Footprinting

Il **footprinting** è un’attività fondamentale per un hacker e consiste nella ricerca di più informazioni possibili riguardo il bersaglio da attaccare. Le informazioni possono essere raccolte in diversi modi.

Informazioni pubblicamente disponibili

1. Pagina web e sito dell’organizzazione: le pagine web della vittima offrono spesso molteplici informazioni da collezionare, in particolare nel **sorgente** della pagina si possono trovare informazioni utili come indirizzi IP o versioni dei software. Inoltre, si può procedere **enumerando** il dominio, ricercando con un approccio brute force tutte i possibili indirizzi (ad esempio, dato il dominio [www.example.com](http://www.example.com) potremmo verificare se vi è anche un dominio vpn.example.com, dato che potrebbe rappresentare un ottimo entry point). Questa operazione può essere automatizzata con strumenti quali **OWASP** **DirBuster**. Chiaramente, qualsiasi informazione disponibile sul sito web può potenzialmente essere interessante: ad esempio, una pagina di aiuto agli utenti per l’accesso alla VPN, oppure un numero di telefono di supporto tecnico potrebbero essere sfruttate anche dall’hacker, che fingendosi un utente legittimo potrebbe riuscire ad acquisire ulteriori informazioni o vantaggi.
2. Aziende partner: spesso le aziende principali commissionano a terzi le attività informatiche. Questo potrebbe essere particolarmente pericoloso (e vantaggioso per gli hacker) perché, sebbene l’azienda principale sia piuttosto attenta in tema di sicurezza, non è detto che anche il partner lo sia altrettanto, e potrebbe quindi rappresentare un ottimo **entry point**. Nella pagina web dell’azienda (o nel suo sorgente) è probabile trovare dei riferimenti all’effettivo sviluppatore.
3. Dettagli sulla sede: raccogliere dati sulla sede fisica può essere utile per pianificare attacchi fisici (ingresso fisico nella sede, tentativi di attacco alla rete wireless, ricerca di dati nella spazzatura, attacchi con pen-drive). Le informazioni possono essere raccolte attraverso il sito web dell’azienda e attraverso google maps/earth.
4. Informazioni sul personale: conoscere il personale può essere utile per una molteplicità di attacchi, sia di social engineering che informatici. Le informazioni possono essere raccolte in vario modo, tra cui le pagine gialle o i social network. Può essere anche utile analizzare le offerte di lavoro della società, al fine di captare eventuali informazioni tecniche, come il firewall o l’IDS in uso.
5. Eventi: cambiamenti all’interno della società (ammodernamenti, licenziamenti, fusioni, rapida crescita) possono destabilizzare la normale organizzazione e rendere la sicurezza trascurata in favore di altre priorità.
6. Internet archive: le vecchie pagine web archiviate, ottenute attraverso wayback machine o google cache, possono essere utili e rivelare informazioni altresì nascoste.
7. Motori di ricerca e metadati: esistono una serie di stringhe speciali che inserite in Google restituiscono output molto interessanti per un hacker. È possibile, ad esempio, cercare server che permettono una connessione desktop remoto da Internet. Inoltre, vi sono dei tool come FOCA, che permettono di ricercare documenti in un dominio web e analizzarli alla ricerca di **metadati**.

*Contromisure:* buona parte di queste informazioni sono necessariamente pubbliche. Tuttavia, è buona norma revisionare le informazioni pubblicamente disponibili e rimuovere quelle superflue.

WHOIS e DNS

I server WHOIS permettono di ricercare tutti i domini appartenenti al bersaglio. Per effettuare la ricerca si possono utilizzare tool automatizzati, oppure seguire l’albero gerarchico dall’ ICANN fino al server WHOIS di riferimento per l’organizzazione.

Una volta ottenuto l’elenco di domini posseduti da un’organizzazione si può procedere interrogando i DNS. L’interrogazione dei DNS fornisce una serie di record e di informazioni. In particolare, alcuni DNS potrebbero essere mal configurati e restituire anche gli indirizzi interni all’azienda e non esposti ad internet.

Network recoinnassance

Identificate le potenziali reti bisogna cercare di determinare le loro topologie.

Il tool per eccellenza per questo tipo di attività è **traceroute**. Esso invia dei pacchetti con TTL incrementale nella speranza di ricevere un ICMP-time\_exceeeded da ogni dispositivo che incontra, andando a tracciare la serie di dispositivi nel percorso. Di default il tool invia pacchetti UDP in Linux e ICMP in Windows. Esiste una versione modificata del tool che permette di scegliere la **porta**. La scelta della porta è importante perché alcuni firewall potrebbero lasciar passare solo determinate porte, come ad esempio la 53 per le query DNS. Esistono ulteriori versioni che permettono il traceroute anche su altri protocolli come TCP.

*Contromisure:* molti **IDS** presenti sul mercato riescono a individuare i traceroute. Si può inoltre limitare l’invio di pacchetti ICMP\_Time\_exceeded.

Scanning

Nel footprinting abbiamo ottenuto una visione generale e d’insieme del bersaglio, abbiamo cercato di acquisire più informazioni possibili come indirizzi IP e server DNS. In questa fase l’obiettivo diventa analizzare nel dettaglio i possibili entry points per elaborare una strategia d’attacco ben precisa e dettagliata.

# Determinare i sistemi attivi

## Ping sweep

Si invia una sequenza di ping su un blocco di indirizzi al fine di valutare quali host sono attivi e rispondono. Il ping può essere effettuato su una serie di protocolli diversi, come ICMP, TCP o UDP.

## Ricerca di host ARP

#### ARP-SCAN

Se l’attaccante si trova sullo stesso segmento di rete della vittima l’operazione più rapida da effettuare è uno scan ARP: viene richiesto il MAC address corrispondente a determinati indirizzi IP, gli host che rispondono alla richiesta sono sicuramente attivi. La scansione può essere fatta con il tool **arp-scan**, indicandogli il dominio di applicazione.

#### NMAP

Nmap è il tool per eccellenza per lo scanning. Per quanto riguarda la ricerca di host ARP, essa può essere effettuata con il parametro -PR. Solitamente non si vuole che effettui anche lo scan delle porte, pertanto si utilizza il parametro -sn. Il comando finale sarebbe: **sudo nmap -sn -PR 192.168.0.1/24**

## Ricerca di host TCP/UDP

ICMP è un protocollo molto utile in caso di diagnosi, ma può essere anche molto utile per un hacker, pertanto viene spesso amministrato, limitato o bloccato nelle reti. A volte lo scanning può essere effettuato solo su altri protocolli come TCP o UDP. Nmap permette la ricerca delle porte su un IP, oppure la scansione di una specifica porta su un range di indirizzi con l’opzione -p.

nPing è un tool versatile per effettuare diversi tipi di scansioni. Tra queste permette anche di effettuare scansioni TCP o UDP.

Prevenzione: come prima cosa è necessario limitare il traffico ICMP al necessario, consentendo solo il ping verso specifici host in una DMZ e provenienti da specifici sorgenti (in questo modo non si intacca la funzionalità di diagnosi ma si limita quella di scanning).

# Determinare i servizi in ascolto

Fin’ora abbiamo determinato i sistemi attivi, ora bisogna andare a vedere quali servizi sono in esecuzione su di essi e rispondono alle richieste. Vediamo nel dettaglio le varie possibili scansioni:

Scansione TCP connect: l’attaccante effettua una connessione completa con il bersaglio, effettuando il three-way handshake (SYN; SYN/ACK; ACK). Questa scansione, a causa dei tre pacchetti scambiati, è abbastanza lenta e rumorosa, e può pertanto mettere in allerta alcuni sistemi.

Scansione SYN TCP: la scansione è “half-open”, ovvero avviene un solo scambio di pacchetti (SYN; SYN/ACK), che è sufficiente a sapere se l’host accetta connessioni. Poiché la connessione non viene effettivamente aperta ma lascia l’host in sospeso, può temporaneamente invalidare il servizio se vengono effettuate molte scansioni. Il bersaglio potrebbe anche rispondere con un pacchetto “RST/ACK”, nel qual caso la porta sarebbe chiusa.

Scansione FIN TCP: in base allo standard RFC, l’host che riceve un pacchetto FIN su una porta chiusa dovrebbe rispondere un pacchetto RST, o ignorarlo se lo riceve su una porta aperta. Molti sistemi non seguono questa norma, rendendo questa scansione efficace solo per alcuni sistemi Unix.

Scansione Xmas Tree TCP: questa scansione invia un pacchetto FIN, URG e PUSH. In base allo standard RFC il bersaglio dovrebbe rispondere con un pacchetto RST sulle porte chiuse e ignorare i messaggi sulle porte aperte.

Scansione ACK TCP: vengono inviati dei pacchetti ACK in direzione della rete. Lo standard RFC prevede che se si riceve un pacchetto ACK non richiesto bisogna rispondere con RST. In genere, un firewall stateless non può bloccare i pacchetti ACK, essendo necessari per il corretto funzionamento delle connessioni, mentre un firewall stateful può bloccarli in base allo stato della connessione. Questa scansione permette quindi di comprendere che tipo di firewall è in uso nella rete bersaglio.

Scansione null TCP: si invia un pacchetto con tutti flag nulli. In base all’RFC l’host dovrebbe restituire un RST su tutte le porte chiuse.

Scansione di finestre TCP: sfrutta dei dettagli implementatici di alcuni sistemi per differenziare porte aperte e chiuse. Analizza il campo “window” dei pacchetti RST ricevuti. Alcuni sistemi utilizzano un valore positivo per le porte aperte e un valore nullo per quelle chiuse.

Scansione RCP TCP: tecnica specifica per sistemi UNIX che ricerca le porte RPC (Remote procedure call) e i relativi programmi e versioni software.

Scansione UDP: si invia un pacchetto UDP ad una porta, se il bersaglio risponde con ICMP port unreachable allora è chiusa, altrimenti si può dedurre che è aperta. Spesso i pacchetti UDP possono essere filtrati, pertanto non ricevere una risposta non è necessariamente indice di porta aperta.

# Rilevamento del sistema operativo

Molte vulnerabilità sono presenti solamente in specifiche versioni di un software e di un sistema operativo, pertanto tanto per un attaccante quanto per un pentester è importante conoscere il sistema operativo in esecuzione nella macchina bersaglio. Come prima cosa si può partire dalle tecniche di scansione dei servizi (utilizzando nmap), dai quali si possono dedurre diverse informazioni sul sistema operativo (ad esempio alcuni servizi esistono solo nel mondo Windows o Linux, o alcuni sistemi operativi hanno specifiche peculiarità). La tecnica più dettagliata è invece detta **stack fingerprinting**, e si effettua attraverso Nmap.

#### Ipotesi basate sulle porte disponibili

Partendo da un port scan si possono effettuare diverse supposizioni. I sistemi Windows sono tutti in ascolto sulle porte 135, 139 e 445 (i sistemi con Windows 95/98 solamente sulla 139). Molti sistemi UNIX datati espongono le porte 111 e diverse porte “alte” oltre la 3277. Inoltre, i sistemi UNIX possono esporre RPC o NFS.

#### Stack fingerprinting

I diversi produttori software durante lo sviluppo di uno stack TCP/IP hanno seguito le indicazioni dell’RFC interpretandole diversamente. Questo si traduce, praticamente, in minime differenze nei pacchetti dello stack, ininfluenti dal punto di vista funzionale, ma presenti e, pertanto, rilevabili. Nmap può facilmente rilevare la versione del sistema operativo nel bersaglio in questo modo, disponendo di diverse possibilità:

* Fin Probe: sebbene le direttive RFC suggeriscano di **non rispondere** in caso di pacchetto FIN non opportuno diretto a una porta aperta, molte implementazioni dello stack (come quelle da Windows Vista in poi) rispondono con un FIN/ACK.
* Bogus Flag Probe: si imposta un flag TCP undefined nell’header TCP di un pacchetto SYN. Alcuni sistemi operativi, come Linux, rispondono con lo stesso flag nel pacchetto di risposta.
* ISN sampling: nelle connessioni TCP gli host devono generare un sequence number (un identificativo della connessione). A seconda delle implementazioni tale valore viene generato in maniera differente. Campionandolo si può riuscire a risalire al modo con cui è stato generato, e, di conseguenza, al sistema operativo corrispondente.
* “Don’t fragment bit” monitoring: Alcuni sistemi operativi impostano questo campo di default per migliorare le prestazioni
* TCP initial window size: si tiene traccia di questo valore. Per alcuni sistemi operativi questo valore è **unico**.
* ACK value: alcune implementazioni inviano gli ACK con lo stesso sequence number della richiesta, altre invece lo incrementano di 1.
* ICMP error messages limitation: alcuni sistemi operativi seguono una direttiva RFC che suggerisce di limitare il numero di messaggi di errore da inviare. Contare la frequenza dei messaggi di errore può ricondurre al sistema operativo.
* ICMP message quoting: le diverse implementazioni di ICMP includono diverse informazioni nei messaggi.
* Error message Integrity: alcune versioni dei SO modificano alcuni campi dell’header quando restituiscono messaggi di errore ICMP.
* TOS (Type of service): per i messaggi “PORT UNREACHABLE” si esamina il campo TOS: molte versioni impostano 0, ma non tutte.
* Fragmentation handling: diverse versioni gestiscono pacchetti parzialmente sovrapposti diversamente. Alcuni sovrascrivono i dati, altri mantengono quelli del pacchetto precedente.
* TCP options: l’RFC 1323 ha esteso le direttive per quanto riguarda le opzioni nei pacchetti TCP rispetto alle direttive RFC 793.

**L’utility nMap utilizza le tecniche appena citate per rilevare il sistema operativo specificando l’opzione -0.**

***Contromisure:*** queste attività generano abbastanza rumore nella rete da poter essere rilevate abbastanza facilmente. Tuttavia, la loro prevenzione è piuttosto complicata. Agire direttamente sul sistema operativo per cambiare i suoi comportamenti è un’attività complessa e scarsamente attuabile. La contromisura più efficace è porre il sistema dietro un firewall robusto e ben configurato.

#### Identificazione passiva del sistema operativo

Le tecniche precedenti inviano specifiche sequenze o tipologie di pacchetti e possono pertanto essere rilevate da un IDS. Talvolta può essere utile adottare un approccio passivo. Questo approccio richiede che l’attaccante sia in grado di intercettare il traffico nella rete, e che quindi disponga di una posizione centrale nella rete o di una duplicazione del traffico in una porta monitor. Alcune **passive signatures** sono:

* TTL: che valore di TTL imposta il sistema operativo nei pacchetti in uscita
* Window size: che valore di dimensione della finestra imposta il sistema operativo nei pacchetti in uscita
* Don’t fragment: il sistema imposta questa flag?

# Elaborare e memorizzare i dati di una scansione

Organizzare i dati acquisiti è cruciale per ottenere un’analisi migliore e più dettagliata.

#### Gestione dei dati con metasploit

Metasploit è in grado di interagire autonomamente con un DB Postgres e collezionarci i dati acquisiti. Ad esempio, attraverso l’utility db\_nmap permette di utilizzare nmap e salva automaticamente il risultato delle scansioni. I risultati salvati nel db si possono poi recuperare ed analizzare a seconda delle necessità.

Enumerazione

L’attività di enumerazione differisce dallo scanning poiché decisamente più intrusiva. Essa mira, infatti, ad una completa conoscenza del bersaglio, anche tramite molteplici connessioni e interrogazioni dirette. Questa fase poiché più rumorosa è anche più rilevabile.

Le tecniche di enumerazione dipendono strettamente dal servizio e dalla specifica implementazione di esso (rilevato attraverso lo scanning nella fase precedente). In genere, l’enumerazione ha lo scopo di acquisire informazioni cruciali per accedere ai sistemi od ottenere privilegi, come nomi utente, file condivisi erroneamente o software non aggiornati.

## Fingerprinting di servizi

Come visto in precedenza, nmap ad ogni scansione indica il servizio associato. Tuttavia durante le scansioni classiche (come ad esempio SYN scan, opzione -sS) il servizio viene ipotizzato principalmente sulla base della porta in ascolto: chiaramente, se un servizio (ad esempio SSH) è configurato su una porta custom, l’intuizione di nmap sarà errata. Effettuando invece la scansione con l’opzione -sV nmap effettua una serie di interrogazioni a tutte le porte, risalendo all’effettivo servizio in esecuzione con molta più precisione. Si noti che questa scansione tende ad essere decisamente più rumorosa.

## Scanner di vulnerabilità

Sul mercato esistono molteplici scanner di vulnerabilità, come Nessus, che hanno a disposizione un database enorme di vulnerabilità ed effettuano automaticamente la scansione sul sistema alla ricerca di esse. Un attaccante potrebbe sfruttarli per ricercare delle vulnerabilità. Questa attività è chiaramente intrusiva e rumorosa, pertanto può essere effettuata solamente quando non sono predisposti dispositivi di rilevamento intrusioni oppure non c’è bisogno di preoccuparsene.

Anche nmap dispone di una simile funzionalità: offre la possibilità di eseguire degli script (in linguaggio Lua) che possono anche effettuare scansioni di vulnerabilità. Ciò è possibile con l’opzione –script <nome\_script> o con l’opzione -sC per eseguire una serie di script di default che effettuano ricerca di versionoi, vulnerabilità e backdoors.

## Banner grabbing

La tecnica di banner grabbing consiste semplicemente nel connettersi ai servizi remoti ed osservarne l’output. Questa tecnica può essere effettuata tramite telnet o netcat.

Con telnet si apre una connessione con l’host sulla porta interessata e si osserva la risposta, ad esempio se si cerca di aprire una connessione telnet sulla porta 80, con altissima probabilità si riceve un messaggio di errore, solitamente indicante anche il server o la sua versione.

Lo stesso si può effettuare con netcat: si apre una connessione su quella porta e gli si inviano dei dati; molto probabilmente si riceverà un messaggio di errore, comprensivo anche di tipologia del server e versione.

## Enumerazione dei servizi di rete comuni

#### Enumerazione di FTP (TCP21)

L’ enumerazione di un server FTP è semplicissima: basta connettersi come utenti pubblici (solitamente con la user “anonymous”) ad un server e visualizzare la lista delle cartelle.

*Contromisure:* FTP dovrebbe essere disattivato, al suo posto bisogna utilizzare le versioni sicure che usano SSH o TLS.

#### Enumerazione di telnet (TCP 23)

Telnet (ormai scarsamente utilizzato) è un servizio di controllo remoto dei sistemi che trasmette i dati in chiaro. In primis, un hacker potrebbe sniffare il traffico ed intercettare le credenziali di accesso, ma può essere anche usato per l’enumerazione del sistema.

Telnet, infatti, all’avvio della connessione mostra un banner di benvenuto, differente da producer a producer. Questo significa che si può risalire facilmente al tipo di dispositivo su cui è in esecuzione (ad esempio un router) ed agire di conseguenza. Alcuni client telnet non richiedono una combinazione user-password, ma solamente una password, per la quale si potrebbe tentare un bruteforce.

Per quelli che richiedono anche una username, bisogna prima enumerare i possibili account esistenti: telnet mostra diversi messaggi di errore tra il caso in cui l’account esista ma la password è sbagliata e quello in cui l’account non esiste affatto. Un hacker può quindi prima enumerare i possibili account e poi provare un bruteforce su quelli esistenti.

*Contromisure:* telnet andrebbe disattivato ed usato SSH in suo favore. Quando non possibile si possono generalizzare i messaggi di errore.

#### Enumerazione di SMTP (TCP 25)

I server SMTP mettono a disposizione due comandi per verificare e mostrare informazioni sugli utenti del dominio. Il comando VRFY permette di verificare se un utente è valido nel dominio, il comando EXPN mostra più informazioni su di un utente valido. Questi due comandi possono essere sfruttati da un attaccante per ricercare nomi utenti validi.

*Contromisure:* versioni aggiornate di quasi tutti i software SMTP permettono di impedire l’utilizzo di questi due comandi ad utenti non autorizzati.

#### Enumerazione del DNS (TCP/UDP 53)

Enumerazione con trasferimenti di zona: un server DNS malconfigurato potrebbe effettuare trasferimenti di zona verso DNS pubblici, rendendo di pubblico accesso diverse informazioni interessanti per un hacker, come gli host interni. Nel caso in cui il bersaglio utilizzi Microsoft Active Directory si potrebbero trovare ulteriori informazioni come gli host responsabili per specifici servizi (ad esempio WWW su server x ecc). Per provare a visualizzare queste informazioni basta fare una query DNS con nslookup chiedendo del dominio oggetto d’esame.

Enumerazione di BIND: BIND è un tipo di server DNS UNIX. La particolarità è che contiene un record di tipo “CHAOS” che indica la versione del software in esecuzione. L’attaccante può effettuare una query con dig (dig @host version.bind txt chaos) per richiedere tale record.

DNS Snooping: questa operazione consiste nel controllare se il record di un dominio è in cache del DNS oppure no. Nel caso lo fosse significa che è stato consultato di recente da uno degli host che usano questo server. Si verifica attraverso il campo “answer” nella risposta: se impostato a 1 allora il record è in cache, altrimenti no.

#### Enumerazione di TFTP (TCP/UDP 69)

TFTP è un protocollo di trasferimento file in chiaro e senza autenticazione. Per scaricare un file è sufficiente conoscere il suo percorso ed il suo nome. Questo fa sì che se i permessi sono malconfigurati TFTP possa permettere agli attaccanti di scaricare file riservati o di sistema, come ad esempio /etc/passwd che contiene la lista di utenti del sistema.

*Contromisure:* utilizzare un protocollo di trasferimento file più sicuro. Se TFTP è imprescindibile utilizzare TCP wrapper e limitare l’accesso tramite firewall e permessi delle directory.

#### Enumerazione di finger (TCP/UDP 79)

Protocollo di Linux che fornisce informazioni sugli utenti nel sistema e sui loro ultimi accessi. Può fornire informazioni utili all’attaccante.

*Contromisure:* non lasciare finger attivo sulla macchina. Se è proprio necessario utilizzare TCP wrappers per loggare gli accessi e un firewall.

#### Enumerazione di http (TCP 80)

L’enumerazione di http fornisce sempre una notevole quantità di informazioni agli attaccanti. Come visto in precedenza buona parte delle informazioni possono essere ricavate direttamente dal sorgente della pagina. Inoltre, con una richiesta HEAD spesso si ottengono ulteriori informazioni sul web server. Per http si può usare netcat, per https si può utilizzare openssl.

Esistono tool automatici che permettono di catturare informazioni dalle pagine web. Uno di questi è Grendel-Scan.

*Contromisure:* poiché gli attaccanti acquisiscono le informazioni dal banner IIS, cambiarlo significa cambiare le informazioni che recepiscono. Inoltre, si può utilizzare il tool Microsoft URLScan che restringe l’accesso ai banner IIS.

#### Enumerazione di MSRPC (TCP 135)

Alcuni sistemi Windows offrono la possibilità di ottenere informazioni sui servizi disponibili in RPC. Attraverso il comando epdump si possono ottenere informazioni come indirizzi IP di macchine che hanno servizi RPC disponibili. Chiaramente, gli indirizzi IP forniscono informazioni preziose all’attaccante.

*Contromisure:* la strategia migliore consiste nel limitare l’accesso alla porta 135. Alcuni servizi però necessitano di MSRPC per funzionare. La soluzione consiste nell’utilizzare un servizio di accesso, come ad esempio una VPN.

#### Enumerazione di NetBIOS (UDP 137)

NetBIOS è un servizio di risoluzione dei nomi utilizzato nelle reti Microsoft. Sebbene sia stato rimpiazzato dal DNS, è ancora attivo su alcune macchine. Esistono diversi strumenti per raccogliere informazioni da esso:

* Enumerazione tramite net view: il comando net view /domain permette di visualizzare i domini presenti nella rete. Il comando net view /domain:<nomedominio> permette di visualizzare le macchine presenti in un certo dominio.
* Nbtscan: in Linux il tool nbtstat permette di collegarsi a una macchina e ottenere la tabella di nomi NetBIOS. Nbtscan permette di applicare nbtstat a tutte le macchine della rete.

*Contromisure:* filtrare la porta 137 sui firewall, consentendone l’accesso solo da determinati host. Disattivare del tutto il servizio se non necessario. Disattivare i servizi Alerter e Messenger sugli host per evitare che vengano condivise informazioni di essi.

#### Enumerazione tramite sessione NetBIOS (TCP 139,445)

Un protocollo spesso preso di mira dagli attaccanti in ambito Windows è SMB. Se SMB è configurato senza alcuna protezione esso permette di effettuare sessioni anonime, ed attraverso esse ottenere importantissime informazioni. È possibile ad esempio:

* Enumerare i file condivisi: si possono visualizzare manualmente le risorse (con il comando net view <device>) oppure affidarsi a un tool di enumerazione come DumpSec, che automatizza il processo di apertura sessione null e richiesta delle informazioni su tutta la rete.
* Enumerazione del registro: l’accesso remoto al registro è permesso di default solamente a credenziali amministratore. Tuttavia, in caso di errata configurazione, è possibile che sia stato permesso l’accesso anche a credenziali null. Attraverso reg query <device>/<key> si può accedere alle chiavi del registro del bersagio. DumpSec fa questo processo in automatico.
* Enumerazione degli utenti: ogni macchina ha un SID (un identificativo univoco). Il SID è preceduto da tre numeri (500, 501,503 ecc) che identificano il tipo di account. Se un attaccante riesce a conoscere il SID di una macchina gli basta utilizzare SID2User per risalire al nome dell’account utente con uno specifico sid.

*Contromisure:* una buona configurazione del firewall dovrebbe impedire l’accesso alle porte 139 e 445 da dispositivi perimetrali. Inoltre, da NT4 Microsoft ha introdotto uno strumento per prevenire l’enumerazione in sessioni null senza dover disattivare il servizio SMB. Tale funzione si chiama RestrictAnonymous e disattiva buona parte delle enumerazioni possibili in sessioni null.

#### Enumerazione di SNMP (UDP 161)

Il protocollo “Simple Network Management Protocol” è concepito per fornire informazioni sulla rete. La sua sicurezza è però scarsa (richiede solo autenticazione tramite password, detta community string, che identifica il livello di permessi disponibili) e molte delle strings di default sono pubbliche. In più SNMP permette ai produttori di personalizzare alcune funzionalità e di fornire più informazioni. I sistemi Windows, ad esempio, forniscono una serie di informazioni sugli account utente in una struttura gerarchica.

*Contromisure:* al primo posto è disattivare il servizio. Quando non possibile si può migliorare la sicurezza cambiando le community strings. Si può inoltre limitare l’accesso alla porta 161 dai dispositivi perimetrali o concedere l’accesso solamente da alcuni dispositivi (quelli di gestione della rete verosimilmente).

#### Enumerazione di BGP (TCP 179)

La backbone di internet è composta da tre livelli:

* Tier 1: i più grandi provider mondiali (circa una dozzina) interconnessi in una peer network.
* Tier 2: intermediari, comprano e vendono connettività (e.g. Tiscali o Fastweb) dal tier 1. Necessitano di comprare connettività per raggiungere qualche porzione di internet.
* Tier 3: comprano connettività e la forniscono ai propri utenti

La rete di ogni provider, qualsiasi sia il livello, prende il nome di Autonomous System (AS).

Al fine di migliorare la connettività si hanno gli IXP: punti di incontro che mettono in comunicazione diverse reti tier 2 e 3, trasformando la struttura ad albero in una a grafo, permettendo di avere “scorciatoie” senza dover passare per la tier 1. I vari provider negli IXP si scambiano traffico, uno dei vari protocolli di routing utilizzati per questo scambio è BGP. Questo protocollo viene usato per guidare i pacchetti, sfruttando degli “As-numbers” (identificativi univoci degli AS).

È possibile interrogare un router pubblico con un ASN o con un IP, e ottenere l’altro. Se si interroga con un ASN si ottengono tutti gli IP associati a tale AS; questo permette di enumerare le macchine.

#### Enumerazione di LDAP (TCP,UDP 369,3268)

Active directory è il protocollo di Microsoft che contiene le informazioni sugli account e le risorse condivise di rete. Ogni macchina inserita in un dominio ha diritto ad accedere alle informazioni di Active Directory, quindi se un attaccante ha accesso, anche guest, a una delle macchine ha la possibilità di enumerare tutto il dominio interno. Per farlo, ha a disposizione un semplice tool di microsoft stessa: ldp.exe.

*Contromisure:* l’accesso ad active directory deve essere ristretto e vietato alle macchine perimetrali. In più, i permessi di accesso devono essere rivisti,

#### Enumerazione di RPC (TCP,UDP 111,32771)

Nel mondo UNIX RPC è utilizzatoda diverse applicazioni per comunicare fra di loro in rete. Il tool rpcinfo permette di enumerare i servizi RPC in ascolto sulle porte remote degli host.

*Contromisure:* utilizzare client RPC con autenticazione e filtrare le porte.

Hacking di Windows

# Attacchi con spoofing

#### Remote password guessing

Se la macchina target ha risorse condivise tramite SMB un trucco semplice ed efficace consiste nel cercare di montare tali risorse: alla richiesta delle credenziali si possono fare tentativi od effettuare un piccolo attacco a dizionario. La risorsa remota potrebbe impedire l’accesso dopo alcuni tentativi errati. Chiaramente, si può facilmente creare uno script per tentare le diverse password in un dizionario.

*Contromisure:*  tra le contromisure principali vi sono l’utilizzo di un firewall per limitare l’accesso a SMB, l’utilizzo di un firewall sull’host per limitare l’accesso ai servizi, limitare i servizi non necessari, imporre l’uso di password forti, impostare una soglia di tentativi prima del blocco dell’account (tramite le security policy) e registrare i tentativi di accesso nei log (tramite le audit policy).

#### Password sniffing

A volte una possibilità di risalire alle credenziali è data dallo sniffing dei pacchetti di autenticazione che transitano in rete. In particolare, il protocollo LAN manager di Microsoft è totalmente vulnerabile poiché si può intercettare lo scambio degli hash delle password e risalire alla loro preimmagine.

*Contromisure:* non utilizzare Microsoft LM

Anche un protocollo di autenticazione robusto come Kerberos non è immune a questi attacchi: nell’implementazione di Windows esso invia un pacchetto di preautenticazione in cui compare un testo in chiaro noto (un timestamp) cifrato con una chiave derivata dalla password dell’utente. Questo pacchetto può essere sfruttato per effettuare un attacco a forza bruta o a dizionario in locale e risalire alla password dell’utente. L’unica difesa verso questo attacco è l’utilizzo di una password robusta.

#### Man in the middle

Alcune vulnerabilità di SMB permettono di portare a termine attacchi MITM, partendo da ARP o DNS poisoning o ingannando l’utente facendolo loggare al proprio server. Lo strumento Cain fornisce diverse possibilità per tentare questo tipo di attacco.

#### Pass the hash

Questo attacco è ancora molto in voga e molto pericoloso, utilizzato principalmente per la propagazione. Richiede, infatti, di aver già compromesso una macchina. Dalla macchina compromessa (con privilegi amministrativi) si può effettuare un dump degli hash delle password delle macchine a cui essa è loggata. Questo permette all’attaccante di autenticarsi presso altre macchine e verosimilmente propagarsi in tutta la rete.

*Contromisure:* questo tipo di attacco è difficilmente mitigabile poiché intrinseco del protocollo NTLM. Una soluzione potrebbe essere l’utilizzo dell’autenticazione a due fattori ma di difficile realizzazione nella realtà.

#### Pass the ticket

Un attacco simile al precedente può essere effettuato anche in presenza di autenticazione con Kerberos. L’attaccante può accedere al ticket di autenticazione e replicarlo.

# Attacchi senza autenticazione

Le seguenti tecniche di attacco non mirano ad intercettare le credenziali, bensì a sfruttare le vulnerabilità dei servizi esposti alla rete.

#### Exploit dei servizi di rete

Esistono dei tool che permettono di sfruttare vulnerabilità note senza sforzo. Uno di essi è Metasploit, che permette anche di personalizzare l’exploit sulla base delle proprie necessità (ad esempio software della vittima, comandi remoti da eseguire, utenti specifici da attaccare).

*Contromisure:* le patches di sicurezza devono essere installate il prima possibile. Nella finestra che intercorre la pubblicazione della vulnerabilità e quella della patch è necessario disporre di fix temporanei, ad esempio limitando l’accesso alle porte interessate.

#### Exploit di end-user applications

Le applicazioni degli utenti sono spesso degli ottimi entry point, poiché presentano molte vulnerabilità facilmente sfruttabili e poco “sotto osservazione”. Un’applicazione particolarmente presa di mira in passato fu Adobe Flash Player, oggetto di numerosissime falle di sicurezza (i relativi exploit sono visibili in Metasploit).

*Contromisure:* utilizzare un firewall personale, installare tutte le patch di sicurezza, non accedere con privilegi di amministratore quando non necessario, innalzare la sicurezza delle macro in Office.

#### Device drivers exploits

L’architettura di Windows si basa sul plug-and-play: il sistema operativo lascia ad un driver specifico il compito di gestire la periferica, permettendo di semplificare di molto l’utilizzo della stessa. Questo fa si che nei sistemi vi siano una miriade di driver installati, inclusi quelli di aziende terze, non sempre sviluppati o mantenuti correttamente. Ad esempio, vi sono alcuni exploit (presenti anche in metasploit) di schede di rete Broadcom e Netgear che sfruttano un buffer overflow per ottenere remote code execution. Questo tipo di vulnerabilità può rappresentare un grave pericolo anche perché i driver solitamente lavorano a livello kernel, e dispongono quindi di privilegi elevati nel sistema.

*Contromisure:* installare gli aggiornamenti dei driver disponibili, disattivare i driver in disuso o a rischio in ambienti pericolosi. Microsoft potrebbe aver parzialmente ridotto il rischio con lo User Mode Driver Framework, un API intermedia tra driver a livello utente e kernel, che dovrebbe limitare le possibilità del driver anche in caso di exploit.

# Attacchi con autenticazione

Una volta ottenuto un qualsiasi accesso ad un sistema ci si può muovere in diversi modi.

#### Privilege escalation

In ambiente Windows vi sono diverse possibilità per aumentare il proprio livello di privilegio nel sistema. Ad esempio, uno dei primi exploit fu getadmin, ma la DLL injection è ancora utilizzata per questo tipo di attività. Il grado più alto di privilegi ottenibili è SYSTEM, ma un amministratore può facilmente raggiungerlo con una serie di piccoli trucchetti.

*Contromisure:* patches di sicurezza, restringere il login interattivo solamente agli account fidati.

# Extracting and cracking passwords

Una volta che un attaccante ha ottenuto i privilegi amministrativi nel sistema solitamente cerca di estrarre quante più informazioni possibili sul resto degli account. Solitamente la prima operazione da fare è disattivare Windows Firewall, che potrebbe rilevare e impedire diverse attività di estrazione dei dati.

#### Grabbing password hashes

Nei sistemi Windows le informazioni degli account locali sono memorizzati nel SAM (Security account manager) mentre quelle degli account di dominio in Active Directory nel controller di dominio. L’estrazione delle password dal sistema può essere effettuata con Cain (fino a Windows XP), il quale sfrutta una DLL injection in un processo in esecuzione con privilegi per estrarre gli hash.

*Contromisure:* questo tipo di attacco non presenta contromisure, bisognerebbe bloccare la possibilità di effettuare DLL injection. Tuttavia, poiché richiede i privilegi di amministratore, il problema è a monte…

#### Cracking password

Una volta ottenuti gli hash delle password si procede ad un attacco per cercare di risalire alla password vera e propria. Gli hash di LM (non più in uso da tempo) presentano delle gravi vulnerabilità che permettono di risalire alla password in pochissimo tempo. In NTLM, ovvero nelle moderne versioni di Windows Microsoft utilizza un nuovo sistema di hashing decisamente più robusto, ma non utilizza alcun “salt” nel calcolare l’hash. L’utilizzo del salt (che Linux invece implementa) sarebbe necessario per impedire attacchi con le rainbow tables (ovvero tabelle hash precalcolate): utilizzare un salt random fa sì che l’hash sia diverso anche per password uguali di utenti diversi e non permette quindi di confrontare l’hash con una tabella di hash precalcolati. Si tenga presente che è importante che l’hash utilizzato sia lento da calcolare: hash prestazionali come SHA non sono sicuri per le password perché aumentano la probabilità di riuscita di attacchi bruteforce.

Altri due attacchi verso un hash sono bruteforce e dictionary: nel primo si tentano tutte le possibili combinazioni di caratteri ammessi di una certa lunghezza, se ne calcola l’hash e lo si confronta con quello estratto, nel secondo si calcolano gli hash di una lista di parole e si confrontano con quello estratto. Le probabilità di successo di questi due attacchi dipendono esclusivamente dalla complessità della password inserita dall’utente.

*Contromisure:* utilizzare una password complessa (ad alta entropia), composta di lettere, numeri, simboli speciali. Creare delle policy di cambio password per limitare la finestra di attacco disponibile per un hacker. È importante che la policy non sia troppo restrittiva, perché potrebbe indurre gli utenti a scegliere password deboli dovendole cambiare troppo di frequente.

#### Dumping cached passwords

<TODO>

# Remote control and backdoor

#### Command-line remote control

Una volta che l’attaccante è riuscito ad entrare nel sistema può voler consolidare il suo controllo sulla macchina, ad esempio aprendo una backdoor per il controllo remoto. Per farlo può utilizzare netcat, che attraverso le opzioni “-l” (listen) “-e”(execute) “-d” (stealth mode) e specificando una porta con “-p” si può mettere in ascolto netcat su una determinata porta e fargli eseguire un programma desiderato quando riceve una connessione su quella porta.

#### GUI remote control

L’attaccante può anche connettersi all’interfaccia grafica, sfruttando il servizio di desktop remoto (porta 3389) se abilitato, oppure installando VNC, un servizio simile. L’installazione di VNC può essere molto utile, poiché richiede solamente di copiare l’eseguibile nel bersaglio e modificare alcuni parametri di configurazione per evitare che si apra un prompt all’utente.

# Port redirection

Un attaccante è in grado di sfruttare una macchina compromessa per aggirare misure di sicurezza come un firewall. Ad esempio, il firewall potrebbe bloccare ssh (porta 21) verso la macchina A, ma consentire le query DNS (porta 53) verso la macchina B. Se l’attaccante riesce a compromettere B la può configurare in maniera tale da re indirizzare tutti i pacchetti verso la porta 21 di A, senza che il firewall se ne renda conto.

Il reindirizzamento può essere effettuato in Windows attraverso il tool fpipe di McAfee: è sufficiente inserire il numero di porta da reindirizzare (ad esempio la 53), l’IP di destinazione ed eventualmente la porta sorgente (quella da cui far uscire i pacchetti reindirizzati).

# Covering tracks

Una volta che gli attaccanti si sono intrufolati nel sistema cercheranno di coprire il più possibile le proprie tracce al fine di non farsi scoprire e installeranno delle backdoor per poter accedere nuovamente al sistema.

#### Disabling auditing

L’auditing sarebbero le varie impostazioni di logging degli eventi presenti nei sistemi Windows. Un attaccante appena ottiene accesso al sistema spegne i log attraverso il comando “auditpol /disable” e li riattiva una volta terminato l’attacco con “auditpol /enable” (per lasciare meno tracce possibili).

#### Clearing the event log

Il log degli eventi può essere svuotato del tutto dall’attaccante (l’unico evento rimanente è quello della cancellazione). È possibile sia tramite il visualizzatore degli eventi di Windows che tramite il tool “elsave”.

#### Hiding filles

Gli attaccanti possono voler lasciare una serie di strumenti nel sistema. Una possibilità per nasconderli è quella di renderli dei file nascosti, attraverso il comando “attrib +h [file]”.

#### Alternate Data Strems (ADS)

NTFS permette di inserire più data streams in un file (funzionalità inserita per ragioni di compatibilità). Per accedere agli ADS bisogna utilizzare il comando [nomefile]:[ADS]. Un attaccante può nascondere il codice binario da eseguire in un ADS e lanciarlo attraverso il comando start.

# General Countermeasures to Authenticated Compromise

Se una macchina è stata compromessa con i permessi di amministratore la miglior operazione da fare è formattare e reinstallare poiché vi sono infiniti modi con cui l’attaccante potrebbe aver piazzato un backdoor. Se non si vuole formattare vi sono quattro principali aree da controllare: nomi di file, chiavi di registro, processi e porte di rete.

#### Ricerca di file sospetti

Un attaccante potrebbe aver lasciato nel sistema alcuni degli strumenti da lui utilizzati, si può provare a ricercare i più comuni come netcat o vnc. Bisogna tenere presente che i file molto spesso potrebbero essere stati rinominati e pertanto è utile effettuare una scansione con un software antivirus. Inoltre esistono strumenti che permettono di identificare se vi sono stati cambiamenti ai file di sistema.

Tra le directory che vanno assolutamente esaminate vi sono quelle relative all’avvio automatico come quelle di startup.

#### Voci del registro di sistema

Un’occhiata al registro di sistema può rivelare la presenza di alcuni software non desiderati. Ad esempio controllando in HKLM/Software e HKEY\_USERS/default/software si possono trovare le chiavi utilizzate dai software e si può scovare ad esempio la presenza di VNC.

Inoltre, nel registro di sistema sono presenti delle chiavi che permettono di avviare un programma all’avvio del computer. È bene analizzare queste chiavi per assicurarsi che sia tutto in ordine.

#### Processi

Analizzare i processi in esecuzione permette di capire se vi sono processi insoliti ed eventualmente terminarli.

#### Porte

L’utility netstat permette di visualizzare le connessioni attive o in ascolto e le relative porte. In particolare, il comando -aon mostra tutti i socket e gli indirizzi numerici.

# Windows Security features

#### Windows Firewall

Di default da Windows XP Microsoft rende attivo un firewall host based sulle macchine molto restrittivo. Tale firewall blocca di default moltissime porte in ingresso, limitando fortemente la possibilità di sfruttare certe vulnerabilità.

#### Aggiornamenti automatici

Le patch di sicurezza sono cruciali per gararntire un sistema sicuro. I sistemi Windows sono configurati di default per aggiornarsi automaticamente ed installare le più recenti patch in automatico.

#### Group policies

Questa funzionalità permette di impostare delle policy di sicurezza sia a livello locale che a livello di dominio, memorizzate nella active directory.

#### Bitlocker and EFS

EFS (Encrypted file system) è un file system sviluppato da Micrososft che permette di crifrare file o cartelle in modo trasparente. EFS è concepito per permettere sempre un recupero dei file, e necessita quindi dell’esistenza di un default recovery agent (funzionalità poi rimossa da Windows XP in poi). L’agente di recupero può essere anche un amministratore di rete, il che rende la funzionalità utile in contesti aziendali in cui gli utenti possono necessitare di criptare i file ma essi devono essere sempre recuperabili.

Le chiavi di EFS vengono memorizzate in locale, il che lo rende piuttosto fragile poiché accedendo all’hard disk da un altro sistema operativo è possibile arrivare alle chiavi.

Bitlocker è un sistema di cifratura di interi dischi rigidi. Questo sistema memorizza le chiavi localmente in maniera sicura. Esiste un attacco detto cold boot attack che permette di risalire alle chiavi aumentando il ghost time della RAM congelandole. L’attaccante spegne il computer e raffredda le RAM, riuscendo così a far rimanere i dati in essa, poi fa il boot da una pen-drive apposita per leggere una porzione di RAM ed esporta le chiavi.

Advanced persistent threats

In generale gli APT sono le minacce rappresentate dall’azione di gruppi organizzati che mirano ad un obiettivo preciso e a lungo termine, con l’obiettivo di acquisire informazioni sensibili come informazioni finanziarie, sociali, politiche o segreti industriali. Il termine APT descrive i tre aspetti che contraddistinguono questo tipo di minacce:

* Advanced: gli hacker hanno ottime conoscenze di hacking e sono in grado anche di sfruttare vulnerabilità zero-day.
* Persistent: gli hacker hanno obiettivi a lungo termine e lavorano per raggiungerli.
* Threats: rappresentano una minaccia per la sicurezza dell’organizzazione.

In generale, un APT non mira a danneggiare il sistema obiettivo, bensì a rimanere il più possibile di basso profilo e nascosto con l’obiettivo di raccogliere più informazioni possibili. Le tecniche utilizzate sono varie, e comportano anche l’utilizzo di phishing, malware realizzati ad hoc e ingegneria sociale. In generale, un APT si compone di diverse fasi:

1. Targeting: come per tutti gli attacchi, una volta individuato un obiettivo è necessario studiarlo nel minimo dettaglio per avere un piano di azione. Gli hacker studiano possibili punti di accesso e relative vulnerabilità, inviano email di phishing o fanno ingegneria sociale per collezionare informazioni utili.
2. Access/compromise: gli hacker sfruttano le informazioni raccolte per ottenere l’accesso al sistema. Ottenuto l’accesso studiano nuovamente come compromettere ulteriori sistemi come server web o DNS.
3. Reconnaissance: gli hacker effettuano una ricognizione sulla rete cercando di collezionare quante più informazioni possibili, come nomi di dominio, name server, account amministrativi ecc. Cercano inoltre di nascondere le loro operazioni disattivando i log di sistema.
4. Lateral movement: una volta individuate le informazioni giuste, gli hacker effettuano dei movimenti laterali, ovvero accedono agli altri sistemi a cui hanno accesso grazie a quanto raccolto prima.
5. Data collection and exfiltration: gli hacker collezionano i dati che desiderano e mettono in piedi una comunicazione con server esterni a cui inviarli. L’invio può essere effettuato sfruttando tecniche crittografiche personalizzate e con un approccio “goccia a goccia” oppure tutti insieme.
6. Administration and maintenance: gli hacker si occupano di mantenere il loro accesso finché richiesto, anche cercando di monitorare eventuali contromosse della vittima.

#### Operazione Aurora

Nel 2009 alcune big-tech e aziende della difesa statunitensi sono state vittima di furto di informazioni per circa 6 mesi. Questo APT sembra essere nato da alcune email di phishing con un link ad un sito web che sfruttava una vulnerabilità di Internet Explorer durante l’esecuzione di JavaScript per ottenere RCE. Questa vulnerabilità permetteva agli hacker di trasferire un trojan e attraverso di esso installare un backdoor.

# Esempi di strumenti e tecniche APT

## Attacco Gh0st

Questo attacco mirò ad governo tibetano in esilio e ad alcune imprese tibetane. Questo attacco sfruttava un sofisticato malware RAT (remote access trojan) capace di moltissime funzioni di controllo remoto, tra cui: rimozione di rootkit esistenti, file manager completo (capace di leggere file ed esplorare cartelle), controllo remoto dello schermo, shell remota, spionaggio della webcam, ascolto del microfono.

L’attacco parte con una email di phishing (contenente una finta notifica di errato pagamento) che conduce l’utente ad una pagina web. La pagina web sfruttava delle vulnerabilità per installare una backdoor persistente (in grado di sopravvivere al riavvio). La backdoor contattava poi la CC e cercava nuovi host da attaccare.

## Attacco gh0st – tecniche investigative

Vediamo nel dettaglio le operazioni di investigazione effettuate su questo attacco. Innanzitutto, gli investigatori riuscirono a risalire ad una copia della email di phishing. Da essa poterono effettuare delle analisi sul dominio del link malevolo, utilizando whois e robtex, scoprendo che l’IP era già stato associato ad alcune campagne di spam.

#### Indicatori di compromissione – raccolta dei dati

I malware sfruttano diversi meccanismi per poter sopravvivere ad un riavvio del sistema, tra cui specifiche chiavi nel registro, creazione di servizi, modifica di servizi esistenti, sovrascrittura del MBR o del BIOS. Una procedura RFC identifica l’ordine corretto con cui raccogliere i dati da analizzare sulla base della loro volatilità.

#### Immagine della memoria

La prima cosa da fare è un dump della memoria. Il dump può essere ottenuto attraverso FTK Imager e analizzato con altri tool. L’analisi della memoria è particolarmente utile perché molti strumenti utilizzati mirano a nascondersi, ma a tempo di esecuzione sono costretti a rivelare la loro vera natura. Inoltre, i dati criptati sono decrittati in memoria quando è necessaria la loro elaborazione.

#### File di paging

Allo stesso modo, i file di paging e di ibernazione contengono parte del contenuto della memoria, e sono quindi analizzabili allo stesso scopo.

#### Analisi della memoria

L’analisi può essere effettuata attraverso il tool Volatility Framework, che permette di recuperare l’elenco di processi in esecuzione, le connessioni di rete attive (ed i relativi processi che le utilizzano), le DLL in uso ed altre informazioni utili.

#### Master file table

Nei file system NTFS la master file table è una tabella contenente tutti i metadati dei file, quali date di creazione ed ultima modifica o nomi dei file. Queste informazioni possono essere importantissime durante le indagini perché permettono di ricostruire l’ordine cronologico degli eventi.

#### Rete/processi/registro

Poiché presumibilmente gli hacker hanno effettuato connessioni verso altre macchine, è importante verificarle attraverso il comando “netstat -ano”, che permette di visualizzare tutte le connessioni attive e le porte in ascolto, comprensive del PID del processo che le sta usando.

#### File hosts

Una modifica al file hosts potrebbe rappresentare effettivamente un attacco di spoofing, pertanto è bene controllare che il file non sia stato modificato.

#### Currports

Lo strumento currports rappresenta graficamente le sessioni di rete, rappresentando la connessione, il processo che la sta usando ed eventuali moduli/DLL. Ottenute tali informazioni un analista può procedere analizzando i moduli o gli eseguibili.

#### Process explorer

Process explorer permette di visualizzare informazioni importanti su di un processo in esecuzione. Permette ad esempio di visualizzare le DLL in uso, i thread in esecuzione o le connessioni di rete usate dal processo.

#### Process monitor

Process monitor permette di visualizzare tutte le interazioni con il kernel che avvengono nel sistema. Permette cioè di visualizzare accessi al registro di sistema, accessi ai file, accessi alla rete o creazioni di processi.

#### VMMap

Tool che permette di visualizzare la memoria virtuale di un processo e controllare le stringhe caricate.

#### Cache DNS

Un’occhiata alla cache DNS potrebbe fornire informazioni su possibili vettori d’accesso.

#### Registry query

Le più importanti chiavi da controllare nel registro sono run e runOnce poiché sono quelle responsabili dell’avvio automatico dei programmi. Inoltre, è utile controllare la chiave services alla ricerca di servizi strani o sospetti.

#### Operazioni pianificate

Il comando schtasks permette di vedere le operazioni pianificate nel sistema, e verificare se vi siano strani programmi o script programmati.

#### Event log

Il tool psloglist permette di visualizzare il log di eventi, inclusi i comandi lanciati da eventuali attaccanti.

#### Prefetch directory

Contiene la lista degli ultimi 128 programmi eseguiti nel sistema. Chiaramente durante un’indagine può rivelare se è stato eseguito recentemente un malware.

#### File di interesse

Una volta raccolti i file soggetti a sovrascrittura, si può passare alla raccolta dei file di interesse per l’attacco. Ad esempio il file ntuser.dat fornisce informazioni sul profilo dell’utente, mentre l’analisi dei file del desktop remoto fornisce informazioni sui server acceduti di recente.

#### Log degli antivirus

L’antivirus potrebbe essere stato abilmente compromesso per escludere dalle analisi eventuali directory contenenti un malware, oppure potrebbe aver utilizzato particolari algoritmi di packing del malware, in ogni caso è importante quindi visualizzare anche i suoi log.

# Linux APT attack

#### Indicatori di compromissione

Come prima cosa visualizziamo la cronologia dei comandi bash impartiti (bash\_history). Osserviamo inoltre le porte in ascolto con netcat. Procediamo poi con lsof a controllare i file aperti ed i servizi in ascolto.

Non c’è alcuna regola con cui un hacker può nascondere i suoi file, tuttavia alcuni dei trucchi più comuni sono RAM disks, file system virtuale /dev o cartelle temporanee come /tmp.

Il comando “ls -a -l” ci permette di visualizzare i file evidenziando eventuali caratteri speciali nella stringa. Questo potrebbe essere utile per notare alcuni file o directory dai nomi apparentemente innocui.

Se eventualmente troviamo gli script utilizzati dall’attaccante è necessario analizzarli. Una prima analisi la possiamo fare con strings, che ci restituisce tutte le stringhe trovate nel sorgente dello script.

Dagli script è necessario cercare di risalire alle operazioni effettuate dall’attaccante.

Possiamo inoltre utilizzare il comando find, che permette di fare ricerche molto specifiche su directory e file.

#### Poison Ivy

Poison ivy è stato un malware molto famoso intorno al 2010, poiché era disponibile pubblicamente in rete e anche “open source”. È stato usato anche (ma non solo) in campagne APT, diffuso attraverso email di phishing. Il tool una volta installato oltre a fornire una serie di backdoor permette il controllo remoto del dispositivo.

#### TDSS

Questo tipo di malware era particolarmente difficile da individuare e instaurava una particolare architettura: generava una serie di canali crittati con altri host vittima, creando una grande rete peer-to-peer difficile da rilevare ed utilizzabile come botnet, anche a noleggio.

Remote connectivity and VOIP hacking

# Hacking dial-up connections

#### Footprinting del numero telefonico

Il primo passo da compiere è ovviamente conoscere il numero telefonico del bersaglio. Si può partire dall’elenco telefonico, conoscere il prefisso di una determinata azienda e comporre tutti gli interni corrispondenti, oppure, tramite ingegneria sociale, cercare di ottenere il numero bersaglio da qualcuno che lo conosce interno all’azienda oppure da un operatore della compagnia telefonica. Un’altra possibilità potrebbe essere il sito web dell’azienda oppure un registro WHOIS, dove spesso si trova la voce “administrative contact”, comprensiva di nome e numero di telefono del soggetto.

#### Wardialing

Con questo termine si fa riferimento alla pratica di “bruteforcing” di un certo prefisso telefonico: l’attaccante utilizza dei tool per comporre tutti i numeri di telefono presenti in un determinato range e determina se ad uno di essi è presente un terminale informatico attaccabile. I seguenti aspetti sono da considerare riguardo il wardialing:

* Hardware: quali e quanti modem utilizzare. Bisogna scegliere un modello di modem affidabile. È utile mettere più modem in parallelo a comporre numeri per velocizzare il processo.
* Aspetti legali: in molti paesi le attività di wardialing o similari sono illegali. Quando si effettuano penetration test o simili è necessario coprire gli aspetti legali con contratti e scarichi di responsabilità.
* Costi accessori: le tariffe telefoniche sono costose, in particolare quelle internazionali. Nel caso si lavori per qualcuno è importante pianificare il possibile costo delle operazioni.
* Software: esistono tre principali tool: WarVOX, TeleSweep, PhoneSweep.

#### Brute-force script

Una volta che si possiede il risultato del wardialing, il passo successivo è classificare i vari numeri in “penetration domains”. Generalmente i domini sono definiti sulla base della facilità di exploit e sono:

* Low Hanging fruit: nessuna o scarsa autenticazione, facilmente attaccabili.
* Single authentication, unlimited attempts: vi è una password ma il modem non riattacca dopo una serie di tentativi errati
* Single authentication, limited attempts: vi è una password ed il modem riattacca dopo una serie di tentativi errati
* Dual authentication, unlimited attempts: utilizza ID e password e non riattacca
* Dual authentication, limited attempts: utilizza ID e password e riattacca.

#### Misure di sicurezza per le connessioni dial up

1. Elencare tutte le linee dial-up esistenti dell’organizzazione.
2. Posizionare tutte le connessioni dial-up in una DMZ, separata dalla rete interna da un firewall e da un IDS.
3. Rendere i numeri di telefono delle connessioni diversi da quelli dei telefoni aziendali, quindi difficili da trovare.
4. Verificare che i locali contenenti le apparecchiature siano fisicamente sicuri.
5. Monitorare i log delle connessioni, cercando per attività insolite come chiamate nelle ore notturne.
6. Non divulgare informazioni non necessarie.
7. Richiedere l’autenticazione multi-fattore.
8. Richiedere l’autenticazione con chiamata di conferma.
9. Assicurarsi che il reparto del supporto tecnico sia pienamente a conoscenza della riservatezza delle informazioni.
10. Centralizzare la fornitura della connettività dial up in un unico reparto dell’azienda.
11. Stabilire delle policy di sicurezza per questa divisione che ad esempio limitino l’accesso tramite dial-up a casi eccezionali.
12. Ripartire dal punto 1.

# Hacking di centralini telefonici

Alcuni centralini hanno sempre aperte le connessioni per la diagnostica e la manutenzione, spesso malprotette con password di default o password deboli.

# Hacking di sistemi voicemail

Molte segreterie telefoniche hanno password corte e spesso solamente numeriche, perciò facilmente indovinabili attraverso attacchi bruteforce. Tuttavia, per portarli a termine è necessario avere il numero di telefono dal quale si accede alla segreteria telefonica. Successivamente si può procedere con uno script per fare l’attacco.

# Hacking delle VPN

Per quanto riguarda le VPN IPSec, esse sono innanzitutto inizializzate attraverso il protocollo IKE, suddiviso in due fasi. La fase 1 è responsabile per l’autenticazione delle due parti e lo stabilimento di un canale sicuro tra esse. Tale fase può avvenire in due modalità: la main mode, che autentica entrambe le parti attraverso tre handshake a due vie, stabilendo anche un canale sicuro, e la aggressive mode, che invece autentica le due parti in tre messaggi ma non stabilisce un canale sicuro.

#### Google hacking for VPN

Una specifica ricerca so Google (filetype:PCF site:<dominio>) permette di trovare eventuali file di configurazione delle VPN nel dominio bersaglio. Questo fornisce un grande aiuto poiché permette di sapere che tipo di VPN è utilizzata. Inoltre, spesso nei file PCF vi possono essere memorizzate password criptate con un algoritmo debole, facilmente decrittabile.

*Contromisure:* chiaramente, i file PCF non dovrebbero essere pubblici su internet ed è bene quindi verificare che non lo siano.

#### Probing IPSec servers

Si possono utilizzare degli strumenti per determinare se la VPN IPSec è in ascolto e quali parametri utilizza. Tramite nmap si può scansionare la porta UDP500, mentre tramite ike-scan o ike-probe si possono ottenere ulteriori dettagli come la modalità IKE per la fase 1.

#### Aggressive mode attack

Attraverso ike-probe determiniamo se il bersaglio supporta l’aggressive mode. Se la risposta è affermativa possiamo catturare i messaggi di autenticazione forniti dal server ed effettuare localmente un attacco bruteforce. Durante la aggressive mode è infatti possibile intercettare un hash della PSK, e successivamente attraverso un attacco bruteforce invertire l’hash.

#### Attacco alla VPN citrix

La soluzione citrix permette di condividere non solo l’intero desktop di un sistema, ma anche solamente alcune applicazioni consentite. Il problema è che condividere solamente un’applicazione dà un falso senso di sicurezza a chi configura la VPN, perché molto spesso da applicazioni innocue di Windows si può riuscire ad arrivare ad una shell dei comandi. Di seguito alcuni esempi di come è possibile a seconda dell’applicazione disponibile:

* Guida di Windows: in molte applicazioni è presente la guida di Windows, accessibile premendo F1. Nella guida sono presenti diverse voci come “come aprire un prompt dei comandi” che permettono attraverso un click di aprire il prompt. L’attaccante non deve fare altro che aprire la guida dell’applicazione consentita e cercare in essa la voce che permette di aprire il prompt.
* Microsoft office: oltre alla già citata guida, Office (se non configurato correttamente) permette di eseguire delle macro VBA, al cui interno è possibile eseguire applicazioni tramite le API di Windows. Si può creare una macro ed eseguire cmd.exe o explorer.exe.
* Task manager: se è possibile avviarlo con ctrl+shift+esc è possibile andare su file->esegui-> ed eseguire cmd.
* Stampa: la finestra di stampa su file, come stampa in PDF, permette di navigare il file system.

*Contromisure:* Posizionare citrix in un ambiente monitorato e ristretto. Utilizzare l’autenticazione multi-fattore.

# Attacchi a VOIP

La maggior parte delle soluzioni VOIP utilizza almeno due protocolli: uno per la segnalazione ed uno per il trasporto del traffico cifrato. I protocolli di segnalazione più comuni sono H.323 e SIP. Il primo è più utilizzato ma il secondo sta prendendo piede, offrendo anche alcune funzionalità in più come l’instant messaging. Il protocollo SIP opera sulla porta TCP/UDP 5060 ed è simile ad http nel funzionamento, consentendo diverse funzionalità a seconda del “metodo” richiesto (apertura o chiusura di una comunicazione, ack ecc).

Per il trasporto solitamente si utilizza RTP, che trasporta il traffico voce codificato, in combinazione con RTCP, che si occupa di trasportare le informazioni di controllo, come il QoS.

#### Scansione SIP

Come per tutti gli attacchi, la prima cosa da fare è conoscere chi e cosa attaccare attraverso una scansione SIP, con tool come SiVuS o svmap.

#### Ricerca TFTP

Alcuni dispositivi VOIP fanno affidamento ad un server TFTP da cui recuperare la propria configurazione. Se troviamo tale server (ad esempio attraverso nmap) è possibile tentare di accedervi (anche tramite bruteforce) e recuperare tale configurazione, che può contenere anche nomi utente e password.

*Contromisure:* implementare restrizioni di accesso al server TFTP, consentendo l’accesso solo agli IP dei telefoni.

#### Enumerazione di utenti SIP

SIP è un protocollo VOIP, e pertanto permette, oltre alle già citate tecniche di wardialing manuali o automatiche, di enumerare gli utenti sfruttando il suo server. I gateway SIP possono presentare specifiche leggermente differenti a seconda dell’implementazione, ma comunque fanno filtrare alcune informazioni. L’idea di base è contattare il server chiedendo informazioni su di un utente ed osservare la risposta: tra un utente valido ed uno non valido vi sono spesso delle differenze. In più, esistono dei tool come sipscan che possono effettuare queste operazioni in automatico.

#### Interception attack

In questo attacco si procede intercettando una comunicazione tra due utenti. Il primo passo da fare è essere in grado di intercettare il traffico in transito. Per fare ciò, se non ci si trova direttamente sul canale di comunicazione, è possibile provare tecniche di redirezione del traffico come la ARP spoofing, in cui si convince qualche nodo della rete di essere il corretto next-hop per la destinazione che ci interessa. Successivamente si intercettano i pacchetti con un dumper come tcpdump o wireshark. Poi è necessario individuare il codec utilizzato: il campo media format del pacchetto SIP contiene questa informazione. Successivamente si può procedere alla decodifica con dei tools.

#### Denial of service

Si può effettuare inviando un grande numero di chiamate false che segnalino traffico (SIP INVITE)

Hacking wireless networks

# Richiami di infrastruttura

#### Avvio della sessione

Al momento della connessione il client invia un pacchetto *probe request* su tutti i canali, richiedendo il SSID desiderato. Se presente, l’access point richiesto risponde con un *probe response*. A questo punto avviene una fase di “autenticazione” che non è l’autenticazione con password ma solamente la negoziazione dei parametri di sicurezza della connessione. Al termine di questa vengono poi messi in pratica i meccanismi di sicurezza e se tutto va per il verso giusto la connessione viene avviata.

#### Meccanismi di sicurezza

* **Filtro sugli indirizzi MAC:** gli access point possono consentire l’accesso solo a degli specifici MAC address e possono quindi ignorare richieste di connessione provenienti da indirizzi non autorizzati.
* **Reti wireless nascoste:** normalmente gli access point pubblicano a intervalli regolari un beacon, ovvero un pacchetto che comunica la presenza di un certo SSID. È possibile disattivare questa funzionalità, rendendo leggermente più difficile l’individuazione dell’access point.
* **Non rispondere a probe request pubblici:** i client possono richiedere la presenza degli access point inviando un pacchetto probe request senza SSID, a cui in teoria tutti gli access point dovrebbero rispondere. È possibile non rispondere a queste richieste rendendo la rete parzialmente nascosta.

#### Autenticazione

IEEE 802.11 offre due modalità di autenticazione: PSK ed enterprise. Nella prima tutti gli utenti che si collegano alla rete condividono la stessa password, ed è necessario inserire quella per connettersi. Nella seconda un server RADIUS è responsabile della gestione delle credenziali e l’utente si limita a presentarsi con le sue credenziali aziendali.

#### Encryption

Vi sono tre diversi protocolli di encryption disponibili:

* WEP: completamente insicuro, praticamente in disuso.
* TKIP: una versione migliorata di WEP che non presenta particolari vulnerabilità (sebbene sia comunque sconsigliato).
* AES: standard più sicuro.

Le reti che offrono solamente connettività TKIP sono dette WPA, mentre quelle che offrono sia TKIP che AES sono dette WPA2.

# Strumenti

Per l’hacking delle reti wireless sono necessari alcuni strumenti particolari. Non tutte le schede di rete permettono il controllo di basso livello e pertanto non sono tutte compatibili. A volte sono necessarie delle antenne particolari che permettono di aumentare il guadagno, o un GPS per memorizzare la posizione di un determinato access point.

# Ricerca e monitoraggio di reti wireless

Per rilevare la presenza di un AP vi sono due approcci:

* Attivo: l’attaccante invia una seria di probe request e tiene nota di tutti gli AP che rispondono. Poiché solitamente le probe request vengono ignorate questa modalità risulta scarsamente efficace.
* Passivo: l’attaccante monitora la rete e annota tutti i beacon degli AP che riceve. Intercettando il traffico si può anche rilevare la presenza di una rete nascosta ed il suo SSID.

# Sniffing di reti wireless

In alcuni contesti (come ad esempio access point pubblici) il traffico di rete non viene cifrato ed è pertanto intercettabile. Se poi non vi è cifratura ad alcun livello è possibile leggere il traffico in chiaro. Per poter intercettare il traffico è necessario avere una scheda compatibile con la monitor mode. Il traffico catturato può essere visualizzato con Wireshark.

# Attacchi DOS

Il protocollo 802.11 prevede la possibilità da parte dell’AP di inviare un frame di disconnessione, ovvero comunicare al client di disconnettersi da esso. Un attaccante può forgiare tale pacchetto e forzare la disconnessione dei client dall’AP. Solitamente deve continuare ad inviare questi pacchetti per evitare che i client si riconnettano.

# Attacchi contro la cifratura

## Attacchi contro l’algoritmo WEP

Per cifrare i dati WEP utilizza la password ed un vettore di inizializzazione (IV) pseudorandom. La vulnerabilità principale è rappresentata dal fatto che l’IV è di soli 24bit e pertanto debole: in una connessione vi possono essere delle collisioni, ma può anche essere direttamente bruteforcato a seconda degli attacchi. In generale, un attacco richiede un buon numero di pacchetti intercettati ed effettua un’analisi statistica su di essi.

#### Attacco passivo

Nell’attacco passivo l’attaccante pazientemente intercetta una moltitudine di pacchetti (circa 60000) e poi tenta di risalire alla password attraverso aircrack-ng.

#### ARP replay con falsa autenticazione

Con questo attacco l’obiettivo dell’attaccante è ottenere più IV possibili nel minor tempo possibile. L’attaccante intercetta dei pacchetti cercando di individuare pacchetti ARP broadcast (riconoscibili poiché hanno MAC destination BC e dimensione fissa a 86 o 68 byte). Dopodiché li ritrasmette più e più volte all’ AP, il quale a sua volta lo inoltra ai client. Chiaramente, il numero di messaggi inviati è piuttosto alto, e questo permette di intercettare una lunga serie di IV in poco tempo.

Questo attacco per funzionare ha bisogno che i pacchetti provengano da un MAC address autenticato nella rete. È possibile intercettare un MAC valido ed utilizzarlo per l’attacco oppure effettuare la cosiddetta “false authentication”: in alcuni casi l’access point può essere configurato per consentire la connessione liberamente e stabilire successivamente i parametri di autenticazione (ovvero è permessa la connessione ma prima di poter comunicare è necessario fornire la password). Se l’attaccante si collega, anche prima di inserire la password potrebbe essere riconosciuto come valido e potrebbe pertanto riuscire ad inviare pacchetti ARP.

# Attacchi contro l’autenticazione

## Attacchi contro WPA-PSK

Poiché il protocollo non presenta particolari vulnerabilità, l’unica strada da percorrere è la possibilità di brute force della password, possibile però solamente nel caso di password deboli o brevi. L’attacco richiede di intercettare un 4-way handshake utilizzato da un client legittimo e dall’AP per connettersi. Questo perché i pacchetti dell’handshake sono tutti generati a partire dalla chiave e sono quindi necessari per sapere se la password è corretta. A questo punto si può procedere con diverse strategie come un attacco **brute force** (in cui vengono provate tutte le possibili combinazioni di caratteri di una determinata lunghezza), sfruttando aircrack-ng o soluzioni simili, oppure un attacco **a dizionario** (in cui vengono testati i valori presenti in una lista di parole). Un’ulteriore possibilità è rappresentata dalle **rainbow tables** ovvero delle tabelle di hash precalcolati, tuttavia non sono particolarmente efficaci per PSK poiché i pacchetti dell’handshake dipendono anche dall’SSID della rete, e pertanto sono utili solamente per specifici SSID. Esistono inoltre dei software che permettono di velocizzare il bruteforce sfruttando una GPU.

## Attacchi contro WPA Enterprise

La sicurezza di Enterprise dipende dalla sicurezza dello specifico protocollo EAP in uso. Per identificare il protocollo si può intercettare un handshake iniziale e attraverso wireshark risalire al tipo di protocollo.

#### LEAP

Questa tecnologia è stata sviluppata da Cisco ad inizio 2000 ma presenta una grave falla: essa utilizza un meccanismo challenge-risposta trasmesso in chiaro. Un attaccante che è in grado di intercettare entrambe può effettuare un brute-force. Questo protocollo è ormai in disuso, tuttavia anch’esso con una password piuttosto robusta sarebbe sicuro.

#### EAP-TTLS e PEAP

Questi due protocolli sono i più comuni EAP ed operano in modo molto simile: stabiliscono un tunnel TLS tra client non autenticato e server RADIUS. In questo modo l’access point (e gli sniffer) non hanno modo di vedere il contenuto della comunicazione. Le credenziali vengono trasmesse all’interno del tunnel con diversi protocolli, persino in chiaro, affidandosi alla sicurezza di TLS. L’obiettivo dell’attaccante diventa quindi quello di attaccare il tunnel. Rompere TLS al momento sembra impossibile, quello che però è possibile fare è impersonare l’access point ed il server RADIUS, ottenendo le credenziali dell’utente. Questo attacco è possibile fintanto che l’infrastruttura è configurata male ed i client non devono verificare l’identità del server RADIUS con il certificato.

Hacking di dispostivi hardware

# Accesso fisico

#### Lock bumping

Una serratura protegge l’accesso attraverso una serie di pistoncini di lunghezze diverse spinti verso il basso da molle: la chiave corretta contiene una serie di spine della lunghezza adatta ad allineare tutti i pistoncini e permettere la rotazione del cilindro esterno. Una bump key è una chiave che ha tutte le spine alla lunghezza minima: questo fa si che per una frazione di secondo i pistoncini scendendo si trovino alla giusta altezza. Con un po’ di pratica questa tecnica è in grado di aprire molte tipologie di serrature.

#### Cloning access cards

Molte strutture proteggono l’accesso attraverso badge di riconoscimento RFID o a banda magnetica.

La maggior parte delle carte a banda magnetica memorizzano le informazioni in chiaro su tre tracce di dati. È sufficiente disporre di un lettore di carte collegato ad un computer per esportare tutti i dati da esse ed eventualmente copiarli su di una nuova carta.

Le carte RFID sono più moderne e solitamente adottano alcuni meccanismi di cifratura. Spesso però questi meccanismi sono proprietari e possono presentare delle vulnerabilità: ne è il caso la metropolitana di Boston, in cui uno studente del MIT è stato in grado di clonare e generare le carte.

Per essere sicuro, un sistema RFID richiede un algoritmo crittografico considerato sicuro, ed una sua sicura implementazione. Il meccanismo di funzionamento è asimmetrico con challenge-response: il chip contiene la chiave privata, riceve una challenge quando avvicinato al sensore e risponde basandosi sulla chiave privata. Il lettore autentica la risposta attraverso la chiave pubblica.

# Hacking devices

#### Bypass ATA password

Questo meccanismo offre una sicurezza minima: richiede la password all’avvio del PC tramite il BIOS ma non cripta ne autentica i dati, si limita a proteggere l’accesso agli stessi. Molte unità però accettano il comando di aggiornamento della password senza richiedere la password originale poiché presumono che il BIOS abbiano già autenticato la password corrente. È sufficiente quindi disporre di un BIOS in grado di impostare la password ATA e di un’unità sbloccata. Si avvia il computer con l’unità sbloccata e si entra nel bios, poi si sostituisce il disco rigido con quello bloccato e si imposta la nuova password dal BIOS. Al riavvio l’unità dovrebbe richiedere la nuova password e permettere l’accesso.

# Default configurations

Alcune configurazioni di default dei dispositivi vengono rilasciate con incuria, risultando in vulnerabilità diffuse ovunque.

#### EEEPC 701

Questo netbook usciva di fabbrica con diversi servizi attivi di default, tra cui uno sfruttabile da un modulo di metasploit standard. Ogni dispositivo era vulnerabile.

#### Password standard

Molti dispositivi, come i router, escono di fabbrica con la stessa password di amministratore, rendendoli particolarmente vulnerabili. Persino dei bancomat furono affetti da questa problematica.

# Hardware devices revers engineering

## Mapping device

Il primo passo da effettuare per reversare un dispositivo hardware è la rimozione dei coperchi e delle coperture. Poi si rimuovono le protezioni fisiche presenti sui chip con solventi appositi.

La maggior parte dei circuiti integrati presenta lo schema e altre informazioni disponibili nel web. È sufficiente identificare il tipo di circuito (spesso viene stampigliato il codice identificativo su di esso) ed effettuare una ricerca sul web.

## Sniffing bus data

Le informazioni che viaggiano su di un bus hardware sono solitamente non protette, e pertanto suscettibili ad essere intercettate ed analizzate. Lo sniffing dei dati può essere un lavoro semplice o difficile a seconda del tipo di dispositivo e dell’esperienza posseduta. In generale si utilizza un analizzatore logico per visualizzare e registrare i segnali che transitano in un bus.

#### Sniffing wireless interface

Un primo passo verso l’hacking di un dispositivo wireless è conoscere il suo FCC ID, che permette di risalire ad informazioni utili come frequenze e tipo di modulazione utilizzata. A quel punto si può procedere osservando lo spettro radio dove il dispositivo comunica e demodulando il segnale, risalendo ai bit che lo compongono. Chiaramente, se il segnale è criptato correttamente i dati non saranno fruibili.

#### Firmware reversing

Molti dispositivi per funzionare necessitano di un firmware, spesso memorizzato in memorie EEEPROM. Alcuni dispositivi hanno pubblici gli aggiornamenti del firmware, scaricabili dai siti dei produttori. Essi possono essere analizzati con software come IDA pro alla ricerca di informazioni sensibili (come chiavi crittografiche o password di default) o vulnerabilità da sfruttare. A volte si trovano anche backdoor di test lasciate “involontariamente”. I firmware possono anche essere estratti direttamente dal chip, sfruttando degli EEEPROM readers, e poi flashati nuovamente su di essi.

Hacking web e database

# Hacking di server web

In questa sezione vediamo alcuni attacchi tipici contro i software di web server come Apache.

#### File di esempio

Alcuni produttori inseriscono dei file di esempio che mostrano le funzionalità del software. In passato è capitato che alcuni di questi file di esempio venissero preinstallati, e che quindi finissero pubblicati sul web ad insaputa del programmatore. Alcuni di questi file permettevano persino di visualizzare il codice sorgente della pagina.

#### Accesso al codice sorgente

La logica applicativa potrebbe permettere in qualche modo di visualizzare file di sistema o codice sorgente.

#### Server extensions

Le funzioni base offerte da un web server non sempre sono sufficienti e nel caso i programmatori spesso ricorrono ad estensioni, le quali frequentemente presentano problemi di sicurezza.

#### Buffer overflow

Come per tutte le applicazioni, anche i web server sono vulnerabili ai buffer overflow. Una vulnerabilità di questo tipo può persino permettere di ottenere RCE. Diversi applicazioni di web server hanno sofferto di questa vulnerabilità, tra cui Microsoft IIS e Apache. Queste vulnerabilità possono spesso essere patchate facilmente.

#### DoS

Questo attacco può essere perpetrato verso i web server in due modi: a forza bruta o sfruttando delle vulnerabilità. In entrambi i casi l’effetto è lo stesso.

## Scanner di vulnerabilità per server web

Vi sono diversi strumenti utili ad effettuare vulnerability scanning sui web server, i più importanti sono Nikto e Nessus.

# Hacking di web applications

Oltre agli attacchi ai server web, gli attaccanti possono attaccare direttamente le applicazioni hostate su di essi. L’ approccio in questo caso è leggermente diverso poiché l’attaccante si concentra su applicazioni personalizzate.

## Ricerca di applicazioni web vulnerabili (google dorks)

Attraverso Google si possono effettuare diverse ricerche utili per trovare server web malconifgurati, ad esempio:

- “index of /admin” o “index of /password” per trovare web server malconfigurati con pagine interne esposte.

## Web crawling

Questa attività consiste nello scaricare quanto più contenuto possibile da un web server al fine di trovare informazioni utili ed entry points. Esistono diversi applicativi per fare ciò, tra cui wget e ttrack.

## Valutazione delle applicazioni web

Vi sono diversi aspetti da valutare quando si analizza un’applicazione web, partiamo innanzitutto dai tool necessari.

#### Plug-in per il browser

Esistono diversi plug-in che permettono di intercettare e modificare i dati che il client invia al server, uno di questi è tamperdata.

#### Suite di strumenti

Fiddler è un server proxy che fa da intermediario e permette di intercettare e modificare tutte le richieste che transitano per esso. Anche burp suite è un software di questo tipo e permette anche di effettuare operazioni automatiche sulle richieste come sostituire una stringa.

#### Security scanner

Questi software sono delle suite all-in-one che permettono di testare applicazioni web, a partire dal loro download e dalla verifica della piattaforma, fino a fornire una valutazione del grado di sicurezza. Due di questi sono HP Web inspect e Rational AppScan.

# Vulnerabilità più frequenti delle applicazioni web

OWASP fornisce un elenco delle vulnerabilità più frequenti presenti nei siti web.

#### Attacchi XSS

Questo tipo di attacchi sfruttano siti mal-configurati (solitamente nella sanificazione degli input) ma a differenza di altri attacchi utilizzano il server solamente come veicolo per portare a termine l’attacco verso l’utente finale. L’attaccante infatti sfrutta il server per inserire uno script malevolo in una pagina che visualizzeranno altri utenti (ad esempio un social network). L’attacco più semplice vede l’inserimento di uno script che richiede cookie di sessione di altri siti web.

#### SQL Injection

Nei siti web dinamici solitamente i dati sono memorizzati in un database e vengono recuperati attraverso delle query. L’obiettivo in questo tipo di attacco è cercare di modificare la query e ottenere dal database dati sensibili. Il problema si verifica se l’input non è sanificato, ad esempio nel caso di una form che permette la ricerca di un utente in una lista. Vi sono anche pagine web che non mostrano l’output di una query, ma che possono comunque essere vulnerabili alla cosidettta blind SQL injection. In questo caso, sebbene l’output della query non venga mostrato, si cerca di indovinarne l’esito valutando altri parametri come ad esempio il tempo di risposta.

#### Automatic SQL Injection tools

Al fine di effettuare SQL Injection velocemente (in particolare le blind) può essere utile sfruttare dei tool come SQL Power Injection o Absinthe.

*Contromisure:*

* Validazione dell’input: una corretta validazione dell’input è cruciale e dovrebbe essere effettuata seguendo il principio “vincola, valida e ripulisci” ovvero vincolo del contenuto dei dati, controllo su di essi e pulizia.
* Sovrascrivere i messaggi d’errore: ritornare sempre un errore generico senza mostrare il vero errore (dal quale un attaccante potrebbe ricavare preziose informazioni).
* Usare variabili bind: in particolare nei framework di sviluppo queste variabili sono quasi obbligatorie, ed evitano ogni possibilità di forgery di richieste SQL.

#### Cross site request forgery (CSRF)

Questo attacco sfrutta l’autenticazione attraverso i cookie per effettuare richieste ad insaputa dell’utente finale. L’attaccante crea un sito web ad-hoc con all’interno un contenuto nascosto, ad esempio un tag HTML img. Il browser dell’utente quando carica la pagina invierà anche una GET all’indirizzo presente all’interno del tag al fine di caricare l’immagine. Tuttavia, tale indirizzo potrebbe corrispondere a qualsiasi cosa, anche ad un’azione di un sito web a cui l’utente è loggato, come un social network o il sito di home banking. L’attaccante quindi costringe il browser dell’utente ad inviare una richiesta a sua insaputa.

*Contromisure:* utilizzare un token casuale. Durante un accesso legittimo al sito web, l’utente richiede la pagina desiderata ed il server gli invia anche un token contenente un valore random. Successivamente, quando l’utente necessita di effettuare delle operazioni il server gli richiede il token inviato in precedenza, senza il quale non procede nelle operazioni. L’attaccante non ha modo di forgiare il token.

#### http response splitting

Vulnerabilità nelle applicazioni web che derivano dalla mancanza di sufficiente validazione dell’input. Il funzionamento è simile all’XSS. Un utente malintenzionato sfrutta la presenza di metodi di redirect per far effettuare all’utente delle richieste a siti web.

#### Wrong hidden tags usage

Alcune pagine web mal-realizzate possono essere state programmate per memorizzare dei dati da inviare al server all’interno di tag HTML nascosti. Ad esempio un ecommerce invece di memorizzare il prezzo degli elementi a back-end potrebbe averli memorizzati in tag html nascosti nella pagina inviata all’utente. Un attaccante che scopre questa falla può cambiare i prezzi a piacimento.

#### Server side include (SSI)

Alcune applicazioni web permettono di effettuare operazioni sul sistema a partire dall’input, ad esempio attraverso la funzione exec. Se l’input non è correttamente validato l’attaccante può inviate un comando SSI all’interno di un form e cercare di eseguire comandi remoti attraverso di esso.

# Hacking di database

Il database è spesso il cuore dei dati sensibili di un’organizzazione, ed è perciò spesso oggetto di attacchi. Gli attacchi ai database, come per i server web, possono mirare al software del database o alla logica dell’applicazione in esecuzione.

#### Ricerca di database

Normalmente i database non sono direttamente raggiungibili da internet, ma a volte può capitare. Conoscendo un range di indirizzi è possibile scansionarlo attraverso nmap alla ricerca del database. La scansione può essere effettuata attraverso alcuni script che permettono di dialogare con tutti le principali implementazioni di database SQL.

*Contromisure:* non esporre mai il database ad internet, separare correttamente la rete interna utilizzando firewall e DMZ, eseguire strumenti di rilevamento intrusioni.

## Vulnerabilità dei database

#### Attacchi di rete

Tutte le piattaforme adottano un processo listener di rete per gestire le comunicazioni. Se tale processo presenta delle vulnerabilità un attaccante potrebbe sfruttarle attraverso un buffer overflow o un attacco simile.

#### Bug dell’engine

L’engine del database è un software molto complicato, realizzato di molteplici processi che si occupano di garantire il corretto funzionamento del database. Un software così complesso può sicuramente presentare delle vulnerabilità, alcune delle quali potenzialmente sfruttabili da un attaccante.

*Contromisure:* applicare sempre le patch di sicurezza degli aggiornamenti.

#### Oggetti del database vulnerabili

Nei sistemi database sono spesso integrati degli oggetti aggiuntivi al fine di estendere le funzionalità del software. Alcuni di questi oggetti potrebbero essere vulnerabili e sfruttabili

*Contromisure:* applicare le patch di sicurezza, non consentire l’accesso a oggetti non necessari agli utenti.

#### Password deboli o predefinite

Se il database non fosse stato configurato correttamente potrebbe presentare una password debole o predefinita. Un attaccante senza molto sforzo può tentare un attacco con un dizionario di password comuni.

Hacking mobile

# Hacking android

## Fondamenti di Android

Al suo nucleo Android ha un kernel linux per processori ARM, che fornisce le funzionalità basilari del sistema operativo, come la gestione dei processi, della memoria e del risparmio energetico. Al di sopra del kernel vi è uno strato di librerie native, che forniscono funzionalità alle applicazioni come riproduzione di audio e video, connessione di rete, accesso ai sensori come il GPS ecc. Al di sopra vi è poi il livello applicativo, con un insieme di componenti software che aiutano lo sviluppatore nella scrittura di applicazioni, semplificando ad esempio la realizzazione dell’interfaccia grafica.

Un componente particolare e importante è la Dalvik Virtual Machine (ora ART) che esegue ogni app in una istanza riservata.

Per quanto riguarda la sicurezza, i dati dell’utente sono crittografati con AES e la partizione di sistema è montata come sola lettura. In più, il file creati da un’applicazioni non possono essere acceduti o modificati da un’altra.

# Hacking di Android

#### Rooting dei dispositivi

Di default l’utente di Android non gode di privilegi amministrativi. Attraverso dei software appositi è possibile sbloccare questi permessi per l’utente. Questa operazione prende il nome di “rooting” e fornisce all’utente pieno controllo del dispositivo, con tutti i pregi ed i rischi che ne derivano. Un’applicazione utile è SuperUser, che permette all’utente di scegliere quali applicazioni avviare con privilegi di root.

#### Installazione di app native

Poiché Android è basato su Linux è possibile eseguire applicazioni native di Linux sui dispositivi, tuttavia, se si prova ad avviare un binario compilato direttamente sul telefono non ci si riesce perché la compilazione è avvenuta per x86, mentre Android utilizza un processore ARM. È necessario quindi un software, detto cross-compiler, che permette di compilare il software per la piattaforma ARM.

#### Installazione di tool di sicurezza

Esistono diversi tool e porting di strumenti di sicurezza di Linux, tra cui:

* BusyBox: è un’applicazione che offre un set di tool UNIX da console come tar o wget.
* TCPdump: permette la cattura dei pacchett (funziona da terminale).
* Nmap: scanner di rete.
* Netcat

#### Trojan app

Queste app solitamente si fingono applicazioni legittime ma nascondono comportamenti malevoli. Vengono realizzate impacchettando l’applicazione legittima all’interno del software malevolo a cui viene dato l’aspetto dell’app (icona e nome). Per comprendere l’operazione di packing, capiamo prima come funziona un file android .apk. Esso è un file compresso (come un zip) e all’interno contiene due componenti fondamentali: il manifest, che fornisce ad Android le informazioni essenziali dell’applicazione ed i permessi richiesti, e classes.dex, ovvero l’eseguibile che contiene il codice compilato.

Le applicazioni in Android possono non avere un solo entry point (possono ad esempio essere avviate dall’icona o con un broadcast receiver).

Per creare il malware le operazioni svolte solitamente sono disassembly del dex, codifica del nuovo manifest e firma dell’apk risultante. L’operazione di disassemblaggio viene svolta attraverso il tool apktool, successivamente vengono effettuate le modifiche al disassemblato. Infine, è necessario generare una nuova firma (che sarà diversa da quella originale) e firmare il file.

# Hacking di dispositivi Android altrui

Versioni vulnerabili di Android potrebbero fornire la possibilità ad attaccanti di effettuare attacchi remoti.

#### Remote shell via webkit

Una vulnerabilità nel motore del browser (webkit) nella gestione dei numeri a virgola mobile permette di ottenere una shell remota sul dispositivo. La vulnerabilità è stata poi fixata in Android 2.2.

#### Remote rooting

Anche avendo ottenuto la shell, l’attaccante manca ancora dei permessi di root con cui effettuare la maggior parte delle operazioni malefiche. Per ottenerle poteva sfruttare degli exploit, come Exploid e RageAgainstTheCage.

#### Data stealing vulnerability

Una vulnerabilità permette ad un sito web malevolo di accedere ai dati memorizzati sul dispositivo. L’exploit avviene attraverso una pagina PHP ed un payload javascript malevolo. Il processo però non avviene del tutto in background, poiché compare una notifica. L’attaccante deve inoltre conoscere il percorso del file che vuole estrarre.

#### Remote shell with zero permissions

Un’altra via di accesso è rappresentata dall’evasione dal meccanismo di gestione dei permessi. Vi sono delle tecniche per arrivare ad eseguire operazioni riservate, ovvero con permessi “systemorsignature” riservati solamente ad app di sistema o firmate con la stessa firma delle app di sistema. Le tecniche variano a seconda dell’operazione desiderata:

* **Reboot**: è possibile riavviare il telefono attraverso un DoS, ottenibile ad esempio creando troppe notifiche “toast”.
* **Receive\_boot\_complete**: è possibile impostare un’applicazione in avvio automatico all’accensione anche senza dichiarare il broadcast receiver nel manifest, esso funzionerà lo stesso.
* **Internet**: normalmente per accedere ad internet le app hanno bisogno del permesso “internet” inserito nel manifest. È possibile evitare questo permesso aprendo il browser di sistema su uno specifico URL attraverso la funzione “startActivity”; questa operazione però aprirà a tutti gli effetti il browser dell’utente, per nascondere l’attività ha senso effettuare l’operazione solamente a schermo spento, controllabile con una specifica funzione. Infine, per ricevere dati direttamente nell’applicazione, si può impostare un receiver personalizzato per uno specifico URL, in maniera tale che quando il browser visiterà (o verrà reindirizzato) verso tale indirizzo si aprirà in automatico l’applicazione a cui verranno passati i dati.

#### Capability leak

Alcune applicazioni stock espongono dei loro permessi alle altre, lasciando la porta aperta per il loro sfruttamento. Questi leak possono essere “espliciti” ovvero avvenire attraverso lo sfruttamento di un componente di un’applicazione, come un Activity o un service oppure “impliciti”, ovvero quando attraverso uno specifico tag del manifest le applicazioni acconsentono alla condivisione dei permessi tra tutte le applicazioni firmate con la stessa firma.

#### Malware su URL

Android permette l’installazione di app anche da sorgenti esterne al Play Store, incluso il browser web. L’utente può capitare su una pagina web malevola che gli scarica l’apk e lo invita ad installarlo. Al momento dell’installazione l’utente visualizza i permessi richiesti dall’app ma potrebbe comunque installarla. Questa tecnica è stata utilizzata in due famosi trojan bancari che una volta installati intercettavano e reinviavano tutti gli sms ricevuti ad un server remoto, permettendo di intercettare le OTP utilizzate dalle banche per autorizzare i pagamenti.

*Contromisure:* disattivare l’installazione di app da sorgenti sconosciute.

#### Skype vulnerability

Un altro modo di attaccare Android è attaccando applicazioni vulnerabili presenti nel dispositivo. Un possibile attacco di questo tipo era possibile nell’applicazione Skype, poiché memorizzava nel dispositivo tutte le informazioni personali dell’utente (come contatti e contenuto dei messaggi) senza crittografia e con i permessi mal configurati. È sufficiente esplorare il file system per trovare il database SQLite dell’applicazione usato per memorizzare i dati e navigarlo.

#### Carrier IQ

Questo software fu al centro di un caso mediatico in America nel 2011. Questa applicazione era preinstallata da diversi provider ed era nascosta nel dispositivo e sempre in esecuzione. Il suo scopo era raccogliere dati per ottenere delle metriche per migliorare il servizio di rete. Il problema è che i dati raccolti (come posizione, chiamate ricevute, attività di SMS) non erano anonimi, poiché erano identificati attraverso l’IMEI del dispositivo e l’identificativo della SIM.

#### Google Wallet

Google Wallet è un’applicazione che promette di sostituire gli strumenti di pagamento come le carte di credito con il telefono. L’applicazione permette all’utente di memorizzare i suoi dati di pagamento e di assicurarli dietro un PIN di quattro cifre, richiesto al momento del pagamento. Dei ricercatori hanno però scoperto che l’hash del PIN insieme al suo salt vengono memorizzati in un database SQLite protetti solamente dalle protezioni delle applicazioni di Android (ovvero limitazione dell’accesso allo spazio di altre applicazioni), aggirabile attraverso il root. Un dispositivo con permessi di root è quindi in grado di ottenere l’hash del PIN e craccarlo in pochi secondi essendo lungo solamente quattro cifre.

*Contromisure:* non rootare un dispositivo con dati sensibili come i dati di pagamento.

# Android come piattaforma di hacking portatile

Poiché i dispositivi Android integrano il kernel Linux, sono disponibili moltissimi validi strumenti di hacking per questa piattaforma:

* Network sniffer (Shark for root): utilizza una versione cross-compilata di tcpdump per mostrare i pacchetti catturati o salvarli in un file pcap.
* Network spoofer: applicazione che effettua un attacco di ARP Spoofing per redirezionare il traffico verso un server web a scelta dell’utente.
* Connect cat: similmente a netcat permette di connettersi ad un host e scambiarci traffico di rete.
* Nmap for Android: porting di nmap per android.

# Difendere il proprio Android

Vediamo alcuni consigli di base per aumentare la sicurezza del proprio dispositivo:

* Mantenere la propria periferica al sicuro: per un attaccante che dispone di accesso fisico al dispositivo è solo questione di tempo prima che venga attaccato, pertanto la prima cosa da fare è non farselo rubare.
* Bloccare il dispositivo: bloccare l’accesso al dispositivo con PIN o pasword.
* Non installare applicazioni da fonti sconosciute: non installare applicazioni non provenienti dal Play Store.
* Utilizzare un software di sicurezza come un antivirus
* Impostare la crittografia dell’intero dispositivo.

# iOS

## History

La storia di iOS inizia negli anni ’80 quando Steve Jobs, cacciato da Apple, fonda NEXT e sviluppa un sistema operativo con un kernel parzialmente basato su BSD e con linguaggio di sviluppo Objective C. All’acquisizione di NEXT da parte di Apple nel 1996 inizia lo sviluppo di Mac OS X, che si fonda proprio sul sistema operativo di NEXT. Nel 2007 la Apple commercializza l’iPhone, che utilizza una versione ridotta di OS X al suo interno. Gli iPhone utilizzano processori ARM.

## Sicurezza

Inizialmente iPhone non permetteva l’installazione di app di terze parti, fino all’introduzione dell’AppStore. Molte misure di sicurezza sono state aggiunte, come l’esecuzione di app sotto permessi non root (denominati “mobile”), il supporto alla sandbox e la verifica della firma del codice sia a tempo di caricamento che a runtime. Inoltre, iPhone supporta ASLR e PIE, che randomizzano la memoria ed il base address delle applicazioni in esecuzione.

## JailBreaking

Apple ha sempre impedito agli utenti di prendere pieno controllo del proprio dispositivo e di installare applicazioni di terze parti. Il processo di “evasione” da queste restrizioni è detto jailbreaking, e solitamente viene realizzato sfruttando alcune vulnerabilità. In termini di sicurezza, un dispositivo con jailbreak potrebbe essere meno sicuro, sia perché i software che sfruttano gli exploit potrebbero effettuare altre modifiche al dispositivo senza che l’utente se ne accorga, e sia perché il dispositivo con jailbreak ha la verifica della firma delle applicazioni disattivata, e pertanto si potrebbero installare applicazioni potenzialmente maligne.

Il processo di jaibreaking può essere effettuato principalmente in due modi: attraverso il boot oppure “remoto”.

#### Jailbreak basato sul boot

In questa modalità si scarica un tool di jailbreak ed un’immagine del sistema operativo (detta IPSW). Successivamente si collega il dispositivo al computer e lo si avvia in modalità DFU, ovvero aggiornamento del firmware. Si avvia il tool di jailbreak, gli si passa l’immagine scaricata e lo si avvia. In automatico verrà installata l’immagine modificata con jailbreak attivo.

#### Jailbreak remoto

Esistono (esistevano) delle vulnerabilità di Safari che permettevano di effettuare il jailbreak solamente scaricando un PDF modificato appositamente da un sito web. Uno di questi siti era jailbreakme.com.

# Hacking di telefoni altrui

Dal punto di vista dell’hacking remoto il sistema operativo iOS è piuttosto particolare poiché limita ogni servizio non indispensabile dall’accesso esterno. Questo fa sì che il sistema operativo di per sé sia piuttosto difficile da attaccare. L’attenzione degli hacker è perciò rivolta verso le app che vengono installate nei dispositivi, nelle quali si riscontrano ovviamente vulnerabilità, sia in quelle di Apple che in quelle di terze parti.

#### Le vulnerabilità di JailbreakMe

L’exploit di JaibreakMe sfrutta due vulnerabilità per effettuare il Jailbreak. La prima consiste in una vulnerabilità nel lettore di PDF di Safari, in particolare per quanto riguarda la gestione dei font, e permette all’attaccante di eseguire codice da remoto. Se l’exploit della prima vulnerabilità ha successo viene poi sfruttata una vulnerabilità del kernel per fare privilege escalation, ottenere pieno controllo del dispositivo ed effettuare il jailbreak. Questo tipo di exploit viene effettuato solamente per avere il jailbreak del dispositivo, tuttavia un attaccante potrebbe seguire un simile path per scopi malevoli e prendere controllo del dispositivo solamente facendo visitare all’utente una pagina web.

*Contromisure:* effettuare sempre i più recenti aggiornamenti software. Non effettuare il jailbreak del proprio dispositivo principale poiché i dispositivi con jailbreak non possono ricevere aggiornamenti.

#### Attacchi iKee!

Nel 2009 questo worm compromise degli iPhone con jailbreak in Australia. Il suo funzionamento era semplicissimo: poiché gli iPhone con jailbreak permettevano di abilitare SSH, esso scannerizzava i blocchi di indirizzi dei provider (quindi quelli assegnati poi ai dispositivi mobile) alla ricerca di dispositivi con SSH aperto e tentava l’accesso con le credenziali di default. Se l’utente non aveva cambiato le credenziali di openSHH di default il worm otteneva l’accesso al dispositivo ed inizialmente effettuava solamente operazioni innocue come cambiare lo sfondo e impostare un servizio per replicarsi (che effettuava scansioni ed inviava se stesso). Successivamente nacquero alcune versioni che invece portavano a comportamenti malevoli, in particolare facevano diventare il dispositivo parte di una botnet controllata dall’esterno.

*Contromisure:* non effettuare il jailbreak, oppure, nei dispositivi jailbroken, limitare i servizi attivi all’essenziale.

#### Attacco man-in-the-middle (FOCUS11)

In una dimostrazione di sicurezza, gli attaccanti crearono una rete wifi con un nome simile al nome di una rete reale (si pensi ad esempio alla rete wifi di uno starbucks), per ingannare gli utenti e farli connettere alla propria. La rete era configurata per reindirizzare il traffico verso la rete reale, permettendo agli attaccanti di effettuare a tutti gli effetti un attacco man-in-the-middle. Gli attaccanti potevano inoltre sfruttare una vulnerabilità nella validazione dei certificati per forgiare certificati ad-hoc per i siti web visitati dagli utenti. Nella dimostrazione gli attaccanti modificavano la pagina web di gmail (generando anche un certificato apposito) inserendo nella pagina un PDF nascosto contenendo l’exploit di jailbreakme leggermente modificato per essere invisibile (non installava Cydia né mostrava niente all’utente durante l’installazione) ed al termine del jailbreak abilitava SSH e VNC, dando completo controllo remoto agli attaccanti. Questo attacco era molto plausibile che potesse accadere anche nel mondo reale, e pertanto molto pericoloso.

*Contromisure:* oltre ad effettuare sempre i più recenti aggiornamenti software è bene tenere a mente che gli access-point pubblici possono essere comunque pericolosi. Pertanto, se nel dispositivo sono presenti informazioni molto riservate, è bene connettersi solamente a reti private ed evitare gli access point pubblici.

#### App malevole: Handy Light, InstaStock

Come già detto in precedenza, Apple permette di installare sul dispositivo solamente app firmate da Apple stessa e pubblicate nell’app store. Il processo di pubblicazione di un app include il superamento di una lunga serie di requisiti e di un processo di verifica di sicurezza dell’app. Tale processo è piuttosto sicuro visto che di rado si osservano malware nell’app store, tuttavia non è infallibile. È il caso di HandyLight ed InstaStock. La prima si presentava nell’appstore come una banale torcia, ma permetteva all’utente, impostando la giusta combinazione di colori, di attivare il tethering wifi del dispositivo (all’epoca vietato da Apple). Questo comportamento è sfuggito al processo di verifica e l’app ha quindi ottenuto la pubblicazione.

La seconda app invece era un vero e proprio malware. All’apparenza si proponeva di permettere all’utente di controllare il prezzo delle azioni che desiderava, ma di nascosto poteva eseguire codice. L’applicazione sfruttava una vulnerabilità nel compilatore JIT di safari (che fu inserito per poter visualizzare contenuti JavaScript nelle pagine web). L’accesso al compilatore sarebbe in teoria dovuto essere permesso solamente a Safari, ma una vulnerabilità permetteva a qualsiasi applicazione di accedervi. InstaStock accedeva al compilatore e riusciva ad eseguire codice non firmato sfruttandolo. L’app era anche in grado di contattare una C2 e di ricevere istruzioni da essa.

*Contromisure:* non è possibile stabilire se un’applicazione nell’app store è sicura oppure no, tuttavia si può essere ragionevolmente sicuri del fatto che lo sia poiché il processo di verifica delle app di Apple è piuttosto sicuro.

#### App vulnerabili

L’attenzione degli attaccanti non si è focalizzata molto sulle applicazioni, tuttavia rappresentano sicuramente una possibile superficie di attacco interessante. Le app installate nel dispositivo possono avere delle vulnerabilità di sicurezza tali da mettere in pericolo i dati personali dell’utente. È il caso dell’app Citi che memorizzava in chiaro nella memoria alcuni dati di accesso al conto bancario e che sarebbero potuti essere facilmente recuperati nel caso in cui un attaccante avesse avuto accesso fisico al dispositivo. Un bug nella verifica dei certificati dell’app PayPal permetteva invece all’attaccante di effettuare attacchi man-in-the-middle, riuscendo ad impersonificare il server e modificare i dati in transito, inclusi quelli dei pagamenti.

*Contromisure:* effettuare sempre gli aggiornamenti software.

#### Accesso fisico

Poiché i dispositivi mobile vengono portati ovunque, possono essere facilmente oggetto di furto o perdita. Un attaccante nel momento in cui ottiene accesso fisico al dispositivo riesce facilmente ad accedere a molti dati memorizzati all’interno; ad esempio, attraverso una procedura di jailbreak e accesso alla keychain del dispositivo riusciva a rubare molte password memorizzate.

*Contromisure:* è importante utilizzare software di cifratura per i dati importanti ed impostare una password o un PIN di almeno 6 cifre al dispositivo.