M3_W11D2

Report su Metasploitable (192.168.50.100)
Comandi utilizzati per la scansione del sistema target (nmap -O/-sS/-sT/-sV)

Report Metasploitable				
IP	Operating System	Port (Open)	Service	Version
192.168.50.100	Linux 2.6.X	21	ftp	vsftpd 2.3.4
192.168.50.100	Linux 2.6.X	22	ssh	OpenSSH 4.7p1 Debian Subuntul (protocol 2.0)
192.168.50.100	Linux 2.6.X	23	telnet	Linux telnetd
192.168.50.100	Linux 2.6.X	25	smtp	Postfix smtpd
192.168.50.100	Linux 2.6.X	53	domain	ISC BIND 9.4.2
192.168.50.100	Linux 2.6.X	80	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
192.168.50.100	Linux 2.6.X	111	rpcbind	2 (RPC #100000)
192.168.50.100	Linux 2.6.X	139	netbios-ssn	Samba smbd 3.X - 4.x
192.168.50.100	Linux 2.6.X	445	microsoft-ds	Samba smbd 3.X - 4.x
192.168.50.100	Linux 2.6.X	512	exec	netkit-rsh rexecd
192.168.50.100	Linux 2.6.X	513	login	OpenBSD or Solaris rlogind
192.168.50.100	Linux 2.6.X	514	shell	Netkit rshd
192.168.50.100	Linux 2.6.X	1099	java-rmi	GNU Classpath grmiregistry
192.168.50.100	Linux 2.6.X	1524	bindshell	Metasploitable root shell
192.168.50.100	Linux 2.6.X	2049	nfs	2-4 (RPC #100003)
192.168.50.100	Linux 2.6.X	2121	ccproxy-ftp	ProFTPD 1.3.1
192.168.50.100	Linux 2.6.X	3306	mysql	MySQL 5.0.51a-3ubuntu5
192.168.50.100	Linux 2.6.X	5432	portgresql	PostgreSQL DB 8.3.0 - 8.3.7
192.168.50.100	Linux 2.6.X	5900	vnc	VNC (protocol 3.3)
192.168.50.100	Linux 2.6.X	6000	X11	(access denied)
192.168.50.100	Linux 2.6.X	6667	irc	UnrealIRCd
192.168.50.100	Linux 2.6.X	8009	ajp13	Apache Jserv (Protocol v1.3)
192.168.50.100	Linux 2.6.X	8180	http	Apache Tomcat/Coyote JSP engine 1.1

Descrizione dei servizi sopra elencati:

FTP: (File Transfer Protocol) servizio che consente il trasferimento di file tra un client e un server.

SSH: (Secure Shell) protocollo di rete che consente l'accesso remoto tramite una connessione crittografata.

TELNET: protocollo di rete che consente agli utenti di stabilire sessioni di comunicazione bidirezionali su una rete di computer.

SMTP: (Simple Mail Transfer Protocol) protocollo di comunicazione utilizzato per l'invio e la ricezione di messaggi di posta elettronica su Internet.

DOMAIN: protocollo DNS (Domain Name System), essenziale per la risoluzione dei nomi di dominio in indirizzi IP e viceversa su Internet.

HTTP: (Hypertext Transfer Protocol): Protocollo di comunicazione utilizzato per il trasferimento di pagine web e altri dati su Internet.

RPCBIND: (Remote Procedure Call Bind): Servizio che ascolta richieste di chiamate a procedure remote e le associa a un numero di porta.

NETBIOS-SSN: (NetBIOS Session Service): Servizio che fornisce sessioni NetBIOS affidabili tra due computer su una rete.

MICROSOFT-DS: (Microsoft Directory Service): Servizio utilizzato da Microsoft Windows per l'accesso ai file e ai servizi di directory.

EXEC: Protocollo che consente l'esecuzione di comandi o programmi su un host remoto.

LOGIN: Servizio che gestisce l'autenticazione degli utenti su un sistema.

SHELL: Interfaccia che consente agli utenti di interagire con il sistema operativo eseguendo comandi.

JAVA-RMI: (Java Remote Method Invocation): Meccanismo che consente ai metodi di oggetti Java di essere invocati da un'altra JVM, eventualmente su un'altra macchina.

INGRESLOCK: Servizio utilizzato per il blocco e la gestione delle risorse nel sistema di gestione del database Ingres.

NFS: (Network File System): Protocollo che consente a un computer di accedere ai file su un altro computer su una rete in modo trasparente.

FTP: (File Transfer Protocol): Protocollo utilizzato per il trasferimento di file tra un client e un server su una rete TCP/IP.

MYSQL: Sistema di gestione di database relazionali open-source.

POSTGRESQL: Sistema di gestione di database relazionali open-source.

VNC: (Virtual Network Computing): Protocollo utilizzato per controllare e visualizzare desktop remoti.

X11: Protocollo di comunicazione utilizzato per gestire finestre grafiche su sistemi Unix e simili.

IRC: (Internet Relay Chat): Protocollo di comunicazione testuale utilizzato per la messaggistica istantanea su Internet.

AJP13: (Apache JServ Protocol): Protocollo utilizzato per la comunicazione tra un server web e un contenitore servlet, spesso associato ad Apache Tomcat.

HTTP: (porta 8180): Una porta alternativa per il servizio HTTP, spesso utilizzata per applicazioni web che richiedono una configurazione personalizzata.