paolo macchi

CEH Security

note preparazione CEH

Certified Ethical Hacker

Paolo macchi - IFTS 2020

Indice generale

Ethical hacker

“An **ethical hacker,** also referred to as a white hat hacker, is an information security expert who systematically attempts to penetrate a computer system, network, application or other computing resource on behalf of its owners -- and with their permission -- to find security vulnerabilities that a malicious hacker could potentially exploit. “

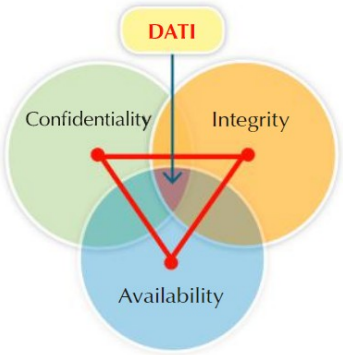
https://searchsecurity.techtarget.com/definition/ethical-hacker

“A **Certified Ethical Hacker (CHE)** is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s).”

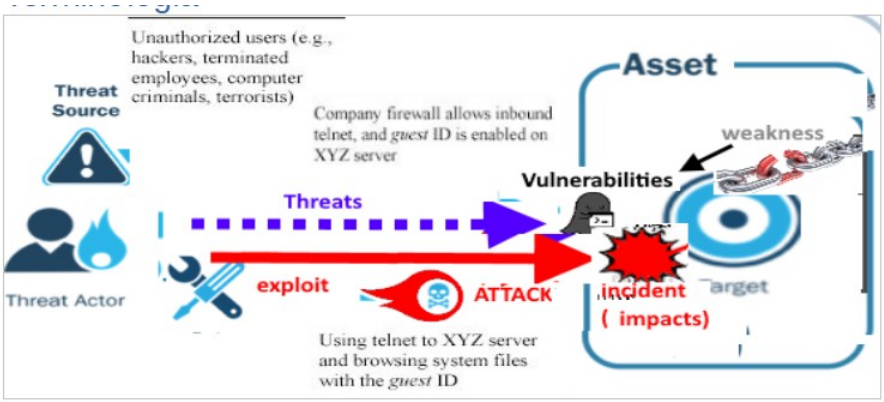
https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
https://www.udemy.com/course/certified-ethical-hacker-practice-tests/

06 System Hacking - Introduction to Ethical Hacking

- CIA



(cfr. Gateway. Sistemi e reti- Vol. 3 - Codice EAN: 9788849420760 https://tinyurl.com/r58vbsw)



(cfr. Incidenti e Password (Paolo Macchi) - https://moodle.isisfacchinetti.it/mod/data/view.php?d=21&rid=736

Aspetti legali

- **ARTICOLO 615 ter, Codice PenaleSezione IV – Dei delitti contro la inviolabilità del domicilio.** Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicu-rezza ovvero vi si mantiene contro la volontà espres-sa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.La pena è della reclusione da uno a cinque anni:
  - 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abu-so dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore pri-vato, o con abuso della qualità di operatore del sistema;
  - 2) se il colpevole per commettere il fatto usa violen-za sulle cose o alle persone, ovvero se è palese-mente armato;
  - 3) se dal fatto deriva la distruzione o il danneggia-mento del sistema o l’interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi in-formatici o telematici di interesse militare o relativi all’ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di inte-resse pubblico, la pena è, rispettivamente, della re-clusione da uno a cinque anni e da tre a otto anni.Nel caso previsto dal primo comma il delitto è puni-bile a querela della persona offesa; negli altri cas
- Il **Decreto Legislativo 231/2001** ha introdotto in Italia il **Sistema di Responsabilità Amministrativa dell’Ente i**n base alla quale qualora un soggetto, dipendente o collaboratore, operante in una società, commetta uno dei reati presupposto, previsti dal D.lgs. 231/2001, a vantaggio della società stessa, *questa potrà essere condannata e subire una delle sanzioni* previste dallo stesso D.lgs. 231/2001. Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto. Tra i vari reati presupposto, per i quali la società può essere chiamata a rispondere, rientrano: ...,

Frode informatica in danno dello Stato o di un Ente pubblico e il trattamento illecito di dati,..Per essere esonerata dalla responsabilità amministrativa, la società deve dimostrare di aver adottato ed efficacemente attuato, prima della commissione del reato, un modello di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi

- **L. 262/05 "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari"** Legge 262/05 Le disposizioni introdotte dalla L. 262/05, conosciuta anche come "Legge sul Risparmio", coinvolgono tutte le aziende, italiane ed estere, quotate sul mercato italiano, e introduce una serie di adempimenti a cui le aziende devono uniformarsi. Tali adempimenti hanno influenza su diversi aspetti, da quello societario a quello organizzativo, dalle comunicazioni sociali al controllo interno. La normativa prevede infatti:
  un rafforzamento delle responsabilità a livello dirigenziale in merito alle comunicazioni sociali, con impatto nei ruoli e nelle responsabilità dell'alta direzione e del controllo interno;

- **Legge 196 Privacy**
  https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29
  GDPR =>> rilevare, gestire e comunicare entro 72 ore gl iincidenti informatici (4% del fatturato)
  (https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/
  https://www.cybersecurity360.it/cultura-cyber/reati-informatici-quali-sono-e-che-cosa-si-rischia/)

ettercap-ng -M:arp -T // // -i wlan0mon

Panoramica

- ***ASSET =*** *l'insieme di beni (dati e persone necessarie all'erogazione di un servizio IT) che vanno tutelati*
- ***RISCHIO (risk)= PROBABILITA'x IMPATTO.*** *Il rischio è il prodotto di due fattori: –La probabilità che un evento dannoso si possa verificare e l'impatto, nel senso delle conseguenze che l'evento dannoso avrebbe sul sistema se si verificasse. Il rischio deve essere gestito attraverso azioni mirate a ridurre uno o entrambi i fattori che lo costituiscono.*
- ***MINACCIA*** *(threat) è un* ***evento esterno*** *=* ***atto volontario o evento accidentale che può causare la perdita di una proprietà di sicurezza.*** *- Una minaccia è qualsiasi azione, accidentale o deliberata, che potrebbe comportare la violazione di qualche obiettivo di sicurezza e può sfruttare una vulnerabilità • Una minaccia* ***dipende sempre da un fattore esterno al sistema*** *che può essere di origine naturale o antropica; • ESEMPI: – Attacco «Hacker»: minaccia deliberata di origine antropica; – Smarrimento password (fig aa)*
- ***DEBOLEZZA (*** *weaknesses)* ***= errori che possono condurre a vulnerabilità*** *(Software weaknesses are errors that can lead to software vulnerabilities.)* - **CWE™** is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
  esempio: *CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')*
  http://cwe.mitre.org/data/definitions/120.html#Demonstrative%20Examples
- ***VULNERABILITA'*** *(vulnerability) è un* ***evento interno = errore che può essere direttamente sfruttato da un hacker per accedere alle risorse critiche*** *(A software vulnerability, such as those enumerated on the* ***Common Vulnerabilities and Exposures (CVE®) List****, is a mistake in software that can be directly used by a hacker to gain access"; vedi anche* https://nvd.nist.gov/ https://cve.mitre.org/ *- esempio:* https://cve.mitre.org/data/refs/index.html *(CVE Reference Key/Map)*
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-5195
  - *Una vulnerabilità è una debolezza intrinseca di un sistema informatico; A differenza delle minacce non dipende da agenti esterni ma è una proprietà del sistema stesso (es errori di programmazione)*
  - *Le vulnerabilità sono qualsiasi difetto software o hardware.*
  - ***NOTA*** *What is the difference between a software vulnerability and software weakness? . What is the relationship between CWE and CVE? https://cwe.mitre.org/about/faq.html#A.1*

- ***EXPLOIT = sfruttare una vulnerabilità.*** *Dopo aver acquisito conoscenza di una vulnerabilità, i malintenzionati tentano di sfruttarla con un programma scritto per sfruttarla*
- ***ATTACCO*** *(attack)= "**atto volontario**" **per la realizzazione pratica di una minaccia.** Se un agente esterno attua una minaccia che sfrutta una vulnerabilità si ha una violazione di un obiettivo di sicurezza;*
- ***EVENTO (NEGATIVO) = "evento accidentale**" per la **realizzazione pratica di una minaccia***
- ***CONTROMISURE*** *= azioni che vengono intraprese per proteggere le vulnerabilità*
- **Ese**mpio Vulnerabilità : **Dirty COW** (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-5195 https://nvd.nist.gov/vuln/detail/CVE-2016-5195 - "dirty cow" bersaglia tutti i kernel precedenti al 2016. Ci sono moltissime versioni dell'exploit dirty cow. Ad esempio la versione creata dall'utente firefart ci permette di modificare il file /etc/passwd cambiando la password dell'utente root.

	copy-on-write (COW) - Un utente locale senza privilegi poteva usare questo difetto per ottenere l'accesso in scrittura a una memoria in sola lettura e quindi aumentare i privilegi sul sistema. Unica soluzione: aggornamento: Debian/Ubuntu: $ sudo apt-get update && sudo apt-get upgrade && sudo apt-get dist-upgrade

Le 4 principali "nuove" minacce: *(cfr. Incidenti e Password (Paolo Macchi) - https://moodle.isisfacchinetti.it/mod/data/view.php?d=21&rid=736*

- Hacking - Le minacce possono essere classificate in tre tipi diversi:
  - Minaccia alle reti - Ci possono essere diverse fasi, tra cui: raccolta di informazioni; intercettare i dati;
    - lo Spoofing; • Attacco MITM; • SQL injection; • ARP poisoning; • DoS;
  - Minacce all'host - sono gli attacchi diretti all'obbiettivo per forzare la sicurezza di esso e prelevare le informazioni. Le possibili minacce possono essere:
    - Attacco di un malware; • Footprinting; • Dos; • inserimento di una Backdoor; • etc.
  - Minacce alle applicazioni - se non sono state prese appropriate misure di sicurezza nel programmare un applicazione, i bug in essa possono essere utilizzati per trovare vulnerabilità e sottrarre (o danneggiare) i dati in essa. Alcuni esempi di attacchi:
    - Convalida errata dei dati; • Rilevazione delle informazioni; • problemi di Buffer overflow; • attacchi alla crittografia; • e altri ancora.
- Le fasi di un attacco sono cinque
  - Esplorazione e Footprinting
  - Scanning & Enumeration
  - Guadagnare l'accesso: è la fase più importante, in cui si riesce ad attaccare l'obbiettivo ed accedervi (può essere un sito web, una rete o un applicazione).
  - Mantenere l'accesso: in questa fase l'hacker può cercare di guadagnare i permessi di root (backdoor o un trojan)
  - Pulire le traccie: ad esempio essere la cancellazione dei file di log
- Metodologie per il password cracking
  - Attacco a dizionario: in questo attacco, un file di testo (il dizionario) è caricato all'interno del sistema
  - Attacco a forza bruta: l'attacco a forza bruta consiste nel provare ogni singola possibile combinazione fino a che non si trova quella corretta.
  - Ibrido: combinazione delle precedenti tecniche

- Attacco passivo online questa tecnica consiste nel monitorare la rete in modo da catturare un'eventuale password. Non è intrusiva, in quanto non si viene riconosciuti nel monitoraggio e dopo averla sniffata si può tranquillamente craccare sul proprio dispositivo.
  - Ci sono tre sottotipi:sniffing di rete; Man-in-the-Middle (tradotto Uomo nel mezzo); • Replay;
- Attacco attivo online -è la via più semplice per avere accesso al sistema, i principali sono:indovinare la password;
  - Keylogger; • Phishing;
- Esempio pratico sono entrato in una macchina UNIX utilizzando una vulnerabilità di Samba. Ora voglio trovare e craccare le password del sistema, come posso fare? Quando sono nel sistema, entro nella cartella delle password e apro il file shadow. Le password non sono ovviamente in chiaro, e per essere visualizzate necessitano di essere craccate. Per farlo utilizzerò uno dei sofware più utilizzati, ossia John. Copio quindi le password trovate in un file di testo sul mio dispositivo, apro John (versione GUI), carico il file e lancio l'attacco. Dopo pochi minuti trova subito la password di root (123456)

MalwareOgni software che causa danni al computer o alla rete è considerato software maligno, detto anche Malware, inclusi i virus, i trojan horse, worms, rootkits, scareware e spyware.

L'analisi di un malware consiste nel disassemblare lo stesso per capire come funziona, come identificarlo e come eliminarlo.

Ci sono due tipi diversi di approcci all'analisi di un Malware

Esistono diverse tipologie di malware.

Le più importanti macro categorie sono:

Backdoor: codice che si autoinstalla in un computer per permettere l'accesso ad un altra persona;

Botnet: simile alla backdoor, permette all'attaccante di accedere al sistema, solitamente tutti i computer infettati con la stessa botnet ricevono la stessa istruzione contemporaneamente;

Rootkit: sono solitamente in coppia con altri malware, come una backdoor, in modo da rendere il codice difficile da decifrare;Trojan: programma maligno mascherato da qualcosa di benigno; Worm o virus: parti di codice che si diffondono copiandosi in altri programmi, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono in altri computer tramite lo spostamento dei file infetti da parte dell'utente; Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati, come la digitazione sulla tastiera o del mouse; Ransomware: virus che cripta tutti i dati (la maggior parte, a seconda delle estensioni specificate dal programmatore) di un dispositivo. Per riottenerli bisogna pagare una cifra prestabilita per poter decrittografare i file; ..e molti altri ancora.

- Alternate Data Streams (ADS): i file invisibili di Windows

  Gli Alternate Data Streams sono disponibili unicamente su partizioni NTFS.

  In questo tipo di filesystem le informazioni su file e cartelle sono memorizzate in una tabella chiamata Master File table (MFT).

  In questa regione del disco ogni file è identificato da una collezione di oggetti chiamati attributi.

  Il fattore importante per le nostre considerazioni è che NTFS permette la creazione di più di un attributo dati per ogni singolo file.

- La Steganografia è definita come l'arte di nascondere dati all'interno di altri dati senza essere scoperti da fonti esterne.

  Vengono rimpiazzati bit inutili e non utilizzati all'interno di file immagini, video o audio con bit precisi e scelti da noi.

  L'obbiettivo è lo stesso della crittografia, ossia inviare file senza che enti o persone esterne possano scoprire ciò che stiamo inviando.

- L'hacking di un router

  I nostri computer, cellulari, stampanti e sempre più spesso televisori o altri dispositivi sono connessi simultaneamente ai router domestici, i quali ci permettono di connetterci alla rete esterna e navigare in internet.

  - Purtroppo (o per fortuna) anche questi sono vulnerabili ad attacchi esterni o interni e devono essere protetti sempre al massimo, in modo che nessuno possa prendere il controllo dei nostri dispositivi passando da essi.

I passi da effettuare per entrare in un router sono:

1. Identificare lo stesso (indirizzo IP, marca, modello); 2. Scansionare le porte attive; 3. Entrare nel router; 4. Craccare la password; 5. Analizzarlo dall'interno, ossia: a) controllare gli utenti; b) analizzare le informazioni; c) monitorare il traffico; d) inserire una backdoor; e) e molto altro.

Con FTP

- ESEMPI
  - **Lazagne**: https://github.com/AlessandroZ/LaZagne ==> lo scarichi, lo metti sul desktop e lo lanci! (The **LaZagne project** is an open source application used to **retrieve lots of passwords** stored on a local computer. Each software stores its passwords using different techniques (plaintext, APIs, custom algorithms, databases, etc.). This tool has been developed for the purpose of finding these passwords for the most commonly-used software.)
  - **Mimikatz** x Windows

07 Malware Threats

- Un trojan, nell'ambito della sicurezza informatica, indica un tipo di malware, ed è definito come un programma maligno mascherato da qualcosa di benigno (il nome infatti deriva da Cavallo di Troia in esplicito riferimento alla leggenda Greca). Un trojan è utilizzato per entrare nel computer della vittima senza esser riconosciuto, accedere ai dati dello stesso e/o causare danno.È bene ricordare che i trojan hanno lo stesso livello di privilegi dell'utente che lo avvia. Quindi se sarà un utente normale, senza troppi privilegi, esso potrebbe causare pochi danni, ma se è l'amministratore (cosa molto comune con Windows e l'utilizzo privato) esso può danneggiare notevolmente il dispositivo.

  Rubare informazioni sensibili come email, password, carte di credito; • Utilizzare il computer della vittima come "disco esterno" per salvare e nascondere informazioni illegali; il sistema compromesso può essere poi utilizzato per scopi illegali, come parte di un attacco dos o come botnet.Un sistema può essere infettato in diversi modi, tra i quali: il trojan è inserito in un programma shareware o freeware. L'utente installa tutto il pacchetto inconsciamente, insieme al virus; • click su banner pubblicitari maligni. Negli ultimi tempi sono divenuti sempre più frequenti, anche nei siti porno o di torrent; • possono essere inviati tramite email, come allegato. Solitamente il messaggio arriva da un contatto fidato, il quale a sua volta era stato infettato; • tramite accesso fisico, come un'USB o un CD

  - **RAT** (Remote Access Tool): server (C&C) + client esempio https://github.com/n1nj4sec/pupy

    "Programs for remote access to a computer or other device connected to the Internet or a local network. Remote administration tools can be part of a software product or come as separate utilities. RAT enables remote configuration of applications and devices.

    Remote administration is critical in terms of information security. Developers employ authorization and encryption tools in its implementation.

    RAT vulnerabilities can be exploited by cybercriminals to run malware on victim computer" (https://encyclopedia.kaspersky.com/glossary/rat-remote-access-tools/)

- Cosa è una Botnet

  Il termine Botnet deriva dalla parola roBOT NETwork, il quale fornisce già spiegazione abbastanza chiara di cosa possa essere.

  Essa è un'enorme rete formata da dispositivi informatici compromessi (infettati quindi da Malware) e collegati ad Internet, controllati da un unica entità, il botmaster.

  Una Botnet può avere sia scopi benevoli che malevoli, e può:

  • operare su una grande rete di computer da remoto; • scansionare automaticamente i dispositivi e le reti ad essi collegati; • creare attacchi DOS; • effettuare attacchi spam; • compromettere altri dispositivi. Esistono due tipi principali di botnet:

  • Centralizzate: sono comandate da un unico C&C, il quale impartisce i comandi e le controlla in modo totale. Se il botmaster viene però rintracciato e reso innocuo, esse non svolgeranno più la loro funzione; • Decentralizzate (tramite p2p): sono collegate tra di loro come una rete di pari ed ognuna impartisce ordini ai suoi nodi vicini. In questo modo se ne viene fermata una, le altre compiono comunque il loro lavoro.

Driver Verifier opera testando ciascun driver che viene caricato all'avvio di Windows; quando rileva qualcosa di "anomalo", esso arresta il sistema, mostrando la classica "finestra blu" (nota come BSOD – Blue Screen Of Death), dove viene dettagliatamente esposto il problema. verifier.exe, tasklist , services.msc (naturalmente accessibile anche tramite pannello di controllo-->strumenti di amministrazione-->servizi)

Una volta che il virus ha avuto accesso al sistema e si presenta come processo in esecuzione in memoria deve provvedere a garantirsi la sopravvivenza per il futuro, in caso contrario allo spegnimento del sistema cesserebbe di esistere.

Il metodo impiegato è quello di sfruttare supporti non volatili da usare come ospite: filesystem di dischi fissi, dischi removibili, risorse di rete etc. Si illustrano di seguito alcune tecniche di replica usate dai virus.Virus a sovvrascrittura si sostituiscono completamente al file ospite. Il file sostituito deve essere un file eseguibile (.exe, .com, .bat, .scr solo per citarne alcuni).

Quando l'utente o il sistema invocherà il file pensando che sia quello legittimo in realtà attiverà il virus che verrà caricato in memoria.

Le Macro delle applicazioni MS Office sono script programmati in VBA (Visual Basic for Application) che possono essere inclusi in documenti Word, Excel, Access etc…

- l virus in questo caso possiede una parte sempre residente in memoria che monitora alcune chiamate a funzioni del sistema operativo effettuate dai programmi. In questo modo, per esempio, un Boot Virus può verificare se una applicazione chiede di leggere il settore di boot o l'MBR.
- La principale differenza tra i virus e i worm: questi ultimi si replicano usando i protocolli di rete e le sue falle note, garantendosi un'autonomia invidiabile (fanno tutto da soli, si replicano ed infettano senza alcuna interazione degli utenti), mentre i virus possono diffondersi solo se veicolati da mezzi fisici o virtuali ben indirizzati come supporti rimovibili o email e richiedono in ogni caso un minimo d'interazione da parte degli utenti (devono essere eseguiti e avviati). In sostanza sono molto simili tra loro, ma un Worm ha un livello di replicazione molto più alto e spesso arreca danno senza nemmeno avviarlo e moltiplicandosi all'infinito in un solo PC intasando il disco rigido e la rete.

  lcuni esempi di worm "Iloveyou" e il temuto worm "Conficker"
- un malware recente molto avanzato che integra al suo interno le caratteristiche nocive di virus, trojan e worm.
- Ransomware

  Questa variante di trojan è molto pericolosa ed è responsabile della perdita di numerosi miliardi di dollari in tutto il globo, con tantissimi file personali cancellati e criptati per sempre! Una vera e propria piaga sociale, a detta di molti analisti.

08 Sniffing

09 Social Engineering

10 Denial-of-Service

WEB

https://it.wikipedia.org/wiki/HTTP_Strict_Transport_Security

http://blog.sistemieservizi.net/wp-content/uploads/2016/06/infographic_hacker_update-gp-trans.png

https://www.garanteprivacy.it/regolamentoue/databreach

MALVERTISING

18 IoT Hacking

Shodan

MIRAI : Botnet con dispositivi IoT

- Module 01: Introduction to Ethical Hacking
- Module 02: Footprinting and Reconnaissance
- Module 03: Scanning Networks
- Module 04: Enumeration
- Module 05: Vulnerability Analysis
- Module 06: System Hacking
- Module 07: Malware Threats
- Module 08: Sniffing
- Module 09: Social Engineering
- Module 10: Denial-of-Service
- Module 11: Session Hijacking
- Module 12: Evading IDS, Firewalls, and Honeypots
- Module 13: Hacking Web Servers
- Module 14: Hacking Web Applications
- Module 15: SQL Injection
- Module 16: Hacking Wireless Networks
- Module 17: Hacking Mobile Platforms
- Module 18: IoT Hacking
- Module 19: Cloud Computing
- Module 20: Cryptography