Name = Aadish Rakesh Chougala

Reg number = 21BCE5296

College = Vellore institute of Technology, Chennai

Email = aadishrakesh.chougala2021@vitstudent.ac.in

Assignment number 2

Kali linux tools study work

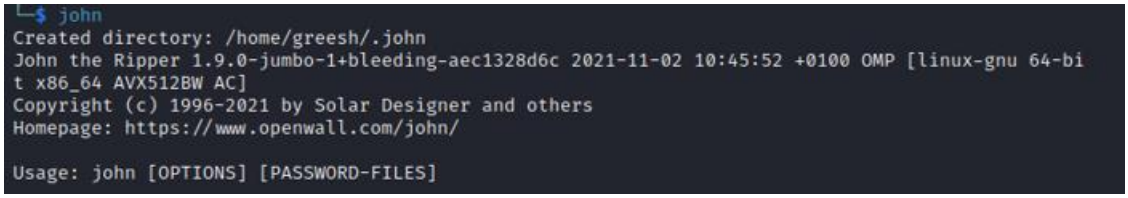
A Linux distro with Debian roots called Kali Linux is supported by Offensive Security. Devon Kearns and Mati Aharoni created it. For people who work in the fields of cybersecurity and analysis, or, to put it simply, network analysts and penetration testers, Kali Linux is an operating system that was specifically created for them.

You may save a lot of time and effort by using Linux utilities.

John the Ripper

If desired, John the Ripper can automatically mail users a warning message about weak passwords, which are those that are simple to guess or crack using brute force.

Along with the crypt (3) password hash types that are most frequently seen on different Unix variants, Kerberos AFS and Windows NT/2000/XP/2003 LM hashes are supported out of the box. Additional hash types can be added with submitted patches.



Metasploit Framework

Rapid7 Technologies created the open-source Metasploit tool. One of the most popular penetration testing frameworks in use today. It includes a ton of exploits that can take advantage of operating system or network vulnerabilities. However, by utilizing "port forwarding," Metasploit can be used for hosts located on the internet. Metasploit typically operates via a local network. Metasploit is mostly a CLI-based tool, but it also includes a GUI package called "Armitage" that makes use of Metasploit more practical and convenient.

```
msf6 > use exploit/multi/browser/adobe_flash_shader_drawing_fill
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show options

Module options (exploit/multi/browser/adobe_flash_shader_drawing_fill):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Retries  true             no        Allow the browser to retry the module
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen
                                        on. This must be an address on the local mac
                                       hine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is
                                       randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is r
                                       andom)
```

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, p
                                        rocess, none)
   LHOST     192.168.0.185    yes       The listen address (an interface may be spec
                                        ified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

```
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show targets

Exploit targets:
================

    Id  Name
    --  ----
=>  0   Windows
    1   Linux


msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > set target 1
target => 1
msf6 exploit(multi/browser/adobe_flash_shader_drawing_fill) > show payloads

Compatible Payloads
===================

   #   Name                                              Disclosure Date  Rank    Chec
k  Description
   -   ----                                              ---------------  ----    ----
-  -----------
   0   payload/generic/custom                                             normal  No
   Custom Payload
   1   payload/generic/debug_trap                                         normal  No
   Generic x86 Debug Trap
   2   payload/generic/shell_bind_tcp                                     normal  No
   Generic Command Shell, Bind TCP Inline
   3   payload/generic/shell_reverse_tcp                                  normal  No
   Generic Command Shell, Reverse TCP Inline
   4   payload/generic/ssh/interact                                       normal  No
   Interact with Established SSH Connection
   5   payload/generic/tight_loop                                         normal  No
   Generic x86 Tight Loop
   6   payload/linux/x86/chmod                                            normal  No
```

Nmap

Network recon/scanning is done using the free and open-source network scanner Nmap. It is used to look up hosts, ports, and services on a network, along with their versions. To get the required results, it sends packets to the host and then examines the responses. One of the most widely used tools for reconnaissance is it.

```
└─$ nmap -sV 172.67.75.162
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 21:59 IST
Nmap scan report for 172.67.75.162
Host is up (0.041s latency).
Not shown: 995 filtered tcp ports (no-response), 1 filtered tcp ports (host-
unreach)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Cloudflare http proxy
443/tcp  open  ssl/https?
8080/tcp open  http          Cloudflare http proxy
8443/tcp open  ssl/https-alt cloudflare
```

```
└─$ nmap -A 172.67.75.162
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 22:00 IST
Nmap scan report for 172.67.75.162
Host is up (0.049s latency).
Not shown: 995 filtered tcp ports (no-response), 1 filtered tcp ports (host-
unreach)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Cloudflare http proxy
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
|_http-server-header: cloudflare
443/tcp  open  ssl/https     cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: cloudflare
8080/tcp open  http          Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
8443/tcp open  ssl/https-alt cloudflare
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
```

```
└─$ nmap -p 443 172.67.75.162
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 22:01 IST
Nmap scan report for 172.67.75.162
Host is up (0.056s latency).

PORT    STATE SERVICE
443/tcp open  https
```