Name : Sanketh

Reg. No: 145CS21704

Date : 28-02-2023

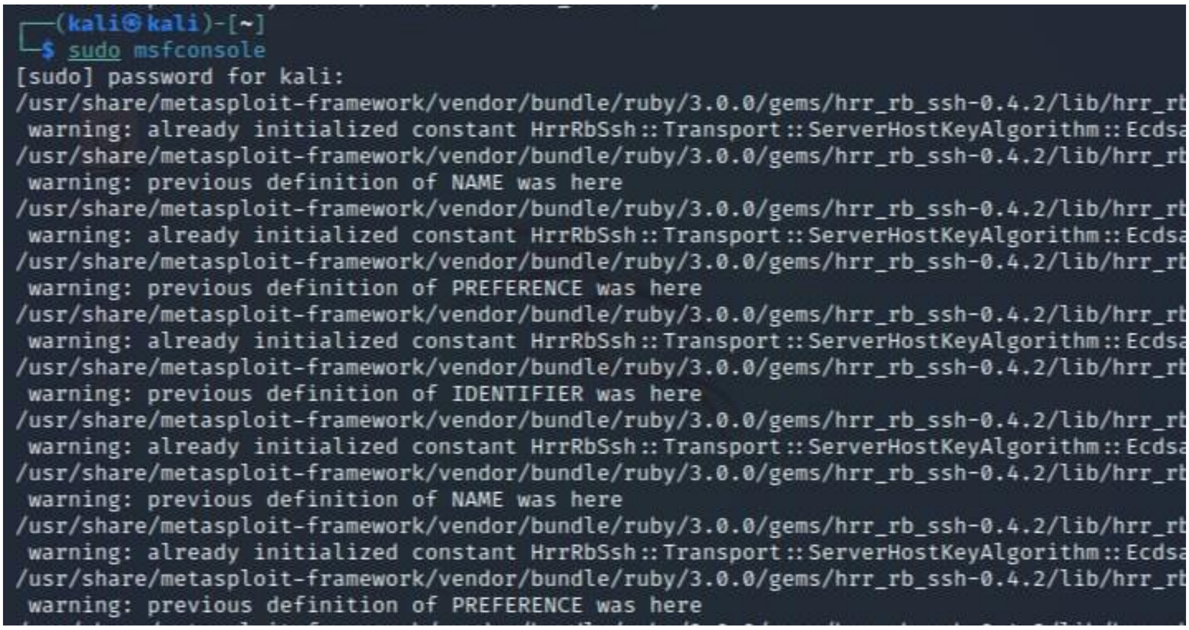
Task:1

1. **Dos attack using nmap:**

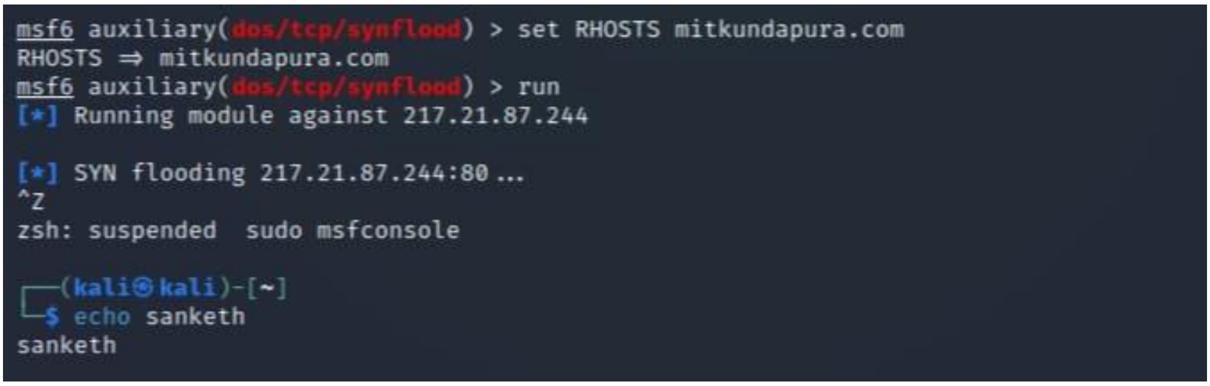
   The nmap scripting engine has numerous scripts that can be used to perform dos attack.This specific recipe will demonstrate how to locate dos scripts,identity the usage of the script.

   command:

   - $ 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
 warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::Ecdsa
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::Ecdsa
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::Ecdsa
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::Ecdsa
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::Ecdsa
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb
 warning: previous definition of PREFERENCE was here
```



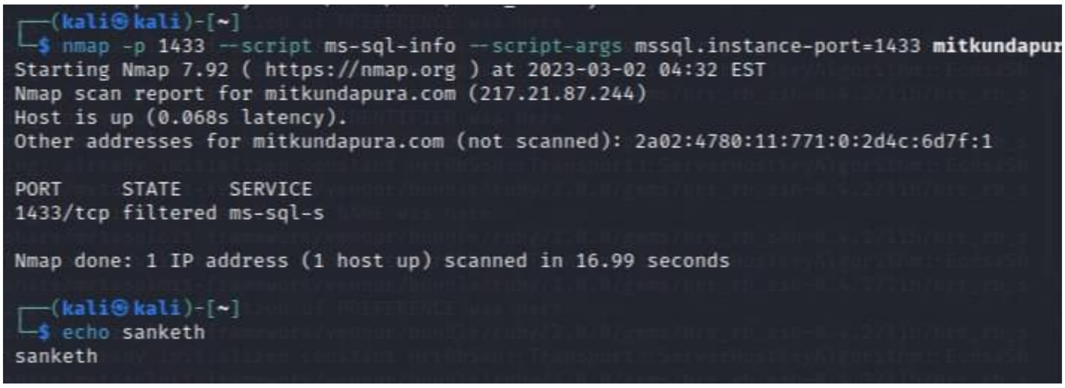
```
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS mitkundapura.com
RHOSTS ⇒ mitkundapura.com
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 217.21.87.244

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

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

2. **<u>Sql empty password enumeration scanning using nmap</u>:**

Nmap is one of the most popular tool used for the enumeration of the target host.Nmap can use scans that provide os,version and service detection for individual or multiple devices.

Command:

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



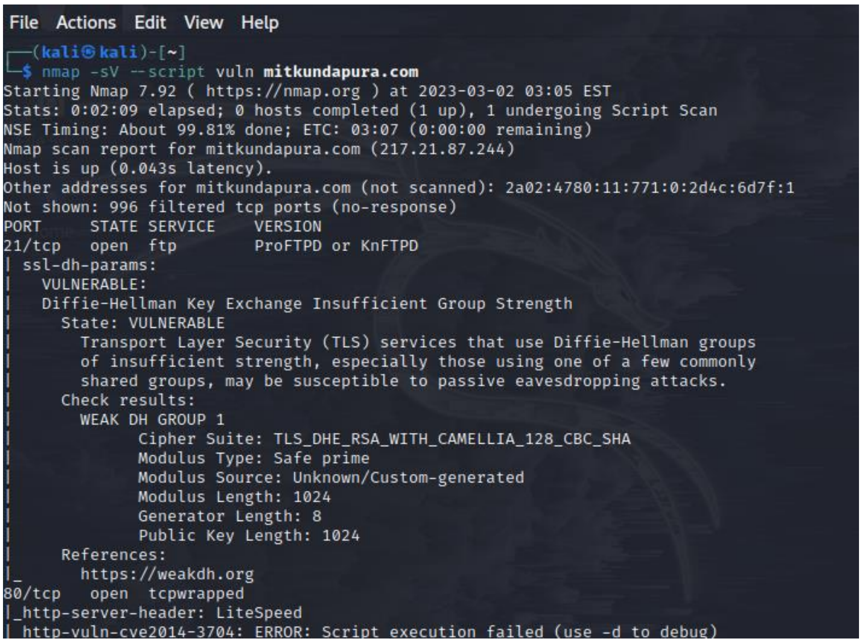
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1433 --script ms-sql-info --script-args mssql.instance-port=1433 mitkundapur
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:32 EST
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.068s latency).
Other addresses for mitkundapura.com (not 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 16.99 seconds

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

3 Vulnerability scan using nmap:

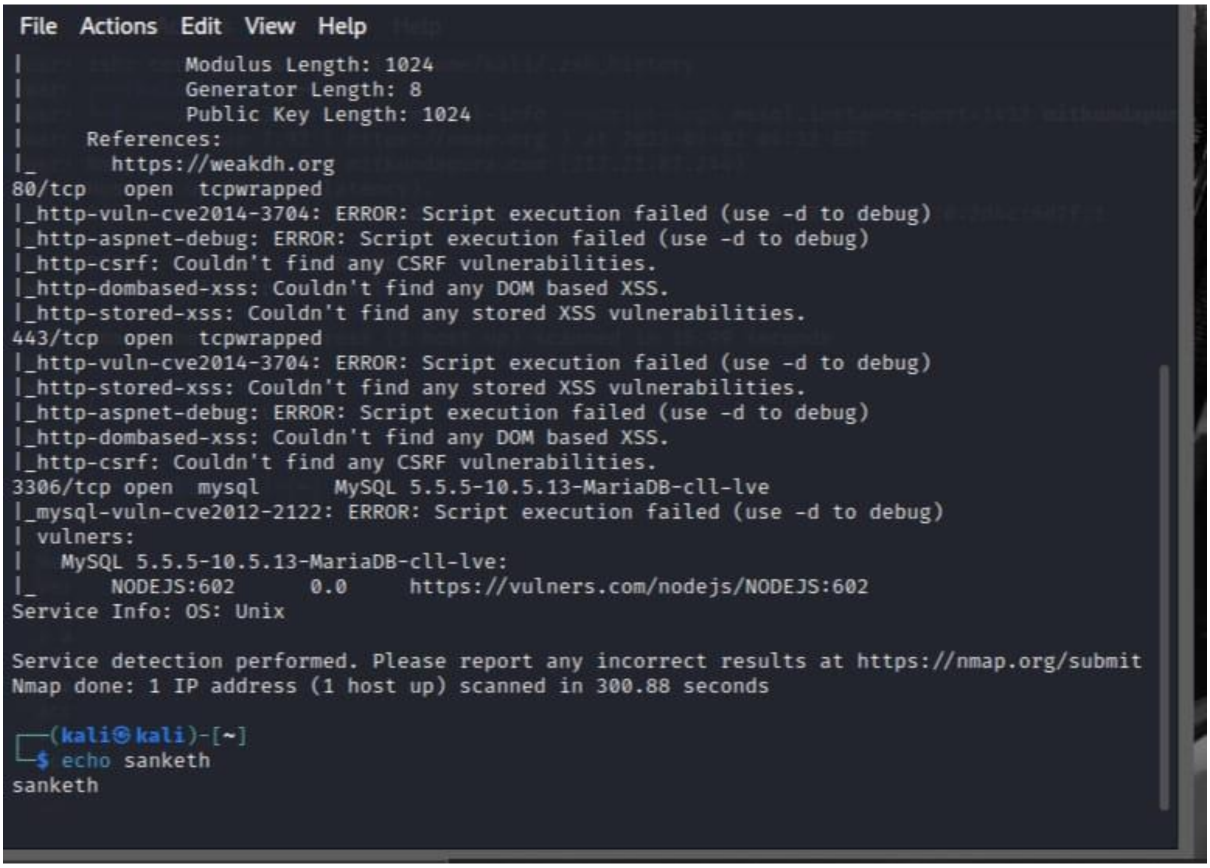
One of the most well known vulnerability scanner is nmap_vulner.Thenmap script engine searches HTTP responses to identity CPE’s for the script.

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 03:05 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)
```



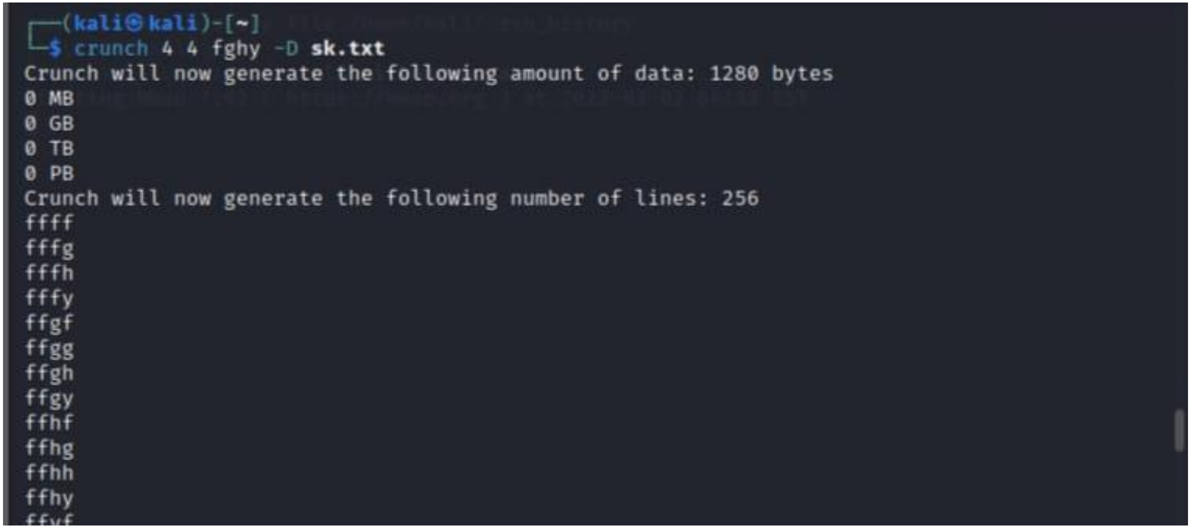
```
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
80/tcp   open  tcpwrapped
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open  tcpwrapped
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
3306/tcp open  mysql      MySQL 5.5.5-10.5.13-MariaDB-cll-lve
|_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
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 300.88 seconds

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

4 Create a password list using charecters “fghy” the password should be minimum and maximum length 4 letters using tool crunch

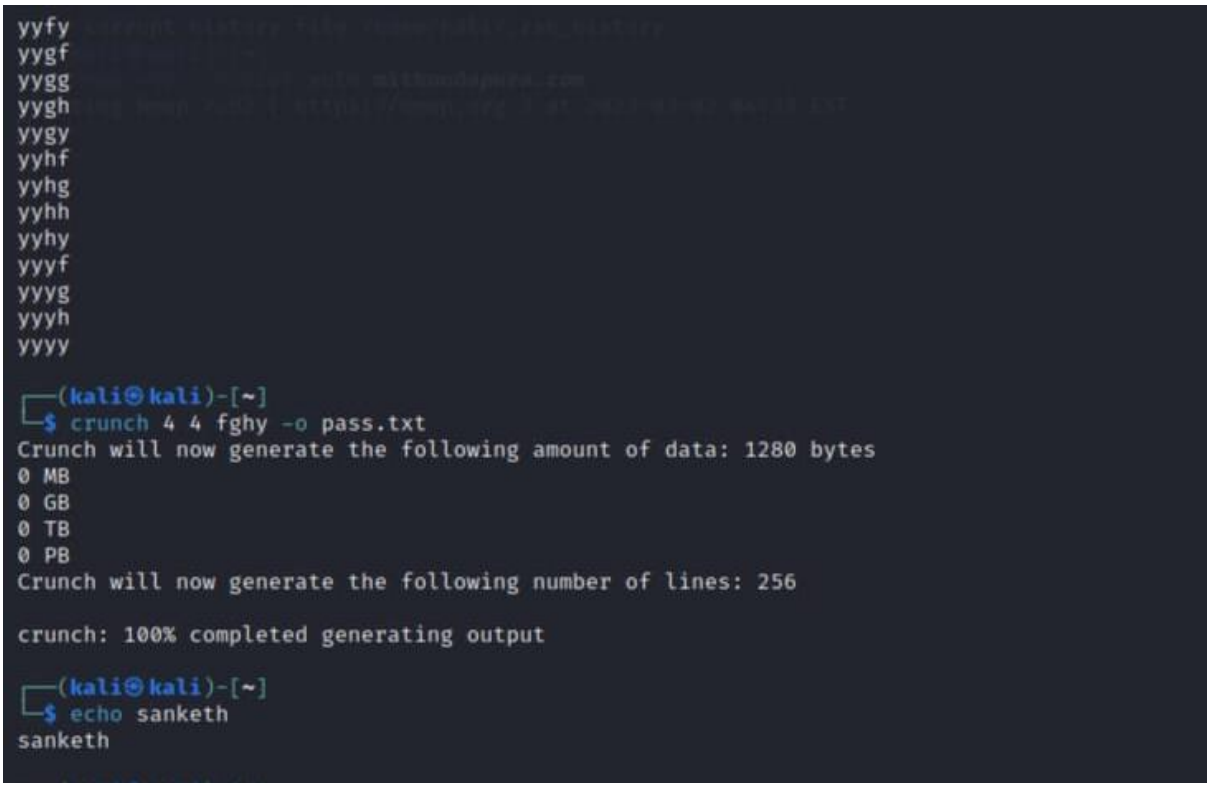
Generate all possible combinations of the characters "fghy" with a length of characters and output them to a file called "wordlist.txt". We can adjust the minimum and maximum length by changing the first two parameters (4 4 in this example) to the desired values.

Command:

```
$crunch 4 4 fghy –o pass.txt
```



```
┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -D sk.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
ffff
fffg
fffh
fffy
ffgf
ffgg
ffgh
ffgy
ffhf
ffhg
ffhh
ffhy
ffyf
```



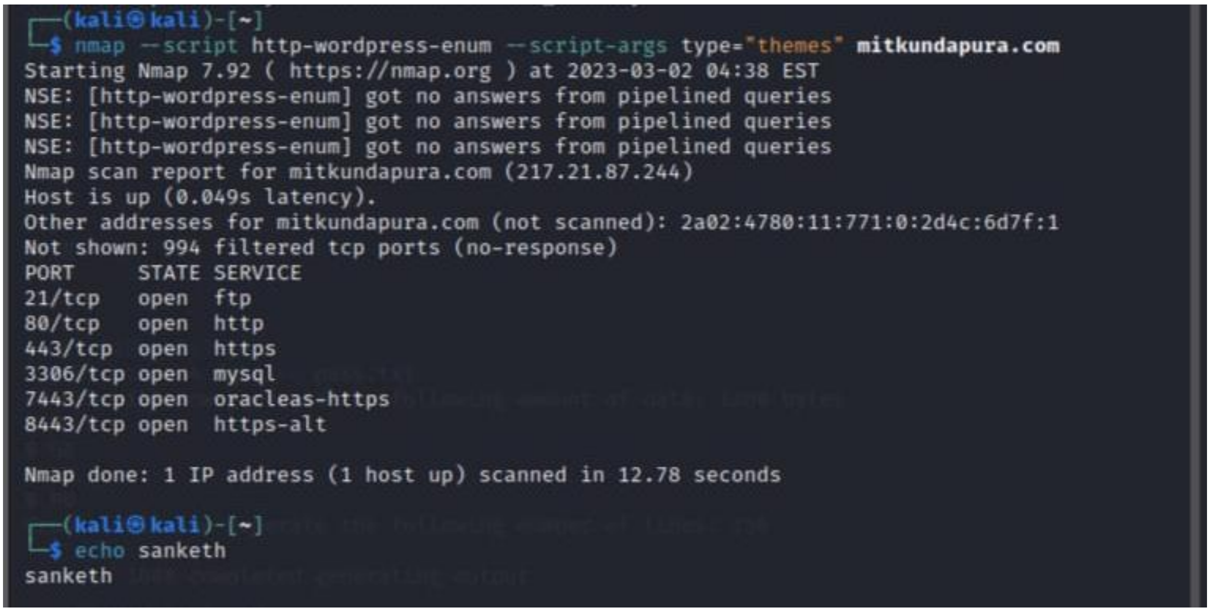
```
yyfy
yygf
yygg
yygh
yygy
yyhf
yyhg
yyhh
yyhy
yyyf
yyyg
yyyh
yyyy

┌──(kali㉿kali)-[~]
└─$ crunch 4 4 fghy -o pass.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 sanketh
sanketh
```

5 **Wordpress scan using nmap:**

Word press as a publishing platform,security testing is the important part of ensuring the installation is secure.Nmap has a couple of NSE scripts specifically for the testing of wordpress installations.

Command:

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



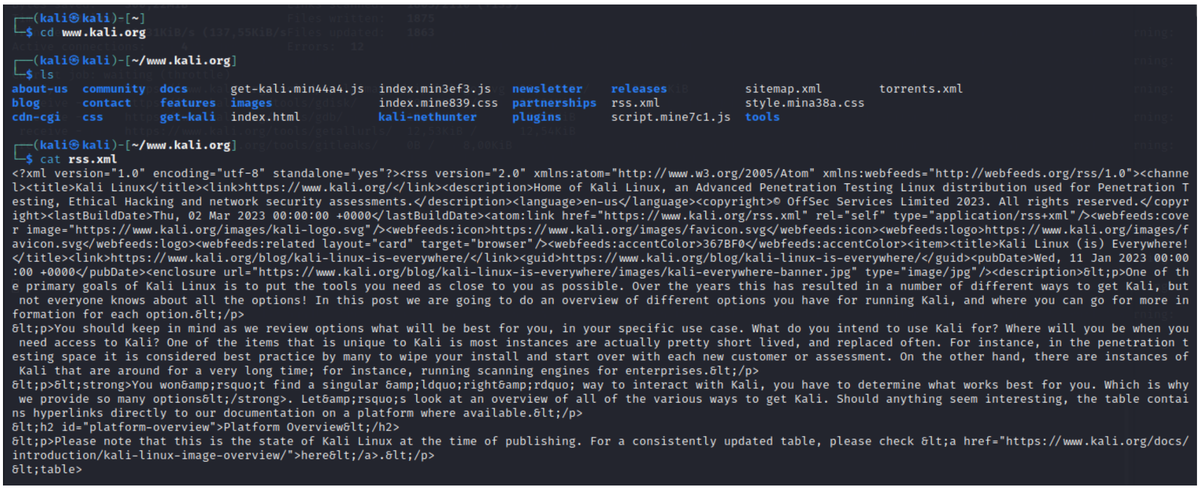
```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-wordpress-enum --script-args type="themes" mitkundapura.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-02 04:38 EST
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
NSE: [http-wordpress-enum] got no answers from pipelined queries
Nmap scan report for mitkundapura.com (217.21.87.244)
Host is up (0.049s latency).
Other addresses for mitkundapura.com (not scanned): 2a02:4780:11:771:0:2d4c:6d7f:1
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
7443/tcp open  oracleas-https
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 12.78 seconds

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

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

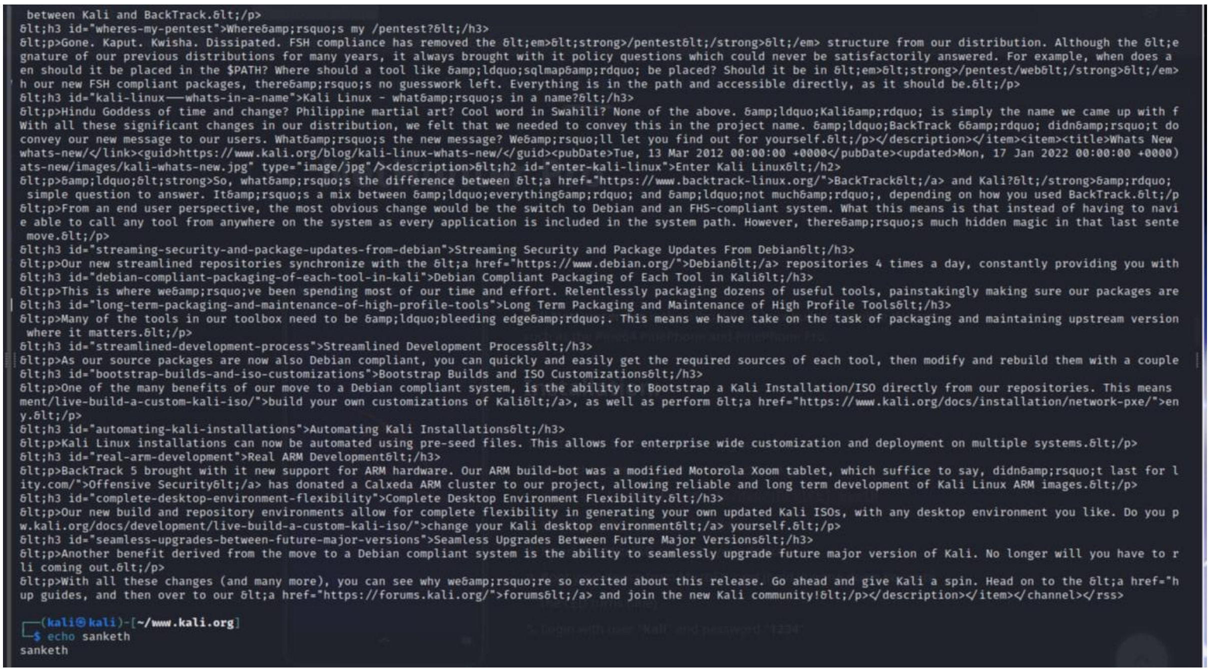
HTTrack is a free and open source website copying tool that allows you to download an entire website to your local computer for offline browsing.

Command for copying website:

$httrack www.kali.org



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

┌──(kali㉿kali)-[~/www.kali.org]
└─$ ls
about-us  community  docs      get-kali.min44a4.js  index.min3ef3.js   newsletter    releases           sitemap.xml       torrents.xml
blog      contact    features  images               index.mine839.css  partnerships  rss.xml            style.mina38a.css
cdn-cgi   css        get-kali  index.html           kali-nethunter     plugins       script.mine7c1.js  tools

┌──(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:webfeeds="http://webfeeds.org/rss/1.0"><channe
l><title>Kali Linux</title><link>https://www.kali.org/</link><description>Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration T
esting, Ethical Hacking and network security assessments.</description><language>en-us</language><copyright>© OffSec Services Limited 2023. All rights reserved.</copyr
ight><lastBuildDate>Thu, 02 Mar 2023 00:00:00 +0000</lastBuildDate><atom:link href="https://www.kali.org/rss.xml" rel="self" type="application/rss+xml"/><webfeeds:cove
r image="https://www.kali.org/images/kali-logo.svg"/><webfeeds:icon>https://www.kali.org/images/favicon.svg</webfeeds:icon><webfeeds:logo>https://www.kali.org/images/f
avicon.svg</webfeeds:logo><webfeeds:related layout="card" target="browser"/><webfeeds:accentColor>367BF0</webfeeds:accentColor><item><title>Kali Linux (is) Everywhere!
</title><link>https://www.kali.org/blog/kali-linux-is-everywhere/</link><guid>https://www.kali.org/blog/kali-linux-is-everywhere/</guid><pubDate>Wed, 11 Jan 2023 00:00
:00 +0000</pubDate><enclosure url="https://www.kali.org/blog/kali-linux-is-everywhere/images/kali-everywhere-banner.jpg" type="image/jpg"/><description>&lt;p>One of th
e primary goals of Kali Linux is to put the tools you need as close to you as possible. Over the years this has resulted in a number of different ways to get Kali, but
 not everyone knows about all the options! In this post we are going to do an overview of different options you have for running Kali, and where you can go for more in
formation 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 use Kali for? Where will you be when you
 need access to Kali? One of the items that is unique to Kali is most instances are actually pretty short lived, and replaced often. For instance, in the penetration t
esting space it is considered best practice by many to wipe your install and start over with each new customer or assessment. On the other hand, there are instances of
 Kali that are around for a very long time; for instance, running scanning engines for enterprises.&lt;/p>
&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 determine what works best for you. Which is why
 we provide so many options&lt;/strong>. Let&amp;rsquo;s look at an overview of all of the various ways to get Kali. Should anything seem interesting, the table contai
ns hyperlinks directly to our documentation on a platform where available.&lt;/p>
&lt;h2 id="platform-overview">Platform Overview&lt;/h2>
&lt;p>Please note that this is the state of Kali Linux at the time of publishing. For a consistently updated table, please check &lt;a href="https://www.kali.org/docs/
introduction/kali-linux-image-overview/">here&lt;/a>.&lt;/p>
&lt;table>
```



```
 between Kali and BackTrack.&lt;/p>
&lt;h3 id="wheres-my-pentest">Where&amp;rsquo;s my /pentest?&lt;/h3>
&lt;p>Gone. Kaput. Kwisha. Dissipated. FSH compliance has removed the &lt;em>&lt;strong>/pentest&lt;/strong>&lt;/em> structure from our distribution. Although the &lt;e
gnature of our previous distributions for many years, it always brought with it policy questions which could never be satisfactorily answered. For example, when does a
en should it be placed in the $PATH? Where should a tool like &amp;ldquo;sqlmap&amp;rdquo; be placed? Should it be in &lt;em>&lt;strong>/pentest/web&lt;/strong>&lt;/em>
h our new FSH compliant packages, there&amp;rsquo;s no guesswork left. Everything is in the path and accessible directly, as it should be.&lt;/p>
&lt;h3 id="kali-linux——whats-in-a-name">Kali Linux - what&amp;rsquo;s in a name?&lt;/h3>
&lt;p>Hindu Goddess of time and change? Philippine martial art? Cool word in Swahili? None of the above. &amp;ldquo;Kali&amp;rdquo; is simply the name we came up with f
With all these significant changes in our distribution, we felt that we needed to convey this in the project name. &amp;ldquo;BackTrack 6&amp;rdquo; didn&amp;rsquo;t do
convey our new message to our users. What&amp;rsquo;s the new message? We&amp;rsquo;ll let you find out for yourself.&lt;/p></description></item><item><title>Whats New
whats-new/</link><guid>https://www.kali.org/blog/kali-linux-whats-new/</guid><pubDate>Tue, 13 Mar 2012 00:00:00 +0000</pubDate><updated>Mon, 17 Jan 2022 00:00:00 +0000)
ats-new/images/kali-whats-new.jpg" type="image/jpg"/><description>&lt;h2 id="enter-kali-linux">Enter Kali Linux&lt;/h2>
&lt;p>&amp;ldquo;&lt;strong>So, what&amp;rsquo;s the difference between &lt;a href="https://www.backtrack-linux.org/">BackTrack&lt;/a> and Kali?&lt;/strong>&amp;rdquo;
 simple question to answer. It&amp;rsquo;s a mix between &amp;ldquo;everything&amp;rdquo; and &amp;ldquo;not much&amp;rdquo;, depending on how you used BackTrack.&lt;/p
&lt;p>From an end user perspective, the most obvious change would be the switch to Debian and an FHS-compliant system. What this means is that instead of having to navi
e able to call any tool from anywhere on the system as every application is included in the system path. However, there&amp;rsquo;s much hidden magic in that last sente
 move.&lt;/p>
&lt;h3 id="streaming-security-and-package-updates-from-debian">Streaming Security and Package Updates From Debian&lt;/h3>
&lt;p>Our new streamlined repositories synchronize with the &lt;a href="https://www.debian.org/">Debian&lt;/a> repositories 4 times a day, constantly providing you with
&lt;h3 id="debian-compliant-packaging-of-each-tool-in-kali">Debian Compliant Packaging of Each Tool in Kali&lt;/h3>
&lt;p>This is where we&amp;rsquo;ve been spending most of our time and effort. Relentlessly packaging dozens of useful tools, painstakingly making sure our packages are
&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 packaging and maintaining upstream version
 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, then modify and rebuild them with a couple
&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 directly from our repositories. This means
ment/live-build-a-custom-kali-iso/">build your own customizations of Kali&lt;/a>, as well as perform &lt;a href="https://www.kali.org/docs/installation/network-pxe/">en
y.&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 deployment 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 suffice to say, didn&amp;rsquo;t last for l
ity.com/">Offensive Security&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 any desktop environment you like. Do you p
w.kali.org/docs/development/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 version of Kali. No longer will you have to r
li 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="h
up guides, and then over to our &lt;a href="https://forums.kali.org/">forums&lt;/a> and join the new Kali community!&lt;/p></description></item></channel></rss>

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