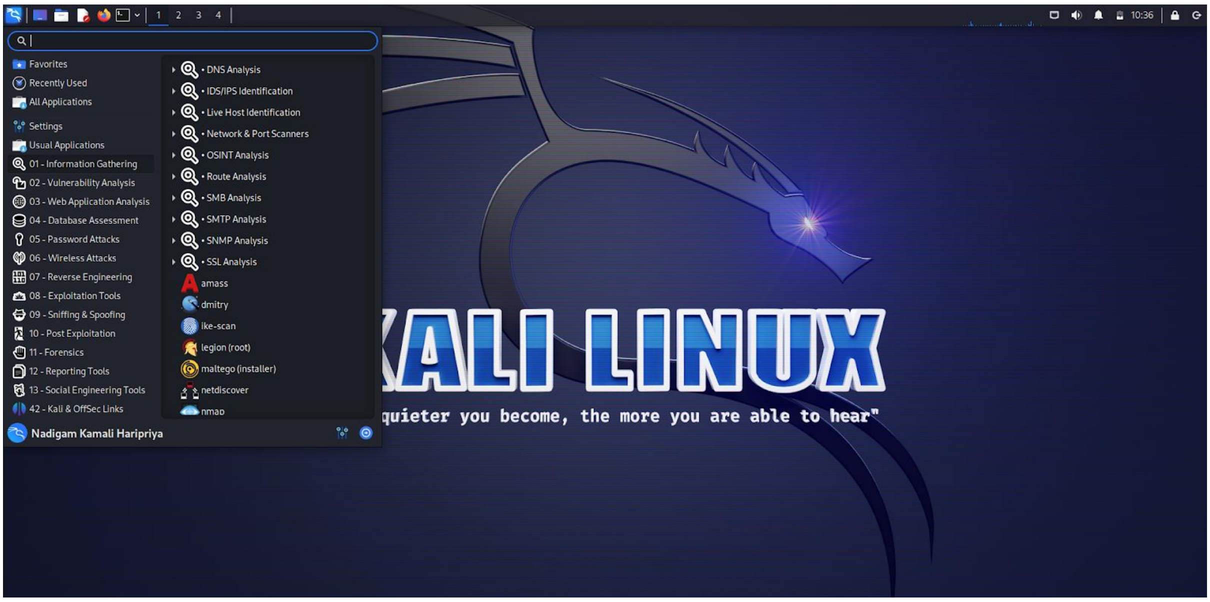
AI for cybersecurity with IBM Qradar
Name: Nandigam Kamali Haripriya
Reg No: 21BCE2746

Assignment - 2

Explore 10 different labs in Kali Linux and explore and make document on any website of your choice.

The 10 libraries in Kali Linux Applications are as follows:



1. Information Gathering
2. Vulnerability Analysis
3. Web Application Analysis
4. Database Assessment
5. Password Attacks
6. Wireless Attacks
7. Reverse Engineering
8. Exploitation Tools
9. Sniffing & Spoofing
10. Post Exploitation

Information Gathering

An information-gathering mission in cybersecurity is the act of collecting information about a potential target. This could be done for penetration testing, network security monitoring or other cybersecurity tasks. Cybercriminals employ many of the same techniques when gathering information about potential targets. This is why it is important to familiarize yourself with the tools that are used in this step, so you can identify and stop any unauthorized information gathering on your network. Information gathering is necessary when performing any type of cybersecurity task because it gives the user more knowledge about target systems and networks in order to make an informed decision on how they want to proceed with their attack vector. Information gathering is a crucial skill that you must learn if you want to be a cybersecurity consultant. Information gathering consists of obtaining and analyzing information about your target and any lapses in their defenses. To complete an information-gathering exercise, you need to strategically plan what kind of information you want to collect about a target system.

Through Information Gathering Library we can find:
i) DNS records (what domains do they have? What subdomains exist?)
ii) IDS/IPS events (intrusion detection systems and intrusion prevention systems)
iii) Network scanning (scanning for ports, MAC addresses and banner grabbing of a target's systems)
iv) Operating systems (can detect operating systems and serve exploits if it is vulnerable)
v) Routing (network configurations that can be found)
vi) Ports (sometimes these are opened and can provide information about the server's software or services it provides)
vii) Users (find out who is logged in on a target system or what their account privileges are)
viii) Systems information. Items such as SMB open network shares and running processes for user accounts with non-privileged access
ix) SSL (are the systems or websites protected with secure sockets layer certificates)
x) VPN (are there VPNs running on the network and are they authorized?)
xi) Voice over IP (Modern telephony uses this protocol to make voice calls. Are these protocols on their own VLAN? Can these packets be intercepted?
xii) SNMP (are there any devices with SNMP running on them? Are they accessible?
xiii) Email addresses (can email addresses be intercepted for further cybercrimes such as phishing or ransomware payloads?))

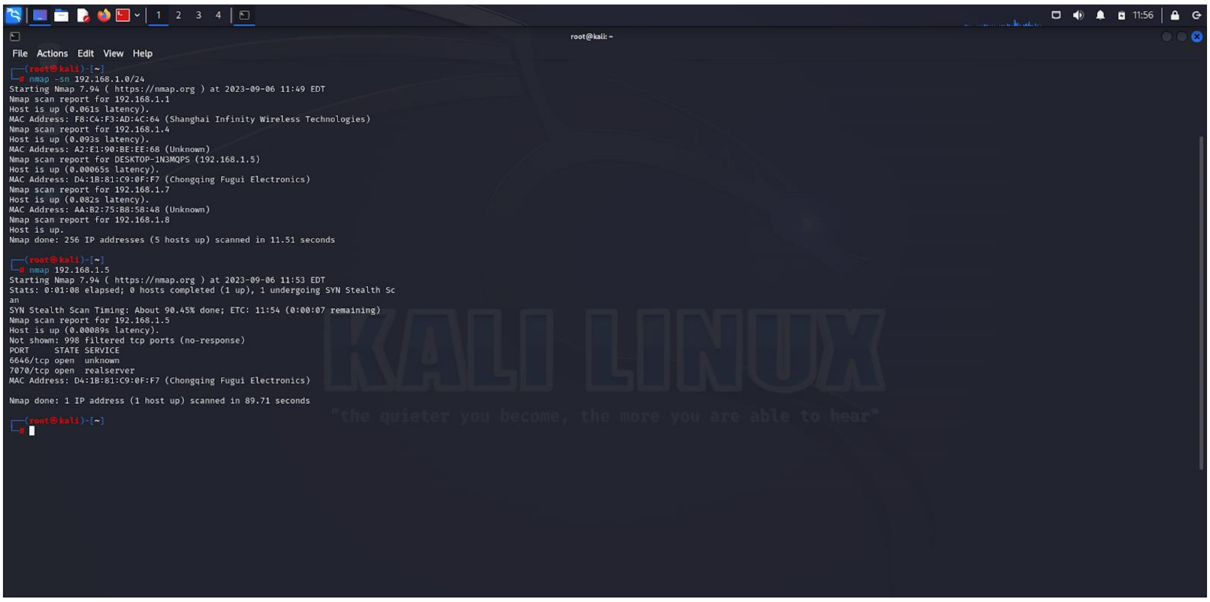
Some of the tools involved in Information Gathering in Kali Linux are:

1. amass
2. N - Map
3. dmitry
4. maltego
5. spiderfoot

N- Map

Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes:

- Real time information of a network
- Detailed information of all the IPs activated on your network
- Number of ports open in a network
- Provide the list of live hosts
- Port, OS and Host scanning



```
┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.1.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 11:49 EDT
Nmap scan report for 192.168.1.1
Host is up (0.061s latency).
MAC Address: F8:C4:F3:AD:4C:64 (Shanghai Infinity Wireless Technologies)
Nmap scan report for 192.168.1.4
Host is up (0.093s latency).
MAC Address: A2:E1:90:BE:EE:68 (Unknown)
Nmap scan report for DESKTOP-1N3MQPS (192.168.1.5)
Host is up (0.00065s latency).
MAC Address: D4:1B:81:C9:0F:F7 (Chongqing Fugui Electronics)
Nmap scan report for 192.168.1.7
Host is up (0.082s latency).
MAC Address: AA:B2:75:B8:58:48 (Unknown)
Nmap scan report for 192.168.1.8
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 11.51 seconds

┌──(root㉿kali)-[~]
└─# nmap 192.168.1.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 11:53 EDT
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 90.45% done; ETC: 11:54 (0:00:07 remaining)
Nmap scan report for 192.168.1.5
Host is up (0.00089s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
6646/tcp open  unknown
7070/tcp open  realserver
MAC Address: D4:1B:81:C9:0F:F7 (Chongqing Fugui Electronics)

Nmap done: 1 IP address (1 host up) scanned in 89.71 seconds

┌──(root㉿kali)-[~]
└─# 
```

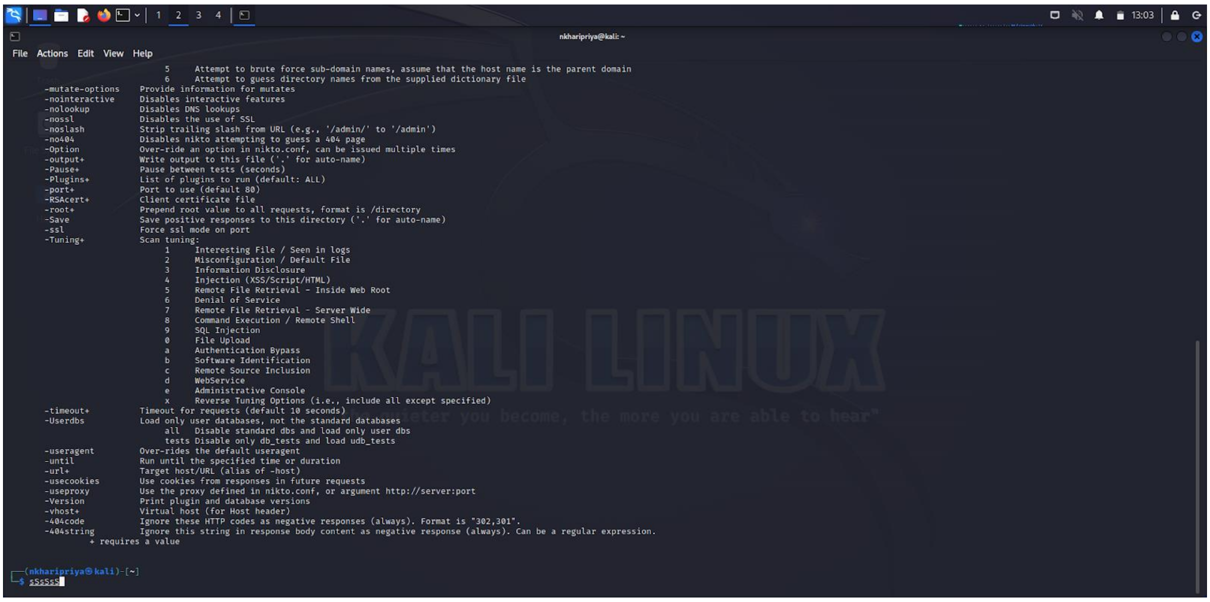
Vulnerability Analysis

Vulnerability Analysis is one of the most important phases of Hacking. It is done after Information Gathering and is one of the crucial steps to be done while designing an application. The cyber-world is filled with a lot of vulnerabilities which are the loopholes in a program through which a hacker executes an attack. These vulnerabilities act as an injection point or a point that could be used by an attacker as a launchpad to execute the attack.

Kali Linux comes packed with 300+ tools out of which many are used for vulnerability analysis. Though there are many tools in Kali Linux for vulnerability analysis, here is the list of most used tools.

Nikto

Nikto is an Open-Source software written in Perl language that is used to scan a web-server for vulnerabilities that can be exploited and can compromise the server. It can also check for outdated version details of 1200 servers and can detect problems with specific version details of over 200 servers. It comes packed with many features, a few of them are listed below.
Full support for SSL
Looks for subdomains
Supports full HTTP Proxy
Outdated component report
Username Guessing



```
                 5     Attempt to brute force sub-domain names, assume that the host name is the parent domain
                 6     Attempt to guess directory names from the supplied dictionary file
   -mutate-options   Provide information for mutates
   -nointeractive    Disables interactive features
   -nolookup         Disables DNS lookups
   -nossl            Disables the use of SSL
   -noslash          Strip trailing slash from URL (e.g., '/admin/' to '/admin')
   -no404            Disables nikto attempting to guess a 404 page
   -Option           Over-ride an option in nikto.conf, can be issued multiple times
   -output+          Write output to this file ('.' for auto-name)
   -Pause+           Pause between tests (seconds)
   -Plugins+         List of plugins to run (default: ALL)
   -port+            Port to use (default 80)
   -RSAcert+         Client certificate file
   -root+            Prepend root value to all requests, format is /directory
   -Save             Save positive responses to this directory ('.' for auto-name)
   -ssl              Force ssl mode on port
   -Tuning+          Scan tuning:
                 1     Interesting File / Seen in logs
                 2     Misconfiguration / Default File
                 3     Information Disclosure
                 4     Injection (XSS/Script/HTML)
                 5     Remote File Retrieval - Inside Web Root
                 6     Denial of Service
                 7     Remote File Retrieval - Server Wide
                 8     Command Execution / Remote Shell
                 9     SQL Injection
                 0     File Upload
                 a     Authentication Bypass
                 b     Software Identification
                 c     Remote Source Inclusion
                 d     WebService
                 e     Administrative Console
                 x     Reverse Tuning Options (i.e., include all except specified)
   -timeout+         Timeout for requests (default 10 seconds)
   -Userdbs          Load only user databases, not the standard databases
                 all   Disable standard dbs and load only user dbs
                 tests Disable only db_tests and load udb_tests
   -useragent        Over-rides the default useragent
   -until            Run until the specified time or duration
   -url+             Target host/URL (alias of -host)
   -usecookies       Use cookies from responses in future requests
   -useproxy         Use the proxy defined in nikto.conf, or argument http://server:port
   -Version          Print plugin and database versions
   -vhost+           Virtual host (for Host header)
   -404code          Ignore these HTTP codes as negative responses (always). Format is "302,301".
   -404string        Ignore this string in response body content as negative response (always). Can be a regular expression.
           + requires a value


┌──(nkharipriya㉿kali)-[~]
└─$ sSsSsS
```

Web Application Analysis

Web Application is a dynamic response web page that helps in a better and interactive client-server relationship. These tools identify and access websites through the browser to check any bug or loophole present, which could lead any information or data to lose. For example, there is a website with a payment gateway then these web analyzers check if sufficient authentication and authorization are present on the site. These web application uses:

SQL injections
Denial of service
URL manipulation

Some of the tools are:
Burpsuite
Httrack
Sqlmap
Vega
Webscarab
Wpscan
zap
skipfish
Burpsuite, vega, and web scarab are some most famous tools. Go to “Applications” then in “Web Application Analysis”, you will find these tools.

Database Assessment:

These applications are made to access the database and analyze it for different attacks and security issues. These assessments show some opportunities for improvement and changes. They develop a report of the analysis done on the database system. They perform:
Configuration checking
Examining user account
Privilege and role grants
Authorization control
Key management

Data encryption

Some of the tools are:
Bbqsl
Jsql injection
Oscanner
Sqlmap
Sqlninja
Tmscmd10g
Sqlmap is the most famous database assessment tool. This tool injects SQL injection for scanning, detecting, and exploitation. Go to “Applications” then in “Database Assessment”, you will find these tools.

Password Attacks:
These are basically a collection of tools that could handle the wordlist or password list to be checked on any login credentials through different services and protocols. Some tools are wordlist collectors and some of them are the attacker. Some of the tools are:
Cewl
Crunch
Hashcat
John
Johnny
Medusa
ncrack
John the Ripper and Medusa are the most famous tools. Go to “Applications” then in “Password Attacks”, you will find these tools.

Wireless Attacks:
These tools are wireless security crackers, like breaking wifi – routers, working and manipulating access points. Wireless attacks are not limited to password cracking; these are also used in information gathering and knowing behavior of victims over the internet. For example, the Victim is connected to a compromised access point or a fake access point then it can be used as a Man-in-The-Middle attack. Some of the tools are:
Aircrack-ng
Fern- wifi –cracker
Kismet
Ghost Phisher
wifite
Aircrack-ng and Ghost Phisher are the most famous tools. Go to “Applications” then in “Wireless Attacks”, you will find these tools.

Reverse Engineering:
Reverse Engineering is to break down the layers of the applications or software. This is used in creating cracks and patches for different software and services. These tools reach the source code of the application, understand its working and manipulate according to needs. For example, Reverse engineering tools are also used by High-End companies to know the logic and idea behind the software. Some of the tools are:
Apktools
Ollydbg
Flasm

nasm shell
Most famous tools are ollydbg and apltools. Go to “Application” then in “Reverse Engineering”, you will find these tools.

Exploitation Tools:
These tools are used to exploit different systems like personal computers and mobile phones. These tools can generate payloads for the vulnerable system and through those payloads information from the devices can be exploited. For example, the Victim’s system is compromised using payloads over internet or installing it if physically accessible. Some of the tools are:
Armitage
Metasploit
Searchsploit
Beef xss framework
termineter
Social engineering toolkit(root)
The most famous tool is Metasploit (there are courses to learn Metasploit alone). Go to “Applications” then in “Exploitation Tools”, you will find these tools.

Sniffing and Spoofing:
Secretly accessing any unauthorized data over the network is sniffing. Hiding real identity and creating fake identity and using it for any illegal or unauthorized work is spoofing. IP spoofing and MAC spoofing are two famous and mostly used attacks. Some of the tools are:
Wireshark
Bettercap
Ettercap
Hamster
Driftnet
responder
macchanger
The most used tool is Wireshark. Go to “Applications” then in “Sniffing and Spoofing”, you will find these tools.

Post Exploitation:
These tools use back doors to get back to the vulnerable system i.e., to maintain access to the machine. As the name suggests these are useful or mostly used after an attack has previously been made on the victim’s machine. For example, after an attack victim removed the vulnerability from the system, in this situation if the attacker wants to access data again, then these tools are helpful. Some of the tools are:
MSF
Veil –Pillage framework
Powersploit
Powershell empire
The most famous tool is Powersploit. Go to “Applications” then in “Post Exploitation Tools”, you will find these tools.