CYBER SECURITY

Lezione 00 - Introduzione

PREMESSA - DISCLAIMER

- LE INFORMAZIONI DEL CORSO VENGONO FORNITE PER PURO SCOPO DIDATTICO.
- NESSUNA NOZIONE E APPROFONDIMENTO IN TEMA DI VIOLAZIONI ALLA SICUREZZA VIENE ENUNCIATA CON IL FINE DI INVITARE GLI UDITORI AL CYBERCRIME.
- LO SCOPO DEL CORSO E' ESCLUSIVAMENTE QUELLO DI INDIVIDUARE E RICONOSCERE VULNERABILITA' E AVERE CONOSCENZA DELLE TECNICHE USATE PER SFERRARE ATTACCHI AL FINE DI POTER IMPLEMENTARE UNA POLITICA DI SICUREZZA PER RICERCARE E GARANTIRE LA BUSINESS CONTINUITY ED IL DISASTER RECOVERY.

PREMESSA - DISCLAIMER

- Questo corso è **SOLO per scopi difensivi**. Le abilità che acquisirai in questo corso devono essere usate in contesti validi e autorizzati dove vi è un **esplicito consenso nell'effettuare l'attività di Penetration Testing o di Ethical Hacking.**
- Tutti gli strumenti o tecniche che imparerai in questo corso sono prodotte per essere applicate durante un Penetration Test o attività di "Red Teaming".
- Se utilizzi queste tecniche contro un bersaglio che non è di tua **assoluta proprietà** o del quale non hai il permesso e l'autorizzazione di attaccare **stai violando la legge.**
- Prima di effettuare qualsiasi tipo di Penetration Testing nei confronti di qualsiasi organizzazione, **assicurati SEMPRE di avere una lettera di autorizzazione e un contratto scritto e firmato dalla dirigenza di tale organizzazione** e che ti autorizza quindi a procedere.
- **Effettuare attività di HACKING non autorizzato è considerato un REATO.**
- Devi essere AUTORIZZATO prima di procedere ad effettuare qualsiasi procedura o tecnica qui mostrata.
- In questo corso, potrai creare il tuo laboratorio domestico così da poter condurre ogni test in massima sicurezza e senza danneggiare o interferire con alcunché. **Ed è solo in questo laboratorio che dovrai sperimentare le tecniche qui mostrate.**
- Lo scopo di effettuare un Penetration Testing è quello di rilevare debolezze all'interno di una rete allo scopo di correggere tali debolezze e rendere la rete più sicura.
- **Ricordati di effettuare qualsiasi attività di Ethical Hacking in un ambiente sicuro e in modo responsabile così da incrementare il livello di sicurezza della tua organizzazione.**
- **L'autore non si assume, in ogni caso, nessun tipo di responsabilità relativamente a quanto spiegato e mostrato in questo corso**

Competenze

- Acquisire familiarità con il concetto di *sicurezza informatica*, *sicurezza delle informazioni* e *protezione dei sistemi informativi*
- fornire familiarità con i vari modi di proteggere i dati sia su un sistema "stand alone" che in una rete connessa a Internet;
- mettere gli utenti in condizioni di proteggere i dati aziendali contro perdite, attacchi virali e intrusioni.

Link Utili

- https://it.wikipedia.org/wiki/Portale:Sicurezza_informatica
- https://it.wikipedia.org/wiki/Malware
- https://it.wikipedia.org/wiki/Attacco_informatico
- https://it.wikipedia.org/wiki/Virus_%28informatica%29

Fonte prof. Giovanni Lagorio

Concetti Generali: Sicurezza Delle Informazioni

- Lo Standard ISO/IEC 27001:2005 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) è una norma internazionale che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

Concetti Generali: Sicurezza Delle Informazioni

- Società dell'informazione → uso delle informazioni come parte integrante delle attività umane.
- Sicurezza delle informazioni → componente della sicurezza dei beni in generale, e non si limita alle tecniche per nascondere il contenuto dei messaggi (Crittografia).

La Conoscenza… E' tutto

Έτσι, δεν γνωρίζω

So di non sapere (Socrate)

DATO vs INFORMAZIONE

L'informazione è l'insieme di dati, correlati tra loro, con cui un'idea (o un fatto) prende forma ed è comunicata.[1] I dati oggetto della stessa possono essere raccolti in un archivio o in un'infrastruttura dedicata alla sua gestione, come nel caso di un sistema informativo. Essa è oggetto di studio e applicazione in vari settori della conoscenza e dell'agire umano.

OBIETTIVI FONDAMENTALI

SICUREZZA =

- disponibilità
- integrità
- riservatezza

DISPONIBILITÀ

- La **disponibilità** è il *grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono*.

DISPONIBILITÀ

sistemi, reti e applicazioni

- Normale funzionamento
- ➔fornire il livello di servizio e le prestazioni richieste
- Guasto o di eventi distruttivi
- strumenti e le procedure ➔ ripristino attività in tempi accettabili

DISPONIBILITÀ

GARANTIRE

X l'*inaccessibilità* delle informazioni

- condizioni ambientali idonee
- disponibilità risorse hardware e software a fronte di
  - Problemi interni (guasti, errori, blackout, disastri e altro)
  - Attacchi esterni,

DISPONIBILITÀ

- Sistemi di backup locale e remoto
- Ridondanza dell'hardware e degli archivi,
- Firewall e router
- Sistemi di climatizzazione
- Gruppi di continuità,
- Controllo dell'accesso fisico,
- Monitoraggio delle prestazioni
- …

INTEGRITÀ

- **L'integrità** è il grado di **correttezza**, **coerenza** e **affidabilità** delle informazioni e anche il grado di **completezza**, **coerenza** e **condizioni di funzionamento** delle risorse informatiche.

INTEGRITÀ

hardware e i sistemi di comunicazione,

- ➔fattori come elaborazione corretta dei dati
- ➔livello adeguato di prestazioni
- ➔corretto instradamento dei dati

software

- ➔fattori come la completezza e coerenza dei moduli del sistema operativo e delle applicazioni
- ➔la correttezza dei file critici di sistema e di configurazione.

INTEGRITÀ

Per le informazioni, l'integrità viene meno quando i dati sono alterati, cancellati o anche inventati, per errore o per dolo, e quando si perde, per esempio in un database, la coerenza tra dati in relazione tra loro

INTEGRITÀ : PREVENZIONE

Procedure di manutenzione e diagnosi preventiva, hardware e software X

rilevazione e prevenzione di :

➔accessi illeciti,

➔attacchi virali e intrusioni,

➔applicazioni che minimizzano errori logici e formali di data entry,

➔accesso ristretto alle risorse critiche

➔controllo degli accessi

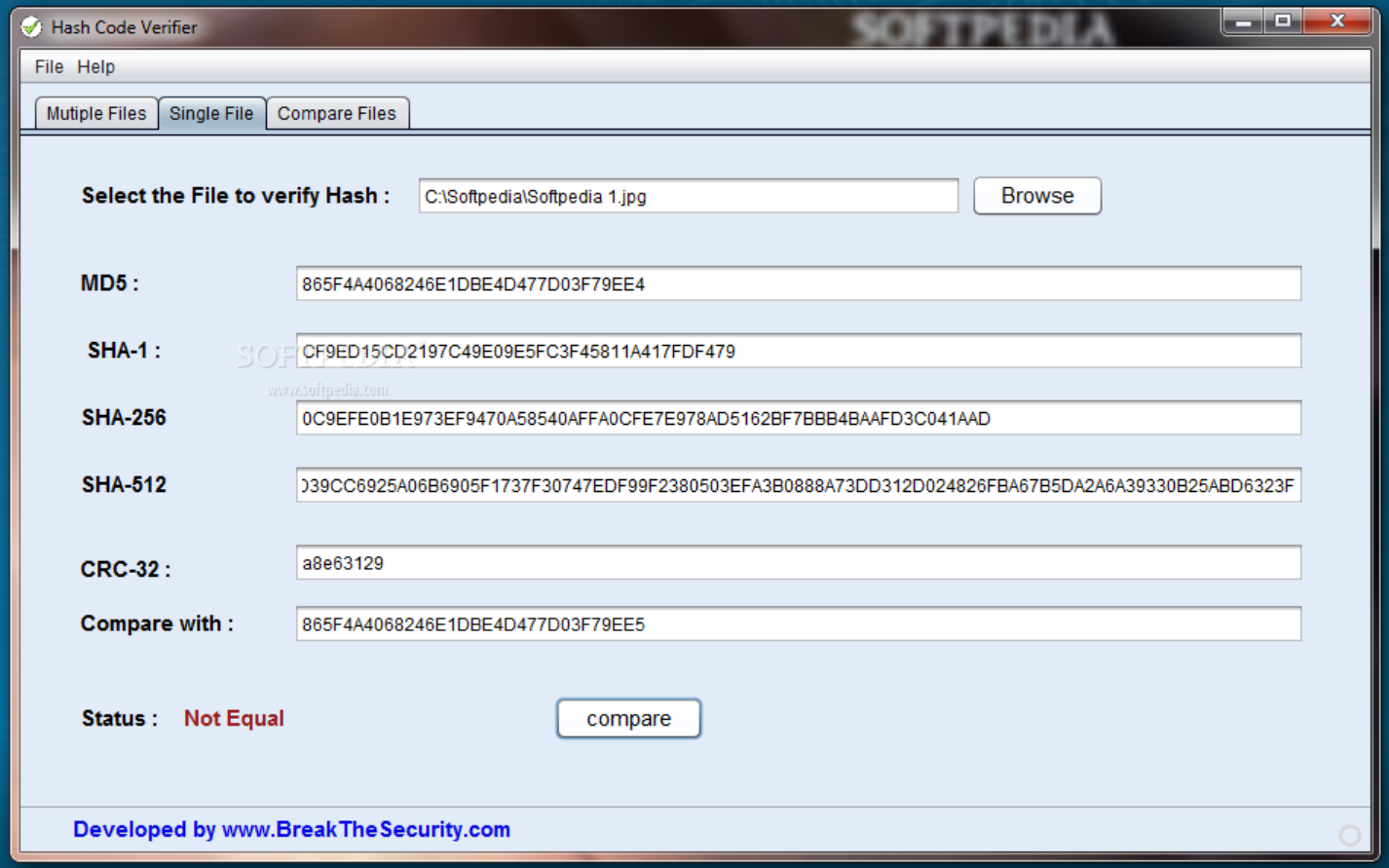
INTEGRITÀ : PREVENZIONE

Esempi

X SOFTWARE

➔hashing del software e comparazione con codice hash del fornitore

· SHA & MD5



RISERVATEZZA

- *La* **riservatezza** *consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate,* e si applica sia all'archiviazione sia alla comunicazione delle informazioni.

RISERVATEZZA : DATI & INFO

- *Un'**informazione** è composta generalmente di più dati in relazione tra di loro, ciascuno dei quali non necessariamente costituisce un'informazione.*

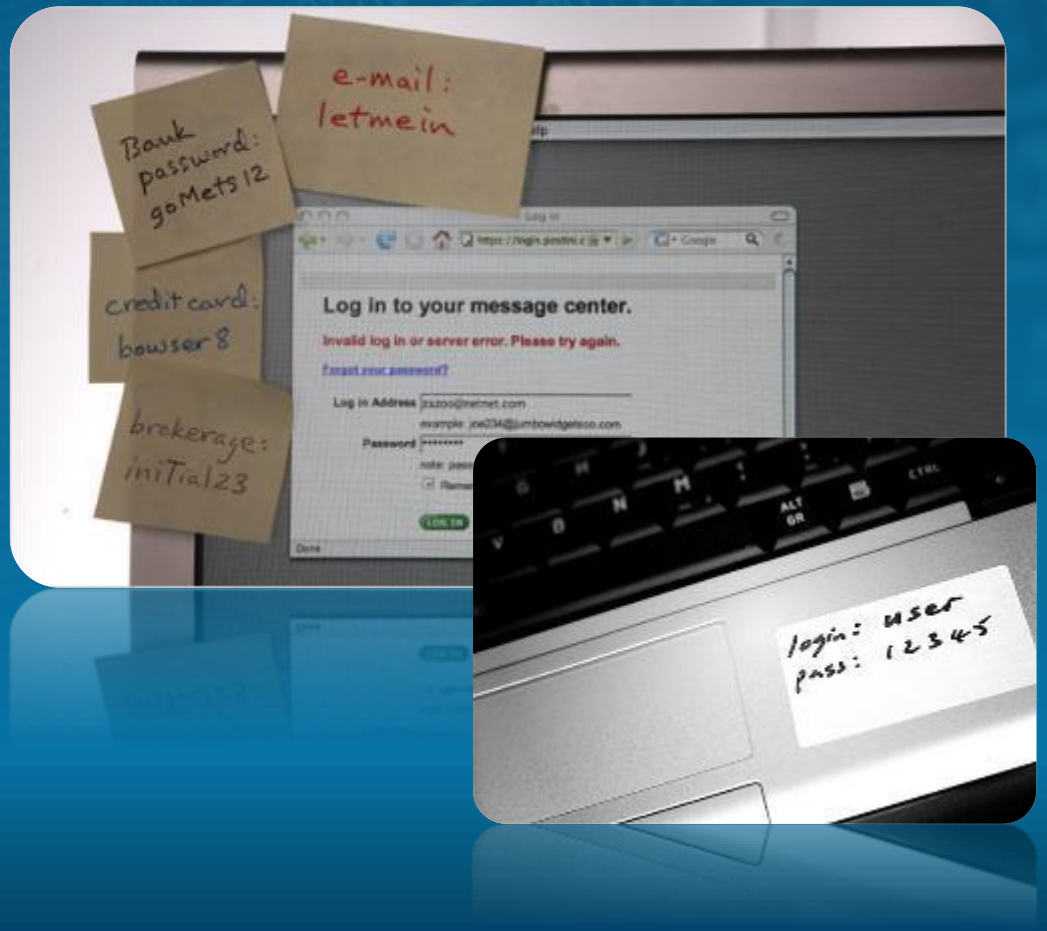
- Mario Rossi e 01/01/2017 ore 10:30 SEPARATI NON sono informazioni, sono DATI.
- Mario Rossi, Apt Scuola e 01/01/2017 ore 10:30 DIVENTANO INFORMAZIONE

RISERVATEZZA : DATI & INFO

- La riservatezza dell'informazione può essere quindi garantita
- → nascondendo l'intera informazione (per esempio con tecniche di crittografia)
- →nascondendo la relazione tra i dati che la compongono.

RISERVATEZZA : FATTORE UMANO

- tenere le password segrete
- controllare gli accessi a reti e sistemi
- rifiutare informazioni a sconosciuti (anche quando affermano di essere tecnici della manutenzione)
- cifrare i documenti e i messaggi riservati
- …



ALTRI OBIETTIVI

- **l'autenticità** garantisce che eventi, documenti e messaggi vengano attribuiti con certezza al legittimo autore e a nessun altro;
- il **non ripudio** impedisce che un evento o documento possa essere disconosciuto dal suo autore.

ALCUNI SPUNTI DI RIFLESSIONE

- Superficialità sui social ➔ Il mago belga
- IoT e dintorni: la tecnologia non sempre aiuta. L'hacker a volte non è quello solito…
- Attenzione alle Fake News…

MA… VUOI CHE CAPITI PROPRIO A…

- Statisticamente è possibile
- Per soldi
- Perché sono la via o il mezzo per raggiungere qualche cosa di più grande
- Per vendetta o per ricattare
- Per dispetto o scommessa
- Per ‘allenarsi’

Dov'e il nemico

https://threatmap.checkpoint.com/

fuori dalla nostra organizzazione

- difesa del perimetro (firewall)

fuori dalla nostra organizzazione, con l'eccezione dei nostri partner

- protezione dell'Extranet

dentro la nostra organizzazione

- >> protezione della Intranet

ovunque !

- protezione delle applicazioni

Da dove parte l'attacco?

Fonti Interne:

- **Dipendenti Malintenzionati:** Gli attacchi possono essere perpetrati da dipendenti attuali o ex dipendenti che hanno accesso privilegiato ai sistemi aziendali.
- **Errori Umani:** Gli errori non intenzionali da parte dei dipendenti, come cliccare su link di phishing o scaricare malware, possono compromettere la sicurezza.

Fonti Esterne:

- **Hacker:** Individui o gruppi che cercano di accedere ai sistemi aziendali per rubare dati, causare danni o ottenere un riscatto.
- **Cyber Gang:** Bande criminali organizzate che utilizzano tecniche avanzate per infiltrarsi nei sistemi aziendali e rubare informazioni sensibili.

Internet:

- **Phishing:** Tentativi di ingannare gli utenti per ottenere informazioni sensibili come password e dati personali.
- **Malware:** Software dannoso che può infettare i sistemi attraverso download non sicuri o allegati email.
- **Attacchi DDoS:** Attacchi che mirano a sovraccaricare i server aziendali, rendendoli inaccessibili.

Da dove parte l'attacco?

- Gli attacchi informatici possono provenire da diverse nazioni e variano a seconda delle dimensioni aziendali.
- Secondo un'analisi di CybergON, le nazioni da cui partono più tentativi di attacchi verso le aziende italiane includono Belgio, Francia, Olanda, Russia, Inghilterra e Bulgaria per le grandi aziende, mentre per le medie imprese gli attacchi provengono principalmente da Stati Uniti, Romania e Austria.
- Per le piccole imprese, gli attacchi sono meno frequenti e provengono da Stati Uniti, Russia, India e Cina.
- Inoltre, è importante notare che le cyber gang spesso utilizzano connessioni da paesi non sospetti per mettere a segno le proprie attività, rendendo più difficile isolare il traffico proveniente da paesi considerati rischiosi

Concetti relativi alla sicurezza informatica

- Minacce informatiche
- Valore delle Informazioni
- Sicurezza personale
- Protezione file

Concetti relativi alla sicurezza informatica

Chi sono gli autori ?

Hacker VS Cracker

Cybercrime

- Bande criminali pagano per l'accesso a computer infetti
  - https://www.cybersecurity360.it/nuove-minacce/cyber-gang-chi-sono-e-come-agiscono/
  - https://krebsonsecurity.com/tag/gangstabucks/
  - Vero e proprio listino prezzi https://dl.packetstormsecurity.net/papers/general/wp-russian-underground-101.pdf
- Servizi *Pay-per-install* permettono l'infezione massiva con un malware scelto dal cliente (spambot, finti antivirus, banking trojans, software per rubare le password/carte di credito), con costi che variano a seconda della posizione geografica delle vittime
  - https://hacktips.it/cosa-come-funziona-pay-per-install-e-distribuzione-malware/
  - Un esempio su Android: http://www.welivesecurity.com/2012/09/12/dancing-penguins-a-case-of-organized-android-pay-per-install/

PERCHE' ? ➔ ARRICCHIRSI & VENDETTA

- Sete di potere, desiderio che la gente parli di se', rivendita di dati e informazioni
- Bande criminali pagano per l'accesso a computer infetti
- Servizi *Pay-per-download* (link) / *Pay per click (sondaggi)*
  - → 3000 client * 0,005 euro * 30 gg * 10 siti (?) → 4500 euro
- Servizi *Pay-per-install* permettono l'infezione massiva con un malware scelto dal cliente (spambot, finti antivirus, banking trojans, software per rubare le password/carte di credito), con costi che variano a seconda della posizione geografica delle vittime
- Vendette, ritorsioni, motivi personali
- Motivi politico-religiosi
- …

PERCHE' ?

- Bande criminali pagano per l'accesso a computer infetti
- Servizi *Pay-per-install* permettono l'infezione massiva con un malware scelto dal cliente (spambot, finti antivirus, banking trojans, software per rubare le password/carte di credito), con costi che variano a seconda della posizione geografica delle vittime
- Vendette, ritorsioni, motivi personali
- Motivi politico-religiosi
- …

Conseguenze di un attacco

- interruzione del servizio
- virus
- accessi non autorizzati
- furti di informazioni riservate
- frodi finanziarie
- sabotaggi
- abuso nell'uso delle reti

IL LINGUAGGI DI PROGRAMMAZIONE

- combo un hacker normalmente conosce uno o più linguaggi di programmazione :
- C / C++: non è semplice ma si possono programmare tool potenti veloci ed efficienti ;
- Asm (alias assembler) è il più difficile e complesso ha il vantaggio di essere incredibilmente veloce e leggero e funziona su tutte le piattaforme
- Java : è semplice da imparare ed è multipiattaforma
- Python : ottimo perché inizia , molto potente e versatile , permette di creare codice praticamente per tutto anche con poche righe

Hacking = Solo Informatica ?

- **Assolutamente no !**
- bisogna conoscere il fattore umano per poterne sfruttare le vulnerabilità
- si infiltra dovunque e in qualsiasi maniera (per esempio sfrutta tutti i social a disposizione contattando non solo la vittima ma anche tutto ciò che la circonda)
- si crea un quadro strategico basato sulla situazione in essere
- tenta di trasformare la situazione o parti di essa a suo vantaggio senza fare troppo rumore
- è molto abile a preservare la sua privacy e a scomparire nel nulla