Date: 26 OCt, 2024

Mentor: Bappi Sir

**Topics:**

Penetration Testing ( means vulnerability finding)

VA (Vul Assessment)

PT (Penetration Test)

**Some suggestions:**

Manually/Automated test kore vul assess kore report korbo.

Low level/mid level ignore korte pari.  
Kintu mid+low mile boro attack hoite pare. Ei jonno penetrating system lage.  
  
**1st step:**

**System hacking:**

* Reconnaissance: research kore info gather
* Network scanning (service ki ki ase, vul ki ki ase, exploit korte pari)
* Gaining access: (Password attack, Pass Cracking, Vul exploitation)

Password attack → sniffings, Trojan, key, logger, spyware

Pass crack → brute force, dictionary attack.

* Maintaining Access:
* Clearing Tracks

**Vulnerabilities exploitation:**

* Identify vulnerabilities.
* Determine risk → Vul gular sathe risk ase kina kono
* Disturbance: Service level/ system level
* 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: Vul trigger kora.

Payload: Access gain korar jonno connection provide kora.

Website:

<https://www.exploit-db.com/>

2.

3.

Payload & Shell:

Shell 2 types

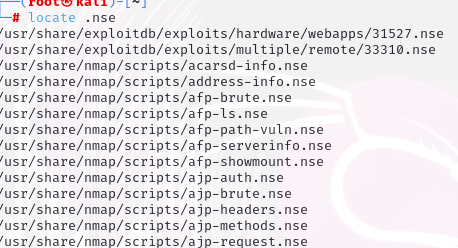
* Bind Shell→ Attacker to target
* Reverse Shell → Target to attacker.

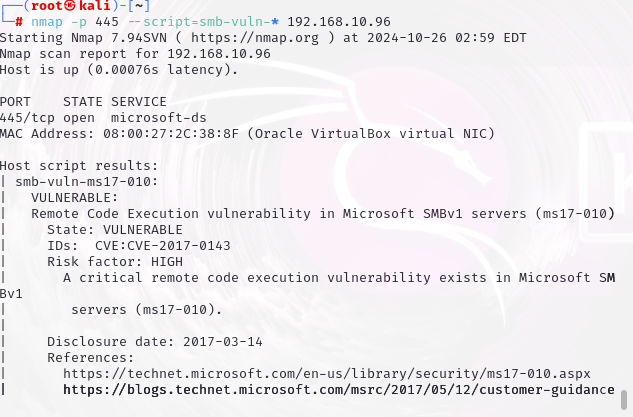
Exploitation Tools:

1. Open source framework (Metasploit)
2. Auxilary
3. exploits
4. Payload
5. Post
6. Encoder
7. Nops: For buffer overflow attacks
8. Evasion :defender ke bypass korar jonno use hoy

Command & Screenshot:



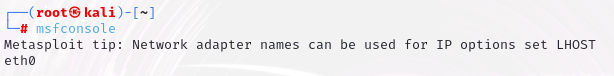




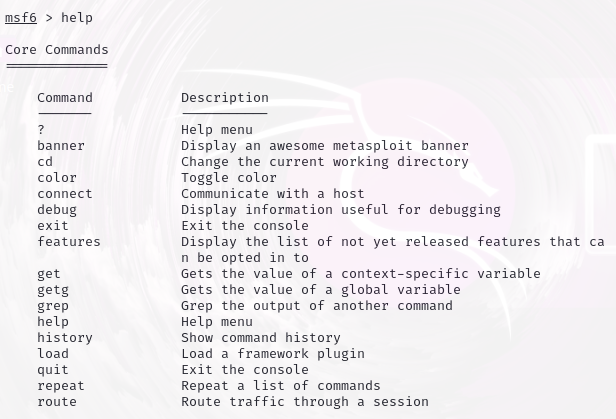
**## Search to google: ms17-010 (For study)**

Metasploit Access er jonno:

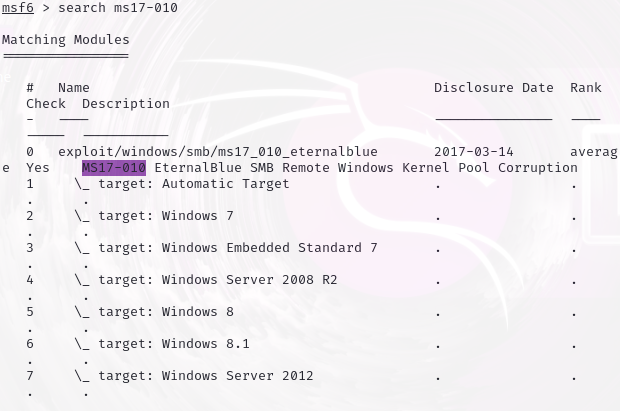
$ msfconsole



           →help



→ search (ip)

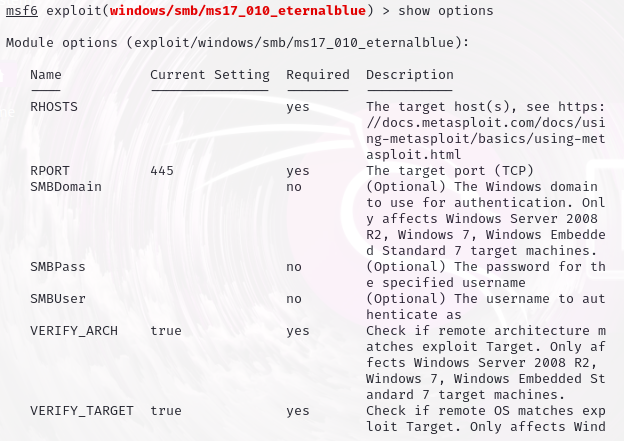


→use

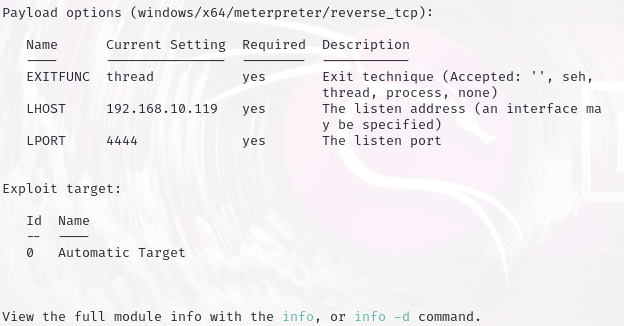
https://lh7-rt.googleusercontent.com/docsz/AD_4nXcOYvNfHwA6Zc5fXWmriRokyjND91ZWxQBD31_MNNJGLcohDWWy-tN4t0dnUkR8hBIexIuRIEbyZ-fI_ZNeH8nQ5n1wbRay6L_ae_ogRQ2UU6nyXGivFa8cL87UsPQPHSLwTE3yTMo4g7hLG9LupPiKWC05?key=h2K3q10Lylhfw04JYyNbcQ

Successful → red colour verdict

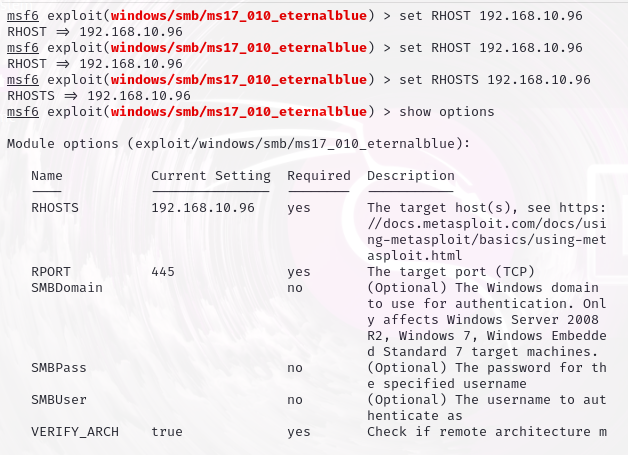
→ show options



RHOST → target host.



→ set



→ set payload

$set LPORT 4321

$run

$(meterpreter>

Vagrantà default id and password.

Exploit successfully run hole meterpeter ashbe.

