

Network Hardening

Università degli Studi di Pisa

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea in *Informatica Applicata*

Stage svolto presso *BK s.r.l*

Tutor Accademico

Prof. Fabrizio Baiardi

Candidato

Dario Maggiari

Tutor Aziendale

Fabrizio Sciarra

Polo Universitario G. Marconi – La Spezia

Introduzione (1)

Un ente *privato* o *pubblico* è e sarà sempre più dipendente:

- ✓ Dal suo sistema informativo.
- ✓ Dal sistema informativo dei partners.
- ✓ Dai sistemi informatici che li interconnettono.

Il “dato” e la “disponibilità dei servizi” sono i beni principali:

- ✓ I dati possono essere:
 - *Personali “sensibili”* (convinzioni religiose, opinioni politiche, etc...)
 - *Informatici* (progetti software, informazioni di vario genere, etc...)
- ✓ I tempi di risposta alle richieste degli utenti devono essere brevi.

Introduzione (2)

La *Sicurezza Informatica* è caratterizzata da:

- ✓ **Segretezza/Confidenzialità:** le informazioni possono essere lette solo da chi ne ha diritto.
- ✓ **Integrità:** le informazioni possono essere modificate solo da chi ne ha diritto.
- ✓ **Disponibilità:** una risorsa deve essere disponibile quando richiesta.
- ✓ **Non Ripudio:** un utente che provoca un danno NON deve essere nella condizione di poter negare le sue colpe.

Il processo di Hardening del Network (1)

Si applica una metodologia per delineare un piano di “*messa in sicurezza del network*” opportunamente efficace ed adeguato alla realtà aziendale considerata.

Si distinguono 3 step principali:

1. *Security Assessment* – Valutazione della Sicurezza.
2. *Security Implementation* – Implementazione delle Contromisure.
3. *Security Management* – Gestione della Sicurezza.

Il processo di Hardening del Network (2)

Security Assessment – Valutazione della Sicurezza – comprende:

- ✓ Identificazione degli Asset.
- ✓ Identificazione delle Vulnerabilità.
- ✓ Identificazione delle Minacce.
- ✓ Identificazione degli Attacchi.
- ✓ Gestione del Rischio:
 - *Analisi del rischio:*
 - Analisi delle vulnerabilità, attacchi, minacce ed impatti.
 - *Controllo del rischio:*
 - Identificazione delle contromisure.
 - Identificazione del rischio residuo accettabile.

Il processo di Hardening del Network (3)

Security Implementation – Implementazione delle Contromisure – comprende:

- ✓ Identificazione ed implementazione dell'architettura di rete adeguata.
- ✓ Implementazione degli strumenti idonei per le policy di sicurezza da applicare.
 - Implementazione degli strumenti per l'Auditing/Presidio.
- ✓ Implementazione degli strumenti adeguati all'esecuzione dei servizi.

Il processo di Hardening del Network (4)

Security Management – Gestione della Sicurezza – comprende:

- ✓ Controlli periodici ed interventi adattivi/perfettivi finalizzati alla verifica e mantenimento nel tempo delle misure di sicurezza applicate.
 - Gestione/Controllo degli strumenti impiegati.
 - Test e valutazione dello stato di sicurezza della rete.

Identificazione degli Asset

Un Asset (letteralmente “*risorsa*”) è un bene aziendale, materiale o immateriale, che deve essere adeguatamente protetto da minacce che possono comprometterlo.

Gli asset considerati sono:

- ✓ Server DNS, MAIL e WEB.
- ✓ Informazioni contenute in un DB.

Questi asset comprendono un insieme di risorse da proteggere:

- ✓ Capacità operativa.
- ✓ Immagine aziendale.
- ✓ Dati e informazioni.

Identificazione delle Vulnerabilità (1)

Una vulnerabilità è un *errore* che genera ripercussioni sulla sicurezza.

Esistono diversi tipi di vulnerabilità:

- ✓ **Vulnerabilità dei componenti informatici:**
 - Vulnerabilità di Sistemi/Applicazioni.
 - Vulnerabilità dei Protocolli.
- ✓ **Vulnerabilità strutturali:**
 - Vulnerabilità legate alle architetture di rete.
- ✓ **Vulnerabilità organizzativo/procedurali:**
 - Vulnerabilità procedurale.
 - Vulnerabilità organizzativa.

Identificazione delle Vulnerabilità (2) – Vulnerabilità dei componenti informatici

Vulnerabilità di Sistemi/Applicazioni:

- ✓ *Vulnerabilità del Software:*
 - *Overflow:* buffer overflow, stack overflow e heap overflow.
 - *Format String:* vulnerabilità delle *format function* (fprintf, printf, sprintf, etc...)
- ✓ *Errori di configurazione:* configurazioni poco robuste e/o inadeguate, ad esempio utenze non protette.

Vulnerabilità dei Protocolli:

- ✓ *Debolezze di progettazione:* permettono attacchi di tipo Spoofing, Hijacking e Sniffing.
- ✓ *Errori implementativi dello stack di rete:* permettono attacchi di tipo DoS/DDoS.

Identificazione delle Vulnerabilità (3) – Vulnerabilità dei componenti informatici

4 stati di una vulnerabilità:

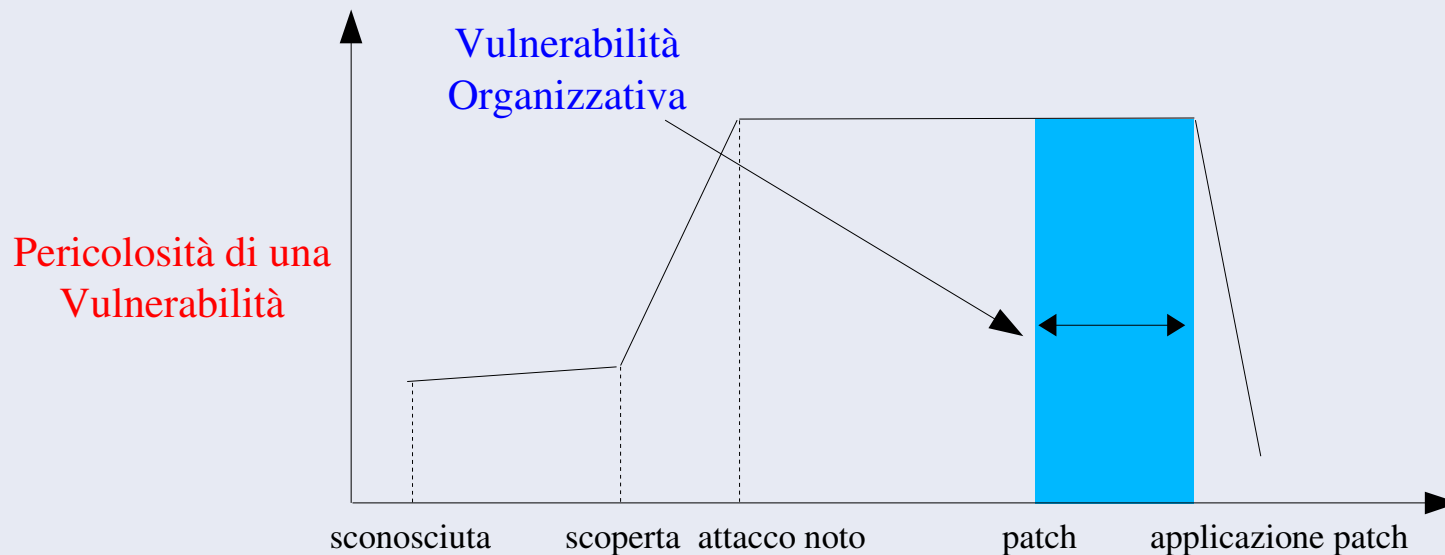
1. Si conosce l'esistenza di una vulnerabilità.
2. Si conosce l'esistenza di una vulnerabilità e di un attacco che la sfrutta.
3. Si conosce l'esistenza di una vulnerabilità e di una patch che la elimina.
4. Si conosce l'esistenza di una vulnerabilità, di un attacco che la sfrutta e di una patch che la elimina.

I sistemi sono attaccati anche quando lo stato della vulnerabilità è il quarto.

In questo caso si ha una *Vulnerabilità Organizzativa*.

Identificazione delle Vulnerabilità (4) – Vulnerabilità organizzativo/procedurali

Vulnerabilità Organizzativa: debolezza dovuta a ritardi nell'esecuzione di interventi aziendali, ad esempio l'applicazione tempestiva di una patch.



Vulnerabilità Procedurale: debolezza logica nell'eseguire determinate operazioni all'interno dell'azienda come, ad esempio, installazione di software o patch di dubbia provenienza ed esecuzione errata della manutenzione.

Identificazione delle Minacce

Una minaccia è un'azione potenziale, *accidentale o deliberata*, che può portare alla violazione di uno o più obiettivi di sicurezza causando un danno.

Le minacce si classificano in base a:

- ✓ **Origine:** ambientale/naturale, umana.
- ✓ **Intenzione:** minacce di tipo deliberato o accidentale.
- ✓ **Risorse compromesse:** hardware, informazioni, dati, capacità operativa, etc...

Si possono combinare le 3 categorie per ottenere una valutazione più efficace.

Nello specifico consideriamo *minacce di tipo deliberato* quali intrusioni all'interno del Network.

Identificazione degli Attacchi (1)

Gli attaccanti possono compromettere:

- ✓ Dati e informazioni.
- ✓ Continuità del servizio.

Un attacco è costituito da diverse fasi:

1. **Mascheramento:** l'attaccante nasconde la propria reale ubicazione.
2. **Raccolta di informazioni:** si identificano i servizi e gli OS utilizzati per individuare vulnerabilità (*port scanning*).
3. **Attacco:** si esegue un programma che sfrutti una vulnerabilità (*exploit*) o, se non è disponibile, si adottano strategie alternative di difficoltà crescente.
4. **Pulizia e controllo del sistema:** si cancellano le tracce dell'intrusione e si installano strumenti per il controllo remoto (*rootkit*).

Identificazione degli Attacchi (2)

Attacchi automatizzabili:

- ✓ Si utilizzano *exploit*, cioè programmi che permettono di eseguire codice arbitrario sfruttando una vulnerabilità del software.
- ✓ Worm come Slammer e CodeRed eseguono attacchi completamente automatizzati.
- ✓ Gli attacchi sono semplificati e aumenta il numero di potenziali attaccanti.
- ✓ La pericolosità di una Vulnerabilità dipende soprattutto da questi attacchi.

Attacchi NON automatizzabili:

- ✓ NON esiste un exploit da utilizzare.
- ✓ Gli attacchi sono sensibilmente meno pericolosi poichè le strategie da applicare richiedono risorse e competenze specifiche.

Identificazione degli Attacchi (3)

Alcuni attacchi:

- ✓ **Redirezione dell'esecuzione:** *exploit* che sfruttano Buffer/Stack/Heap Overflow per eseguire codice arbitrario.
- ✓ **Sniffing:** accesso illecito in lettura ad informazioni trasmesse/ricevute (si utilizzano tecniche di *Spoofing e Hjiacking*).
- ✓ **Insertion Attack:** alterazione di richieste/messaggi su una connessione stabilita da terzi (si utilizzano tecniche di *Spoofing e Hjiacking*).
- ✓ **Smurf/Flood:** DoS/DDoS (i.e. saturazione delle risorse).
- ✓ **Password Cracking:**
 - *Attacchi basati sul dizionario:* si prova un insieme di password “comuni”.
 - *Attacchi di tipo brute force:* si provano sistematicamente tutte le possibili password.
- ✓ **ARP e DNS Cache Poisoning:** “avvelenamento” delle cache tables.

Identificazione delle Contromisure

Per ogni vulnerabilità esiste almeno una contromisura che può essere di tipo:

- ✓ **Fisico:** accessi blindati, canalizzazioni dei cavi di rete, etc...
- ✓ **Organizzativo/Procedurale:** gestione delle password, sistemi di backup, etc...
- ✓ **Tecnico informatico:**
 - Contromisure per garantire il controllo e l'analisi del traffico di rete.
 - Contromisure per garantire identificazione e autenticazione.
 - Contromisure per garantire il controllo degli accessi.
 - Contromisure per garantire l'affidabilità e continuità del servizio.
 - Contromisure per garantire l'audit (registrazione degli eventi).
 - Contromisure per garantire l'accountability (assegnare responsabilità).
 - Contromisure per garantire lo scambio dati sicuro.

Architettura di rete e Controllo e analisi del traffico - *Attività svolta*

Architettura di rete a più livelli di controllo e analisi del traffico.

Firewall Hardware multipli permettono di:

- ✓ Definire modalità specifiche di accesso ai servizi forniti.
- ✓ Realizzare un sistema di alerting distribuito.
- ✓ Separare e controllare le relazioni trust fra le macchine.
- ✓ Realizzare un sistema di analisi del traffico ridondante.
- ✓ Modulare il traffico di rete.

Livelli multipli di **DMZ** permettono di:

- ✓ Definire diversi livelli di criticità per dati ed informazioni.
- ✓ Configurare i servizi adottando soluzioni “alternative” (i.e. split e reverse proxy).

Controllo degli accessi - Attività svolta

Un sistema per il controllo degli accessi coinvolge una tripla

<agenti, risorse, permessi_agenti_su_risorse>

Il controllo degli accessi è implementato a 3 livelli differenti:

1. Livello di rete:

- Politiche di accesso in base al MAC address.

2. Livello di Host:

- Sistemi RBAC (*Grsecurity*) per regolamentare l'accesso alle risorse.
- Chroot Jail per limitare la visibilità del filesystem.

3. Livello Applicazione/Servizi:

- Patch a livello del Kernel Linux (*PAX/Grsecurity*) per regolamentare l'accesso in memoria dei processi: NOEXEC e ASLR (*Address Space Layout Randomization*).

Auditing/Presidio (1) - Attività svolta

Gli IDS sono stati affiancati ai firewall per ottenere proprietà di “difesa e allarme”.

Gli IDS agiscono a differenti livelli:

- ✓ **NIDS** (*Network Intrusion Detection System*): livello di rete.
- ✓ **Shim-IDS**: analizzano il traffico di rete a livello di un singolo host.
- ✓ **HIDS** (*Host IDS – Filesystem Checker*): verificano l'integrità del filesystem.

Gli HIDS sono stati utilizzati in prevalenza per identificare i rootkit “non-LKM” e per l'analisi post-intrusione, mentre gli Shim-IDS per rilevare i tentativi di testare le vulnerabilità della rete.

Auditing/Presidio (2) - Attività svolta

Logging ridondante:

- ✓ Le informazioni sul traffico di rete sono registrate su più firewall hardware.
- ✓ Sui firewall hardware non sono eseguiti servizi. La compromissione delle macchine in DMZ non comporta un'interruzione dell'audit.
- ✓ Sono implementati controlli a livello dei log (*data audit*) per “catturare” la registrazione di eventi anomali come il kill inaspettato dei processi o tentativi di login falliti.

Possibili sviluppi e studi futuri

- ✓ Sistemi di *Log Correlation* per migliorare l'efficienza degli IDS e di eventuali sistemi di IPS.
- ✓ Ulteriori approfondimenti sui sistemi di controllo per gli accessi nei sistemi Linux (MAC, RBAC).

FINE

Network Hardening

FINE

Grazie per l'attenzione!