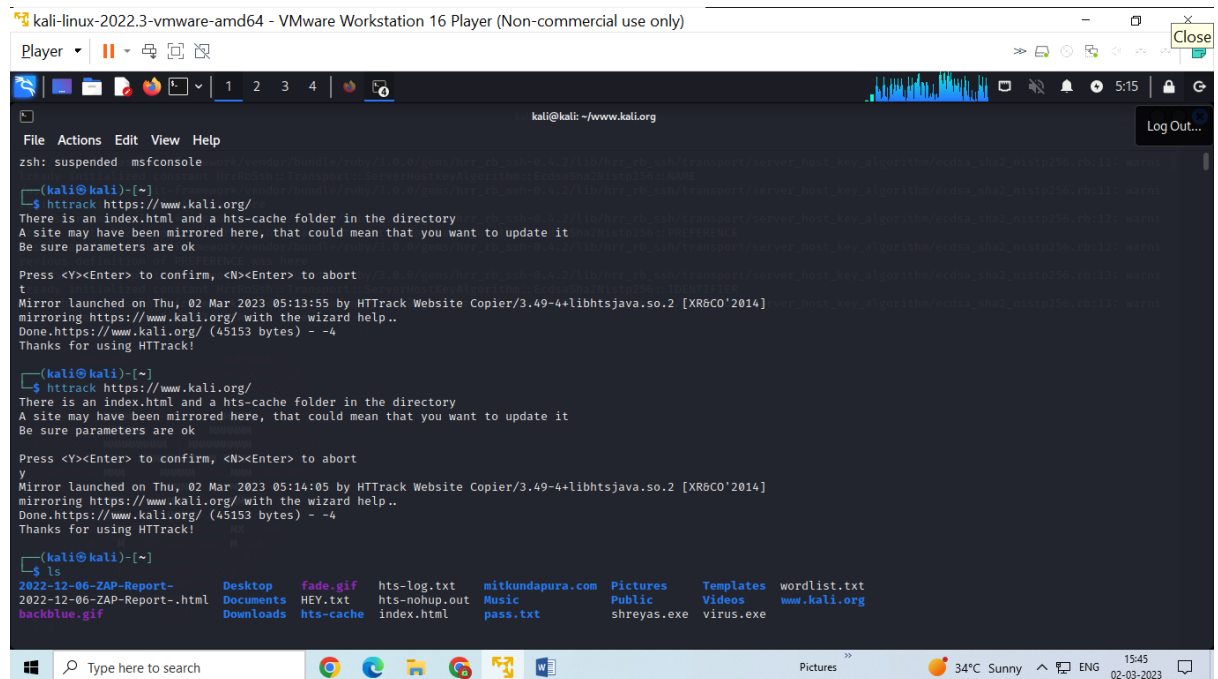
```
Minimize all open windows and show the desktop  
File Actions Edit View Help  
There is a lock-file in the directory  
That means that a mirror has not been terminated  
Be sure you call httrack with proper parameters  
(The cache allows you to restart faster the transfer)  
Press <Y><Enter> to confirm, <N><Enter> to abort  
^Z  
Moving into background to complete the mirror...  
(kali@kali)-[~]  
$ httrack https://www.kali.org/  
There is an index.html and a hts-cache folder in the directory  
A site may have been mirrored here, that could mean that you want to update it  
Be sure parameters are ok  
Press <Y><Enter> to confirm, <N><Enter> to abort  
Mirrors launched on Thu, 02 Mar 2023 04:52:31 by HTTrack Website Copier/3.49-4+libhtsjava.so.2 [XR6CO'2014]  
mirroring https://www.kali.org/ with the wizard help..  
Done.https://www.kali.org/ (45153 bytes) ~ -4  
Thanks for using HTTrack!  
(kali@kali)-[~]  
$ ls  
2022-12-06-ZAP-Report- Desktop fude.gif hts-log.txt mitkundapura.com Pictures Templates wordlist.txt  
2022-12-06-ZAP-Report-.html Documents HEY.txt hts-nohup.out Music Public Videos www.kali.org  
hackblue.gif Downloads hts-cache index.html pass.txt shreyas.exe virus.exe  
(kali@kali)-[~]  
$ echo keerthan  
keerthan
```


6. What is use of HTTrack?command to copy website?

HTTrack is a free and open source website copying tool that allows you to download an entire website to your local computer for offline browsing.

Command for copying website:

\$httrack mitkundapura.com



```
kali@kali: ~/www.kali.org
File Actions Edit View Help
zsh: suspended msfconsole

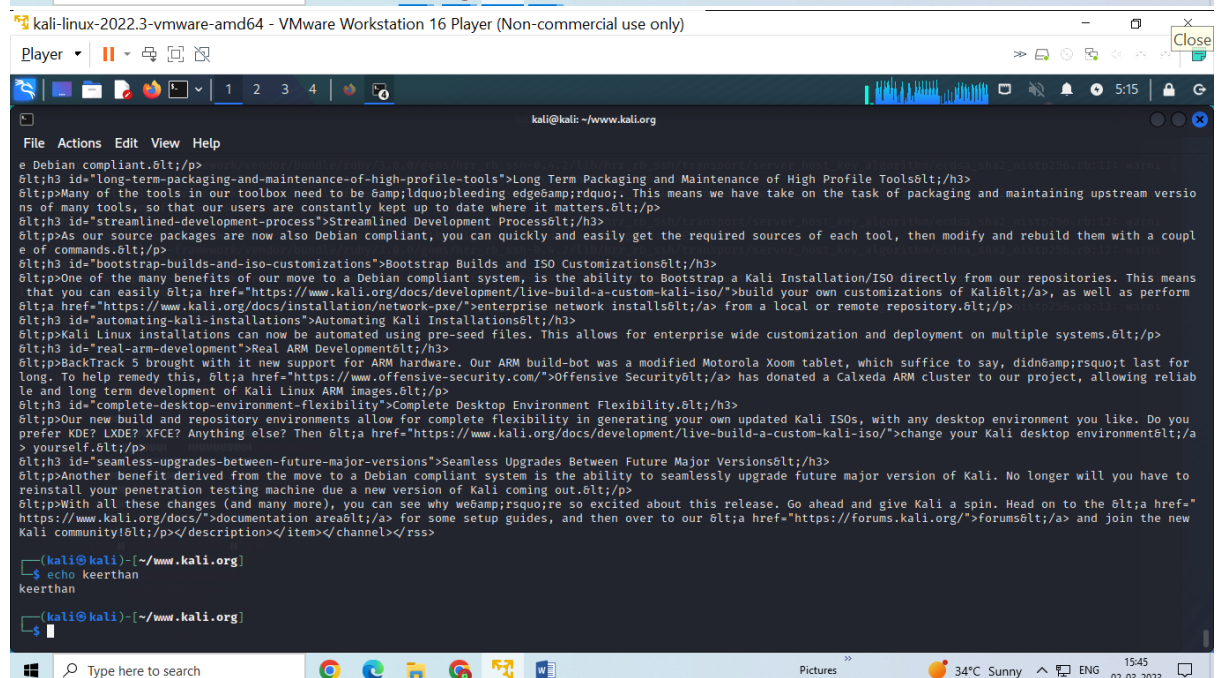
(kali@kali)-[~]
└─$ httrack https://www.kali.org/
There is an index.html and a hts-cache folder in the directory
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok

Press <Y><Enter> to confirm, <N><Enter> to abort
t
Mirror launched on Thu, 02 Mar 2023 05:13:55 by HTTrack Website Copier/3.49-4+libhtsjava.so.2 [XR8CO'2014]
mirroring https://www.kali.org/ with the wizard help..
Done:https://www.kali.org/ (45153 bytes) - -4
Thanks for using HTTrack!

(kali@kali)-[~]
└─$ httrack https://www.kali.org/
There is an index.html and a hts-cache folder in the directory
A site may have been mirrored here, that could mean that you want to update it
Be sure parameters are ok

Press <Y><Enter> to confirm, <N><Enter> to abort
y
Mirror launched on Thu, 02 Mar 2023 05:14:05 by HTTrack Website Copier/3.49-4+libhtsjava.so.2 [XR8CO'2014]
mirroring https://www.kali.org/ with the wizard help..
Done:https://www.kali.org/ (45153 bytes) - -4
Thanks for using HTTrack!

(kali@kali)-[~]
└─$ ls
2022-12-06-ZAP-Report- Desktop f4de.gif hts-log.txt mitkundapura.com Pictures Templates wordlist.txt
2022-12-06-ZAP-Report-.html Documents HEY.txt hts-nohup.out Music Public Videos www.kali.org
backbue.gif Downloads hts-cache index.html pass.txt shreyas.exe virus.exe
```



```
kali@kali: ~/www.kali.org
File Actions Edit View Help

e Debian compliant.</p>
</h3>id="long-term-packaging-and-maintenance-of-high-profile-tools">Long Term Packaging and Maintenance of High Profile Tools</h3>
</p><p>Many of the tools in our toolbox need to be &ldquo;bleeding edge&rdquo;. This means we have take on the task of packaging and maintaining upstream versio
ns of many tools, so that our users are constantly kept up to date where it matters.</p>
</h3>id="streamlined-development-process">Streamlined Development Process</h3>
</p><p>As our source packages are now also Debian compliant, you can quickly and easily get the required sources of each tool, then modify and rebuild them with a coupl
e of commands.</p>
</h3>id="bootstrap-builds-and-iso-customizations">Bootstrap Builds and ISO Customizations</h3>
</p><p>One of the many benefits of our move to a Debian compliant system, is the ability to Bootstrap a Kali Installation/ISO directly from our repositories. This means
that you can easily <a href="https://www.kali.org/docs/development/live-build-a-custom-kali-iso/">build your own customizations of Kali</a>, as well as perform
<a href="https://www.kali.org/docs/installation/network-pxe/">enterprise network installs</a> from a local or remote repository.</p>
</h3>id="automating-kali-installations">Automating Kali Installations</h3>
</p><p>Kali Linux installations can now be automated using pre-seed files. This allows for enterprise wide customization and deployment on multiple systems.</p>
</h3>id="real-arm-development">Real ARM Development</h3>
</p><p>BackTrack 5 brought with it new support for ARM hardware. Our ARM build-bot was a modified Motorola Xoom tablet, which suffice to say, didn&rsquo;t last for
long. To help remedy this, <a href="https://www.offensive-security.com/">Offensive Security</a> has donated a Calxeda ARM cluster to our project, allowing reliab
le and long term development of Kali Linux ARM images.</p>
</h3>id="complete-desktop-environment-flexibility">Complete Desktop Environment Flexibility</h3>
</p><p>Our new build and repository environments allow for complete flexibility in generating your own updated Kali ISOs, with any desktop environment you like. Do you
prefer KDE? LXDE? XFCE? Anything else? Then <a href="https://www.kali.org/docs/development/live-build-a-custom-kali-iso/">change your Kali desktop environment</a>
> yourself.</p>
</h3>id="seamless-upgrades-between-future-major-versions">Seamless Upgrades Between Future Major Versions</h3>
</p><p>Another benefit derived from the move to a Debian compliant system is the ability to seamlessly upgrade future major version of Kali. No longer will you have to
reinstall your penetration testing machine due a new version of Kali coming out.</p>
</p><p>With all these changes (and many more), you can see why we&rsquo;re so excited about this release. Go ahead and give Kali a spin. Head on to the <a href="
https://www.kali.org/docs/">documentation area</a> for some setup guides, and then over to our <a href="https://forums.kali.org/">forums</a> and join the new
Kali community!</p></description></item></channel></rss>

(kali@kali)-[~/www.kali.org]
└─$ echo keerthan
keerthan

(kali@kali)-[~/www.kali.org]
└─$
```