Tecniche di verifica della sicurezza

SECTER/TSECURITY

Beneath the surface, always

AGENDA DI OGGI

- Introduzione
- Enumerazione e Fingerprinting servizi di un sistema
- Enumerazione di un'applicazione web
- Identificare potenziali vulnerabilità
- Verifica e exploitation di vulnerabilità
- Analisi e verifica di un'applicazione web

WHOAMI

DANIELE SCANU

Founder @ Soter IT Security
daniele.scanu@soteritsecurity.com

Daniele Scanu @sk4pwn

SOTER/ITSECURITY
Beneath the surface, always

INTRODUZIONE

Attacchi informatici e analisi di sicurezza

“L’unico sistema veramente sicuro è quello spento, gettato in un blocco di cemento e sigillato in una stanza piombata con delle guardie armate – e anche così ho dei dubbi”

Eugene Howard Spafford

SECTER/SECURITY
Beneath the surface, always

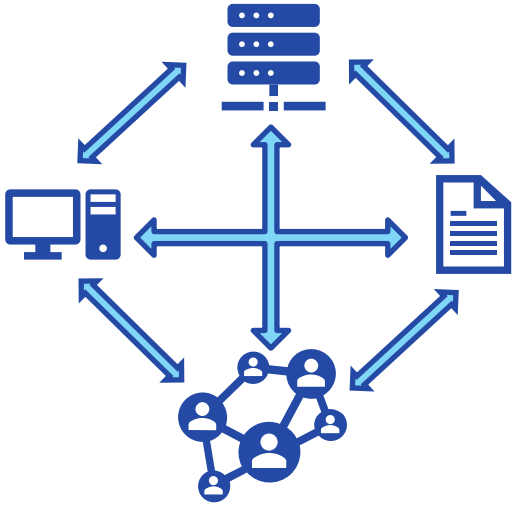
UN ATTACCO INFORMATICO

Il termine **attacco informatico**, si riferisce in generale alla compromissione di uno o più sistemi appartenenti ad una azienda.

Bisogna definire però qual è il **vettore d'attacco**. Si intende cioè il modo in cui un attaccante ha avuto accesso al sistema.

Può essere più o meno sofisticato sulla base di alcuni parametri:

- Difficolta dell'attacco
- Skills tecniche richieste
- Impatto sul sistema



VETTORI D'ATTACCO

PHISHING

Si inganna qualcuno tramite una comunicazione per cercare di ottenere informazioni o direttamente un accesso

VIRUS

L'installazione di un programma malevolo permette di eseguire azioni sulla macchina e sulla rete più o meno invasive.

ACCESSO FISICO

Un attaccante riesce a entrare fisicamente nella struttura e a infiltrarsi nella rete

VULNERABILITA'

Trovare e gestire gli anelli deboli di un sistema (Dal punto di vista tecnico)

MISURE DI PREVENZIONE

Per le prime tre categorie è necessaria la **sensibilizzazione** e avere un occhio di riguardo per le azioni che si compiono ogni giorno.

Tuttavia possiamo assumere che **prima o poi** qualcuno cada nella trappola di un attaccante; è importante considerare sempre il fattore e l'errore umano e nessuno ne è escluso.

Massimizzare la sicurezza a livello tecnico però è sempre possibile cercando di ridurre al minimo il numero di vulnerabilità che un attaccante possa sfruttare al fine di bucare un sistema.

Da una parte vanno sanate quelle che sono le vulnerabilità note in prodotti di terze parti open-source e non, dall'altra è necessario effettuare controlli periodici e sanare le vulnerabilità che derivano dai propri prodotti e dai propri errori di configurazione.

Ma come?

IL VULNERABILITY ASSESSMENT

Il Vulnerability Assessment è tipicamente associato a un test automatico con una revisione finale da parte di un operatore.

I risultati sono verificati alla fine per escludere eventuali falsi positivi e per permettere di verificare.

Spesso viene eseguito in modo ricorrente durante l'anno per accertarsi

Software più comuni per un VA:

- Nessus
- Rapid7

IL PENETRATION TEST

Il **Penetration Test** (PT) è un'attività più approfondita in cui l'effort è per la maggior parte umano ed è effettuato da personale esperto.

Eventuali software e tool sono utilizzati a supporto dell'operato e per poter automatizzare task lunghi e ripetitivi, ad esempio per esfiltrare informazioni da una componente vulnerabile.

In base al perimetro, il PT può essere della seguente tipologia:

- Web
- Mobile
- Infrastrutturale
- IoT

RED TEAM EXERCISE

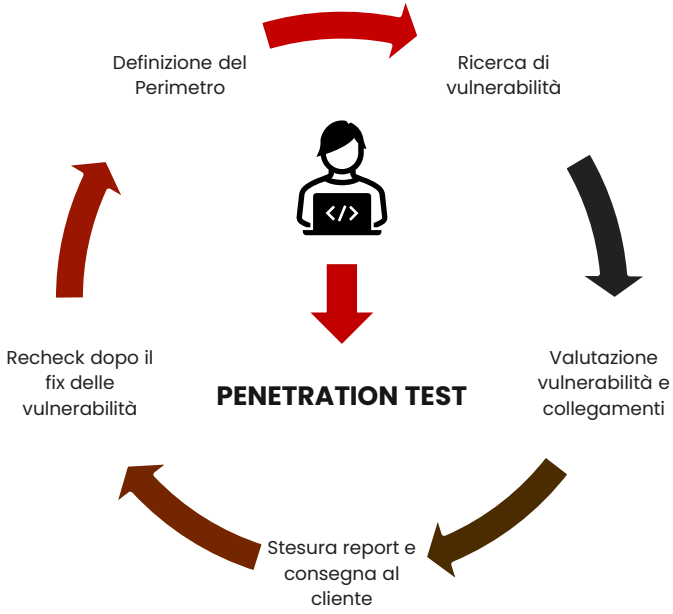
Il Red Team Exercise è un attività più ampia e lunga, e spesso il suo perimetro è molto ampio. L'obiettivo è la ricerca di scenari complessi e reali che potrebbero diventare realtà valutando il massimo risultato raggiungibile da un attaccante.

Il Red Team (il team offensivo) cerca di non allertare né persone né sistemi informatici all'interno dell'azienda e per questo è necessario un'analisi approfondita. Il Blue Team dell'azienda target (il team difensivo, spesso interno all'azienda) viene messo alla prova valutando parametri come:

- Si accorge dell'attacco
- Tempo di reazione
- Mitigation messe in atto

SOTER/ISECURITY
Beneath the surface, always

CICLO DI UN PENETRATION TEST

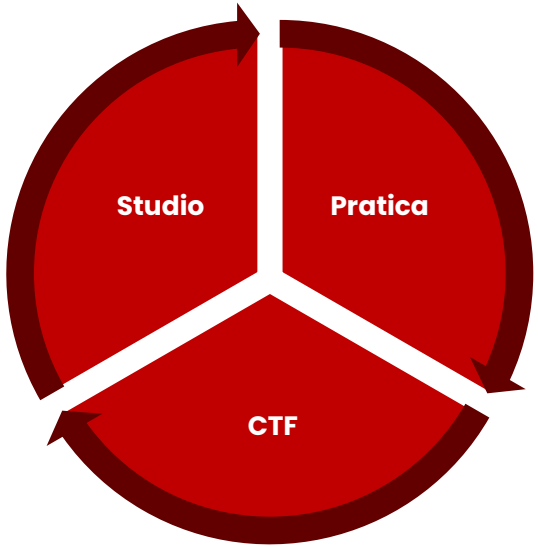


ALLENAMENTO

Come si impara oppure si migliora tecnicamente?

Tramite piattaforme di training, o scaricando macchine virtuali da testare in locale, immaginando che queste siano target del test.

Ci sono competizioni dedicate che si chiamano CTF (Capture The Flag) in cui esistono diverse sfide da portare a termine e della bandiere da catturare per poter guadagnare punti.



LEGALITA’

ATTENZIONE

Condurre test, analisi, attacchi su applicazioni e dispositivi di cui **non** si possiede un permesso scritto è assolutamente vietato in quanto costituisce **attività illegale.**

MANLEVA

Un test di sicurezza richiede di essere formalizzato tramite documenti tra cui la Manleva, ed è un documento importante che distingue un **Penetration Tester** da un **criminale**.

DATI DELLA MANLEVA

Nella manleva vengono inseriti dettagli come l’oggetto dei test (il **perimetro**), **l’indirizzo IP** di provenienza che può condurre i test e la **finestra temporale** in cui il documento ha valenza legale e in cui è permesso effettuare i test.

DISCLAIMER

Non replicate le azioni mostrate durante la lezione di oggi su un altro sistema in Internet

Invece che dire “Don’t try this at home” possiamo dire “provate in ambienti dedicati” dove con ambienti dedicati si intendono piattaforme di training e hacking simulation (HackTheBox, TryHackMe)

INIZIO DELL'ATTIVITA'

Partiamo

La sicurezza di un sistema equivale alla sicurezza del suo anello più debole

SOTER/ITSECURITY
Beneath the surface, always

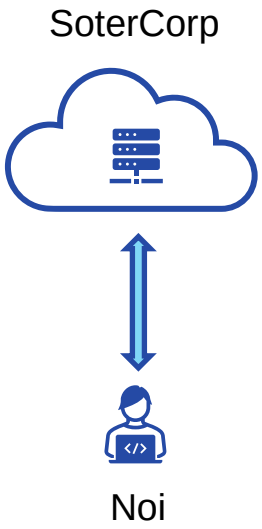
COSA FACCIAMO OGGI

Oggi simuleremo un attacco informatico, ad un server in Internet di una fittizia azienda **SoterCorp**.

Per avvicinarci il più possibile ad un attacco reale e ad un Penetration Test, faremo un PT Infrastrutturale, e verificheremo la sicurezza sia dei servizi esposti sia delle sue (eventuali) applicazioni web. Saranno presenti delle flag, da raccogliere dopo il raggiungimento di un obiettivo.

L'obiettivo è individuare il maggior numero di **vulnerabilità** e raccogliere il informazioni riguardo al target dell'analisi per poter comunicare i risultati al cliente e permettergli di applicare delle **remediation**.

Ogni ora circa ci fermeremo per fare il punto della situazione e per mettere delle Milestone (vedremo dopo).



DETTAGLI ENGAGEMENT

Il perimetro è composto dal seguente host:

- IP: 78.128.99.242 - sotercorp.it

Il PT è da effettuare in **produzione** («il cliente» non ha potuto duplicare l'ambiente in un altro di test), in modalità **Black Box** (sappiamo solo il nome di dominio e l'indirizzo IP).

Viene richiesto di eseguire il test con **metodologia e la testing guide OWASP**.

Viene richiesto di utilizzare una VPN per effettuare i test, in questo modo il «cliente» è in grado di filtrare e riconoscere le richieste in base alla provenienza.

Avete il permesso di mettere in pratica le azioni mostrate, sono vietati attacchi massivi di DoS (attenti ai thread).
*È consigliato l'utilizzo di un Hypervisor di macchine virtuali come **Virtualbox** o **Vmware***
*e l'utilizzo di una macchina virtuale preconfigurata come **Kali Linux** scaricabile pronta all'uso dal sito ufficiale*

PREPARAZIONE DELL'AMBIENTE

Prima di tutto bisogna entrare in VPN, la tecnologia usata dipende dalle scelte del cliente, in questo caso è OpenVPN e il profilo è scaricabile al sito:

http://sotercorp.it/vpn-soter-lab.ovpn

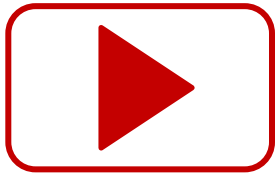
Comando per il collegamento (da terminale):

sudo openvpn vpn-soter-lab.ovpn

Verificare di essere in VPN visitando il link **http://sotercorp.it/ip.php**.
L'indirizzo IP dovrebbe essere il **18.222.225.213.** La VPN è configurata in **split-tunneling**, il traffico diretto al target passeranno dalla VPN, tutto il resto no.

Nel caso faceste delle richieste fuori dalla VPN alla macchina target non succede nulla.
Tuttavia cercate di evitarlo in quanto uscire dalla VPN corretta ci permette di essere riconosciuti come test legittimo.
In ogni caso, è permesso lanciare solo ed esclusivamente i comandi che verranno mostrati durante la lezione.

PREPARAZIONE AMBIENTE



VM, VPN e
Verifiche setup

SOTER/ITSECURITY
Beneath the surface, always

INFORMATION GATHERING

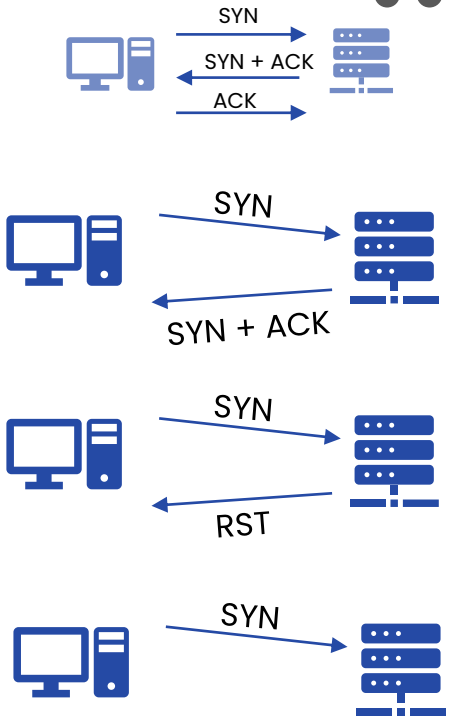
Qualsiasi dettaglio riguardo all'infrastruttura, ai servizi e alle applicazioni come il loro nome e la loro versione può fornire un vantaggio notevole. Grazie a queste informazioni è possibile arricchire la propria conoscenza rispetto al target dell'attacco/analisi e definire meglio la strategia di attacco.

Un attaccante malintenzionato ovviamente non si limiterà al «**perimetro dell'analisi**» come succede durante un **Penetration Test**, ma si potrebbe concentrare su qualsiasi cosa che lo possa aiutare ad ottenere il risultato voluto. Ad esempio colpire direttamente il computer di un dipendente di un'azienda.

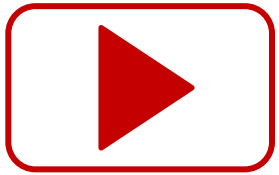
PORT SCAN SU TCP

Come si fa a capire se una porta è aperta oppure è chiusa con il protocollo TCP (Transport Control Protocol)? Connettendosi a una porta con un pacchetto SYN, si attende la risposta dal server. Abbiamo 3 casi:

- Il client riceve il pacchetto con i flag **SYN** e **ACK** entrambi attivi => la porta aperta (**open**)
- Il client riceve il pacchetto con flag **RST** (reset) attivo => la porta è chiusa (**closed**)
- Il client non riceve nulla dopo aver aspettato un tempo definito => (**filtered**) la porta potrebbe essere chiusa oppure potrebbe esserci un firewall



PRIME ANALISI



PORT SCAN E FINGERPRINTING

CREDENZIALI UTENTE

L'accesso a servizi e ad applicazioni è spesso (si spera) protetto da autenticazione, richiedendo all'utente di dimostrare la propria identità. Le informazioni richieste sono la maggior parte delle volte username e password, a volte richiedendo successivamente un secondo fattore (2FA).

Essere a conoscenza di credenziali di un utente potrebbe permettere di accedere a parti di applicazioni protette o a servizi contenenti dati sensibili. È molto frequente infatti che la stessa password venga utilizzata su più servizi/applicazioni.

*Hanno un ruolo fondamentale al giorno d'oggi i **Data Breach**, essenzialmente liste di dati degli utenti estratti dai sistemi informatici delle aziende attaccate. Per controllare se i dati collegati ad un indirizzo email fa parte di qualche data breach è possibile utilizzare il sito **https://haveibeenpwned.com/***

ATTACCHI A FORZA BRUTA

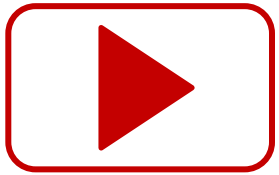
Un attacco bruteforce, o a forza bruta, prova tante combinazioni di credenziali. Se per ogni tentativo è necessario comunicare con il server viene definito **Online** invece per il «crack» di un segreto in locale viene definito **Offline**. Si può distinguere in:

- **Bruteforce puro**: tutti i caratteri in sequenza uno dopo l'altro per formare una stringa di lunghezza incrementale
- **A dizionario**: si utilizza una lista di stringhe, chiamata **wordlist**, esistente o costruita ad-hoc

Possono essere limitati da verifiche anti-automatismo come i captcha oppure da blocchi, temporanei o definitivi, all'account. In ogni caso si cerca di evitare che abbiano successo utilizzando **password solide**, forzando una password policy al momento del cambio password, fare in modo che vengano utilizzati dei **Password Manager** e utilizzando meccanismi di multi-factor authentication (tramite qualcosa che si ha).

*Nonostante sia un attacco da tenere sempre a mente e un server esposto in internet ne sia praticamente sempre vittima, è probabilmente l'ultima carta da giocare per un esperto. Un bruteforce genera in qualsiasi caso un gran numero di **eventi nei log** e potrebbe allertare qualche sistema di protezione oltre che potenzialmente bloccare un utenza.*

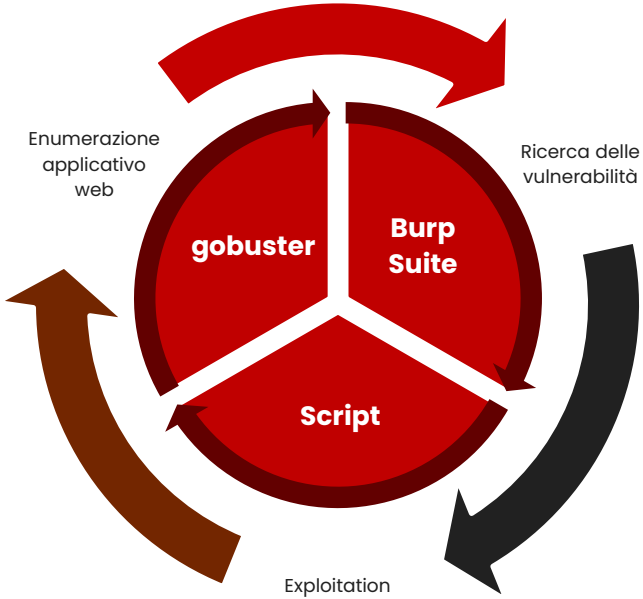
TENTATIVO DI BRUTEFORCE ONLINE



BRUTEFORCE

APPLICAZIONI WEB

Le applicazioni web sono una componente importante all'interno dei sistemi informativi. Nella maggior parte dei casi risultano complesse e di conseguenza possono avere spesso delle problematiche di sicurezza, per tale motivo sono un ottimo target per un attaccante.



VULNERABILITA' WEB

Le vulnerabilità che si possono trovare in un applicativo web possono essere molteplici e diversa tipologia. Quando si analizza un applicativo web è utile fare riferimento alla OWASP Testing Guide.

- INFORMATION GATHERING
- AUTHORIZATION TESTING
- SESSION MANAGEMENT TESTING
- INPUT VALIDATION TESTING
- CONFIGURATION AND DEPLOYMENT MANAGEMENT TESTING
- TESTING FOR ERROR HANDLING
- IDENTITY MANAGEMENT TESTING
- TESTING FOR WEAK CRYPTOGRAPHY
- AUTHENTICATION TESTING
- CLIENT SIDE TESTING
- BUSINESS LOGIC TESTING

EMAIL

Ricordare che le email sono una componente fondamentale a cui gli applicativi web spesso si appoggiano. Esse sono solitamente un anello debole della catena poiché facilmente attaccabili, poiché all'interno possono essere presenti informazioni critiche.

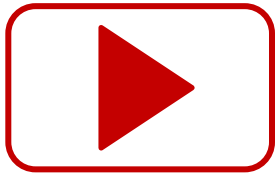
EMAIL FRAUDOLENTI

È necessario sempre proteggersi da possibili email fraudolente che possono portare ad una compromissione della rete aziendale.

DATI SENSIBILI NELLE EMAIL

Spesso, tramite le email, vengono scambiante informazioni potenzialmente sensibili, come dati finanziari o credenziali.

INTERAZIONE CON EMAIL E APPLICAZIONE WEB



WEB E EMAIL

QUIZ 1

Il port scan che abbiamo fatto è un test

a) attivo
b) passivo
c) dipende da quali parametri si usano
d) sia attivo che passivo

Quale di queste informazioni non sono presenti nel documento di manleva

a) Indirizzo IP che può condurre i test
b) Dettagli del report tecnico
c) Finestra temporale dei test
d) Il perimetro

La raccolta di informazioni sui DNS è un test

a) attivo
b) passivo
c) dipende dalla ricerca effettuata

Qual è la prima fase di un Penetration Test

a) Enumerazione
b) Exploitation
c) Ricerca di vulnerabilità

HEY OH, LET'S GO

Security Mindset

"L'unico sistema veramente sicuro è quello spento, gettato in un blocco di cemento e sigillato in una stanza piombata con delle guardie armate – e anche così ho dei dubbi"

Eugene Howard Spafford

SECTER/SECURITY
Beneath the surface, always

SOFTWARE OBSOLETO E VULNERABILE

La presenza di software obsoleto, anche se interessa solo librerie utilizzate da un software, è probabilmente il punto d'ingresso più frequente degli attacchi informatici.

Nuove vulnerabilità vengono rilasciate ogni giorno. Questo perché i ricercatori di sicurezza cercano costantemente nuove vulnerabilità in prodotti open-source e non. Si noti che esistono due modi di fare ricerca:

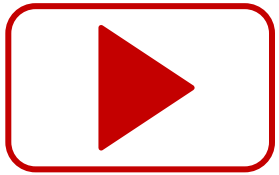
- il modo **etico:** rispettando i termini della «**responsible disclosure**», comunicando le vulnerabilità al team di sviluppo, attendendo il rilascio di una patch per poter rilasciare i dettagli al pubblico

- Il modo **anti-etico**: le vulnerabilità scoperte vengono usate per scopi malevoli oppure vendute online a portali che acquistano 0-day (zero-day) o al miglior compratore

OBIETTIVO DEL PENETRATION TEST

Il Penetration Test identifica sia vulnerabilità note in prodotti di terze parti sia vulnerabilità applicative nei prodotti di proprietà del cliente. Ad esempio in un Penetration Test Web ad un'applicazione web ha l'obiettivo di identificare vulnerabilità del software analizzato. Il software che si analizza è tipicamente un prodotto sviluppato da un applicazione cliente, oppure utilizzato dal cliente di cui si richiede una verifica, previa autorizzazione del proprietario dell'infrastruttura e degli sviluppatori.

EXPLOIT VULNERABILITA' NOTE



SPOTTING THE VULN AND EXPLOITING IT

SECTER/SECURITY
Beneath the surface, always

RISULTATI DI UN PENETRATION TEST

L'output di un test di sicurezza è quasi sempre un **Report**, un documento testuale che contiene i dettagli delle vulnerabilità individuate e informazioni riguardo al sistema analizzato.

E' solitamente composto da due parti:

- Executive summary: la prima parte di un report è più descrittiva, con pochi dettagli tecnici, ha lo scopo di rappresentare sommariamente lo stato di sicurezza di un sistema e deve essere capito anche da chi non ha skill tecniche
- Dettagli tecnici: vengono riportati i dettagli di ogni vulnerabilità attenendosi agli standard scelti (OWASP, metrica CVSS)

SECURITY
Beneath the surface, always

QUIZ 2

Il programma gobuster permette di

a) Sfruttare la vulnerabilità di SQL Injection
b) Enumerare i servizi del server
c) Enumerare le risorse ospitate sul webserver

Cosa significa privilege escalation

a) Ottenere una shell remota sul server tramite una web shell
b) Modificare i privilege associati ad un file
c) Elevare i propri privilegi per a quelli di un utente amministratore del sistema

La vulnerabilità di SQL Injection vista oggi permette di

a) Estrarre file dal server
b) Estrarre informazioni dal database
c) Creare file sul server

Cosa succede se un binario ha il setuid impostato

a) Non ha più i permessi di esecuzione
b) Un utente normale non può più eseguire il binario
c) L'esecuzione del binario verrà fatta con privilegi amministrativi

FINE – Q&A

GRAZIE PER L'ATTENZIONE!
DOMANDE?

SECTER/SECURITY
Beneath the surface, always

LET'S GO

Security Mindset

"L'unico sistema veramente sicuro è quello spento, gettato in un blocco di cemento e sigillato in una stanza piombata con delle guardie armate – e anche così ho dei dubbi"

Eugene Howard Spafford

SECTER/SECURITY
Beneath the surface, always