Overview

In this module, we will dive deep into several different attacks. The objective for each attack is to:

1. Describe it.
2. Provide a walkthrough of how we can carry out the attack.
3. Provide preventive techniques and compensating controls.
4. Discuss detection capabilities.
5. Discuss the 'honeypot' approach of detecting the attack, if applicable.

The following is a complete list of all attacks described in this module:

- Kerberoasting
- AS-REProasting
- GPP Passwords
- Misconfigured GPO Permissions (or GPO-deployed files)
- Credentials in Network Shares
- Credentials in User Attributes
- DCSync
- Kerberos Golden Ticket
- Kerberos Constrained Delegation attack
- Print Spooler & NTLM Relaying
- Coercing attacks & Kerberos Unconstrained Delegation
- Object ACLs
- PKI Misconfigurations - ESC1
- PKI Misconfigurations - ESC8 (Coercing + Certificates)

Lab Environment

As part of this module, we also provide a playground environment where you can test and follow up with the provided walkthroughs to carry out these attacks yourself. Please note that the purpose of the walkthroughs is to demonstrate the problem and not to describe the attacks in depth. Also, other modules on the platform are already covering these attacks very detailedly.

The attacks will be executed from the provided Windows 10 (WS001) and Kali Linux machines. The assumption is that an attacker has already gained remote code execution (of some sort) on that Windows 10 (WS001) machine. The user, which we assume is compromised, is Bob, a regular user in Active Directory with no special permissions assigned.

The environment consists of the following machines and their corresponding IP addresses:

- DC1: 172.16.18.3
- DC2: 172.16.18.4
- Server01: 172.16.18.10
- PKI: 172.16.18.15
- WS001: DHCP or 172.16.18.25 (depending on the section)
- Kali Linux: DHCP or 172.16.18.20 (depending on the section)

Connecting to the lab environment

Cheat Sheet

Table of Contents

Setting the stage
Introduction and Terminology
Overview and Lab Environment

Attacks & Defense
Kerberoasting
AS-REProasting
GPP Passwords
GPO Permissions/GPO Files
Credentials in Shares
Credentials in Object Properties
DCSync
Golden Ticket
Kerberos Constrained Delegation
Print Spooler & NTLM Relaying
Coercing Attacks & Unconstrained Delegation
Object ACLs
PKI - ESC1

Skills Assessment
Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Most of the hosts mentioned above are vulnerable to several attacks and live in an isolated network that can be accessed via the VPN. While on the VPN, a student can directly access the machines WS001 and/or Kali (depending on the section), which, as already mentioned, will act as initial foothold and attacker devices throughout the scenarios.

Below, you may find guidance (from a Linux host):

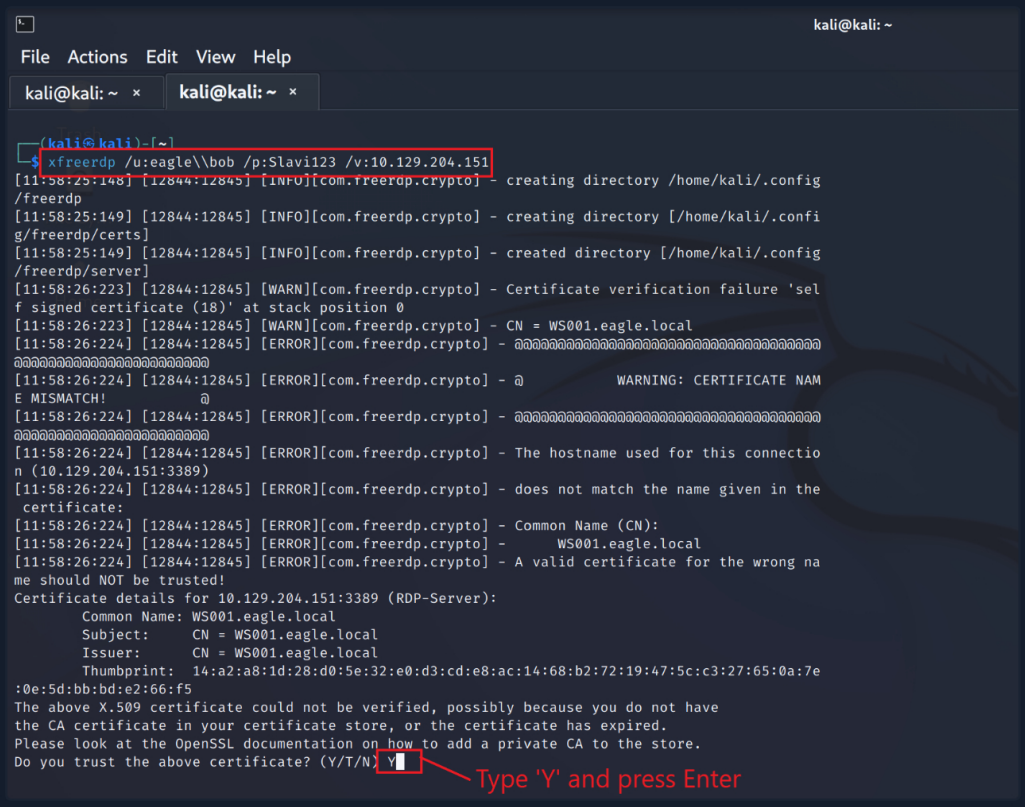
- How to connect to the Windows box WS001
- How to connect to the Kali box
- How to transfer files between WS001 and your Linux attacking machine

Connect to WS001 via RDP

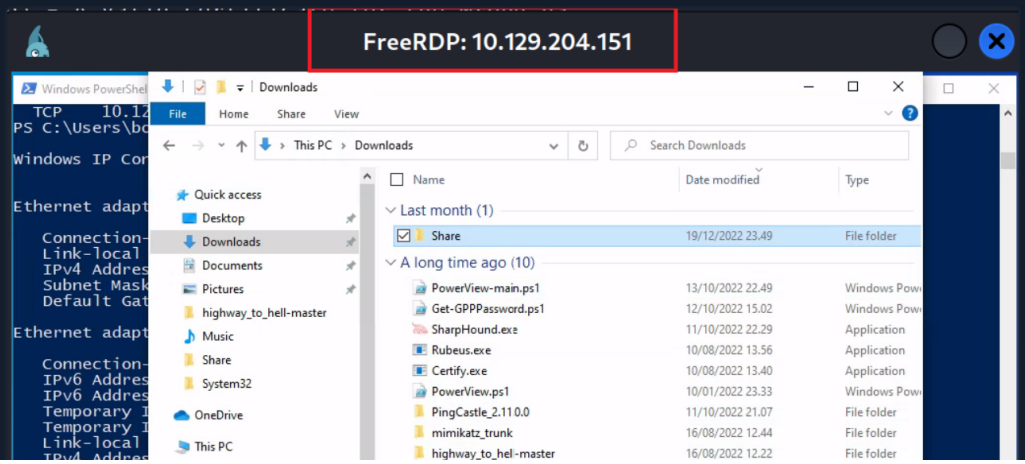
Once connected to the VPN, you may access the Windows machine via RDP. Most Linux flavors come with a client software, 'xfreerdp', which is one option to perform this RDP connection. To access the machine, we will use the user account Bob whose password is 'Slavi123'. To perform the connection execute the following command:

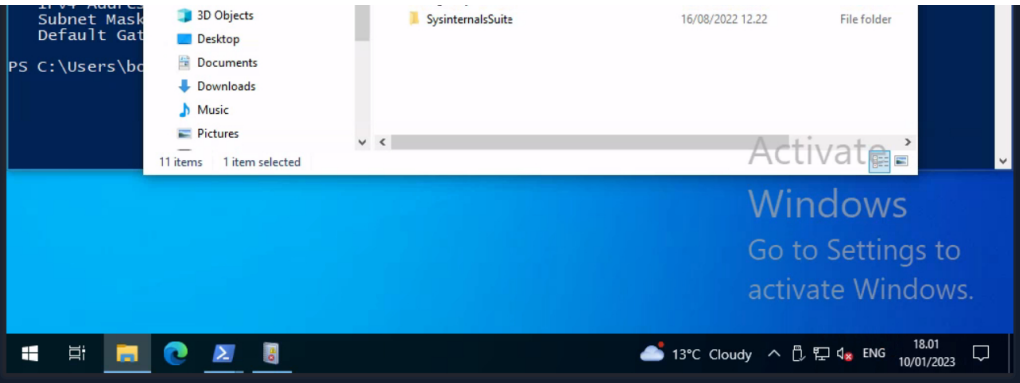
Overview

```
MisaelMacias@htb[/htb]$ xfreerdp /u:eagle\\bob /p:Slavi123 /v:TARGET_IP /dynamic-resolution
```



If the connection is successful, a new window with WS001's desktop will appear on your screen, as shown below:



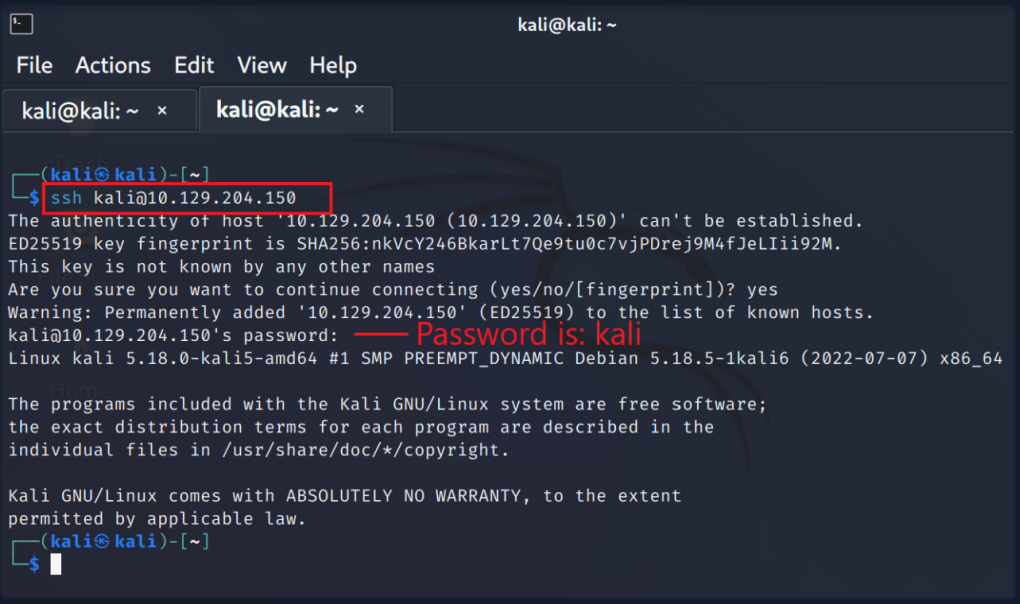


Connect to Kali via SSH

Once connected to the VPN, we can access the Kali machine via SSH. The credentials of the machine are the default 'kali/kali'. To connect, use the following command:

Overview

```
MisaelMacias@htb[/htb]$ ssh kali@TARGET_IP
```



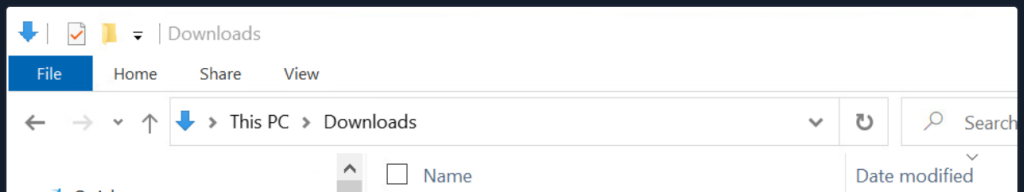
Note: We have also enabled RDP on the Kali host. For sections with the Kali host as the primary target, it is recommended to connect with RDP. Connection credentials will be provided for each challenge question.

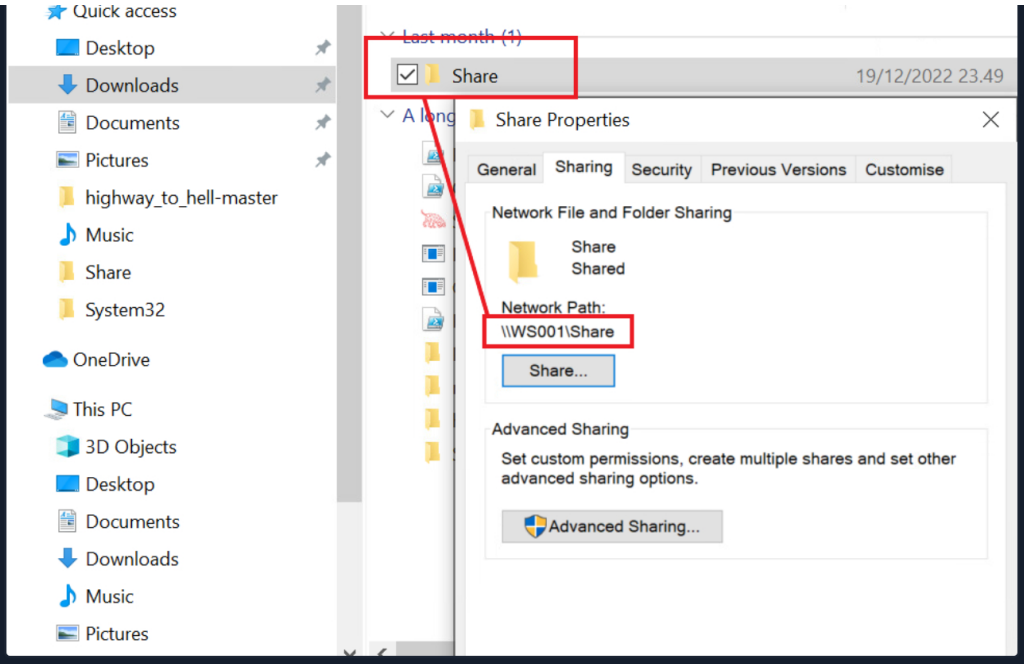
Overview

```
MisaelMacias@htb[/htb]$ xfreerdp /v:TARGET_IP /u:kali /p:kali /dynamic-resolution
```

Moving files between WS001 and your Linux attacking machine

To facilitate easy file transfer between the machines, we have created a shared folder on WS001, which can be accessed via SMB.

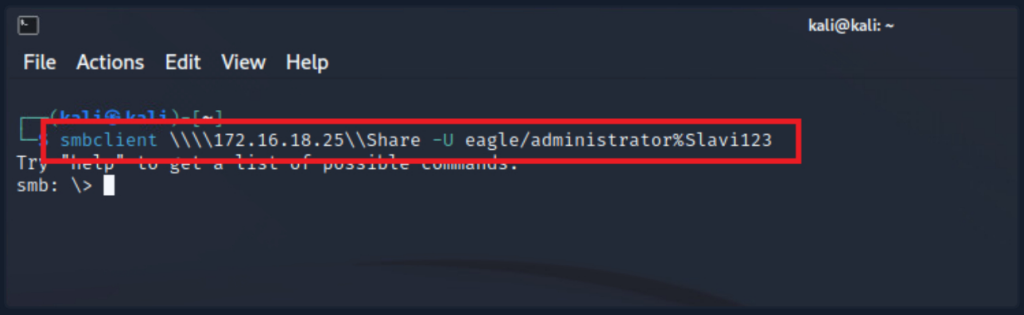




To access the folder from the Kali machine, you can use the 'smbclient' command. Accessing the folder requires authentication, so you will need to provide credentials. The command can be executed with the Administrator account as follows:

Overview

```
MisaelMacias@htb[/htb]$ smbclient \\\\TARGET_IP\\Share -U eagle/administrator%Slavi123
```



Once connected, you can utilize the commands `put` or `get` to either upload or download files, respectively.