

# Security Scan e Penetration Testing

esperienze di una realtà specializzata



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

## Il Net Probing INFOSEC

Relatore: Stefano Venturoli

# Sicurezza informatica

**Confidenzialità:** le informazioni **non** devono essere **accessibili** a coloro che **non** sono **autorizzati**.

**Integrità:** le informazioni **non** devono essere **modificabili** in maniera inaspettata (leggere anche: non autorizzata).

**Disponibilità:** le informazioni **non** devono venir **cancellate** o diventare inaccessibili (leggere anche: protette da eventuali incidenti).

**La sicurezza informatica è la tutela del sistema informativo aziendale dalla violazione da parte di persone non autorizzate.**

# Quali sono i rischi reali?

- frodi a danno dell'azienda o dei suoi clienti

per esempio tramite informazioni acquisite (password per e-banking, numeri di conto, numeri di carte di credito, etc.) o azione diretta (manipolazione transazioni, ordini, fatture, bilanci, etc.).

# Quali sono i rischi reali?

- frodi a danno dell'azienda o dei suoi clienti
- furto di informazioni sensibili

potrebbero venire rubati (e diffusi) o distrutti dati sensibili o vitali quali bilanci, fatture, database di clienti e fornitori, progetti, documenti interni, corrispondenza, etc. .

# Quali sono i rischi reali?

- frodi a danno dell'azienda o dei suoi clienti
- furto di informazioni sensibili
- **impossibilità di fornire servizi/beni ad utenti legittimi**

per esempio a causa di un Denial of Service (DoS), oppure per il fermo necessario a ripristinare i servizi dopo un'intrusione.

# Quali sono i rischi reali?

- frodi a danno dell'azienda o dei suoi clienti
- furto di informazioni sensibili
- impossibilità di fornire servizi/beni ad utenti legittimi
- perdita d'immagine

i vostri clienti (o futuri clienti) potrebbero trovare i vostri servizi poco affidabili o poco sicuri; immaginate solamente quale potrebbe essere la fiducia della clientela verso un sito di e-business in cui gli hacker abbiano scorrazzato liberamente

# Quali sono le corrette modalità di approccio al problema?

- Esistono soluzioni hardware e software ma, per la natura intrinseca di questi prodotti, non saranno **mai sufficienti** al problema.
- Non esiste e non esisterà **mai** una **soluzione definitiva**.
- La sicurezza di un sistema viene valutata dalla resistenza del suo **anello più debole**.
- Per ottenere un sistema che riesca a garantire al meglio gli obiettivi di sicurezza richiesti, bisogna valutare nelle varie componenti i **rischi** che si vengono a generare, tenendo conto dei livelli di protezione che vengono garantiti.

# Perché le soluzioni adottate potrebbero non essere sufficienti?

- i **software** (in particolar modo quelli di sicurezza) **invecchiano** rapidamente
- la **complessità** dei **sistemi** rende difficile implementare correttamente le soluzioni pianificate
- vengono continuamente scoperte **nuove metodologie** di **attacco informatico**
- **manca** nelle aziende e nella società una **cultura** della sicurezza informatica
- un **minimo errore** di sviluppo, impostazione o configurazione può rendere un sistema **vulnerabile ad attacchi**
- un **minimo errore** di sviluppo, impostazione o configurazione può rendere **inefficaci** i sistemi di sicurezza

# Perché serve un Net Probing?

## La verifica dello stato di fatto della rete...

- i miei sistemi sono al sicuro da **attacchi** ed **utilizzi illeciti**?
- la confidenzialità, l'integrità e la disponibilità dei miei dati sono adeguatamente garantite contro i **pericoli**?
- conosco il mio livello di esposizione ai **rischi**?
- la mia immagine è **tutelata**?
- i sistemi di sicurezza sono **posizionati** e **configurati** nella maniera **corretta**?
- sono **idonei** al lavoro che devono svolgere?
- sono in grado di **intercettare** o segnalare tutti gli **attacchi** più recenti?
- il mio staff verifica gli **allarmi segnalati**?

# Perché serve un Net Probing?

i responsabili del settore informatico mi hanno garantito che i nostri sistemi sono sicuri.. perché una verifica?

- le reti si **stratificano** nel tempo
- vengono adottate **soluzioni temporanee** che poi rimangono in produzione
- i responsabili ed i tecnici dei sistemi **cambiano**, spesso **senza** effettuare un adeguato **passaggio di consegne**
- lo staff non ha il **tempo** o le **competenze** necessarie per **aggiornare** o **mantenere** adeguatamente i sistemi
- la complessità dei **sistemi di sicurezza** rende **difficile** una **configurazione** efficace a personale non specializzato

# Perché serve un Net Probing?

## perché in outsourcing?

- per avere una **verifica indipendente**, effettuata da personale non coinvolto nella progettazione e nella manutenzione
- per avere una **valutazione** dello stato di fatto eseguita da **personale altamente specializzato** in problematiche di ICT Security
- per **evidenziare il livello di rischio** di dati e sistemi
- perché permette a tutti i soggetti di **accertare e documentare** la corrispondenza tra lo stato di fatto e lo stato dell'arte richiesto dalla **Legge** (L.675/96 e attuazioni)
- perché permette di assumere le proprie **responsabilità** in modo chiaro, senza essere soggetti a rischi di cui non si è a conoscenza ed individuare le aree scoperte

# Limiti dei tool automatizzati

Esistono una serie di prodotti che permettono di effettuare uno test di sicurezza in maniera automatica..

- nonostante l'interfaccia click & point, **configurare** questi prodotti per effettuare un test **efficace** è **difficile**
- le impostazioni di default spesso **non** sono **ottimali**
- **interpretare correttamente** i risultati richiede **esperienza** e colpo d'occhio
- l'elenco delle **vulnerabilità** ricercate è **limitato a quelle note**
  - non tutte le vulnerabilità sono inserite dai produttori
  - continui aggiornamenti
  - falsi positivi
  - falsi negativi
- non sono in grado di valutare la **gravità dell'esposizione** in base ai dati raccolti

# Limiti dei tool automatizzati

...in particolar modo sono assolutamente carenti

- per verificare **configurazioni particolari**
- per verificare **applicazioni** sviluppate o personalizzate **in-house** o **su richiesta**
- per verificare **applicazioni non largamente diffuse**
- per cercare **vulnerabilità** nella **progettazione** o nelle logiche di **sviluppo** e **configurazione**
- per cercare **vulnerabilità particolari**
  - tecniche di attacco avanzate: spoofing, pacchetti frammentati, protocolli di routing, ...
  - username e password guessing avanzati
  - analisi delle applicazioni web: validazione input e dati passati dall'utente, cookie, url, metodi, campi, query injection, ...
  - social engineering
  - ...

# II Net Probing Infosec

## simulazione di attacco condotta da professionisti

- **team** di "Ethical Hackers" altamente **specializzato**
- **personalizzato** in base alle esigenze del Cliente e alle strutture da testare
- grande **competenza** maturata in anni di **analisi** e **ricerca**
  - su protocolli, sistemi, applicazioni, strutture di rete, ...
  - sulle metodologie di comportamento e attacco hacker
  - sulle tecniche di attacco utilizzate nelle intrusioni reali
- procedure sviluppate e testate nei nostri laboratori seguendo tutte le più **avanzate metodologie** e gli **standard** più **evoluti**
- **continuamente aggiornate** secondo le ultime ricerche di ICT Security ed i trend
  - analizzando tutti i canali informativi ufficiali, ufficiosi o "underground"
  - **ricercando, verificando e approfondendo nei nostri laboratori**

# II Net Probing Infosec

## i punti di forza

- analisi delle **vulnerabilità** generali della **struttura**
- focus particolare sulle **vulnerabilità** di **progetto**
- focus particolare sull'esposizione di **dati sensibili**
- focus particolare sulle applicazioni sviluppate dal cliente
- grande **percentuale di successo**
- **minimo impatto** sui sistemi
- **modulare**
  - da punti di accesso diversi
  - Penetration Test
  - Auditing delle applicazioni
- **report dettagliato**
- eventuale **analisi legale** del livello di esposizione
- riferimenti per la **risoluzione dei problemi**
- possibilità di affidare a Infosec la ripianificazione della struttura e/o le correzioni da apportare

# II Net Probing Infosec

## obiettivi

- ottenere una **mappa completa**
  - reti
  - applicazioni
  - utenti
  - autenticazioni
  - sistemi di sicurezza
  - software
  - servizi attivi
  - servizi raggiungibili pubblicamente
  - dati, archivi, database, ...
  - dati sensibili
  - ...
- ottenere **accesso ai sistemi**
- ottenere **accesso privilegiato** ai sistemi
- verificare il **livello di esposizione** dei sistemi compromessi
  - dati
  - utenti
  - analisi del traffico
  - livello di rischio derivante dall'intrusione
  - possibilità di accedere ad altri sistemi dalla posizione acquisita
  - ...

# Auditing delle applicazioni

## a cosa serve

- **verifica approfondita delle applicazioni**
- **particolarmente utile** per verificare la sicurezza di applicazioni (web e non)
  - portali
  - e-commerce
  - intranet
  - remote banking
  - applicazioni sviluppate in-house o proprietarie
  - ...

## opzioni e moduli

- verifica del sistema ospite (Net Probing, privilege escalation locale)
- analisi da remoto ("black box")
- analisi del progetto
- analisi dei sorgenti
- analisi del traffico
- analisi di file e applicativi
- auditing dei database
- analisi dei binari e reverse engineering

# Auditing delle applicazioni

## per verificare se sia possibile

- compromettere la sicurezza del sistema ospite tramite l'applicazione
- accedere senza i privilegi necessari
- accedere, inserire o modificare dati, file o archivi senza i corretti privilegi
- aumentare illegalmente le capacità di accesso e modifica rispetto ai privilegi concessi
- utilizzare i privilegi di altri utenti
- bypassare la validazione dell'input fornito dall'utente
- estrarre dati sensibili da cookie, url, campi nascosti, file, binari, etc.
- accedere al sistema di management o configurazione
- accedere ad archivi, campi, sezioni dell'applicazione, etc. normalmente non visualizzabili oppure nascosti
- inserire malicious code per attaccare altri utenti e amministratori

# Is Your Business Internet eXposed?



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

## Possiamo aiutarvi!