**Date: 26 OCt, 2024**

**Mentor: Bappi Sir**

**Topics:**

* Penetration Testing
* VA
* PT

Manually/Automated test kore vulnerability assess kore report kora hoy.

Low level/mid level vulnerabilities ignore korte pari.  
Kintu mid+low vulnerability mile boro attack hoite pare. Ei jonno penetration system lage.  
  
**Steps of penetration Test:**

1. **System hacking:**

* Reconnaissance: research kore info gather
* Network scanning (service ki ki ase, vul ki ki ase, exploit korte pari)
* Gaining access: (Password attack, VCracking, Vul exploitation)
* Maintaining Access:
* Clearing Tracks

1. **Vulnerabilities exploitation:**
2. **Identify vulnerabilities:** Vulnerability gular sathe risk ase kina kono.

**Disturbance**: Service level/ system level je kono level ei disturbance thakte pare.

**Payload selection/generate**: Access gain korte help korbe.

**Cyber weapon**: malware(application/script/code). Etc

Open Source tools/paid tools

**Exploit vs payload:**

Almost the same.

Exploit: Vulnerability ke trigger kora.

Payload: Access gain korar jonno connection provide kora.

Website:

1. <https://www.exploit-db.com/>
2. <https://packetstormsecurity.com/>
3. <https://www.rapid7.com/db/>

**Payload & Shell:**

Shell 2 types

* Bind Shell→ Attacker to target
* Reverse Shell → Target to attacker.

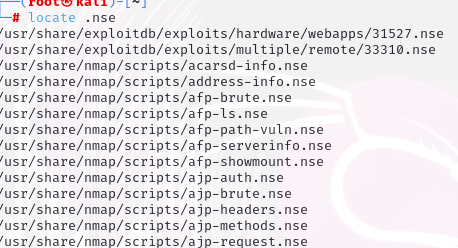
**Exploitation Tools:**

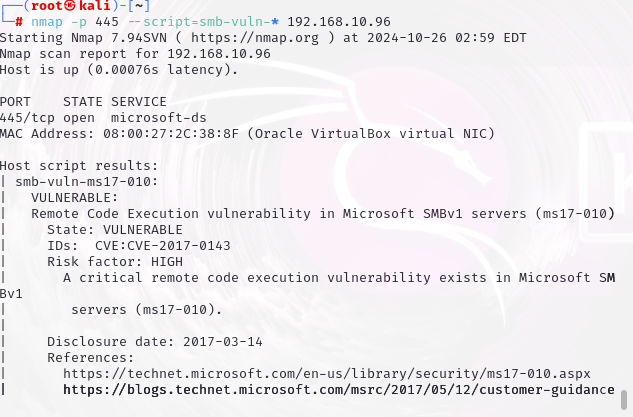
Open source framework (Metasploit) 🡪 To start metasploit comman in kali 🡪 $msfconsole

* Payload: collect for shell
* Post: activity
* Encoder:
* Nops: For buffer overflow attacks
* Evasion : windows/system Defender ke bypass korar jonno use hoy.

**Command & Screenshot:**



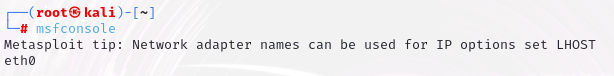




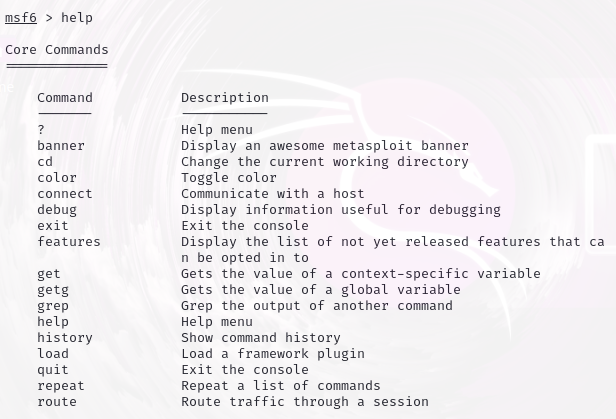
Search to google: ms17-010 (For study)

Metasploit Access er jonno:

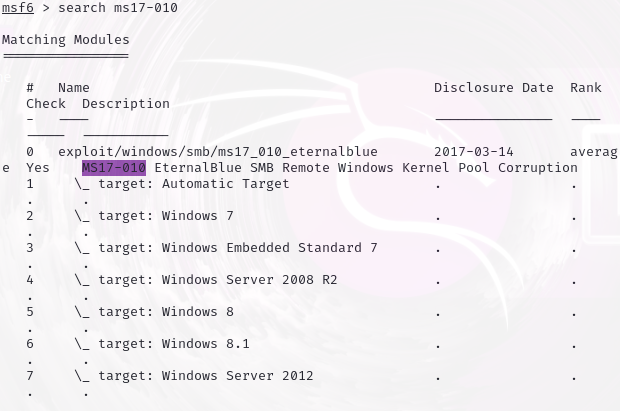
$ msfconsole



           →help



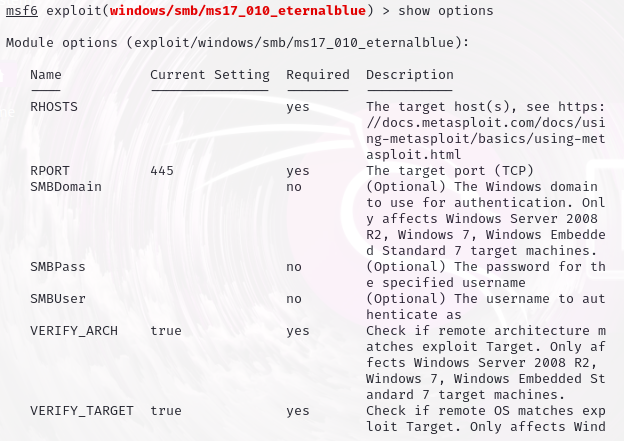
→ search (ip)

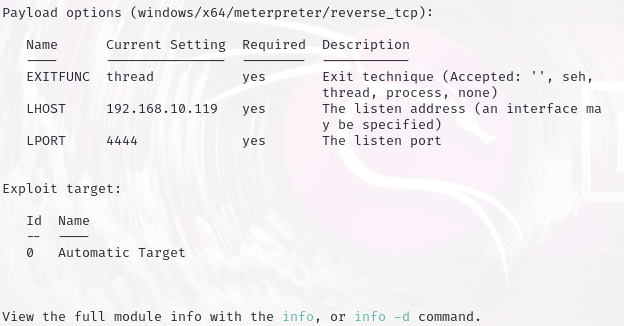


→use

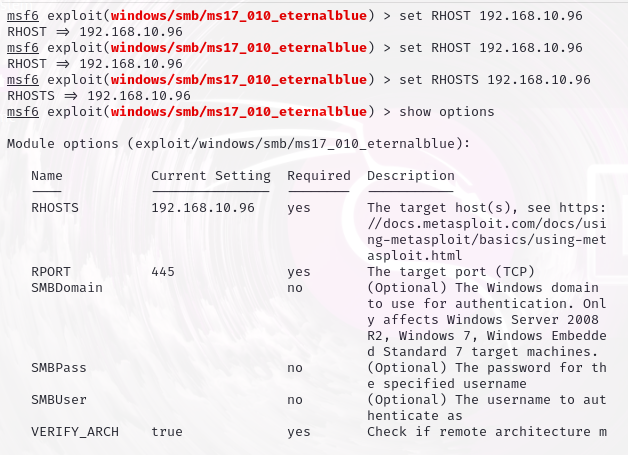
https://lh7-rt.googleusercontent.com/docsz/AD_4nXf0Fv6ORhrw6U35A5wfKbLzgRLitxumIt0jxMktQL46uk3redudw_yKhcrnVAybWR8dsUWLHH-mBocXH0OchSxBc-PhUm0jzpYfAYdxy86D1AiMEK41_U3tihmNN_-Vlc-ULBvND_wiu3tXnprdGCCSwD1g?key=h2K3q10Lylhfw04JYyNbcQ

→ show options



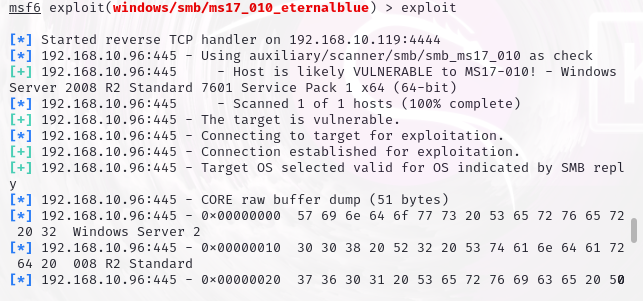


→ set



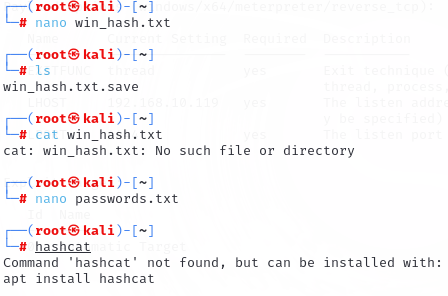
→ set payload

Exploit successfully run hole meterpeter ashbe.



Hash Algo lage, password shoho 1ta text file lage.

HashType: NTLM



$ hashcat -h <For help>

$ hashcat -h  grep

Tools to hack password:

* JOHN the ripper
* Hashcat