“ PENETRATION TEST ”

Nmap e Zenmap

E uma ferramenta utilizada normalmente nas distribuições Linux e também agora esta disponível para Windows.

Esta Ferramenta atua como um Scaner de redes, fornecendo informações como: IPs , port/host , serviços, Mac , Sistemas Operacionais , marca de equipamentos , dentre outros .

O Nmap pode ser utilizado para teste de segurança em redes (testes de penetração) e/ou invasão dos mesmos.

Podemos scanear um Host especifico ou um segmento de rede, exemplo:

- Nmap –sV 192.168.0.3 scanner serviços e portas do host;
- Nmap – F 192.168.0.3 mostra as portas abertas do host;
- Nmap –p 1-1000 192.168.0.3 escaneia as portas de 1 ate 1000 do host.

Nmap -T4 -A -v 192.168.8.0/24 scan intensivo da rede que utilizamos para obter as seguintes informações da Faculdade Senac.

IP	Port/host	Service	Maquina
192.168.8.1	23/tcp	telnet	Switch Dell powerconnect 6248
	80/tcp	http	
192.168.8.107	8080/tcp	http	Windows 8
192.168.8.112	8080/tcp	http	Windows 8
192.168.8.114	80/tcp	http	LINUX 3,11 3,14
192.168.8.121	8080/tcp	http	Windows 8
192.168.8.122	135/tcp	msrpc	WINDOWS SERVER 2008 R2
	139/tcp	netbios-ssn	
	445/tcp	netbios-ssn	
	8080/tcp	http	
	49156/tcp	msrpc	
192.168.8.123	8080/tcp	http	Windows 8
192.168.8.129	8080/tcp	http	Windows 8
192.168.8.131	8080/tcp	http	LINUX 3,11 3,14
192.168.8.132	8080/tcp	http	Windows 8
192.168.8.133	8080/tcp	http	Windows 8
192.168.8.140	135/tcp	msrpc	NOVEL NetWare 6.5
	139/tcp	netbios-ssn	
	445/tcp	microsoft-ds	
	554/tcp	rtsp	
	1110/tcp	nfsd-status	
	2869/tcp	icslap	
	3389/tcp	ms-wbt-server	
	10243/tcp	HTTP	
	19780/tcp	UNKNOWN	
	49152/tcp	msrpc	
	49153/tcp	msrpc	
	49154/tcp	msrpc	

	49155/tcp	msrpc	
	49156/tcp	msrpc	
	49158/tcp	msrpc	
192.168.8.141	135/tcp	msrpc	Win 7 Pro
	139/tcp	netbios-ssn	
	445/tcp	netbios-ssn	
	8080/tcp	http	
	49155/tcp	msrpc	
192.168.8.142	8080/tcp	http	Windows 8
192.168.8.146	80/tcp	http	LINUX 3,11 3,14
192.168.8.147	8080/tcp	http	Windows 8
192.168.8.150	8080/tcp	http	Windows 8

Ferramentas utilizadas para pesquisa foram:

- Sistema Operacional

  Kali Linux, nmap

  Windows, Zenmap