

# Day 12

## Exploitation Analyst

### SSH Protocol:

YouTube:

<https://youtu.be/QPBhfdXhfXw?si=jTIRkLqFNRG4QBdO>

### **What is SSH?**

SSH stands for Secure Shell. It's a protocol to securely connect to remote computers over a network.

### **How it works?**

1. Client generates an asymmetric key pair:
  - Public key
  - Private key
2. Public key is copied to the server, saved in ~/.ssh/authorized\_keys.
3. When the client connects:
  - Server generates a random session key (this is your “new key”).
  - Server encrypts this session key with the client's public key.
4. Server sends this encrypted session key to the client.
5. Client decrypts it using its private key.
6. Now both sides share the same session key (symmetric), used to encrypt the actual SSH session.

### **How this connection differs from that of SSL?**

Step	SSL/TLS (Web/HTTPS)	SSH (Remote Login)
Who generates keys?	Server generates key pair	Client generates key pair
Who holds private key?	Server	Client
Public key stored where?	In a certificate, signed by CA, sent to clients	On server (authorized_keys file)
Who verifies identity?	Client checks CA's signature to trust server	Server trusts client via matching public key
How is session key exchanged?	Client generates session key, encrypts with server's public key	Server generates it, encrypts with client's public key
Authentication	Server is authenticated via CA certificate	Client is authenticated via key possession

Step	SSL/TLS (Web/HTTPS)	SSH (Remote Login)
Use case	Secure websites (e.g., HTTPS)	Secure remote shell access (e.g., ssh user@host)

#### Advantages of SSH:

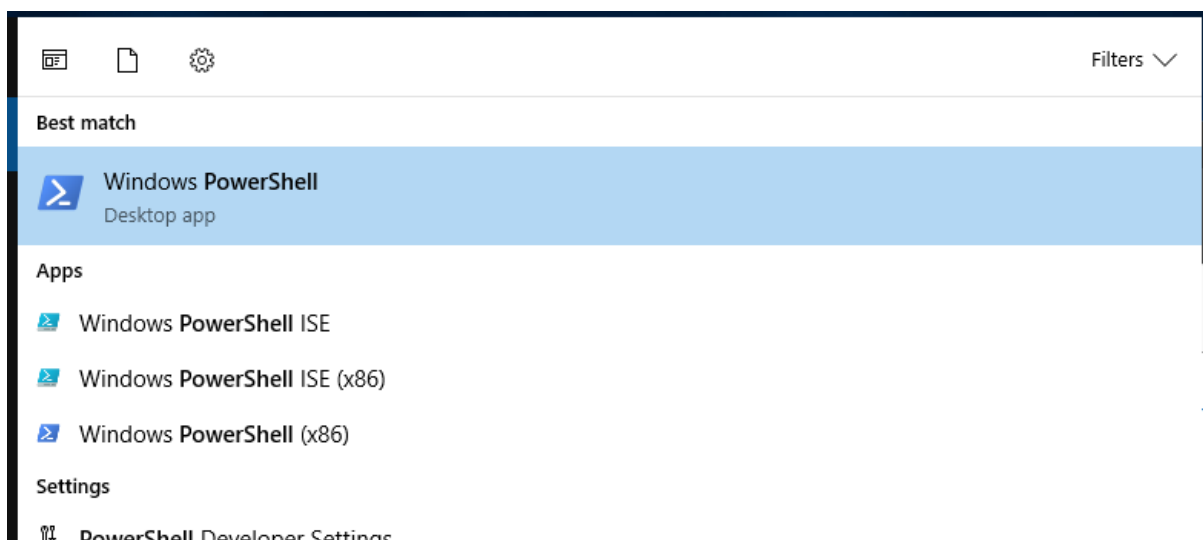
1. Secure Communication: Encrypted data protects against eavesdropping.
2. Authentication Options: Supports passwords and key-based login.
3. Remote Access: Safely control servers over networks.
4. Port Forwarding: Securely tunnel other services (like databases).
5. File Transfer: With SCP or SFTP, send files securely.
6. Integrity & Confidentiality: Prevents tampering and spoofing.

#### Disadvantages of SSH:

1. Setup Complexity: Key management can be tricky for beginners.
2. Risk if Keys/Passwords Leaked: If private key or password is stolen, access is compromised.
3. No Built-in GUI: It's command-line based (hard for non-tech users).
4. Firewall Restrictions: Port 22 might be blocked in some networks.
5. Brute Force Attacks: Needs strong passwords or keys to stay safe.

### Connecting to SSH of Windows 2019 server using id name and password:

Open "PowerShell" in Windows 2019 server in admin mode:



Following screen will appear:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>
```

Type the following command:

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

Operation
Running
[ooooooooooooooooooooo]
```

When the above state changes, type the following:

```
PS C:\Users\Administrator> Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

Path      :
Online    : True
RestartNeeded : False

PS C:\Users\Administrator> Start-Service sshd
PS C:\Users\Administrator> Set-Service -Name sshd -StartupType 'Automatic'
PS C:\Users\Administrator>
```

Note the IP of the Windows 2019: it is 192.168.1.103

```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

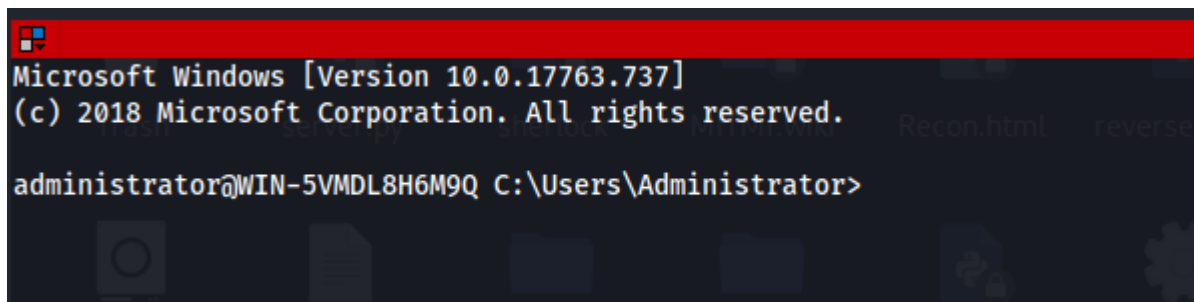
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a099:7e9f:abc9:458b%4
    IPv4 Address. . . . . : 192.168.1.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
PS C:\Users\Administrator>
```

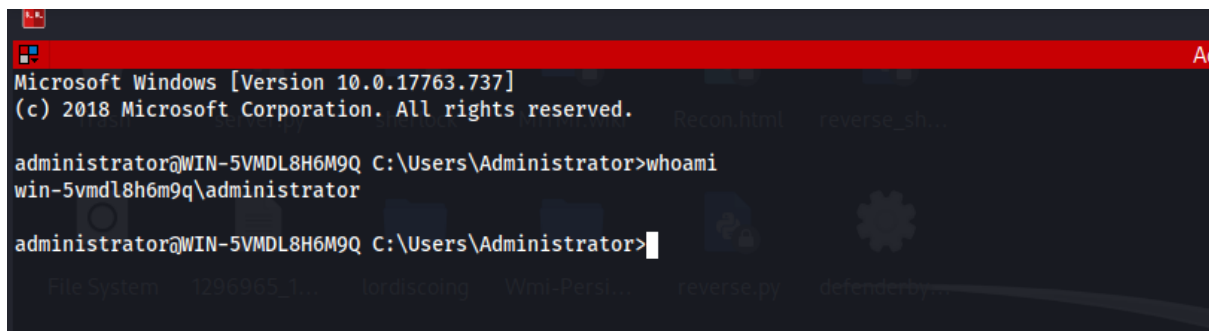
Now, in kali, use below command with the id name of it and IP of the windows 2019:

```
(root@kali)~[~]
# ssh administrator@192.168.1.103
The authenticity of host '192.168.1.103 (192.168.1.103)' can't be established.
ED25519 key fingerprint is SHA256:9T1/GLZG4FfNTJom07qzwhI/JjS9fDSbZqVNUP16bC4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes
```

Once, you write 'yes' (as shown above) and click enter, it will ask for password. Once you entered that: following screen will appear.

A screenshot of a Windows command prompt window. The title bar is red. The text inside shows the Windows version (10.0.17763.737) and copyright (c) 2018 Microsoft Corporation. The prompt is 'administrator@WIN-5VMDL8H6M9Q C:\Users\Administrator>'. The background has a dark blue theme with faint icons of a folder, document, and gear, and some text like 'Recon.html' and 'reverse'.

Proving my identity:

A screenshot of a Windows command prompt window. The title bar is red. The text inside shows the Windows version (10.0.17763.737) and copyright (c) 2018 Microsoft Corporation. The prompt is 'administrator@WIN-5VMDL8H6M9Q C:\Users\Administrator>'. The user has entered 'whoami' and the output is 'win-5vmdl8h6m9q\administrator'. The prompt is now 'administrator@WIN-5VMDL8H6M9Q C:\Users\Administrator>'. The background has a dark blue theme with faint icons of a folder, document, and gear, and some text like 'Recon.html', 'reverse\_sh', 'File System', '1296065\_1', 'lordiscoring', 'Vml-Pera...', 'reverse.py', and 'defenderpy'.

### Why this method is not secure?

1. Brute Force Attacks
  - Attackers can try millions of username-password combos using automated tools.
  - Common usernames like Administrator, root, etc. are easily guessed.
2. Password Reuse
  - Many users reuse passwords across systems. If one is leaked, others are exposed.
3. Keyloggers & Phishing
  - Passwords can be stolen via malware or phishing emails.
4. No Length or Complexity Enforcement by SSH
  - SSH does not force strong password policies by default.
5. No Two-Factor (by default)
  - Password login lacks an extra layer like OTP or hardware key (unless manually added).

### Can SSH username & password be sniffed using Wireshark?

No — not in plaintext. When you use SSH, the entire connection is encrypted.

--The End--