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

Vincenzo Calabrò

Introduzione

Definizioni

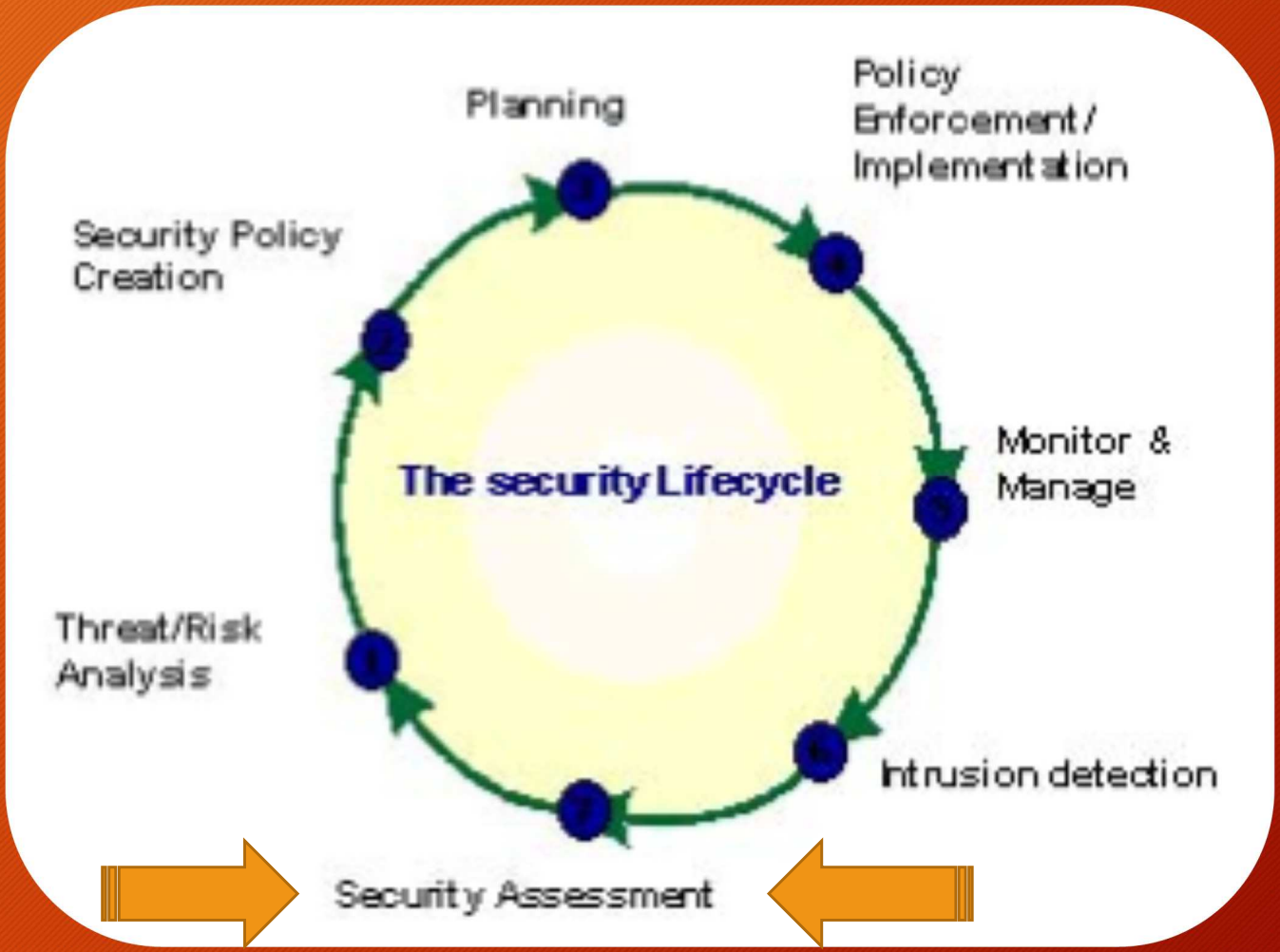
Metodologie

Obiettivo

Agenda

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

"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:

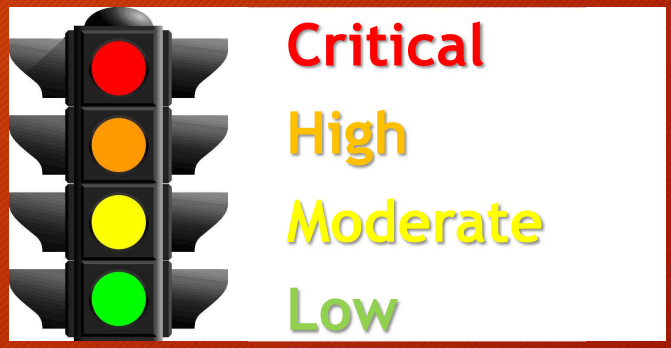
- Requirement Study and Situation Analysis
- Security policy creation and update
- Document Review
- Risk Identification
- Vulnerability Scan
- Data Analysis
- Report & Briefing

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:



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.

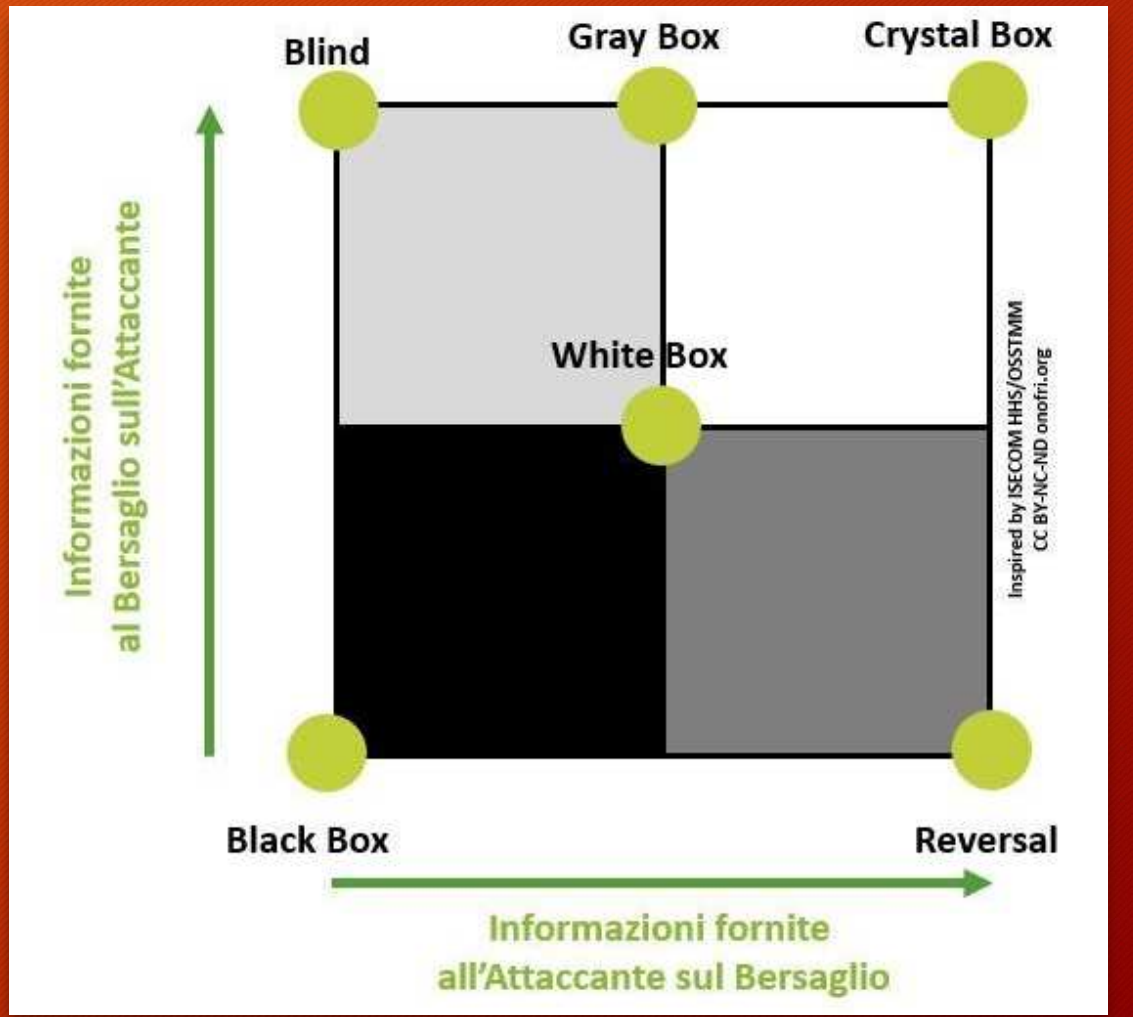
Penetration test interni o esterni, bianchi o neri

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 }

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 8 GB di RAM Minimo 40 GB di Spazio libero su HD	

Lab Schema Virtuale

Target
Server
Linux

Target
Workstation
Windows

Target
Server
Windows

Workstation Kali

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: **NAT (per lavorare come singola WS)**
       HOST (per lavorare con più WS)

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:

- **Windows Server 2008 R2 x64 / Windows 10 Enteprise**
  Windows Server 2000 / Windows XP Professional
  [http://www.microsoft.com]
- **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]

Deploy Targets in WMware

1. Eseguire un'altra sessione di WMware Workstation Player
2. Selezionare il target da provare:
    1. Scompattare l'immagine virtuale scelta
    2. Selezionare «**Open a Virtual Machine**»
    3. Aprire il File «**XXXX.vmx**» o «**XXXX.ovf**»
3. Configurare i seguenti parametri
    1. Memory: 2 GB - Processors: 2 – Hard Disk: 30 GB
    2. Network Adapter: **HOST (per lavorare con più WS)**
4. **Accedere alla nuova macchina virtuale**
    1. Controllare l'indirizzo ip
        - Linux «**ifconfig**»
        - Windows «**ipconfig**»

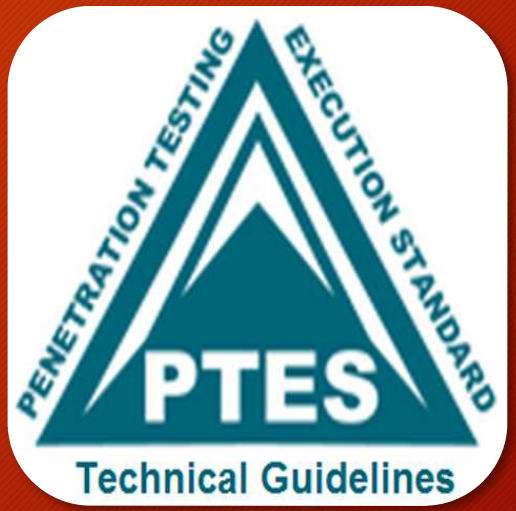
Implementazione del penetration testing

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 è quello di raccogliere più informazioni possibili sul target e produrre un documento utile alla pianificazione della strategia del test:

- When doing a black-box assessment
- Verify (or expand) the scope
- Find targets on the cloud and get authorization to test
- Gather info for testing authentication
- Gather info for social engineering
- Gather technical info on network targets

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

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

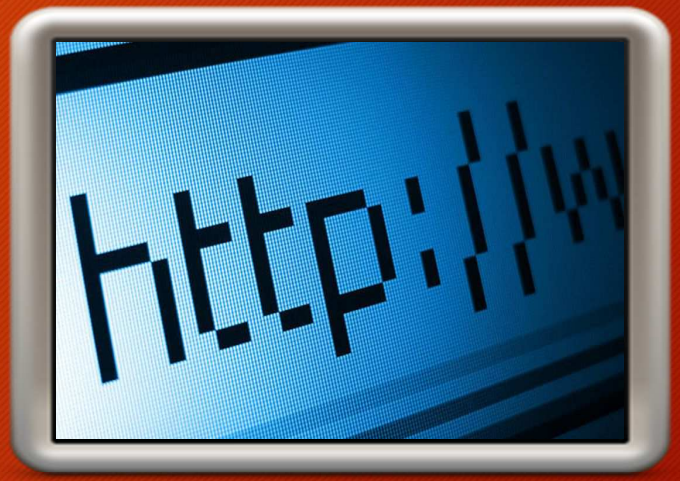
Intelligence Gathering

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.) oppure interrogando il target con tools non «invasivi»

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



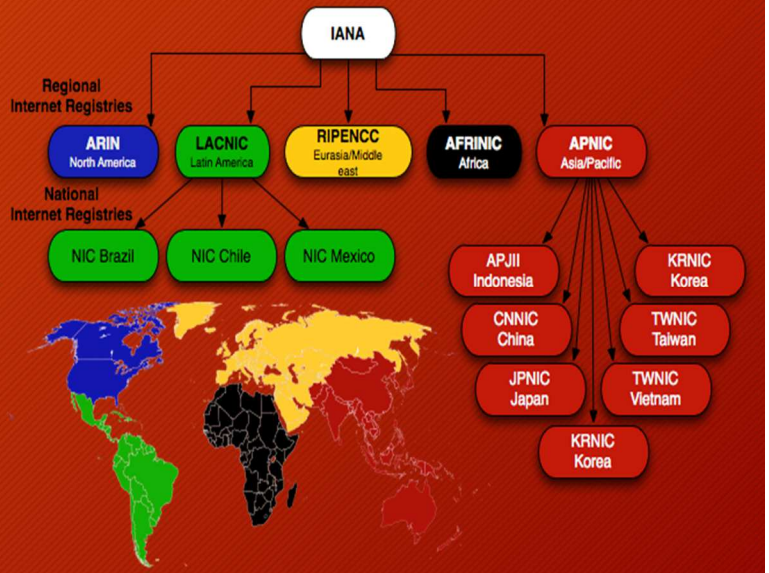
Passive Reconnaissance

OPEN SOURCE INTELLIGENCE (OSINT)

- Relies on public resources (Google, Social Network, BD esterne)
- Doesn't "touch" the target

WHOIS

- We have a domain name to start with …
- When registering a domain you provide a lot of info
- Whois – protocol used to query databases the store the info
- Where are these databases?



WHOIS SEARCH (Registry, Registrar, Registrant)

ES. 1

Tools per il Passive Recon

SEARCH ENGINE RECON

- Detailed search on target
  - Locations
  - Names
  - Telephone numbers
  - Emails
  - Subdomains
  - Etc.
- Google isn’t the only serch engine!

Expand search with Google operators

ES. 2

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"

Tools per il Passive Recon

GOOGLE HACKING DATABASE (GHDB)

- **Google dorks**: Database of query that identify sensitive data and that help us identify vulnerabilities on a web server
  - https://www.exploit-db.com/google-hacking-database

- Automatic tool: **SearchDiggity**
  - [https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/]

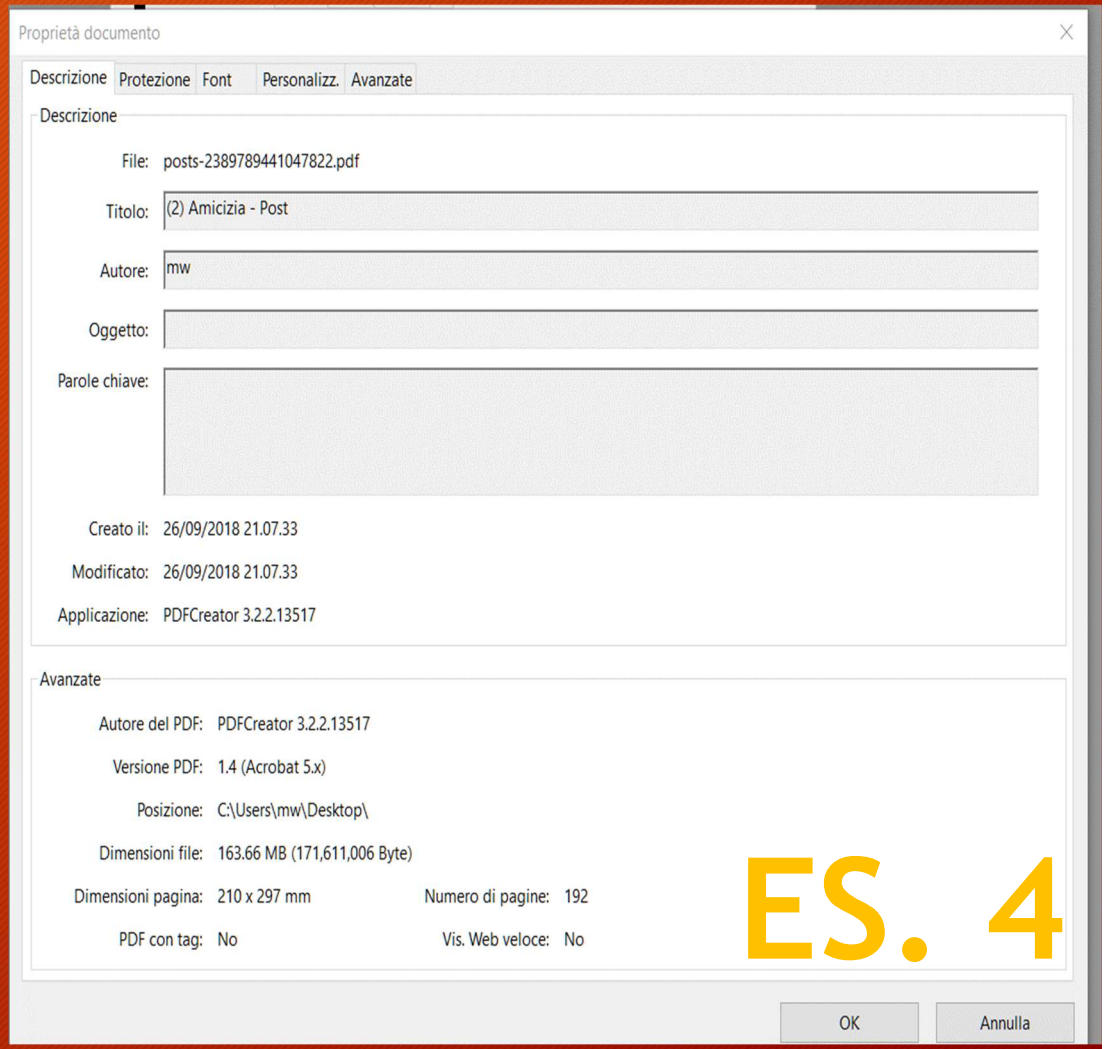
ES. 3

Tools per il Passive Recon

METADATA ANALYSIS

- Data about *data*
- **Info about author, OS, software used, etc.**
- **Useful in identifying client side exploit to use** (e.g. targeting MS Word)

- Automatic tool: FOCA
  Fingerprinting Organizations with Collected Archives



ES. 4

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

Tools per il Passive Recon

SHODAN RECON

- Search engine for Internet connected device
- Interrogates ports and grabs banner
- Require some knowledge in service banner (more on this later)

- SHODAN FILTER
  - **Country**: two letters
  - **Hostname**: specific text in hostname or domain
  - **Net**: specific IP range or subnet
  - **OS**: specific operating system
  - **Port**: specific service

https://www.shodan.io

ES. 5

Tools per il Passive Recon

EMAIL HARVESTING

- **Useful for social engineering attacks**
- **Useful for delivering client side attacks**
- **Could reveal usernames for password attacks**

es.

1. Google Search “*@domain.org” or “*@domain.org” email
2. https://hunter.io/
3. #theharvester -d domain.org -l 500 -b google/bing
4. #msfconsole auxiliary/gather/search_email_collector

ES. 6

Tools per il Passive Recon

All-in-one tool

RECON-NG

- Web recon framework
- Fully featured and interactive
- Requires APIs for certain modules

ES. 7

Active Reconnaissance

L'active reconnaissance interagisce con il Target

TARGET WEBSITE

- Review HTML source code
- Look for hidden comments <and/or ! And/or –
- Look for uninidexed files or directories

Tools

- Wget (mirror sito web su Linux)
- Httrack (mirror sito web su Windows)
- Dirb (Web server directory su Linux)
- Dirbuster (Web server directory su Windows)

ES. 8

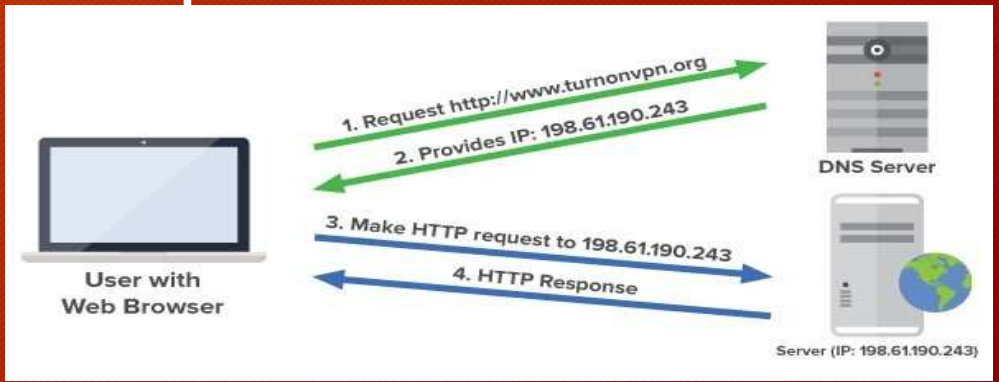
Tools per il Network Mapping

Will usually divulge DNS and Mail server information

- **A** – Address: IPV4 address record
- **AAAA** - Address: IPV6 address record
- **MX** – Mail Exchange: Mail exchange record
- **CNAME** – Alias: e.g. docs.example.com and documents.example.com return same

DNS RECON

- DNS SERVER
- LOAD BALANCER



Tools per il Network Mapping

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

Comandi

- **Ping** consente di testare se una macchina è accesa
- **Whois** è un tool che consente di ottenere le informazioni di registrazione di un dominio
- **Host** risolve l'indizzo ip di una macchina
- **Dnsrecon** consente di interrogare i DNS server
- **Dnsenum** consente di interrogare DNS server + Google
- **Fierce** individua i target esterni e interni ad una rete

ES. 9

Tools per il Network Scanning

SCANNING OBJECTIVES

- Determine live hosts, FWs, routers, etc.
- Determine network topology
- Determine open ports/runnig services and versions
- Determine OS type
- Determine potential vulnerability

Attenzione: il network scanning non autorizzato è illegale!

Tools per il Network Scanning

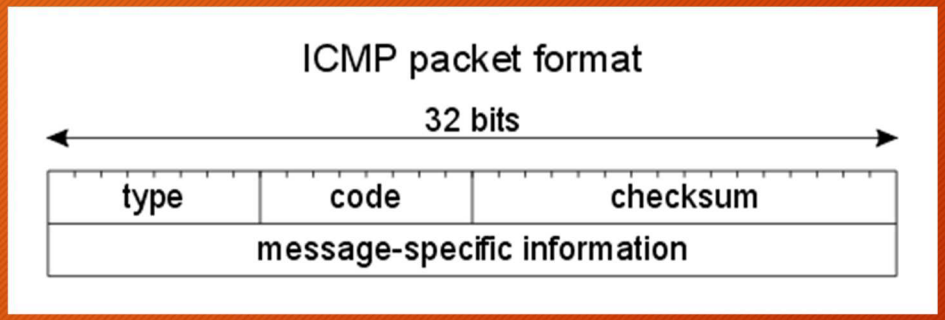
SCANNING TYPES

- Network Sweeping – Identify live hosts
- Network Tracing – Determine network topology
- Port Scanning – Discover open TCP/UDP ports/running services
- OS Fingerprinting – Determine OS type and version
- Versione Scanning – Determine version of service and protocol
- Vulnerability Scanning – Determine potential vulnerabilities

Tools per il Network Scanning

NETWORK SWEEP

- Sfrutta ICMP Packet



- Alcuni ICMP Types:
  - 0 – Echo Reply
  - 3 - Destination Unreachable
    - …
    - …
    - …
  - 8 – **Echo Request (ping)**

ES. 10

Code

0 : Network Unreachable
1 : Host Unreachable
2 : Protocol Unreachable
3 : Port Unreachable

Tools per il Network Scanning

NETWORK TRACE

- E’ utililizzato per scoprire la topologia di una rete, la presenza di router o firewall.
- Sfrutta il campo TTL (TimeToLive) dell’IP Header
- Implementiamo un ICMP Traceroute:
  - Sends ICMP Echo Request (Type 8)
  - Hop decrements TTL to 0
  - Hop replies with ICMP Time Exceeded (Type 11)
  - Final destination replies with ICMP Echo Reply (Type 0)

Tools per il Network Scanning

NETWORK SCANNING

Possible Issues

- Incoming Echo Request (Type 8) blocked
- Outgoing Echo Reply (Type 0) blocked

Solution

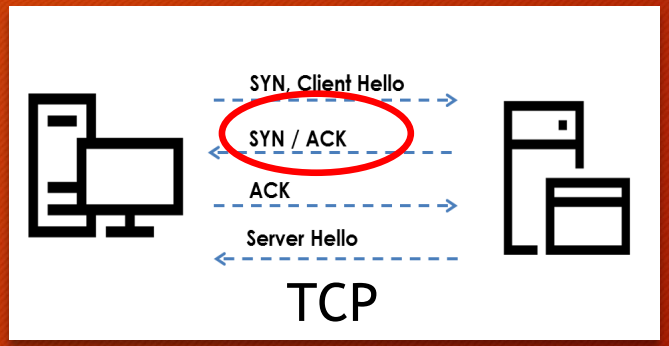
- Test for Timestamp Request (Type 13)
- Test for Address Mask Request (Type 17)
- Use other protocol

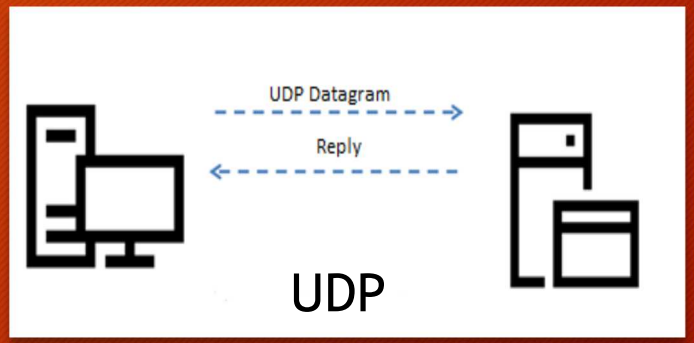
Tools per il Network Scanning

NETWORK SCANNING

Quando l'ICMP (Internet Control Message Protocol) è disabilitato, si utilizzano le TCP/UDP Handles

- **TCP is reliable**
  - correct order
  - errors in packets
  - lost packets
- **UDP is stateless**
  - fire and forget

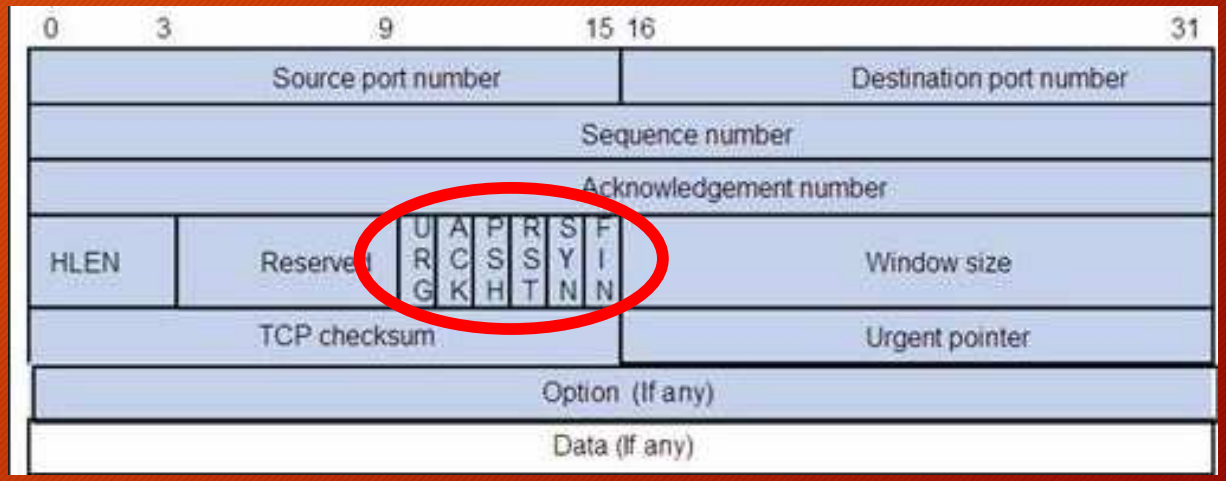




Tools per il Network Scanning

- **UDP PACKET**

- **TCP PACKET**

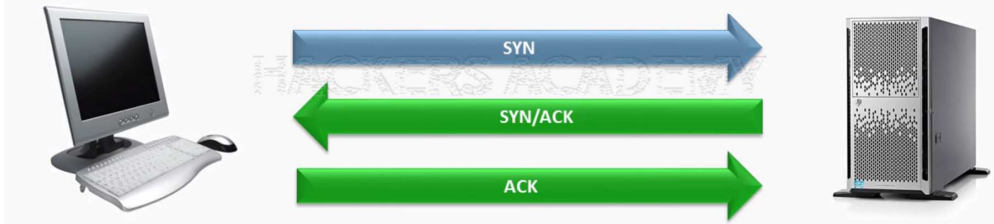


ES. 11

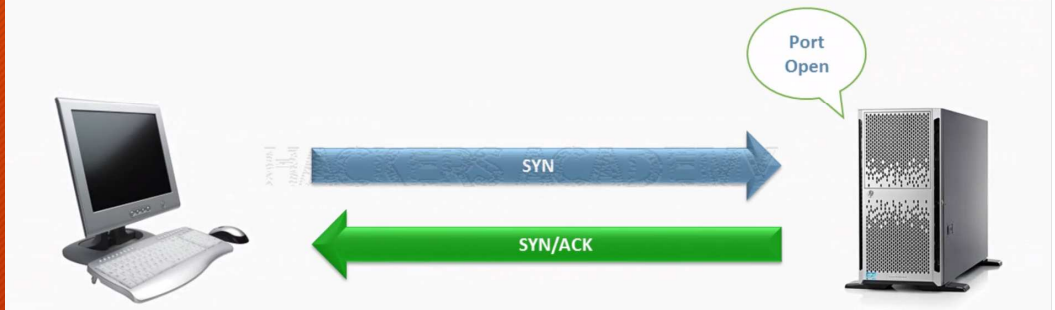
Tools per il Network Scanning

TCP Request and Reply

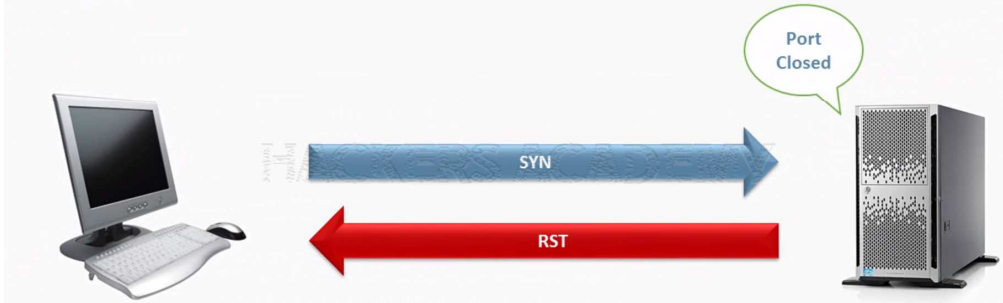
TCP CONNECT SCAN



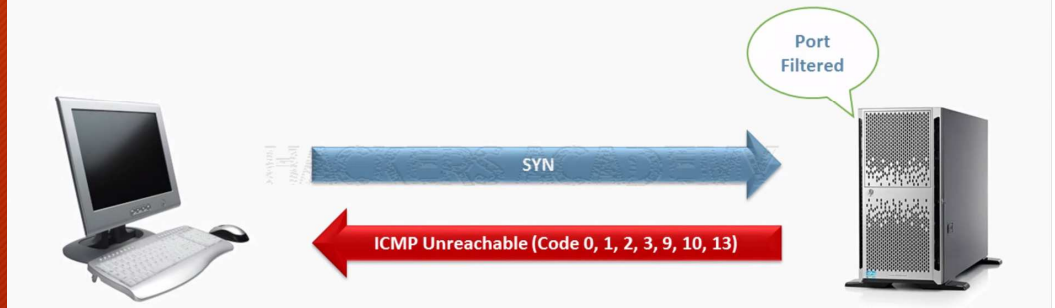
TCP SYN SCAN



TCP SYN SCAN



TCP SYN SCAN

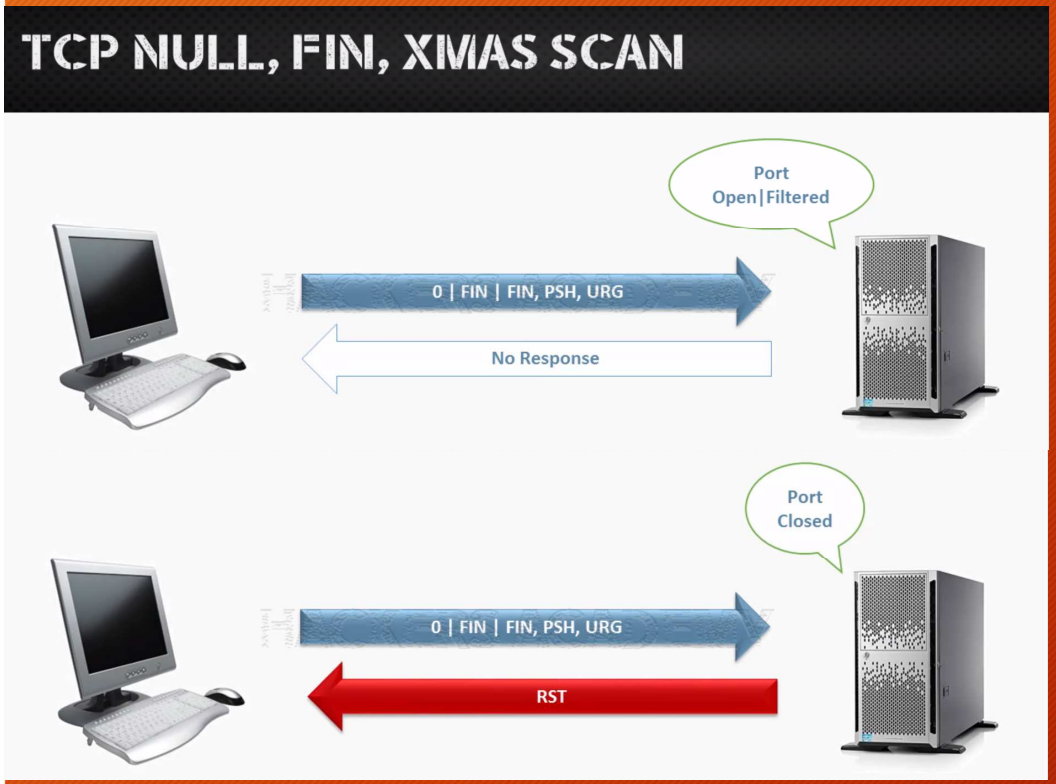


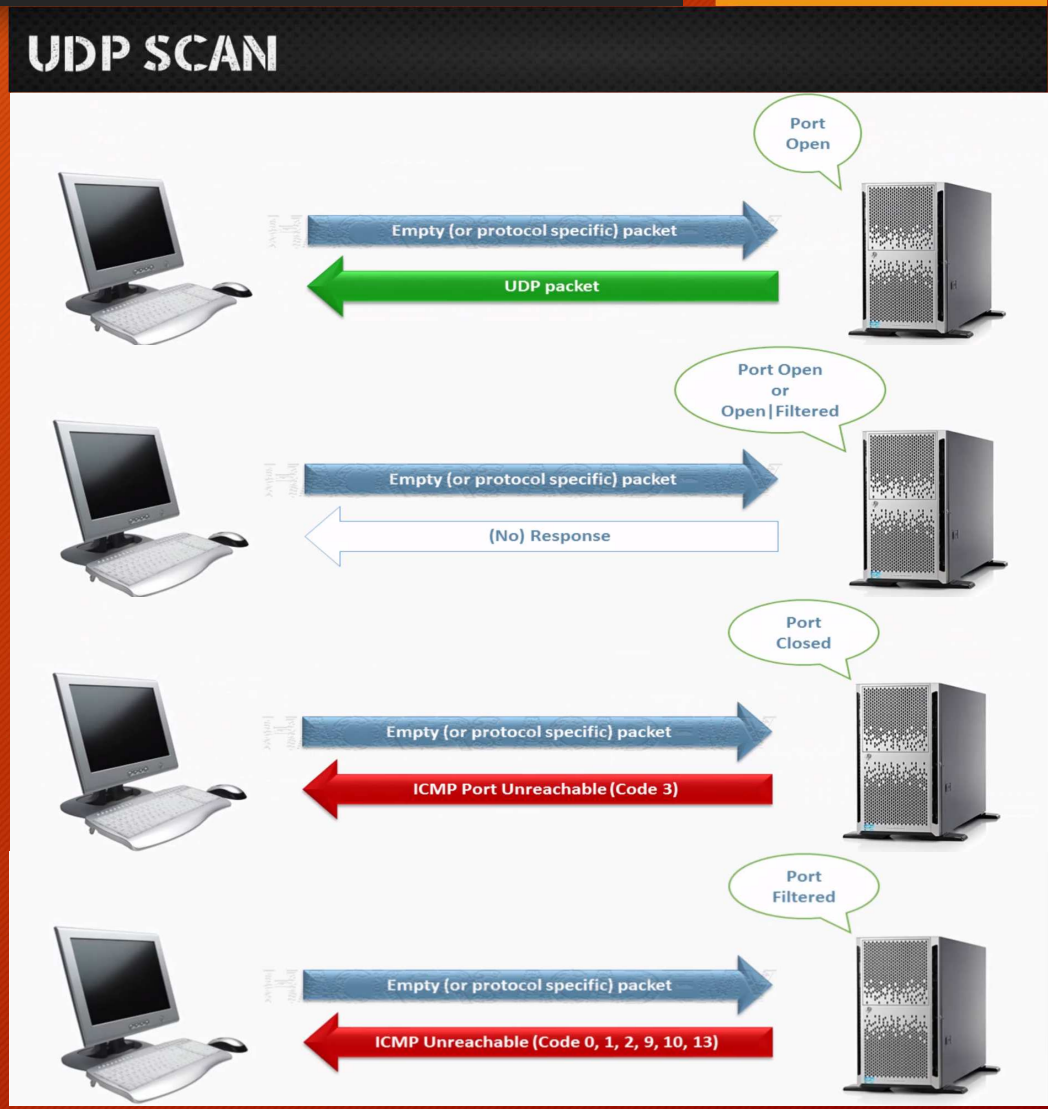
Tools per il Network Scanning

UPD Request and Reply

alternative

TCP Request and Reply



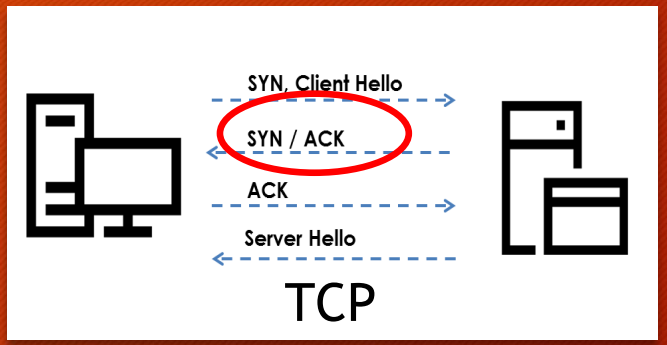


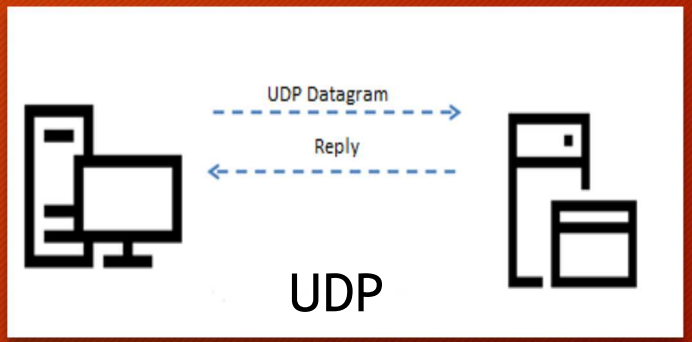
Tools per il Network Scanning

Dopo aver individuato i target dobbiamo scoprire quali ports sono aperti e quali services in «ascolto» .

PORT SCANNING

- **TCP is reliable**
  - correct order
  - errors in packets
  - lost packets
- **UDP is stateless**
  - fire and forget





ES. 12

Tools per il Network Scanning

VERSION SCANNING

- **What service is running on the open port**
  - Without version detection assumes service based on port number
  - What is the exact version of the service
  - Nmap matches response against ones in probes file /usr/share/nmap/nmap-service-probes

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.

ES. 13

Tools per il Network Scanning

OS DETECTION

ES. 14

- The more information the better
- Critical for exploitation phase
- Useful for social engineering
- Active and passive

Passive	Active
• Does not interfere in communication • Identification is based on TCP/IP communication • Could be inaccurate	• Sends various packet types and measures response • Different OSs responds differently • ***Nmap*** needs at least one open and one closed port

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»

Enumeration is:

- More intrusive
- Connect to services and retrieve information
- Enumeration techniques are platform and service specific

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

La tecnica più semplice sfrutta il «banner grabbing», si apre una connessione ad uno specifico servizio, si eseguono dei comandi e si interpreta la risposta.

Dalla risposta si può risalire ad un determinato servizio.

- **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

ES. 15

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

FTP

- File Transfer Protocol
- Typically runs on TCP port 21
- Banner grabbing
- Anonymous FTP
- Read/Write?
- Directory traversal?

SMTP

- Simple Mail Transfer Protocol
- Typically runs on TCP port 25
- **vrfy** - confirms valid users/email box
- **rcpt** - defines recipient
- **expn** - show meners of mailing list

ES. 16

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

NETBIOS

- Network Basic Input/Output System
- An Application Programming Interface (API)
- Allows computers to communicate over **LAN**
- Typically runs on TCP ports 137, 139

SMB

- Server Message Block
- Used for providing shared access to files, printers and serial ports
- Typically runs on TCP port 445
- Run over NetBIOS

ES. 17

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

HTTP/S

- Hypertext Transfer Protocol
- Usually TCP port 80. HTPPS on 443
- There's lot more to it than banner grabbing
- Crawl the website and lokk for:
  - Deleveloper comments
  - Hidden comments/notes/secrets
  - Robots.txt file
  - Etc.

SNMP

- Simple Network Management Protocol
- Tipically runs on UDP port 161
- Designed to provide info about devices, software, etc.
- Protected by password authentication

ES. 18

Tools per l'Enumeration del Web Content

NMAP SCRIPTING ENGINE

- Write and share scripts to automate network tasks
- Enumeration
- Brute force
- Vulnerability identification
- **ls /usr/share/nmap/scripts - https://nmap.org/nsedoc/**

Nmap

> nmap --script smb-os--discovery.nse ip

ES. 19

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

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

esempi
> **nmap -sT *ip*** (servizi attivi 1000 ports)
> **nmap -sT -p 1--65535 *ip*** (servizi attivi su tutti i ports)
> **nmap –sn *ip1-ipn*** ' scansiona la sottorete
> **nmap -T4 -A -v *ip*** ' analizza i primi 1000 ports aperti
> **nmap -O *ip*** ' 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 *ip*** ' controlla tutti i ports TCP
> **nmap -sU -p0-65535 *ip*** ' controlla tutti i ports UDP
> **nmap -sV -sT -p0-65535 *ip*** ' 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

ES. 20

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.)

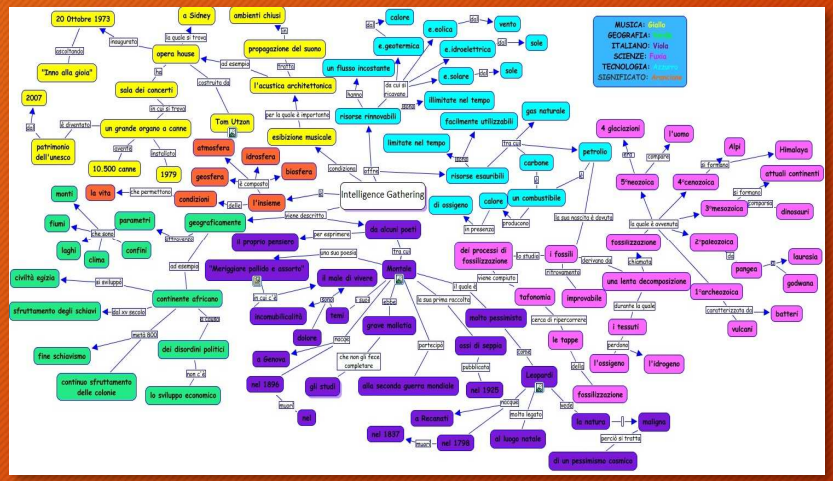
Risultato ottenuto

Abbiamo individuato il server principale: 192.168.xx.xyz

- **S.O.: Windows Server 2008 R2 Standard Edition 7601 SP 1**
- **Servizi:**

```
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
137/udp   open  netbios-ns
139/tcp   open  netbios-ssn
161/udp   open  snmp SNMPv1 server
445/tcp   open  microsoft-ds
2121/tcp  open  ccproxy-ftp
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
49155/tcp open  unknown
```

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.

Esercitazione 1

Intelligence Gathering

Intelligence Gathering: passive

1. Iniziamo a trovare info sul target tramite i motori di ricerca
2. Sfruttiamo il Google Hacking Database (GHDB) (**SearchDiggity**)
3. Meta analisi dei documenti pubblici (**FocaPro**)
4. Interroghiamo **Shodan.io** per trovare host pubblici
5. 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**
6. Apriamo il sito del target per carpire ulteriori informazioni
7. Analizziamo il sito (p.e. il codice html) e file robots.txt
8. Cerchiamo info relative al settore IT e riferimenti tecnici

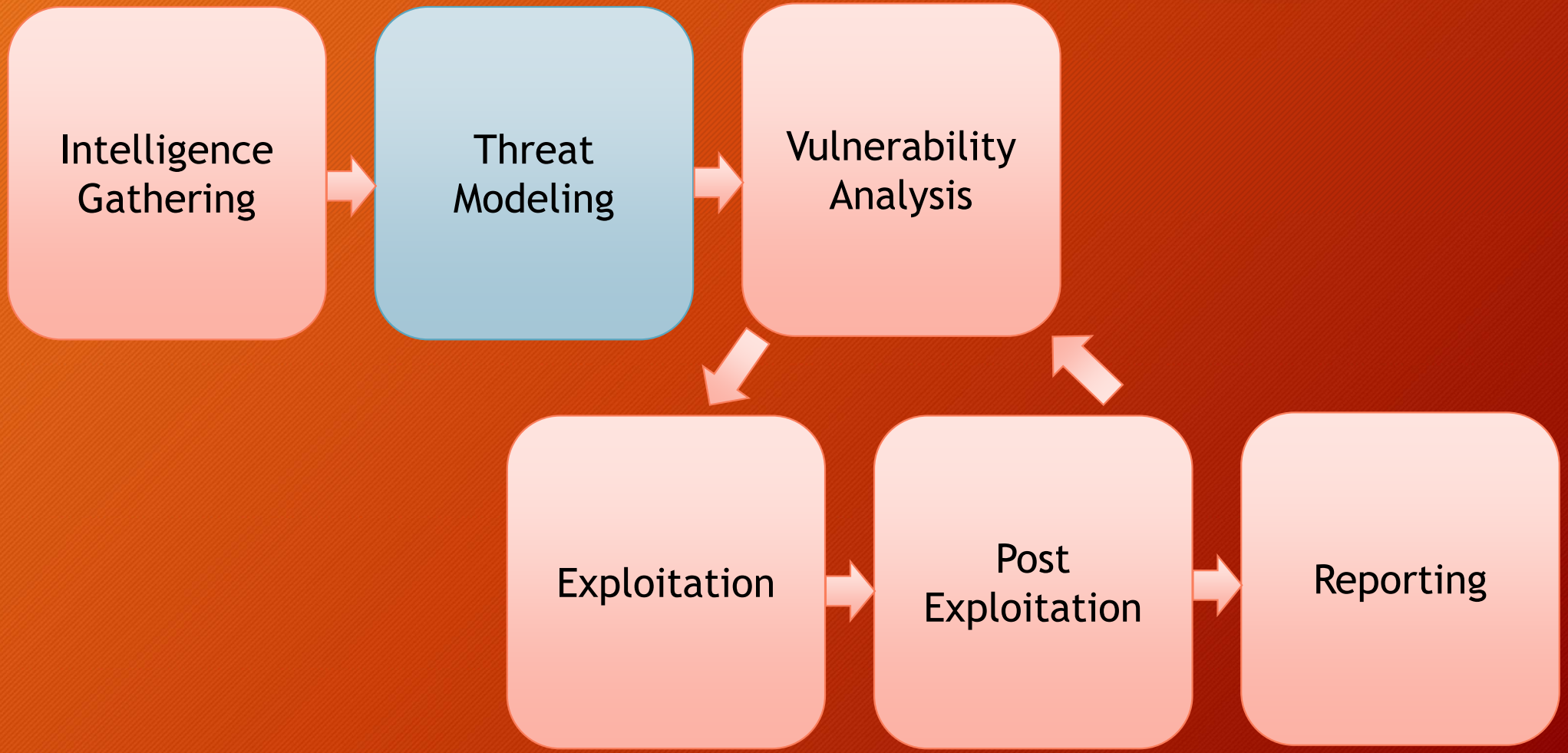
Intelligence Gathering: active

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.

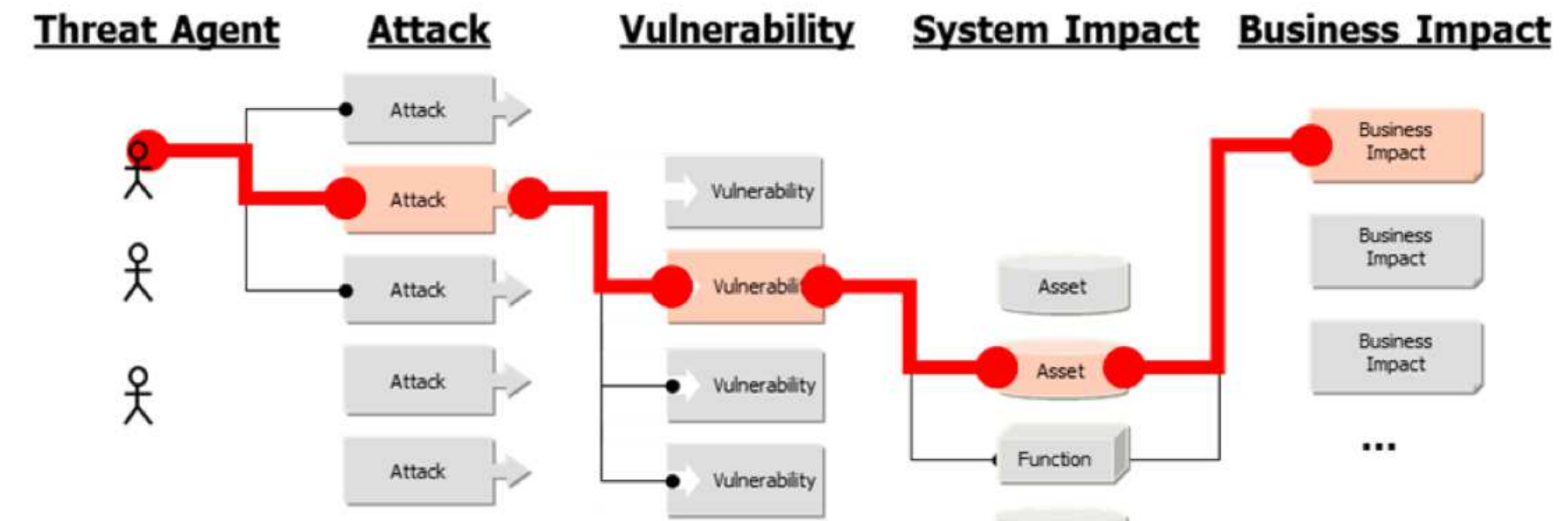
È valido per il tester e per il destinatario, poiché evidenzia la propensione al rischio e le priorità dell'organizzazione.

Il processo di modellazione può essere realizzato in più livelli:

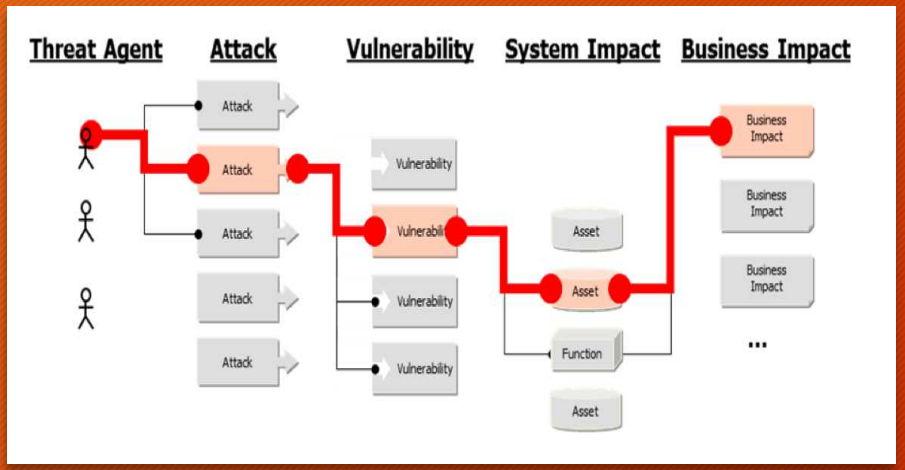
1. *Gather relevant documentation*
2. *Identify and categorize primary and secondary assets*
3. *Identify and categorize threats and threat communities*
4. *Map threat communities against primary and secondary* assets

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, in quanto 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.

Fine prima parte

vincenzo.calabro@unirc.it

linkedin.com/in/vincenzocalabro