Bushra Akter

Class: 14

For password cracking

- John the ropper
- Hashcat

#hashcat –h | grep NTLM

┌──(root㉿kali)-[~]

└─# hashcat -h|grep NTLM

```
┌──(root㉿kali)-[~]
└─# hashcat -h|grep NTLM
   5500 | NetNTLMv1 / NetNTLMv1+ESS                                 | Network Protocol
  27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)                            | Network Protocol
   5600 | NetNTLMv2                                                 | Network Protocol
  27100 | NetNTLMv2 (NT)                                            | Network Protocol
   1000 | NTLM                                                      | Operating System
```

#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 →version

┌──(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 →google search

https://www.urlencoder.org/ →

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