

# Ethical Hacking

Prefazione

# Ethical Hacking

## Perché la Cyber Security è importante

- La **digitalizzazione** coinvolge sempre più aziende
- Lo **spionaggio industriale** è più diffuso
- Il **contrasto al terrorismo online**
- Le **infrastrutture pubbliche** sono i nuovi bersagli
- **Identità Digitale**

# Ethical Hacking

## Digitalizzazione dei processi

- Viene rivisto il modo di lavorare: c'è il passaggio dall'analogico al digitale
- Vengono digitalizzati i processi aziendali di qualsiasi natura (ad es. l'assunzione del personale, la gestione degli impianti produttivi)
- I documenti cartacei vengono digitalizzati
- Il processo di digitalizzazione punta alla semplificazione e snellimento delle procedure

# Ethical Hacking

## Spionaggio industriale - Fattori

- **Geopolitica:** spionaggio cibernetico per influenzare flussi e stabilità geopolitiche
- **Governi:** spionaggio cibernetico per monitorare, controllare, deviare un governo
- **Ricerca e sviluppo:** spionaggio industriale per progredire nella ricerca, acquisendo nuove tecnologie, informazioni e processi
- **Nuove tecnologie:** spionaggio industriale per rubare nuove tecnologie ad aziende e governi

# Ethical Hacking

## Spionaggio industriale - OT Security

**Operational Technology (OT)** è l'uso di hardware e software per monitorare e controllare processi fisici, dispositivi e infrastrutture. I sistemi OT sono presenti in un'ampia gamma di settori e svolgono una serie di compiti che vanno dal monitoraggio di infrastrutture critiche al controllo dei robot in un reparto di produzione.

**SCADA** è uno dei sistemi utilizzati nei processi industriali (ICS)

# Ethical Hacking

## Contrasto al terrorismo - Comunicazioni online

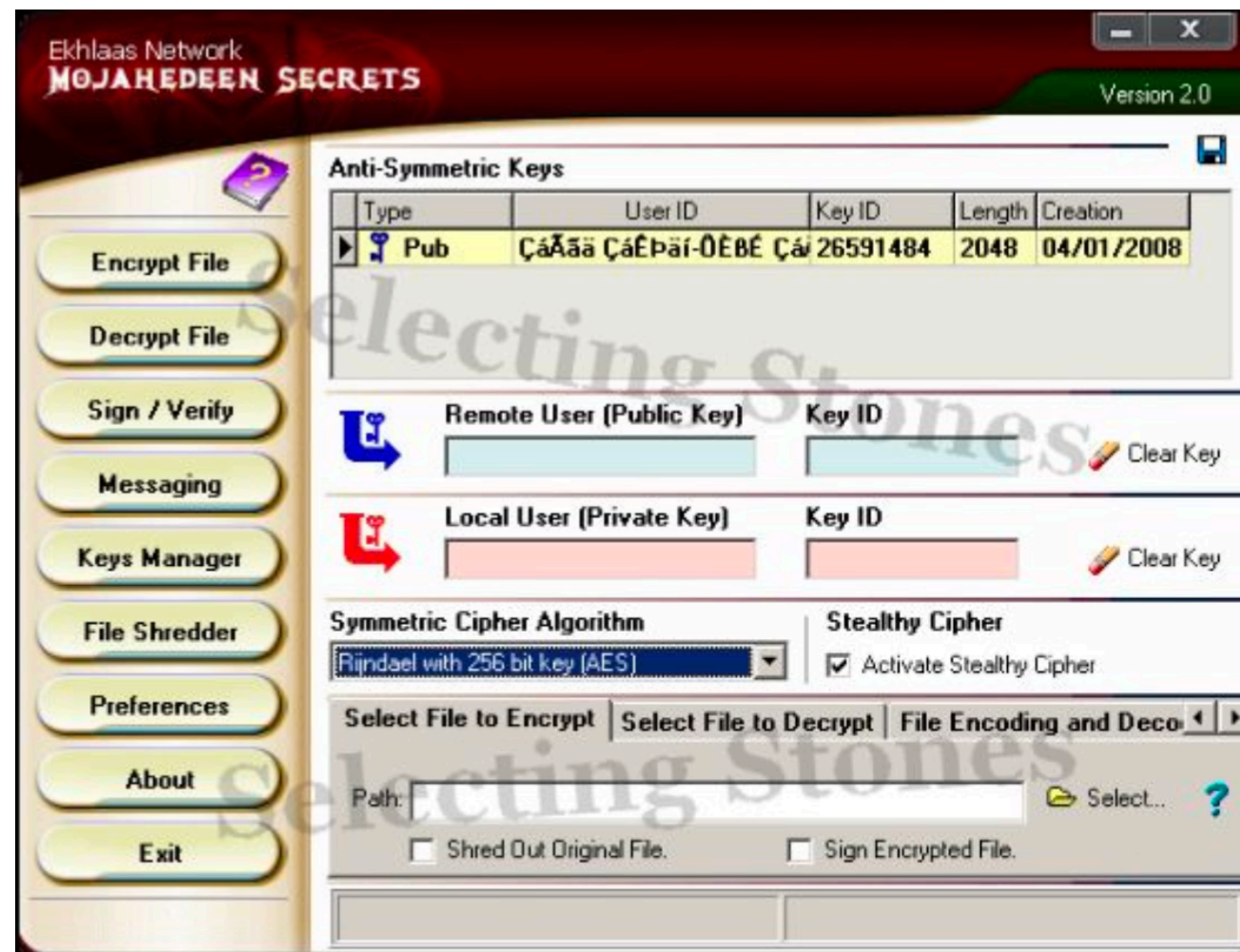
Le organizzazioni terroristiche hanno spostato le fasi di reclutamento e comunicazione online, utilizzando le più disparate tecnologie per perseguire i propri scopi.

- Twitter
- Chat di videogame
- PlayStation Network
- Forum
- Deep Web

# Ethical Hacking

## Contrasto al terrorismo - Comunicazioni cifrate

Utilizzano software appositamente costruiti per comunicare in modo sicuro online. Vengono utilizzati sia algoritmi di cifratura simmetrica sia algoritmi di cifratura asimmetrica.



# Ethical Hacking

## Contrasto al terrorismo - SOCMINT

La **SOCMINT** (Social Media Intelligence) viene usata per spiare le realtà terroristiche, monitorando gli account di soggetti appartenenti a tali gruppi.

Uno dei punti deboli della SOCMINT è la verifica delle informazioni, infatti risulta difficile distinguere i reali segnali di una probabile azione terroristica, dal “rumore” causato da un fanatismo di imitazione che non sfocia in un’azione, per 3 motivi: **falsi positivi**, **falsi negativi** e **disinformazione**.



# Ethical Hacking

## Infrastrutture pubbliche

Le infrastrutture pubbliche offrono un servizio essenziale per i cittadini, esse devono garantire sempre la disponibilità dei propri sistemi. Essendo servizi forniti da un'entità governativa dovrebbero essere sempre garantiti. Contengono inoltre una notevole quantità di dati personali, pertanto necessitano di maggior protezione.

**Sistemi in HA** (High Availability): Sistemi preposti a svolgere lo stesso compito, esposti da un Load Balancer (LB) che ne gestisce il carico.

# Ethical Hacking

## Identità Digitale - Cos'è e dov'è

- L'identità digitale è l'insieme delle informazioni, in un'accezione più ampia è l'insieme delle informazioni presenti online e relative ad un soggetto
- Possiamo tradurre questo concetto come l'insieme di account, email e altre informazioni che fanno riferimento ad una persona
- L'identità digitale è online, però ne fanno parte anche i nostri dispositivi
- Quando viene compromesso un dispositivo, viene compromessa la nostra vita digitale

# Ethical Hacking

## Identità Digitale - Minacce

**Furto d'identità**, succede spesso se si condividono documenti o altri dati personali.

**Ripercussioni sulla vita reale**: diffamazione della persona, cyberbullismo, fake news.

**Problemi di carattere pratico** nel caso di furto di credenziali (ad es. non riuscire ad accedere in banca).

**Comunicazioni** che sembrano essere originate da noi.

# Ethical Hacking

## Identità Digitale - Gestione degli accessi (IAM) 1/4

La questione della gestione delle identità è forse il ramo più “antico” della Sicurezza Informatica.

I primi sistemi per gestire tale problematica risalgono agli anni '80.

Una basilare, ma efficace gestione la troviamo già integrata nel sistema operativo con la funzionalità multi-user.

# Ethical Hacking

## Identità Digitale - Gestione degli accessi (IAM) 2/4

- Esistono svariati software che permettono una gestione capillare degli accessi e delle identità
- Con un solo sistema è possibile abilitare/disabilitare le utenze (anche in maniera automatica) dei dipendenti che entrano nella nostra azienda, cambiano reparto o vanno a lavorare altrove
- Questi sistemi centralizzati spesso sono integrati anche con i business workflow e le policy aziendali

# Ethical Hacking

## Identità Digitale - Gestione degli accessi (IAM) 3/4

L'**Identity Management** è uno degli asset più critici.

È l'insieme dei **processi aziendali** che unitamente ad un'appropriata infrastruttura di supporto permettono la creazione, il mantenimento e l'uso delle identità digitali in un contesto legale, sia esso amministrativo, commerciale, pubblico o privato.

Definisce e gestisce i ruoli e i privilegi di accesso dei singoli utenti della rete in base alle esigenze di business.

# Ethical Hacking

## Identità Digitale - Gestione degli accessi (IAM) 4/4

**Least privilege:** L'utente deve avere solo le autorizzazioni necessarie a svolgere il proprio compito. Ad esempio, un utente che si occupa del budget aziendale non deve avere accesso anche ai server, ma solo accesso alle applicazioni finanziarie necessarie a svolgere la propria mansione.

**Separation of duties:** È il concetto della separazione dei compiti, per evitare frodi e sabotaggi. Un compito per essere portato a termine necessita di più persone e più passaggi. Un esempio è l'accesso ai codici nucleari che necessita di due chiavi fisiche, le cui serrature sono poste a distanza sufficiente perché non sia possibile eseguire l'operazione da soli.

# Ethical Hacking

## Identità Digitale - Modello RBAC

- Con l'aumentare del numero degli utenti, il processo di assegnazione di autorizzazioni individuali diventa sempre più laborioso e soggetto ad errori.
- Un'alternativa flessibile e al tempo stesso efficiente è il controllo degli accessi basato sui ruoli: il **Role Based Access Control**.
- Le autorizzazioni e i permessi sono assegnati al ruolo e non al singolo utente, quindi ad esempio, non sarà solo l'amministratore di sistema X ad avere le autorizzazioni per accedere alle macchine ma tutti quelli che hanno il ruolo di amministratori di sistema



# Terminologia

# Terminologia

- **HACK VALUE** - Nozione che indica quanto ne vale la pena ad acquisire il target
- **VULNERABILITY** - Esistenza di una falla, errore di implementazione o di design che può essere sfruttato da un evento inaspettato per compromettere la sicurezza di un sistema
- **EXPLOIT** - Una breccia nella sicurezza di un sistema IT tramite una vulnerabilità
- **PAYLOAD** - Il payload è la parte di un codice exploit che esegue attività malevole come creare una backdoor o cifrare i file

# Terminologia

- **ZERO-DAY (0day)** - Vulnerabilità non ancora patchata dal vendor. Un attacco 0day sfrutta questo tipo di vulnerabilità prima del rilascio della relativa patch. Fino a quel momento i sistemi non possono essere difesi se non con IA o virtual patching.
- **DAISY CHAINING** - Consiste nell'accedere ad una rete e/o computer e utilizzarli per accedere ad ulteriori reti e/o computer che contengono le informazioni desiderate
- **DOXING** - Pubblicazione di informazioni personali di un soggetto, raccolte da fonti aperte (es. Social Media, OSINT)
- **BOT** - Un bot è un software che può essere controllato da remoto per eseguire o automatizzare determinati task

# Terminologia

## Motivi, scopi e obiettivi degli attacchi

Il **motivo** nasce quando il sistema target memorizza o elabora qualche informazione preziosa e questo porta alla **minaccia** di un attacco al sistema.

Gli attaccanti utilizzano vari strumenti e tecniche di attacco per sfruttare le vulnerabilità di un sistema e raggiungere il proprio **scopo**.

Gli **obiettivi** possono essere: furto di credenziali, furto d'identità, danno d'immagine, manipolazione dei dati, riscatto, ecc.

# Terminologia

## Tipologie di attacchi ai sistemi

Livello	
Sistema Operativo	L'attaccante cerca vulnerabilità nel S.O. o nella configurazione e cerca di sfruttarla per accedere al sistema. Vulnerabilità a livello del S.O.: buffer overflow, bug, patch non installate
Livello Applicativo	L'attaccante sfrutta vulnerabilità nelle applicazioni che vengono eseguite nei sistemi delle organizzazioni per accedere ai sistemi e rubare i dati o manipolarli. Attacchi: buffer overflow, XSS, SQL Injection, man-in-the-middle, session hijacking, DoS
Misconfiguration	Le vulnerabilità dovute a misconfiguration colpiscono principalmente web server, database, reti o possono essere dovute all'utilizzo di framework
Shrink-Wrap Code	L'attaccante sfrutta le configurazioni e le impostazioni di default dei sistemi (o del codice) presenti nell'infrastruttura

# Panoramica sull'Hacking

# Panoramica sull'Hacking

## Chi è un hacker

- Individuo con ottime conoscenze informatiche
- Per alcune persone può essere solo un hobby o un passatempo
- Le intenzioni possono essere sia benevole che malevole: a puro scopo informativo, didattico e per curiosità, oppure per recare danno e trarne vantaggio, facendo qualcosa di illegale

# Panoramica sull'Hacking

## Fasi dell'hacking 1/5

1. **Reconnaissance:** È la prima fase di un attacco ed è puramente informativa. Esiste in modalità passiva e attiva. La **passive recon** non ha interazione con il target, tutte le informazioni ottenute provengono da fonti aperte o da sistemi terzi (ad es. siti web specifici, motori di ricerca). L'**active recon** invece ha un'interazione diretta con il target, andando ad interrogarlo direttamente e cercando di reperire quante più informazioni possibili.



# Panoramica sull'Hacking

## Fasi dell'hacking 2/5

2. **Scanning:** Viene effettuato lo scan della rete del target alla ricerca di informazioni, vulnerabilità, topologia di rete, numerosità dei server e architettura dei sistemi. Le attività di scanning sono separate dalla recon perché implicano un'interazione con il target e sono verticali sugli apparati IT. Gli strumenti utilizzati sono Port scanner, vulnerability scanner e network mapper.

# Panoramica sull'Hacking

## Fasi dell'hacking 3/5

3. **Gaining Access:** La fase di accesso è tra le più importanti, infatti se non abbiamo studiato il nostro target o commettiamo un errore, l'amministratore di sistema potrebbe accorgersene e correre ai ripari. In questa fase viene ottenuto l'accesso al Sistema Operativo o all'applicativo, vengono effettuati password cracking, attacchi DoS e session hijacking.

# Panoramica sull'Hacking

## Fasi dell'hacking 4/5

4. **Maintaining Access:** In questa fase si cerca di consolidare l'accesso guadagnato nella fase precedente. L'obiettivo di questo step è permetterci di poter rientrare nel sistema in un secondo momento (anche gli hacker dormono!). Il mantenimento dell'accesso viene garantito con backdoor, rootkit o trojan.

# Panoramica sull'Hacking

## Fasi dell'hacking 5/5

5. **Clearing Tracks:** Questa è la fase più importante in assoluto (se i nostri scopi sono illeciti), tuttavia quando un cliente ci commissiona un Penetration Test spesso viene saltata, a meno che sia esplicitamente richiesta per testare le capacità del proprio team interno di eseguire analisi forensi e testare i piani di incident recovery.

# Panoramica sull'Hacking

## Ethical Hacking

L'**Ethical Hacking** si basa su tecniche che simulano il comportamento di un attaccante per verificare la possibilità di sfruttare le vulnerabilità presenti.

Gli Ethical Hacker lavorano esclusivamente con il permesso del cliente (target).

Previene che gli hacker possano accedere ai nostri sistemi, ci rendi coscienti delle vulnerabilità presenti nella nostra rete e migliora la **security posture**.

# Controlli per l'Information Security

# Controlli per l'Information Security

## Segregazione delle reti

Il “**Network Security Zoning**” aiuta a monitorare e controllare il traffico in entrata e uscita. Inoltre aiuta le organizzazioni a gestire le proprie reti sicure selezionando il giusto livello di sicurezza in base alle differenti zone delle reti internet e intranet.

# Controlli per l'Information Security

## Policy di sicurezza

1. Identificare i rischi tramite un Risk Assessment
2. Imparare dagli altri e dalle linee guida
3. Includere il management nello sviluppo delle policy
4. Ammende/Multe chiare in caso di mancata conformità
5. Fornire la versione finale della policy a tutti
6. Assicurarsi che tutti abbiano compreso la policy
7. Sviluppare strumenti per rinforzare le policy
8. Formare i dipendenti
9. Rivedere e aggiornare regolarmente le policy



# Controlli per l'Information Security

## Rischio e Risk Management

Il livello di rischio si riferisce al livello di incertezza o aspettativa che un evento negativo possa causare danni al sistema.

Il **Risk Management** porta alla riduzione e al mantenimento del rischio ad un livello accettabile.

### **Fasi del Risk Management:**

Identificazione del rischio -> Risk Assessment ->

Trattamento del rischio -> Tracciamento del rischio ->

Revisione del rischio

# Controlli per l'Information Security

## Incident Management

L'Incident Management è un insieme di processi definiti, volti ad identificare, analizzare, priorizzare e risolvere tutti gli incidenti di sicurezza.

Le fasi si suddividono in:

- Vulnerability Handling
- Incident Handling: Triage, Incident Response, Reporting e Detection, Analisi
- Artifact Handling
- Announcements,
- Alerts

# Information Gathering

# Information Gathering

## Google Dork

Questa tecnica permette di fare ricerche avanzate con Google, utilizzando operatori per creare query più complesse in modo da ottenere informazioni nascoste, che possano aiutare l'attaccante a trovare vulnerabilità.

**CACHE:** Mostra le pagine salvate nella cache di Google

**LINK:** Elenca solo i risultati che hanno collegamenti con la pagina specificata

**LOCATION:** Trova informazioni per una location specifica

**FILETYPE:** Ricerca solo determinati tipi di file

# Information Gathering

## Domain Footprinting - WHOIS

Per ricercare i Top Level Domain e sottodomini di un'azienda si possono utilizzare servizi online come netcraft.com, mentre tool come sublist3r (script Python) servono ad enumerare i sottodomini che a loro volta possono dare informazioni sulla struttura interna dell'azienda.

Una query whois ci permette di scoprire informazioni sul dominio che stiamo analizzando.

# Information Gathering

## Sistemi Operativi, Web Server e Metadati

La determinazione di un **sistema operativo** è essenziale quando vogliamo lanciare un attacco.

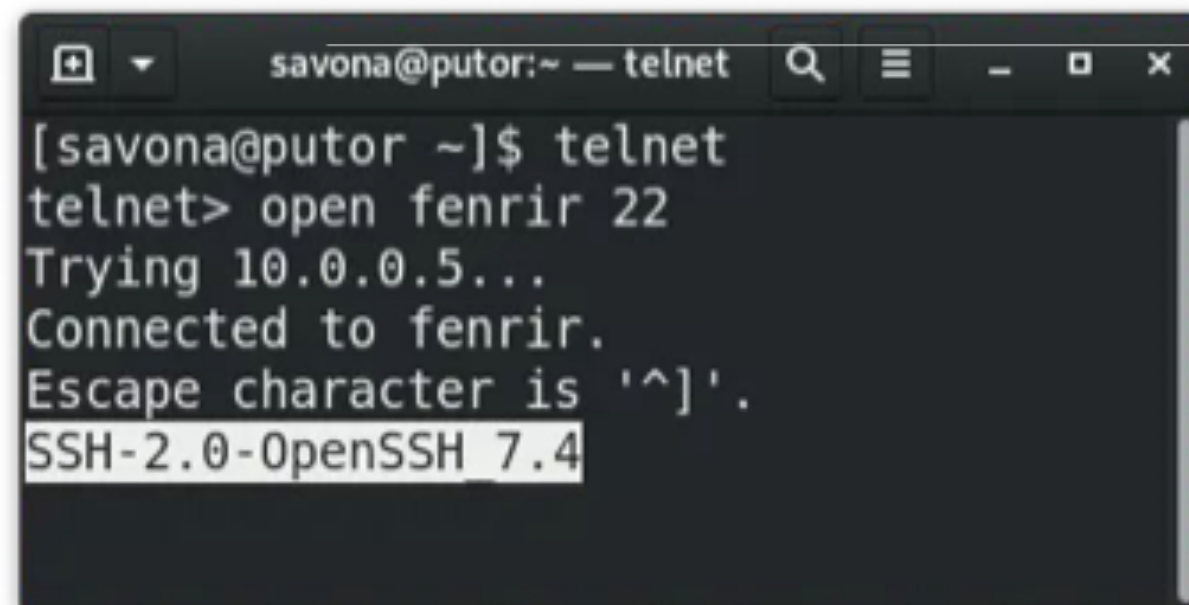
Il footprinting per **siti web** è inteso come il monitoraggio e l'analisi dei siti web del nostro target. Strumenti come BURPSUITE, ZAPROXY o altri tool servono a carpire gli leader, fondamentali per l'analisi del codice HTML e dei cookie.

L'estrazione dei **metadati** può essere utile per ricavare informazioni sui dipendenti così da eseguire ulteriori attacchi (phishing, social engineering).

# Information Gathering

## Banner Grabbing

Il banner grabbing può essere passivo o attivo, è il metodo utilizzato per determinare il sistema operativo del target o le versioni del software esposto.

A terminal window with a dark background and light text. The title bar at the top reads 'savona@putor:~ — telnet'. The terminal content shows a user at the 'savona@putor ~' prompt typing 'telnet'. The telnet client then displays 'telnet> open fenrir 22', 'Trying 10.0.0.5...', 'Connected to fenrir.', and 'Escape character is '^]'. The final line, 'SSH-2.0-OpenSSH 7.4', is highlighted with a light blue selection box.

```
savona@putor:~ — telnet
[savona@putor ~]$ telnet
telnet> open fenrir 22
Trying 10.0.0.5...
Connected to fenrir.
Escape character is '^]'.
SSH-2.0-OpenSSH 7.4
```

# Information Gathering

## Tool

- Maltego
  - Recon-ng
  - FOCA
  - Recondog
  - OSRFramework
  - Sn1per
  - LHF (Low Hanging Fruit)
-