



Crafting and Deploying Malware Using Remote Access Trojan (RAT)

ETHICAL HACKING & LAB 3

Student Info
Name: SRIJA PABBA
Student ID: 00866719
Email:
spabb6@unh.newhaven.edu

Table of Contents

| | | |
|------|--|----|
| I. | Executive Summary | 2 |
| | Highlights | |
| | Objectives | |
| II. | Lab Description Details | 3 |
| | To determine the ports which are open on the firewall. | |
| III. | Supporting Evidence | 12 |
| IV. | Conclusion & Wrap-Up | 16 |
| | Summary with: | |
| | • Observations | |
| | • Identified risks | |
| | • Suggested recommendations | |
| | • Your successes & failures | |
| | • Challenges | |

Executive Summary

Highlights

In this lab, I will simulate a complete cyber attack using tools like nmap/zenmap, Bruter, and DarkComet to gain unauthorized access to a host system. Starting with network scanning from an external address, I will identify open ports on the pfSense firewall, followed by a dictionary attack using Bruter to crack the administrator's password and establish an RDP connection. With access achieved, I will deploy a Remote Access Trojan (RAT) using DarkComet, disguised as a legitimate application, to maintain a persistent connection with the compromised system. This lab showcases key hacking techniques such as network reconnaissance, password exploitation, and remote malware deployment.

Objectives

Port Scanning and Vulnerability Assessment: I'll use nmap/zenmap to examine network structure and pinpoint vulnerabilities by identifying open firewall ports, showing the risks in exposed network services.

Brute-Force Credential Attack: Using Bruter, I will attempt to break the administrator's password through a dictionary attack, highlighting the critical need for strong passwords in preventing unauthorized access.

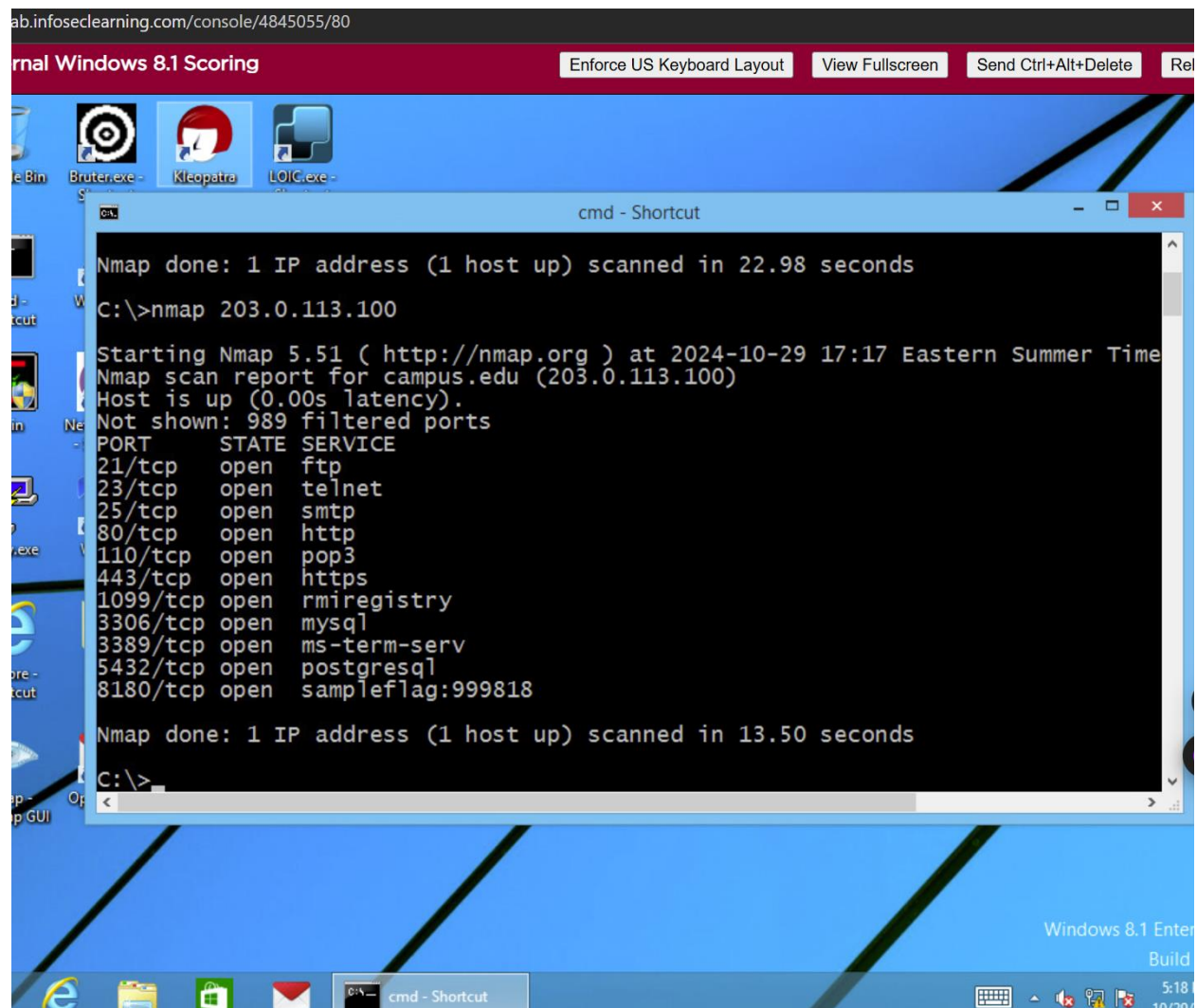
Malware Creation and Deployment: With DarkComet, I'll create a Remote Access Trojan (RAT) and attach a legitimate icon to it, illustrating how attackers mask malware to infiltrate systems.

Backdoor Connection Establishment: By uploading and activating the RAT through RDP, I'll establish a backdoor on the compromised system, demonstrating persistent remote access methods.

Data Exfiltration: Finally, I'll exfiltrate sensitive data from the compromised host, underscoring the severe risks and impacts of data breaches on affected systems.

Lab Description Details

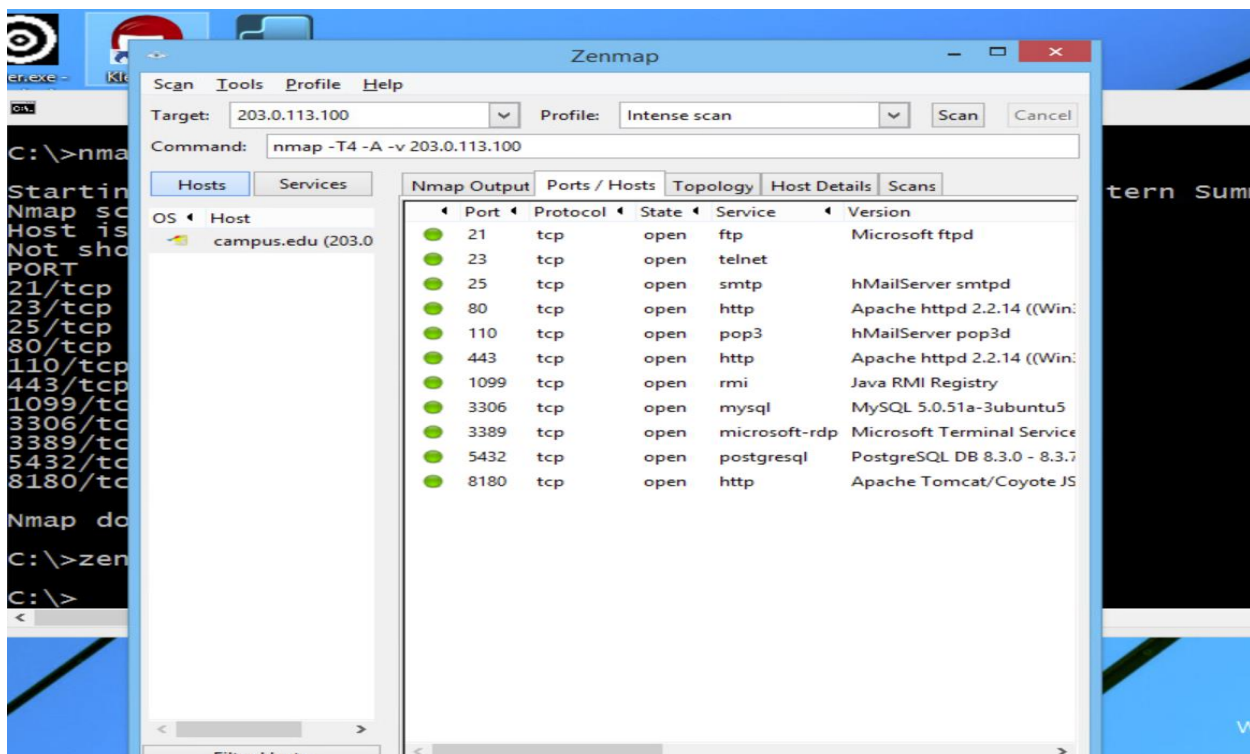
To determine the ports which are open on the firewall.



The screenshot shows a Windows 8.1 desktop environment. A command prompt window titled "cmd - Shortcut" is open, displaying the output of an Nmap scan. The desktop background is blue with several icons on the left, including "Bruter.exe", "Kleopatra", and "LOIC.exe". The taskbar at the bottom shows the Start button, a few application icons, and the system tray with the time 5:18 and date 10/29/2024. The command prompt window shows the following text:

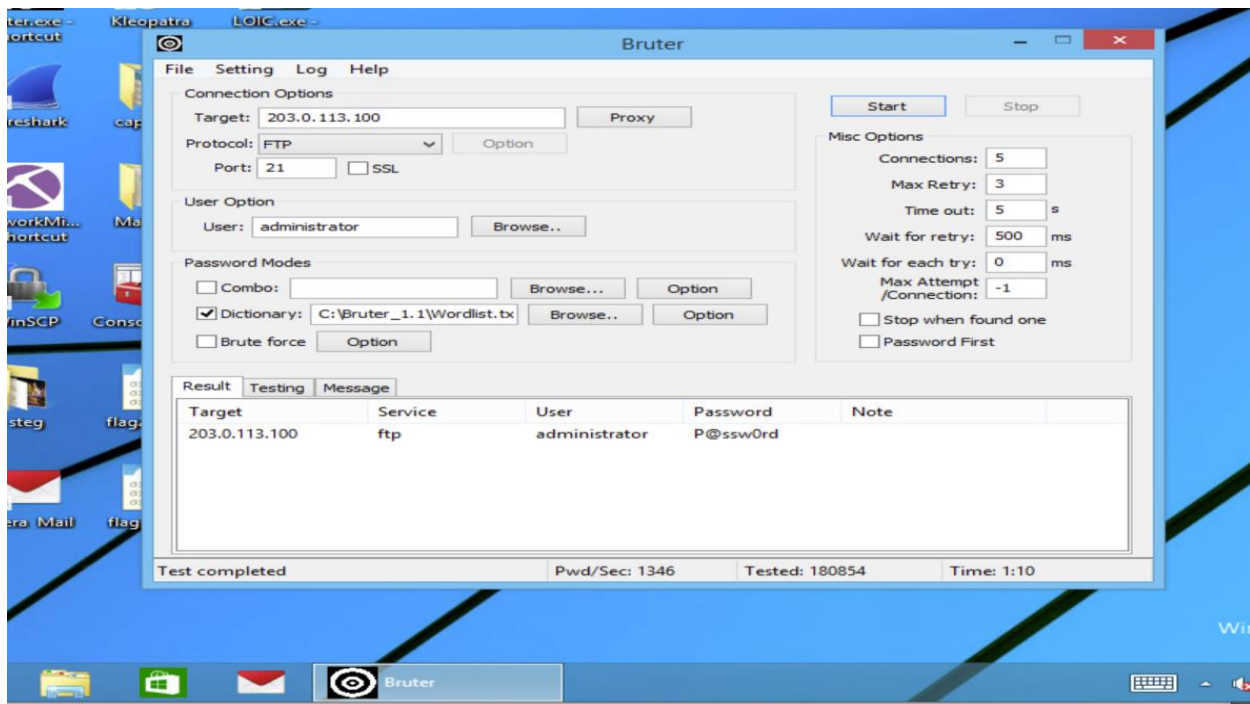
```
Nmap done: 1 IP address (1 host up) scanned in 22.98 seconds
C:\>nmap 203.0.113.100
Starting Nmap 5.51 ( http://nmap.org ) at 2024-10-29 17:17 Eastern Summer Time
Nmap scan report for campus.edu (203.0.113.100)
Host is up (0.00s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
443/tcp   open  https
1099/tcp  open  rmiregistry
3306/tcp  open  mysql
3389/tcp  open  ms-term-serv
5432/tcp  open  postgresql
8180/tcp  open  sampleflag:999818
Nmap done: 1 IP address (1 host up) scanned in 13.50 seconds
C:\>
```

To open Zenmap we use command “zenmap”, when its opened typed the “203.0.113.100 ” in the target box and scanned to launch the intense scan. After the scanning is done we select the Ports/Hosts tab to view the open ports and corresponding banner message that are displayed.



This screenshot shows the open ports corresponding banner messages

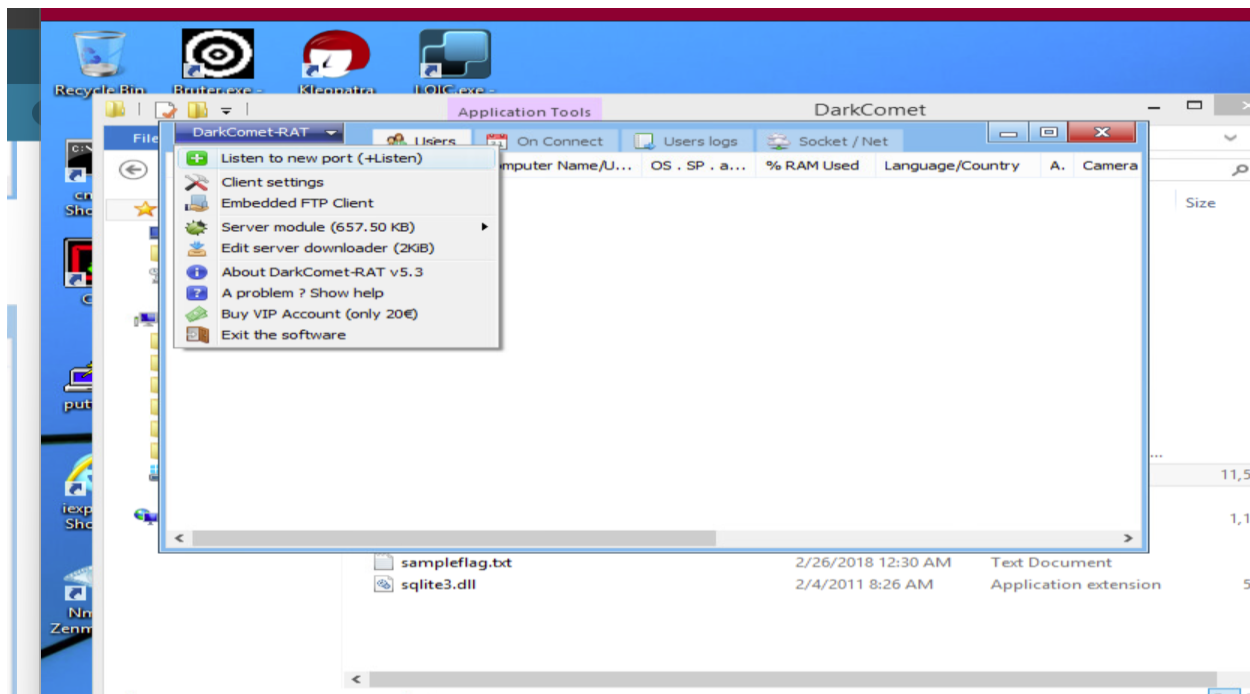
In Bruter.exe-shortcut set the target “203.0.113.100”, for protocol leave as FTP. For port, leave as 21 and User I typed “administrator”. Selected the Dictionary file as “Wordlist.txt” and launched the attack and after sometime attacked is completed and password will be displayed.



This screenshot shows the interface of the bruter.exe-shortcut and showing the password displayed

After clicking on the Malware folder on the Windows 8.1 desktop. **Highlighted** the DarkComet.7z file within the Malware folder. **Right-click** on 7-Zip and Extracted to “DarkComet\”. After **Double-click** on the new DarkComet file folder within the Malware folder on the desktop.

DarkComet-RAT menu bar, **select** Listen to new port (+Listen). **Type 443** in the Listen port box and **click** the Listen button.



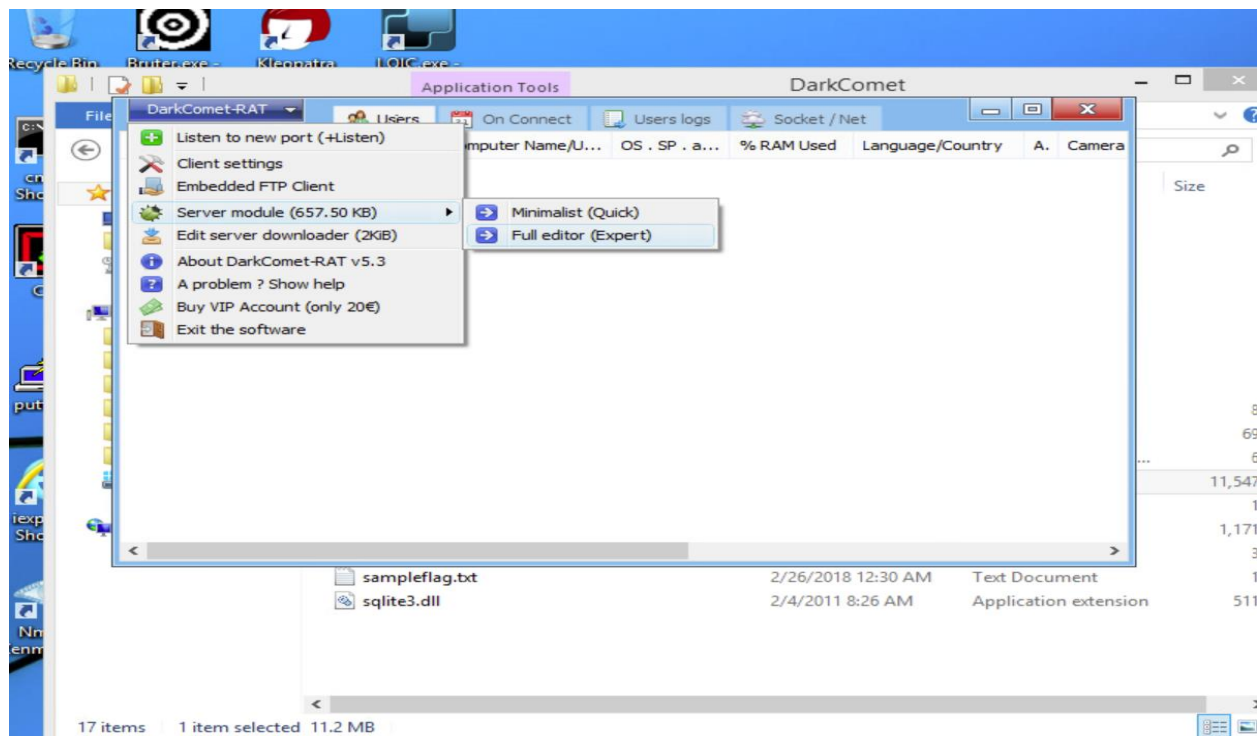
This screenshot shows the interface of the DarkComet-RAT

| ID | IP Wan/[La... | Computer Name/U... | OS . SP . a... | % RAM Used | Language/Country | A. | Came |
|----|---------------|--------------------|----------------|------------|------------------|----|------|
|----|---------------|--------------------|----------------|------------|------------------|----|------|

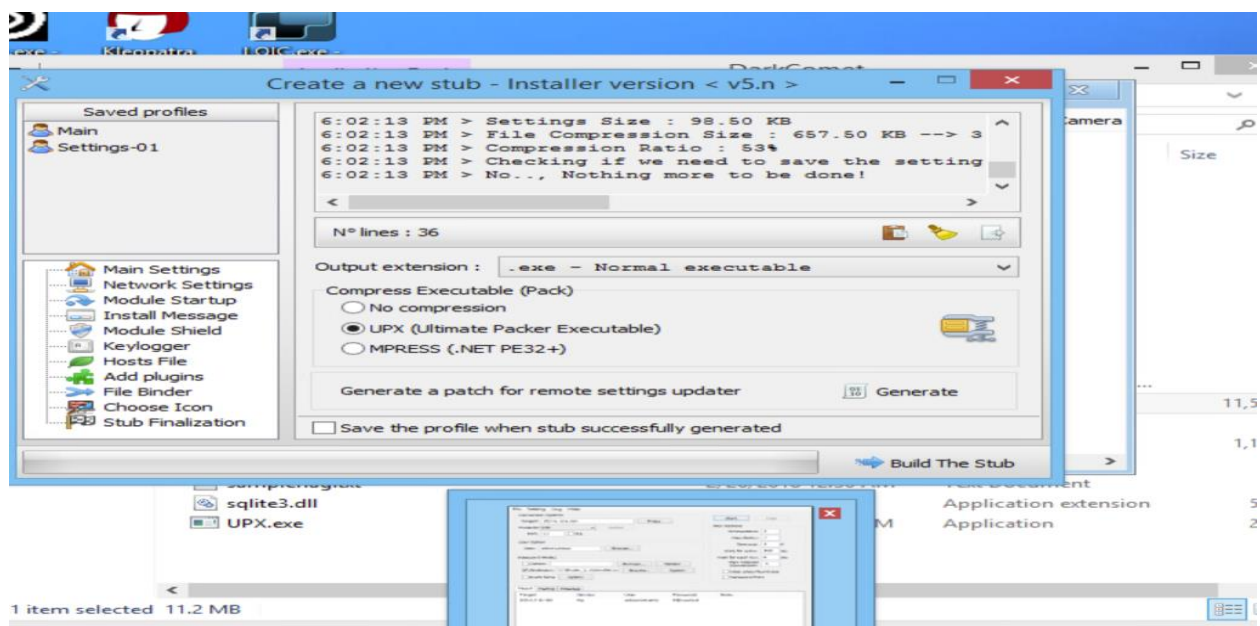


| | | |
|----------------|--------------------|------------------|
| sampleflag.txt | 2/26/2018 12:30 AM | Text Document |
| sqlite3.dll | 2/4/2011 8:26 AM | Application exte |

From the DarkComet-RAT menu bar, **click** Server module (657.50KB) and then **select** Full editor (Expert).

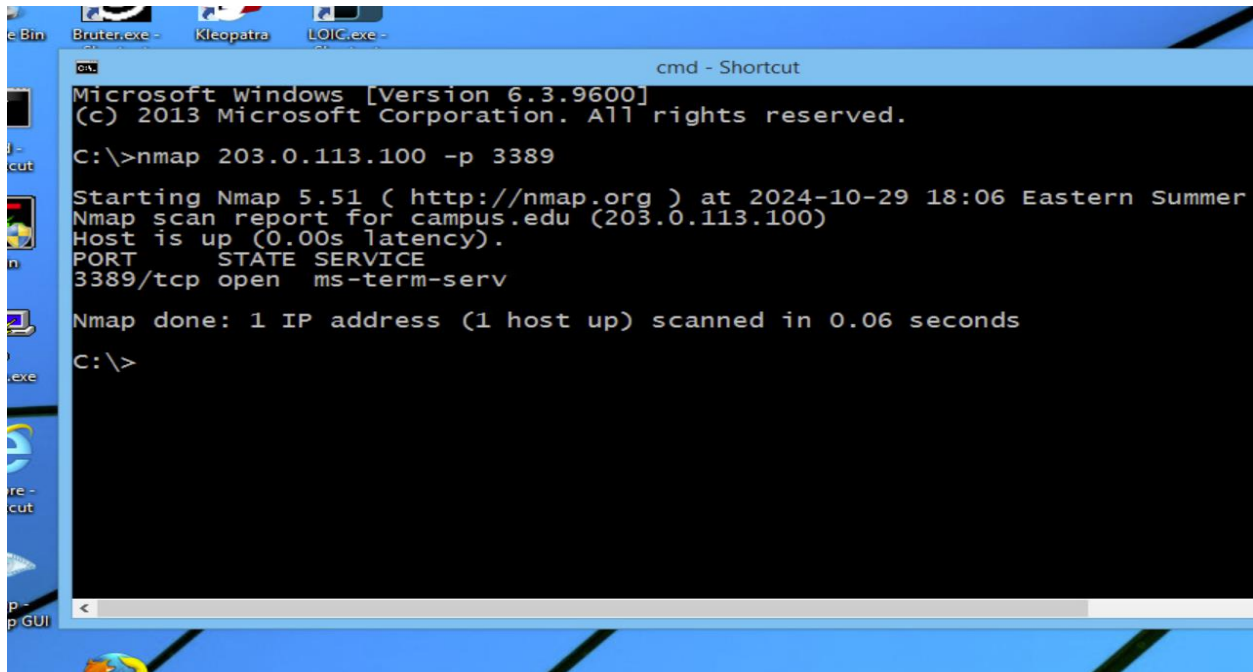


Click Stub Finalization. For the Compress Executable (Pack), **select** UPX (Ultimate Packer Executable). **Click** Build The Stub to create the malware payload.



This screenshot shows that we are building new stub to create the malware payload

Typing the following command “**nmap 203.0.113.100 -p 3389**” in the cmd to determine if RDP is open on firewall.



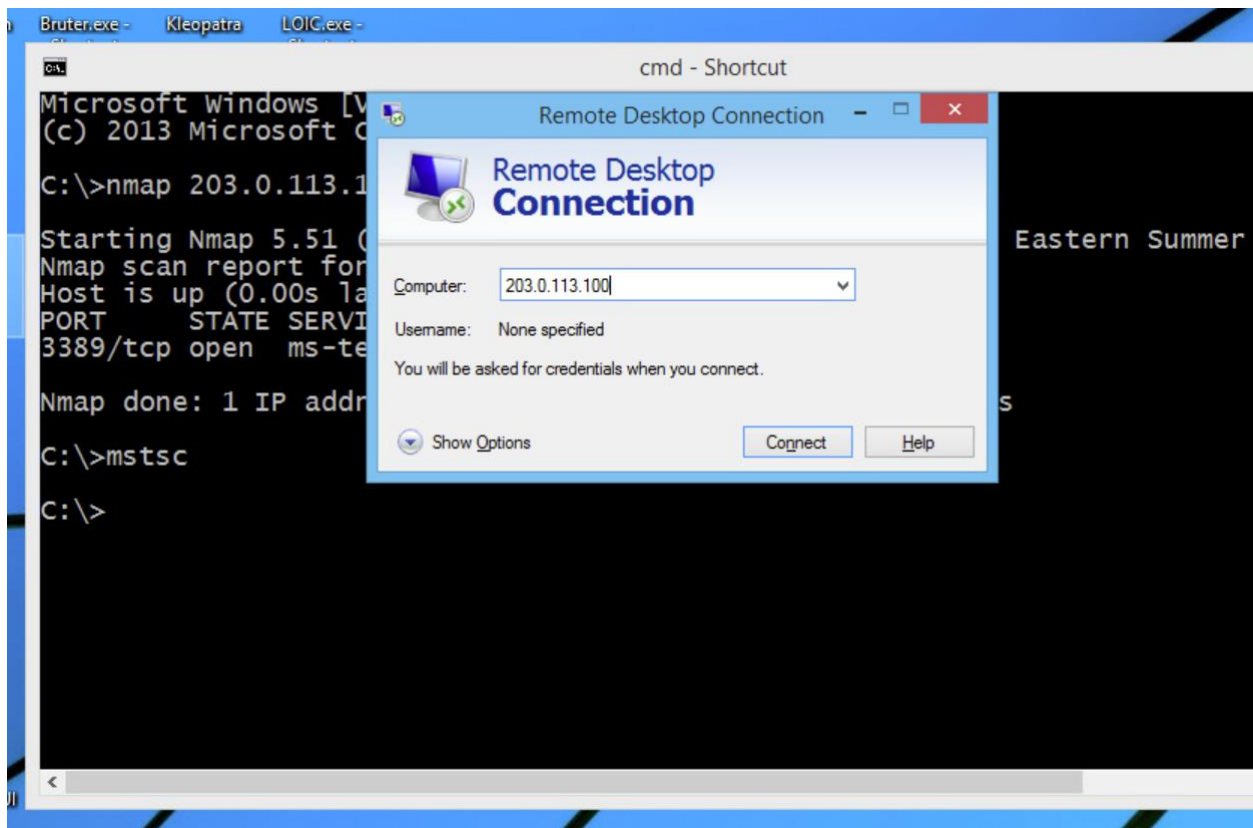
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

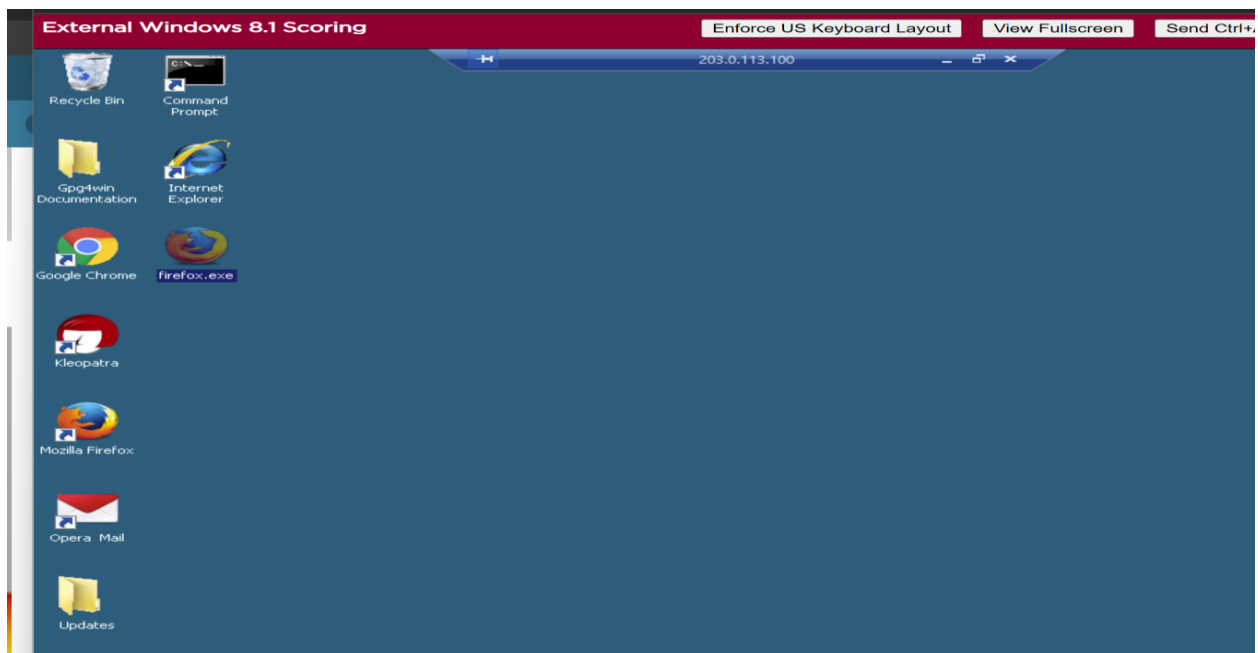
C:\>nmap 203.0.113.100 -p 3389

Starting Nmap 5.51 ( http://nmap.org ) at 2024-10-29 18:06 Eastern Summer
Nmap scan report for campus.edu (203.0.113.100)
Host is up (0.00s latency).
PORT      STATE SERVICE
3389/tcp  open  ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
C:\>
```

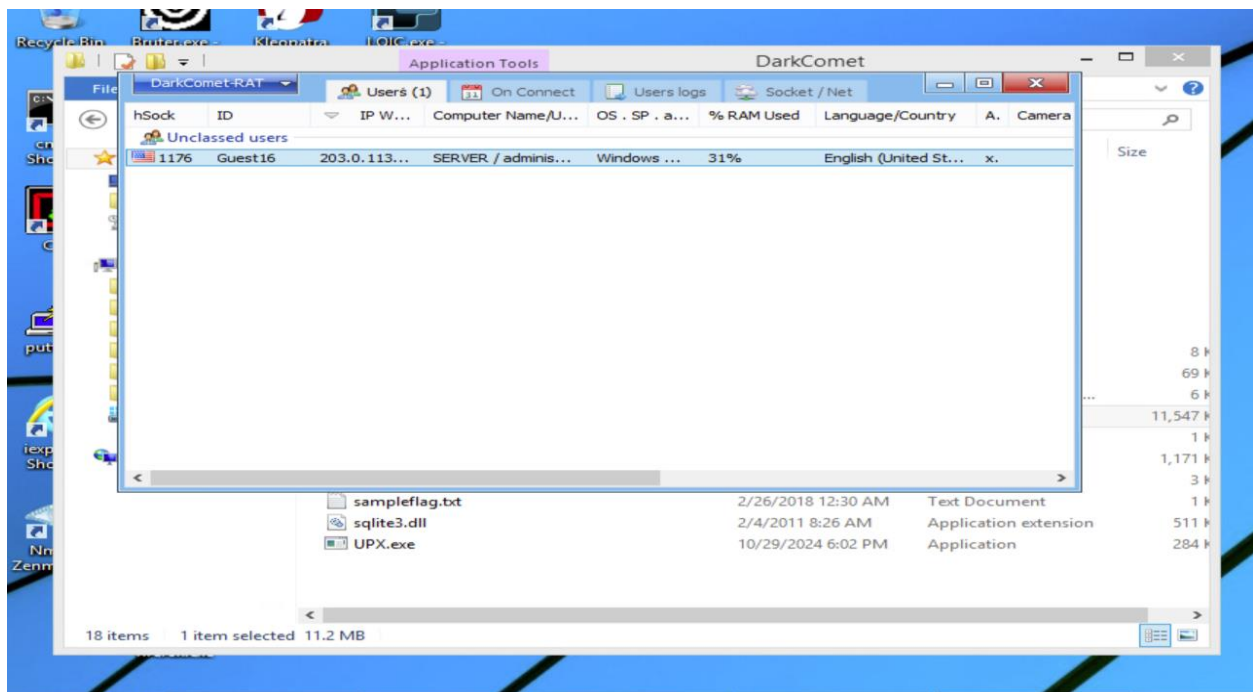
Typing the following command “**mstsc**” to launch the Microsoft Terminals service client. In the computer box after typing the IP address and then click the connect button.

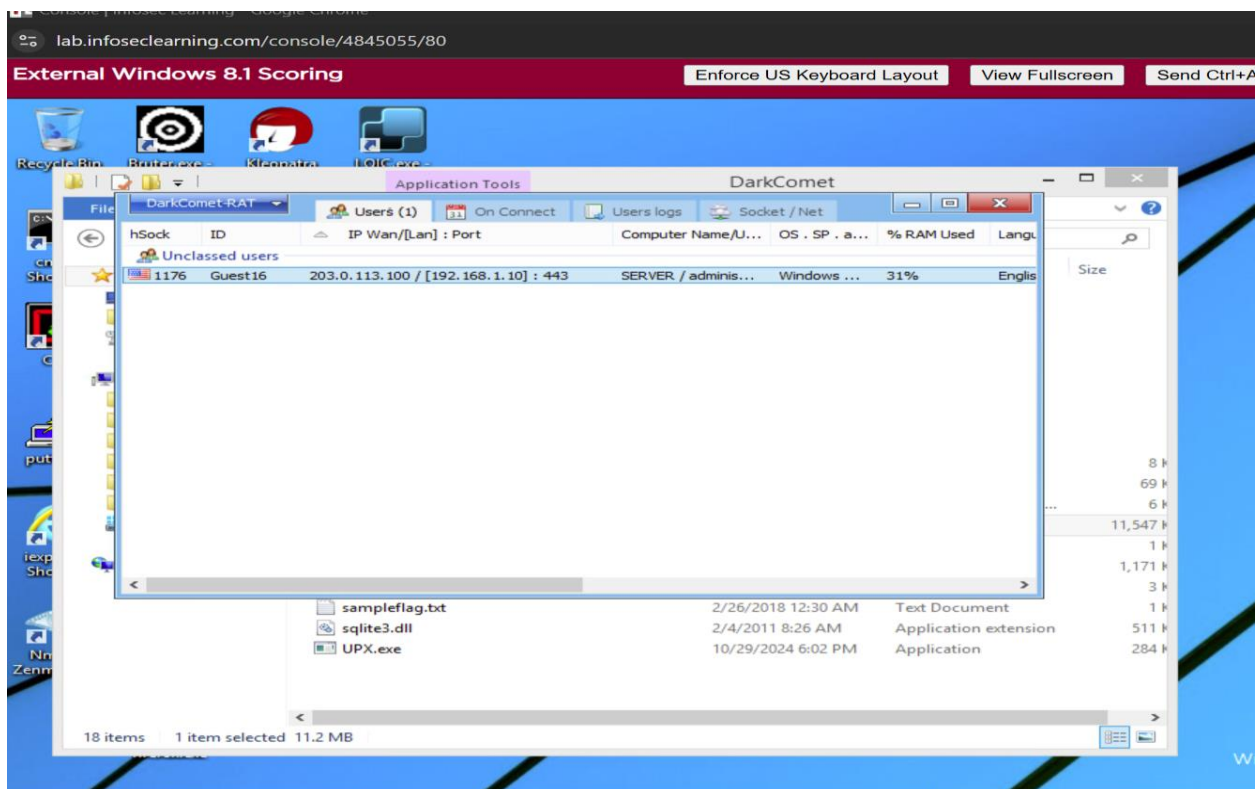




This screenshot shows the remote windows server desktop is displayed on the machine and after pasting the malicious file.

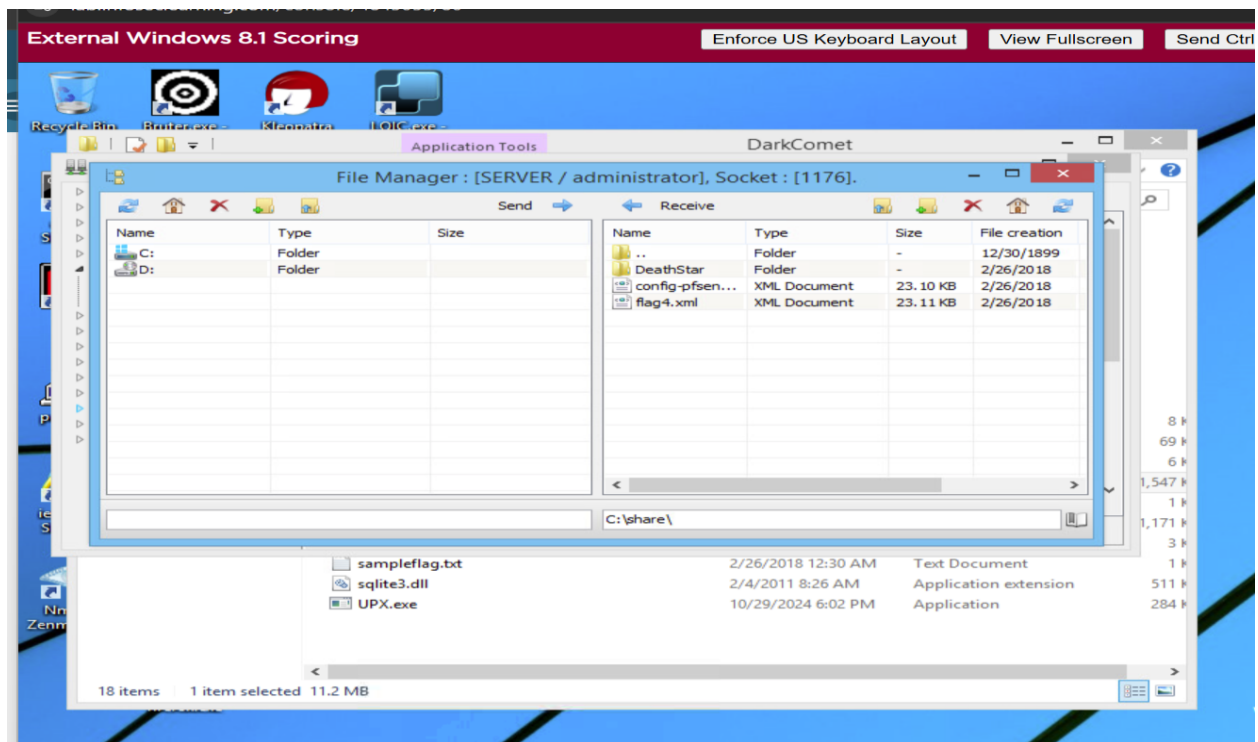
The connection to the victim is displayed in the Darkcomet-RAT console





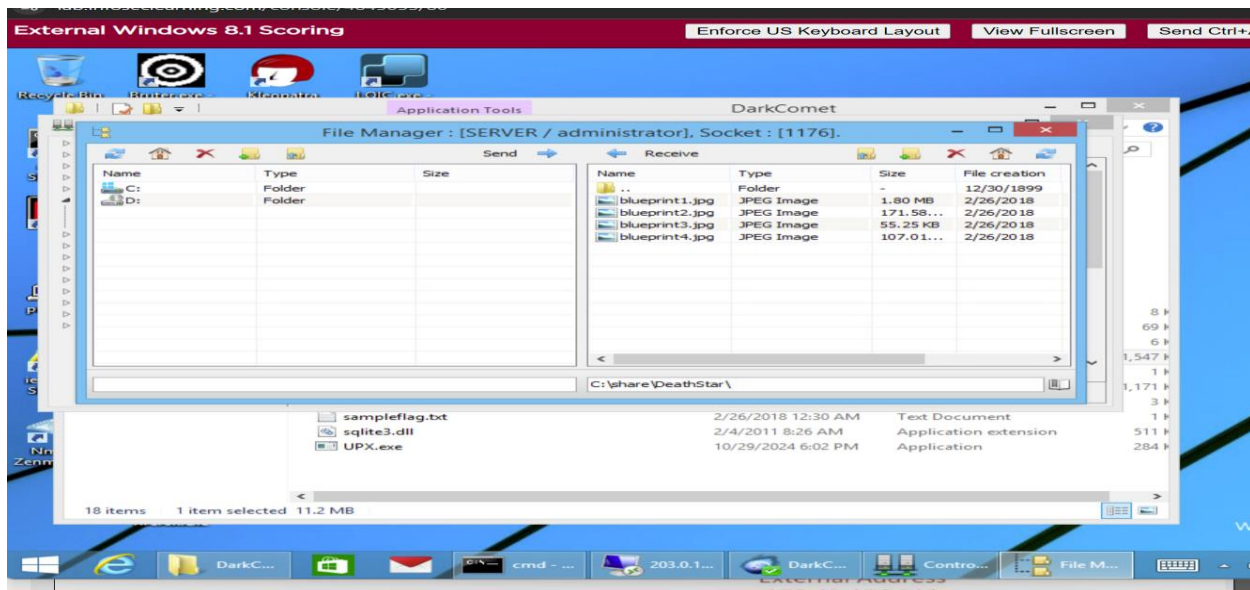
This screenshot shows the internal IP address of the Victim

In system info in the computer information section from the list I opened the files manger and in that opened the file explorer to see the attacker and victim



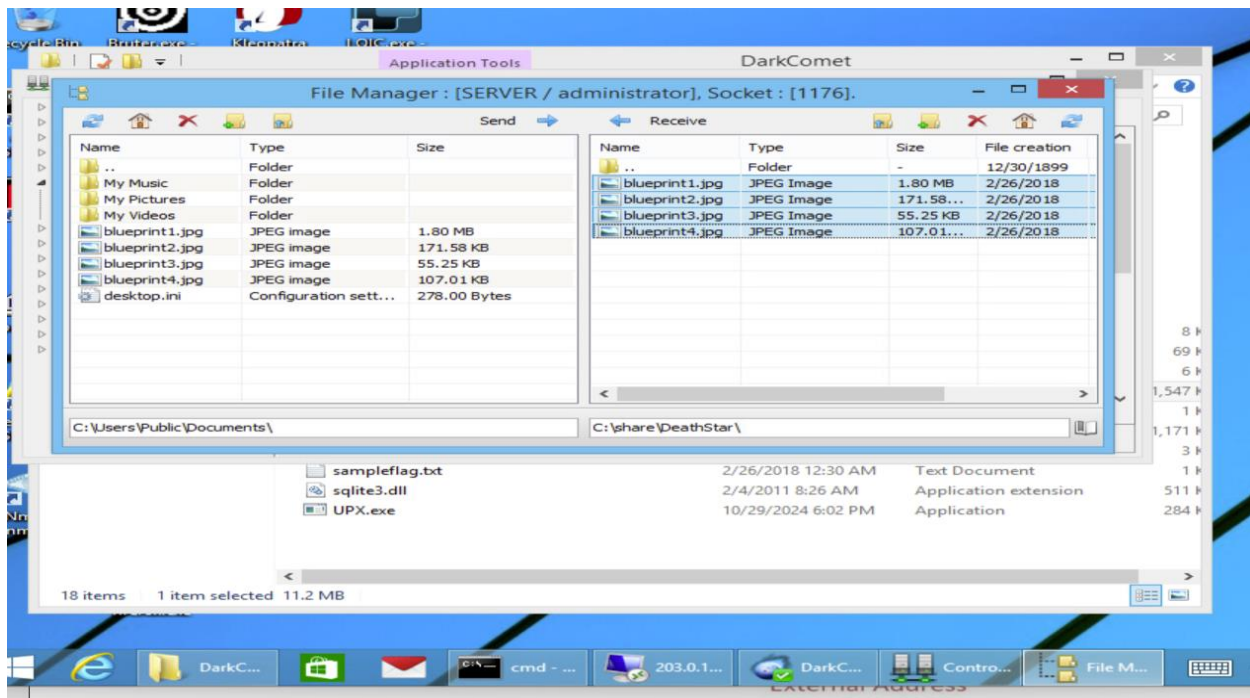
The screenshot shows left side is the attacker and the right side is the victim.

After clicking in the C drive and opening the share folder on the victims machine. I found a deathstar folder. I found four blueprint files in right hand pane

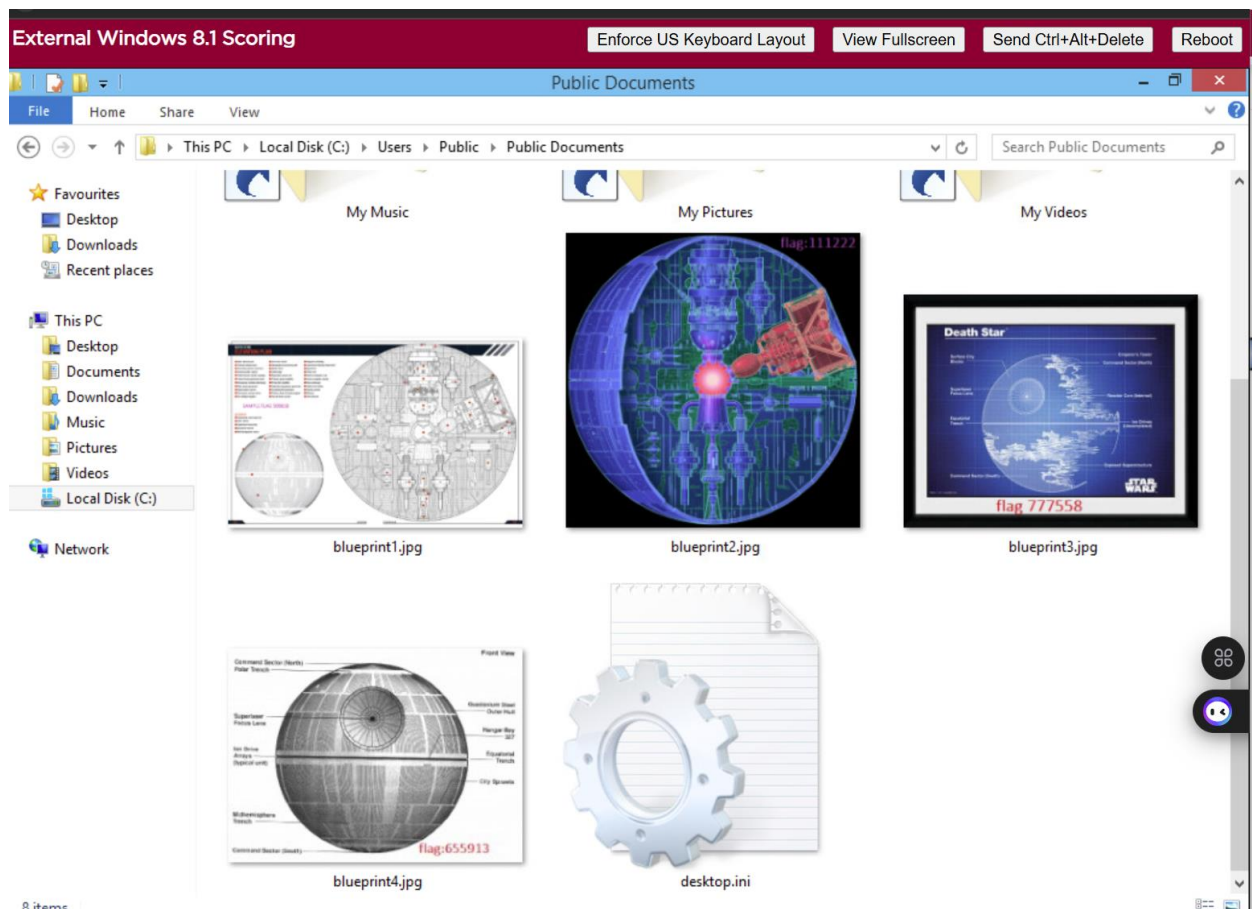


This Screenshot shows the blueprints found on the victim's machine

Selecting all the blueprints and copying them to Documents folder which is in the public folder in the attacker's machine



This screenshot shows the files from the victim's machine in the attacker's machine

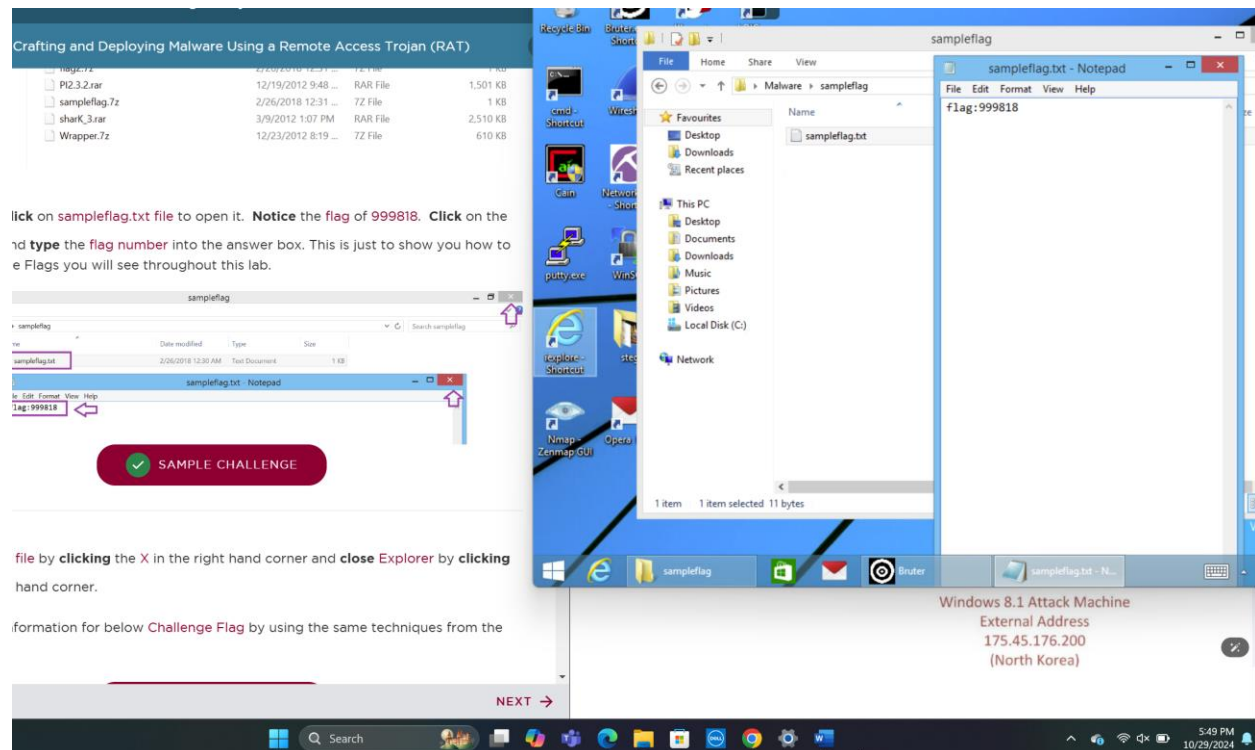


This screenshot shows the blueprints from the victim's machine

Supporting Evidence

These are the challenges tasks in the lab

After opening the Malware folder in Windows 8.1 desktop and after clicking the sampleflag.7z file, hover over 7-Zip, and extracted the “sampleflag\”.



This screenshot shows the sample challenge found in the extracted sampleflag.txt from the sampleflag file folder

Ethical Hacking and Systems Defense

Crafting and Deploying Malware Using a Remote Access Trojan (RAT)

sampleflag.txt - Notepad

✓ SAMPLE CHALLENGE

Clicking the **X** in the right hand corner and **close Explorer** by clicking **corner**.

on for below **Challenge Flag** by using the same techniques from the

✓ CHALLENGE #1

he **Malware** folder on the Windows 8.1 desktop.

The screenshot shows a Windows 8.1 desktop with a blue background. On the desktop is a folder named 'Malware'. A File Explorer window is open, showing the contents of the 'Malware' folder, which contains a single file named 'flag2.txt'. A Notepad window titled 'flag2.txt - Notepad' is open, displaying the text 'flag:343434'. The taskbar at the bottom shows icons for Internet Explorer, the 'flag2' folder, a mail icon, a target icon, and the Notepad window.

Ethical Hacking and Systems Defense

Crafting and Deploying Malware Using a Remote Access Trojan (RAT)

sampleflag.txt

sqlite3.dll

t the information for below **Challenge Flag** by using the same techniques from the

eps.

✓ CHALLENGE #2

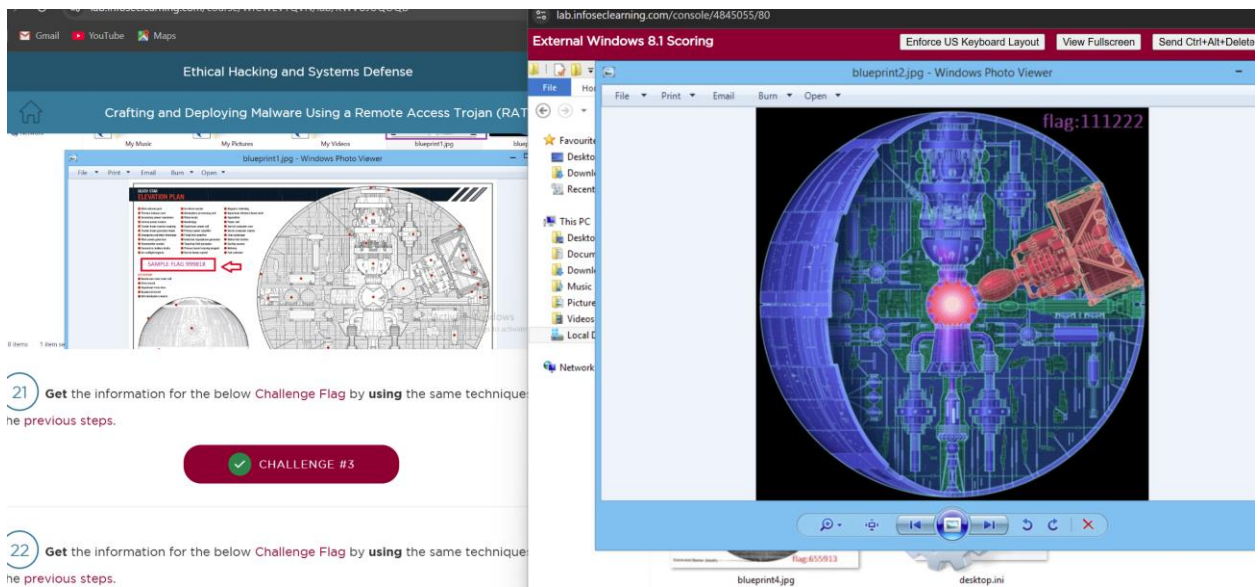
o **exit** and **press Enter**.

able-click on **DarkComet.exe** to launch the program.

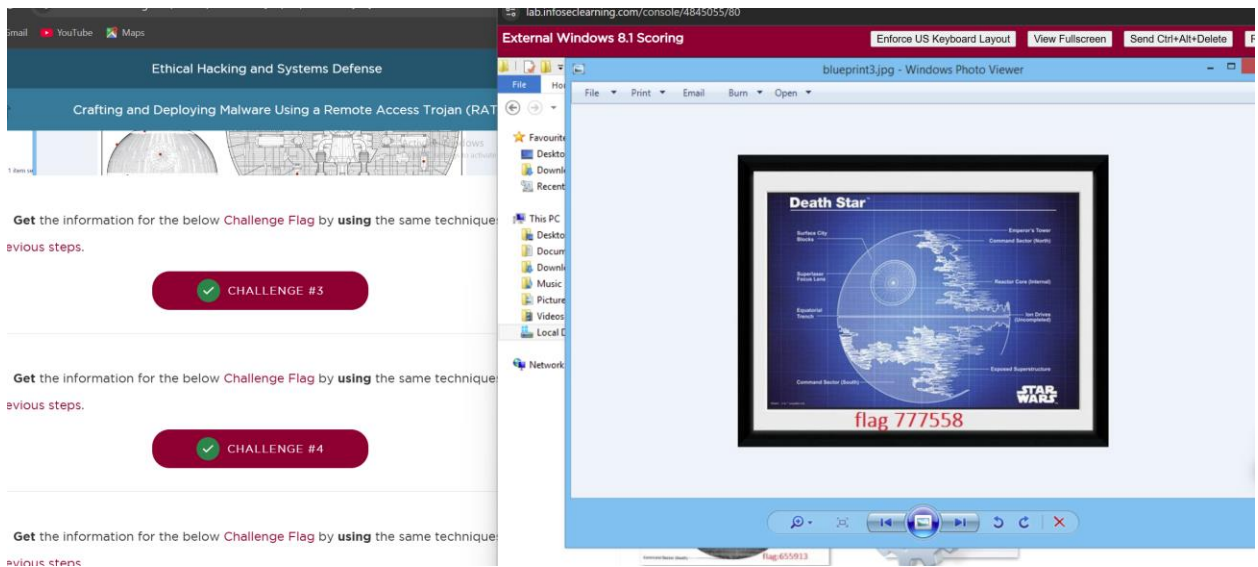
The screenshot shows a Windows 8.1 desktop with a blue background. On the desktop is a folder named 'DarkComet'. A File Explorer window is open, showing the contents of the 'DarkComet' folder, which contains several files including 'flag3.txt'. A Notepad window titled 'flag3.txt - Notepad' is open, displaying the text 'flag:717999'. The taskbar at the bottom shows icons for Internet Explorer, the 'DarkComet' folder, a mail icon, a target icon, and the Notepad window.

| me | Share | View |
|-------------------------|--------------------|-------------|
| ↑ Malware > DarkComet > | | |
| Name | Date modified | Type |
| Celesty Binder | 6/3/2012 9:16 PM | File folder |
| Goodies | 6/3/2012 9:18 PM | File folder |
| Icons | 2/23/2013 10:38 PM | File folder |

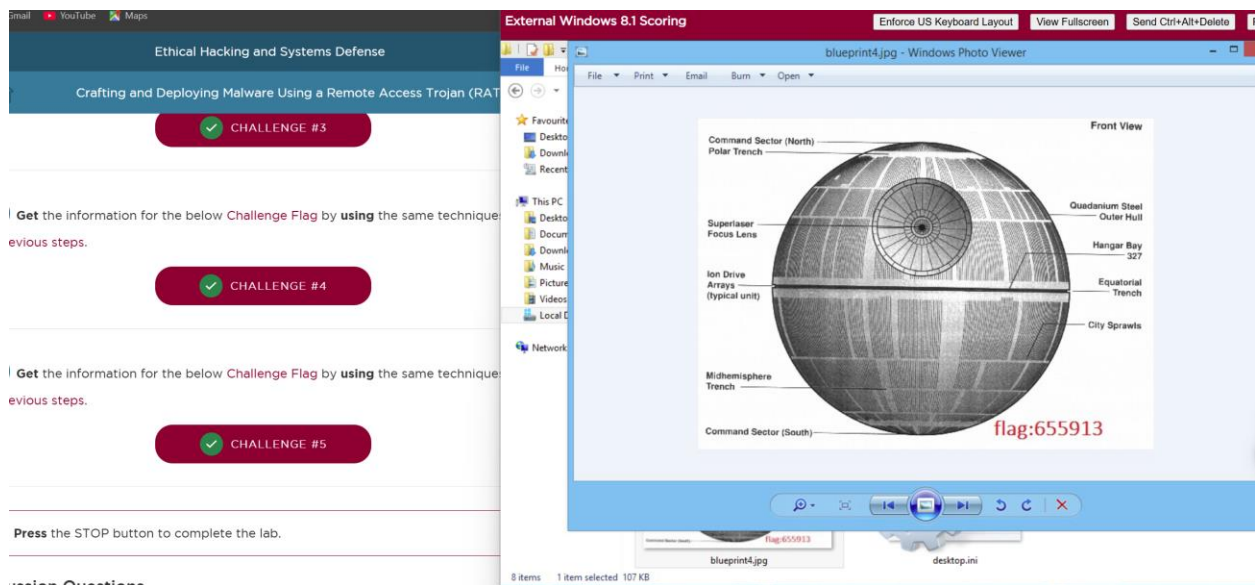
Windows 8.1 Attack Machine
 External Address
 175.45.176.200
 (North Korea)



This screenshot shows the challenge flag found in the Blueprint #1



This screenshot shows the challenge flag found in the Blueprint #2



This screenshot shows the challenge flag found in the Blueprint #3

Conclusion & Wrap-Up

Summary with:

- **Observations**

In this lab, I went through an entire attack scenario, from scanning open ports with nmap and zenmap to deploying malware. I observed that weak passwords and malware disguised as legitimate files can allow attackers easy access and long-term control over a system.

- **Identified risks**

I identified weak password policies and easily disguised malware as major risks. The use of a RAT like DarkComet shows how attackers can maintain control undetected if these issues aren't addressed.

- **Suggested recommendations**

I recommend enforcing stronger password policies, adding multi-factor authentication, and educating users on recognizing potential phishing attempts. Regular updates to antivirus software and active network monitoring would also help reduce risks.

- **Your successes & failures**

I successfully identified open ports, cracked the admin password, and established remote control through a RAT. However, I faced challenges in maintaining a stable connection and avoiding detection by security software.

- **Challenges**

The main challenge was evading detection, especially if antivirus tools were active on the target system. This lab showed me the importance of stealth to bypass both security tools and user awareness.

- This table summarizes risks by priority and outlines steps for strengthening system defenses against each identified threat.

| Risk | Priority | Remediation |
|-------------------------------------|-----------------|--|
| Weak Passwords | High | Enforce complex password policies, implement multi-factor authentication, and conduct regular audits. |
| RDP Vulnerability | High | Limit RDP access to essential users, set up VPN for secure connections, and monitor RDP logs. |
| Malware Installation (Trojan Horse) | High | Deploy robust antivirus and anti-malware solutions, use email filtering, and avoid suspicious downloads. |
| Command & Control via RAT | High | Block common RAT signatures, monitor network traffic for unusual patterns, and enforce firewall rules. |
| Network Scanning Detection | Medium | Implement Intrusion Detection Systems (IDS) to monitor for scans and restrict network scanning tools. |