LINUX SECURITY

[root@shadow]# date
23/11/02 15.00

[root@shadow]# whoami
Scali Omar

Linux Day 2k2

START

NOTE DELL'AUTORE

Le condizioni per l'utilizzo di questo documento sono quelle della licenza standard GNU-GPL, allo scopo di garantire che rimanga un documento libero.

Perché la licenza sia rispettata, è necessario che ogni opera derivata sia rilasciata secondo i termini della stessa licenza GNU-GPL.

Le diapositive dovranno intendersi unicamente come supporto per la relazione orale dell'autore e non come spiegazione esaustiva dell'argomento.

OMAR SCALI Gulch Member
HomePage: http://www.smox.it
GulchPage: http://gulch.crs4.it

Principali minacce ai sistemi

Footprinting:
Enumerazione
Social engineering
Interrogazioni ICMP
Port Scanning

Attacco:
Mappa vulnerabilità
Spoofing
DNS attack
BufferOverflow
Denial of Service (DoS e DDoS)
Worm

Footprinting

Tecnica di ricostruzione del profilo di protezione di una rete o sistema.

Enumerazione:
Processo che consente di identificare i nomi di dominio collegati ad un sistema o ad una rete tramite il reperimento di informazioni disponibili su Internet, InterNIC, ARIN, SamSpade, Whois.

Social engineering:
Recupero di informazioni sui sistemi e sulla rete tramite "truffe" a livello sociale, molti attacchi storici sono stati portati a termine tramite questa tecnica.

Footprinting

Interrogazioni ICMP o Ping sweep:

Processo di ricostruzione di una network map, normalmente il comando ping invia dei pacchetti ICMP ECHO (tipo 8) al sistema target che a sua volta risponde con pacchetti ICMP ECHO_REPLY (tipo 0) indicando che il sistema attualmente è collegato alla rete.

Tool come icmpquery possono:

- Richiedere l'orario del sistema target tramite l'invio di un pacchetto ICMP TIMESTAMP (tipo 13) utile per conoscere il fuso orario del sistema.
- Richiedere la netmask dell'host, tramite un pacchetto ICMP ADDRESS MASK REQUEST (tipo 17).

Footprinting

Port Scanning:

Tecnica di scansione diretta delle porte per stabilire se dei sistemi siano effettivamente in funzione, infatti difficilmente i firewall bloccano pacchetti destinati alle porte comuni come SMTP(25), IMAP(143), POP(110), questo lavoro può essere svolto dal tool nmap prelevabile all'indirizzo www.insecure.org/nmap.

```
# nmap -sP -PT80 192.168.1.0/24
TCP probe port is 80
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host  (192.168.1.2) appears to be up
Host  (192.168.1.3) appears to be up
Host  (192.168.1.4) appears to be up
Host (192.168.1.5) appears to be up
Nmap run completed -- 256 IP address (4 host up) scanned in 2 seconds
```

Attacco

Mappa punti vulnerabili:
Una volta ricostruita la mappa delle rete nmap fornisce i servizi attivi sul sistema, compresa la versione di OS sul server/workstation o router/switch:

```
# nmap -sS -O 24.198.xx.xx
Interesting ports on maine.rr.com (24.198.xx.xx):
(The 1526 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
79/tcp     open        finger
80/tcp     open        http
111/tcp    open        sunrpc
113/tcp    open        auth
443/tcp    open        https
513/tcp    open        login
Remote operating system guess: Linux 2.1.122 - 2.2.16
Uptime 61.750 days (since Sat Dec 22 00:13:33 2001)
```

Attacco

Mappa punti vulnerabili:

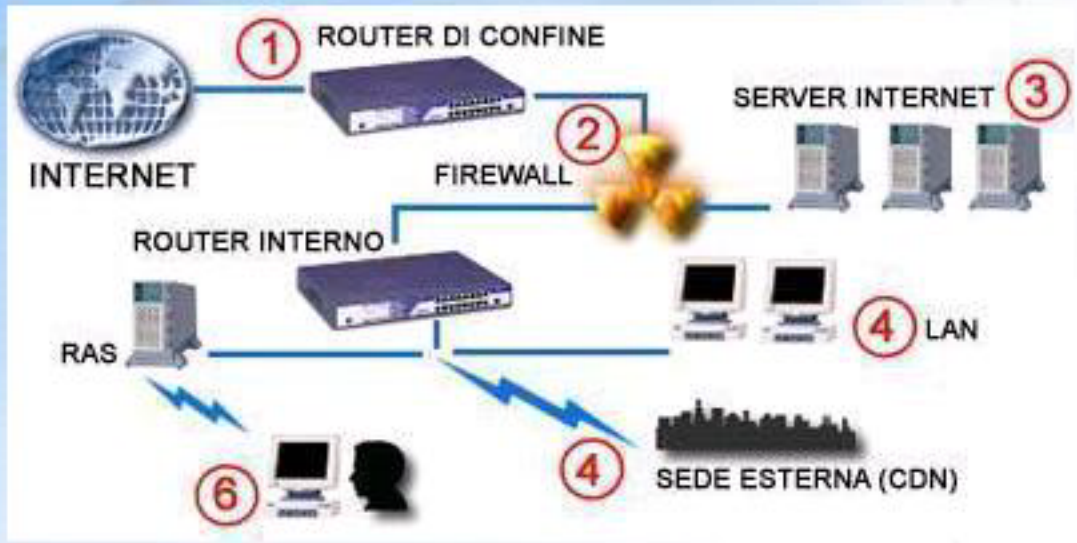
Per la compilazione dei punti vulnerabili esistono varie metodologie, le due maggiormente utilizzate:

- Reperimento di informazioni dai siti specializzati in sicurezza, allo scopo di trovare bug intrinseci al sistema target (CERT, SecurityFocus, ecc...).

- Il secondo metodo consiste nell'utilizzare utility che sono in grado di effettuare tale ricerca autonomamente direttamente sul sistema, i migliori pacchetti gratuiti utili a tale scopo sono Nessus (www.nessus.org) e SAINT (www.wwdsi.com/saint).

Attacco

Probabili vulnerabilità:



Attacco

Spoofing:
Indipendentemente dall'esito dell'attacco un buon cracker cerca sempre di non farsi rintracciare, in America le indagini eseguite sui crimini informatici affermano che la maggior parte dei cracker utilizza almeno due sistemi ponte, ignari di essere stati violati, dove da poi parte l'attacco vero e proprio.

In alternativa è possibile contraffare l'indirizzo ip di provenienza.

L'indirizzo ip di origine da contraffare, si trova nell'header del pacchetto TCP insieme ad altri importanti valori come il numero della porta di destinazione, un numero di ack, un sequenze number, e altri flag.
Potendo modificare tali valori su tutti i pacchetti in uscita è possibile contraffarre il proprio indirizzo, ma non è così semplice anche se non impossibile.

Leggete Security Problems in the TCP/IP Protocol Suite di Steve Bellovin.

Attacco

Attacco al DNS:

Un attacco al DNS ha lo scopo di modificare le tabelle dei nomi in particolare si esegue una contraffazione dei record PTR e le informazioni che esso contiene, in modo che quando il client richiede una ricerca, il server fornisce un indirizzo falso.

Questo indirizzo fornito ovviamente è una macchina sotto il controllo del cracker, immaginate cosa possa accadere se un utente ignaro inserisse il numero di carta di credito su un sito ipotizzato sicuro senza immaginare di essere stato dirottato.

Potete provare sempre a scopo didattico il programma Snoof www.c0p.org.

Attacco

Buffer Overflow:
Una condizione di buffer overflow si riscontra quando un programma, un utente oppure un processo tenta di inserire una quantità di dati superiore, rispetto a quella che un buffer può contenere.

Tale errore normalmente genera un errore del tipo "segmentation violation", che può essere sfruttato dai cracker per ottenere un' accesso al sistema sia locale che remoto.

Tale metodo di attacco riguarda tutti i servizi della macchina target come bind, httpd, ftpd, sshd, telnetd, portmap, nfs, mysql, xserver.

Esistono anche bufferoverflow basati su bug delle librerire locali.

Attacco

Denial of Service (DoS):

Questi attacchi sono i più pericolosi perché tutti i sistemi della rete ne sono soggetti, gli attacchi Dos hanno il compito di saturare le possibili connessioni esterne che un server è in grado di gestire.

Come è accaduto qualche anno fà ad un famoso ISP Americano PANIX che per più di una settimana ha rifiutato i collegamenti Internet a più di seimila utenti.

Normalmente un' attacco DoS punta a consumare la larghezza di banda o ad esaurire le risorse del sistema bersagliato rendendolo incapace di far fronte alle richieste.

Attacco

Denial of Service (DoS): SYN Flood

L'accado di SYN Flood è molto più devastante in quanto sfrutta una baco nella handshake del collegamento. Il problema consiste nel fatto che il server dopo aver risposto con un SYN/ACK alloca una quantità di memoria predefinita per ogni potenziale collegamento non ancora stabilito completamente.

Attacco

Distribuited Denial of Service (DDoS):

Fase A:
Il cracker individua una serie di host su Internet che presentano problemi di security e che possono essere facilmente attaccati.

FaseB:
Gli host individuati vengono attaccati, su uno di essi viene installato il programma master e sugli altri il programma slave.

FaseC:
Il cracker mette in esecuzione il programma master che chiede ai programmi slave di fare migliaia di connessioni su un determinato sito.

TrinOO, Tribe Flood Network e Tribe Flood Network 2000 (Tfn2k) i più famosi tool.

Attacco

Worm:
Morris si accorse che i server UNIX versione Berkeley avevano due problemi di sicurezza che davano accesso al sistema con i permessi di superutente, di conseguenza gli venne la brillante (?) idea di scrivere un programma che avrebbe sfruttato queste due falle autoriproducendosi e infettando nuovi sistemi, così nacque il primo worm.

Attuali worm per LINUX ancora in circolazione:
Ramen (wuftpd - rpc.statd - LPRng)
Lion (bind)
Adore (wuftpd - rpc.statd - LPRng - bind)

Worm benefico: CheeseWorm

Attacco
;-)


HelpDex
shane_collinge@yahoo.com
LET ME SEE THE /ETC/HOSTS FILE OR YOU MAY NOT LIVE TO SEE TOMORROW.
Shane.
Brute access
The access level granted when you hold the power over life & death

Metodologie di Difesa

Prevenzione:
Social engineering
Hardening
Interrogazioni ICMP
PortScanning
Spoofing
BufferOverflow
Antisniffing
Denial of Service (DoS e DDoS)
Difesa attiva: Firewall + IDS

Prevenzione

Social engineering:
Controllare sempre l'identità di chi chiede informazioni sui vs sistemi.
Cifrare i canali di comunicazione.

Hardening:
Metodologia che consente l'individuazione dei servizi non necessari sul sistema con conseguente chiusura di essi.

Prevenzione

Interrogazioni ICMP:

Siete sicuri che avete bisogno del traffico ICMP?
Tale protocollo è utile per la rilevazione dei problemi connessi alla rete, ma se usato in modo improprio si dimostra molto dannoso, vedi attacchi di tipo DoS come smurf.c.

ECHO ed ECHO_REPLY sono solo due dei 18 tipi di questo traffico.

Consiglio comunque di lasciar passare attraverso il firewall i pacchetti ICMP di tipo MTU path discovery, necessari per le operazioni di traceroute e di controllo vario.

Ottimizzazione:
# vi /etc/sysctl.conf
net.ipv4.icmp_echo_ignore_all = 1

Prevenzione

Portscanning:
La scansione delle porte come detto precedentemente viene utilizzata per riconoscere quali servizi TCP o UDP sono attivi su una determinata macchina, anche in questo caso l'intercettazione di questo tipo di attività è fondamentale.

A livello network si può limitare il range di porte disponibili.
A livello host il tool Portsentry si rivela un utile strumento.

Portsentry è un demone che tiene sottocontrollo, eventuali scansioni indirizzate al nostro sistema reagendo di conseguenza.

Prevenzione

Spoofing:

Come abbiamo detto, lo spoofing si basa sull'individuazione della sequenza numerica che contraddistingue un hand-shake di una connessione ip.

Il modo migliore dunque per proteggersi da questo tipo di attacco è chiamato Source Address Verification, che esegue il controllo della provenienza dei pacchetti prima di rispondere su qualsiasi porta, in questo modo evitiamo che la nostra rete accetti pacchetti spoof usati frequentemente in attacchi DoS (Denial of Service).

A livello firewall e network rifiutare pacchetti provenienti da indirizzi locali.

Prevenzione

BufferOverflow:
Difendersi dal buffer overflow non è semplice perché non sempre dipende dall'OS

Tutti gli accorgimenti contro il buffer overflow sono normalmente diretti ai programmatori, come le FAQ del Secure Unix Program (http://whitefang.com/sup), fuori dal nostro campo di azione dunque, noi siamo infatti solamente semplici utilizzatori.

L'unica azione che possiamo intraprendere è quella di rimanere aggiornati su eventuali condizioni dei buffer overflow, magari attraverso la quotidiana lettura degli ultimi bug presenti su http://www.securityfocus.com e http://www.cert.org.
Un'altra possibilità, da esplorare con attenzione, potrebbe essere quella di disabilitare completamente lo stack.

Prevenzione

Antisniffing
Uno sniffer è un programma che funziona in stretto collegamento con l'interfaccia di rete per ascoltare tutto il traffico che attraversa la scheda, piuttosto che intercettare solamente quello diretto ad essa.

La soluzione consiste nell'utilizzo di SWITCH al posto di HUB, lo switch riconosce il traffico che lo attraversa e lo indirizza solamente alla scheda di rete appropriata, perché riconosce l'indirizzo fisico di essa (MAC Adress), oltre ad aumentare notevolmente le prestazioni della rete garantisce la privacy dei dati e la sicurezza di tutto il sistema.

Un'altra soluzione è quella di cifrare tutto il traffico in transito sulla rete (IPSec).

Prevenzione

Attacchi DoS :
Come spiegato nel precedente articolo, tali attacchi sono tra i più pericolosi perché il problema principale consiste nella debolezza del protocollo TCP.

Un'esempio di attacco DoS potrebbe essere quello di spedire una serie di pacchetti ICMP all'indirizzo di broadcast della rete, facendo credere che la richiesta sia partita da un server aziendale interno usato come vittima (vedi attacco smurf).

Tale situazione è devastante perché satura rapidamente la rete, negando ogni tipo di servizio. A livello di router possiamo fare in modo di negare il traffico indirizzato al broadcast di rete.

A livello di sistema Linux possiamo agire sul kernel:

```
# echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

Prevenzione

Denial of Service (DoS): SYN Flood

Controllo tramite netstat delle connessioni in corso, un alto numero di SYN_RECV potrebbe rilevare la presenza di attacco SYN in corso.

Ridurre la durata del periodo di realizzazione della connessione.

Abilitazione dell'opzione SYN Cookie, tale opzione permette al kernel di intercettare e registrare tutti i possibili attacchi SYN, e nel frattempo di avviare un protocollo cifrato detto appunto SYN Cookie per dare la possibilità agli utenti autorizzati di continuare ad usufruire del servizio durante questo tipo di situazione.

```
# vi /etc/sysctl.conf
net.ipv4.tcp_syncookies = 1
```

Prevenzione

Firewall:

Esso in genere è composto da uno o più computer che si interpongono tra le reti private (come la lan locale) e quelle esterne (esempio Internet), il cui compito principale è quello di controllare i dati in transito tra le reti connesse ad esso.

In particolare il firewall viene utilizzato per stabilire quali servizi devono essere accessibili alla rete interna come la posta e il web, e quali possono essere resi disponibili alle reti esterne.

Ipfwadm (2.0) Ipchains (2.2), Iptables (2.4), Ipfilter (BSD)

Prevenzione

Firewall: tipologie di funzionamento

packet filtering
Tale tecnica controlla ogni singolo pacchetto che transita da una rete all'altra, tramite le informazioni contenute all'interno dell' header il pacchetto può essere accettato o rifiutato secondo le politiche espresse in precedenza.

application gateway
In tale situazione l'applicazione chiamata proxy si occupa di autorizzare e inoltrare i pacchetti in transito tramite l'impostazione di coppie account/password e di conseguenza applicare le regole impostate dal packet filtering.

packet inspection
Questo tipo di tecnica esegue ulteriori e approfonditi controlli sul pacchetto in transito, tecnica utilizzata nei sistemi IDS (Intrusion Detection System).

Prevenzione

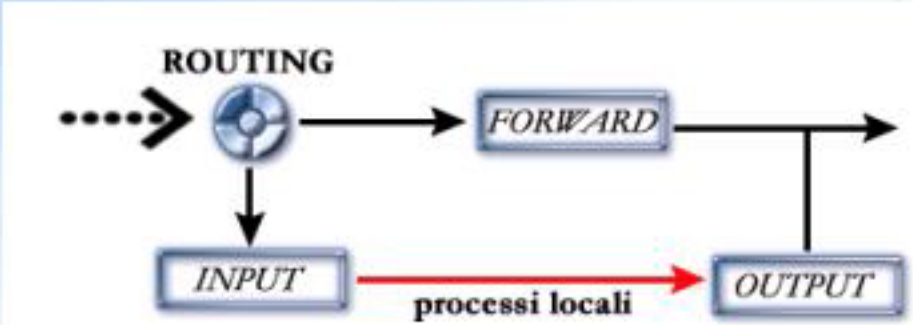
Firewall: sintassi di esempio

```
# iptables -A INPUT -s 192.168.200.0/24 -d 0/0 -i eth0 -j DROP

# iptables -A OUTPUT -d www.msn.it -p tcp -j DROP

# iptables -A INPUT -p icmp -s ! 192.168.0.0/16 -icmp-type 8 -d 192.168.0.0/16  -j DROP

# iptables -A INPUT -p tcp --dport telnet  --syn -j LOG --log-level info --log-prefix " Telnet"
```



PERCORSO PACCHETTI KERNEL 2.4

Prevenzione

Intrusion detection system (IDS)
Sistema intelligente e automatizzato attivo 24 ore su 24 in grado di rilevare e bloccare le intrusioni sui nostri sistemi.

IDS network based (NIDS)
Questa tipologia di IDS viene collocata all'interno della rete e si occupa di monitorare ogni singolo pacchetto tcp/udp entrante nella LAN/WAN aziendale.

IDS host based
Questi IDS sono normalmente installati su singoli host sono in grado di rilevare varie tipologie di anomalie (attività frenetica account, login outime .....)

IDS kernel based
Questo tipo di IDS fortifica il kernel e si occupa di monitorare eventuali cambiamenti dannosi che possono influenzare negativamente il sistema, affidandogli file potenzialmente dannosi.

Prevenzione

Efficacia degli IDS:
Ogni sistema IDS adotta una tecnica di Anomaly Detection che compie una analisti statistica che scova le anomalie rispetto ad un comportamento base, tale sistema ha il vantaggio di rilevare nuovi tipi di attacco ma possiede anche numerosi problemi tra cui la generazione di errori che possono suddividersi in tre tipologie fondamentali.

Falsi positivi: Il sistema genera un' allarme quando considera un'azione anomala come possibile intrusione quando essa non lo è.

Falsi negativi: Tale pericoloso errore viene a crearsi quando il sistema considera un'azione anomala come un'azione legittima da parte dell'utente.

Subversion Errors: Vengono a crearsi quando l'intrusore modifica il comportamento del IDS in modo da ottenere dei falsi positivi e agire in tal modo indisturbato.

Prevenzione:

Schema di un NIDS: