Proof of Concept (PoC) Report: Meterpreter + Mimikatz Tool

1) Tool Name: Meterpreter

Description:

Meterpreter is an advanced, stealthy payload within the Metasploit Framework used for post-exploitation. It provides a powerful interactive shell allowing attackers to control the compromised system.

What Is This Tool About?

Meterpreter allows attackers to execute commands, dump credentials, upload/download files, and pivot into internal networks—all without writing to disk, making it stealthy.

Key Features:

- In-memory payload (stealth)
- Encrypted communication with C2
- File upload/download
- Webcam capture, keylogging, and microphone recording
- Shell and command execution
- Supports privilege escalation
- Port forwarding and pivoting
- Supports scripting and automation
- Compatible with Windows, Linux, macOS, Android

Modules / Commands Used:

- sysinfo – get system info
- getuid – check user privileges
- upload/download – file transfer
- shell – spawn system shell

- migrate – process migration for evasion
- keyscan_start – start keylogger
- screenshot – take screen capture

💡 **How This Tool Helps:**

- Used after exploiting a vulnerability
- Maintains stealthy remote control
- Supports data exfiltration and pivoting
- Ideal for red teaming and adversary simulation
- Forms the backbone of many C2 infrastructures

When to Use During Investigation:

- After successful exploitation
- During lateral movement
- For privilege escalation and reconnaissance
- To exfiltrate sensitive files
- During persistence setup

Best User & Skills Required:

- Red teamers / Penetration testers
- OS knowledge (Windows/Linux internals)
- Network and exploit understanding
- Metasploit familiarity

---

2) Tool Name: Mimikatz

Description:

Mimikatz is a post-exploitation tool used to extract plaintext passwords, hashes, PINs, and Kerberos tickets from memory on Windows systems.

What Is This Tool About?

It targets Windows credential management systems and is widely used for lateral movement and credential dumping in enterprise environments.

Key Features:

- Dump plaintext passwords from memory
- Extract NTLM hashes, Kerberos tickets
- Pass-the-Hash, Pass-the-Ticket, Overpass-the-Hash
- Dump LSASS credentials
- Inject golden tickets
- Token impersonation and privilege escalation
- Can be executed directly or via Meterpreter

Commands Used:

- privilege::debug – enable debug privilege
- sekurlsa::logonpasswords – dump credentials
- sekurlsa::tickets – list Kerberos tickets
- sekurlsa::pth – pass-the-hash attack
- kerberos::golden – create golden tickets

How This Tool Helps:

- Recovers credentials from infected hosts
- Enables lateral movement in enterprise
- Explores AD trust relationships
- Supports Kerberos ticket replay attacks
- Very powerful for post-exploitation

When to Use During Investigation:

- After gaining SYSTEM/root access
- For credential dumping and escalation
- During red team emulations
- In Windows domain compromise scenarios

Best User & Skills Required:

- Red teamers / Advanced pentesters
- Deep knowledge of Windows internals
- Understanding of Active Directory, Kerberos
- Familiarity with PowerShell and C2 frameworks

Attack Flow:

1. **Exploit Target**: Windows 10 machine via EternalBlue or phishing.
2. **Payload**: Deliver Meterpreter reverse shell using Metasploit.
3. **Post-Exploitation**:
   - Use getsystem and migrate to remain hidden.
   - Upload and execute Mimikatz through Meterpreter.
   - Run sekurlsa::logonpasswords to extract cleartext passwords.
4. **Lateral Movement**:
   - Use dumped credentials to RDP or access SMB shares.
   - Dump hashes and perform pass-the-hash to move across machines.