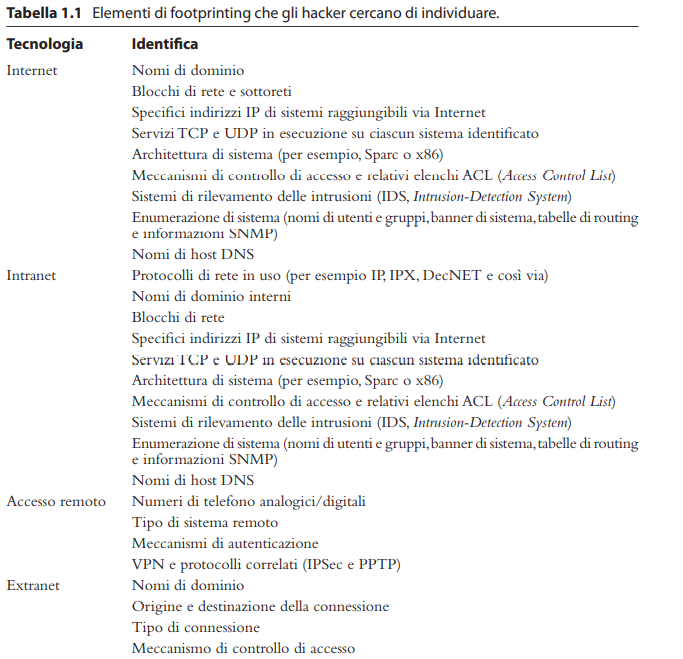
# ­­FootPrinting – Chapter 1

Il footprinting è l’arte di raccogliere informazioni sull’obiettivo da hackerare al fine di creare un profilo (footprint) univoco del bersaglio che descrive tutto ciò che lo riguarda, nel nostro caso: connessioni internet, intranet/extranet, accessi da remoto. Queste informazioni raccontano quello che è lo stato di sicurezza dell’organizzazione in questione.

Il footprinting è utile anche all’organizzazione ste­­ssa, vittima dell’attacco, per capire quali sono le falle del proprio sistema di sicurezza in modo da prevenire gli attacchi.

Gli elementi del footprinting che un hacker studia sono:



Esistono dei passi base per cominciare l’attività di footprinting:

* Definire l’ambito delle proprie attività, cioè definire chi o cosa dell’organizzazione vittima di attacco bisogna studiare: tutta l’organizzazione o limitarsi a certe sedi, a certi partner o siti di disaster-recovery.
* Ottenere le opportune autorizzazioni, livello 8 e 9 del modello osi: politica e finanziamenti.
* Informazioni accessibili al pubblico: la quantità di informazioni riguardanti l’organizzazione disponibile su internet quali:
  + **pagine web aziendali**, possiedono una quantità di dati che possono favorire i malintenzionati. Addirittura, dati sulle configurazioni di sicurezza stessa. È possibile fare un’analisi del codice HTML cercando dei commenti nel testo. Reti private (VPN) utilizzate in alcune organizzazioni che riporta dettagli e informazioni su versione e configurazioni.
  + **organizzazioni correlate**, che magari svolgono compiti di sviluppo web per l’organizzazione e lasciano tracce e commenti nei file di sviluppo diventando essi vittime di possibili attacchi.
  + **dettagli sulla sede e sul personale**: attraverso servizi di localizzazione è possibile avere informazioni utili riguardo accessi, connessioni wireless e tanto altro che riguarda la sede. Possedere invece informazioni del personale permette agli hacker di risalire a delle persone e provare l’accesso remoto con loro identità. Esistono dei servizi, inoltre, di vendite di rubriche intere di dati di persone oltre ai social network stessi. Tutto questo può portare a degli attacchi pishing
  + **eventi:** eventi di qualsiasi tipo che portano a situazioni dove la sicurezza è in secondo piano (durante l’acquisizione di un’organizzazione vi può essere l’unione delle reti aziendali). Oppure quando un’azienda cresce rapidamente, le procedure interne non sempre si adeguano con la stessa velocità.
  + **Politiche per la privacy e sicurezza e dettagli tecnici che indicano i meccanismi di sicurezza attivi,** qualsiasi tipo di informazione che fornisce un’idea sulle politiche riguardanti la privacy o la sicurezza aziendale.
    - **Informazioni archiviate,** è possibile ottenere tramite alcuni siti delle copie archiviate di informazioni non più disponibili, rimossi magari per ragioni di sicurezza
  + **Motore di ricerca e relazione tra dati:** i motori di ricerca trovano tutto lo scibile possibile, e posseggono anche delle funzionalità di ricerca avanzata
* Enumerazione di server WHOIS e DNS: attualmente internet è gestito da un’associazione no profit chiamata ICANN che ha come compito quello di gestire i domini internet, gli indirizzi IP e i parametri di protocollo e numero di porte.  
  Inoltre coordina l’attività del server DNS che sta alla radice di Internet.  
  L’ICANN gestisce una miriade di dati ma la gestione non è centralizzata in un server ma in più server sparsi nel pianeta, chiamati WHOIS.  
  E’ possibile effettuare delle ricerche attraverso i dominio seguendo la tecnica del WHOIS-R dove R sta per i vari registri. Come prima cosa va determinato in quale server WHOIS possiede le informazioni che cerchiamo. Il tutto è gestito tramite l’organismo della IANA. Il Registry di un TLD (top level Domain) contiene informazioni riguardante il Registrar con cui è stato registrato il dominio. Attraverso il Registrar possiamo risalire alle informazioni del Registrant con i relativi nameserver DNS.  
  Le ricerche invece attraversi IP sono effettuate tramite l’organismo della ASO, dell’ICANN. I dettagli relativi agli IP sono mantenuti nei RIR (Regional Internet Registry) che conosce gli intervalli di indirizzi IP che gestisce.
* Interrogazione del DNS: permette l’associazione di un indirizzo IP al nome di un host. Se è configurato a basso livello di sicurezza è probabile vittima di attacco.
* Riconoscimento della rete: determinare la tipologia della rete e i percorsi attraverso strumenti come “tracerouting” che fornisce l’esatto percorso intrapreso da un pacchetto in una rete. Attraverso il percorso svolto dal pacchetto è facile notare quali potrebbero essere i router, firewall o dispositivi simili che permettono l’accesso.

# Scanning – Chapter 2

Le attività di scanning permettono di ottenere diverse informazioni come quelle sui servizi in ascolto o in esecuzione, se i sistemi sono in esecuzione, i dati informativi dei sistemi operativi e dell’infrastruttura.  
  
La ricerca di un sistema attivo o meno è possibile effettuarla attraverso un ping sweep verso alcuni indirizzi IP ottenuti dalla fase di footprinting. Questa tecnica consiste nell’inviare un certo tipo di traffico verso la macchina ed analizzare le risposte ottenute (se vi sono). I tipi di traffico possono essere:

* ICMP, sta per Internet Control Message Protocol. Offre diversi tipi di messaggi per diagnosticare lo stato di un host e il suo percorso di rete. L’obiettivo è quello di bombardare un host con un ICMP ECHO REQUEST ed attente una ICMP ECHO REPLY, che non è altro che effettuare il comando “ping”. Altri messaggi possono essere gli ICMP ADDRESS MASK che identifica la maschera di subnet locale.  
  Utilizzare Nmap con messaggi di tipo ICMP o anche TCP.  
  hping3 e nping forniscono any combinations of flags on any combinations of packet types, spoofing MAC/IP.
* ARP, protocollo che traduce l’indirizzo MAC in indirizzo IP. Utilizzato se si è nella stessa subnet. Si invia una richiesta ARP per ciascun host nella sottorete e tale host viene considerato vivo se viene ricevuta una risposta ARP. Questa tecnica è potente in quanto identifica la presenza di un firewall che filtra richiesto di livello più alto (ICMP, TCP).  
  Le funzioni disponibili sono: ARP-scan, Nmap, Cain
* TCP, UDP: ricerca degli host tramite TCP ed UDP all’interno delle reti che limitano il protocollo ICMP. Molti server mettono a disposizione almeno una porta aperta a cui i client possono collegarsi per svolgere le loro funzioni e queste possono essere delle concessioni molto gradite per gli hacker (magari il server blocca il traffico ICMP ma permette il traffico http sulla porta 80, si può testare questa porta ed aspettare una risposta per determinare lo stato dell’host). Altre volte invece l’utilizzo di desktop remoti in ambiente aziendale deve permettere la disabilitazione di firewall locali permettendo l’accesso al traffico ICMP.  
  Gli strumenti utili in questo caso è Nmap che fornisce una ricerca ARP, ICMP e TCP magari testando tutte le porte di un host. Nel caso di un range di host da testare è utile invece testare alcune porte popolari.   
  Anche SuperScan fornisce dei metodi simili utilizzando ICMP oppure TCP/UDP.  
  Anche nping tramite messaggi TCP/UDP. L’output della richiesta nping è più abbondante di default e fornire informazioni più dettagliate.

## Contromisure contro il ping sweep

Il rilevamento del ping sweep può essere usato per accorgersi del fatto che potrebbe verificarsi un attacco, dato che il ping sweep viene usato per riconoscere lo stato della rete.  
Uno dei metodi usati per rilevare il ping sweep comporta l’utilizzo di programmi IDS (intrusione detection system) di rete come snort.

Alcuni firewall forniscono delle funzioni per rilevare i ping sweep anche se il solo rilevarli è inutile se non vengono gestiti.

La prevenzione è ancora più fondamentale del rilevamento del ping sweep. È possibile, tramite firewall, filtrare i tipi di pacchetti ICMP che sono consentiti per le varie esigenze lavorative.

## Determinare quali servizi sono in esecuzione o in ascolto

Il ping sweep fatto in precedenza ricercava i sistemi attivi. È possibile sondare per ognuno di questi sistemi quali porte e servizi sono disponibili per portare un attacco.

La scansione delle porte previde l’invio di pacchetti a porte TCP o UDP per determinare quali servizi sono in esecuzione on in Listening. Questo tipo di scansione può riportarmi informazioni tipo il sistema operativo del bersaglio o le versioni delle applicazioni.

### Tipi di scansioni:

* Scansione di connessione TCP: questo tipo di scansione effettua la connessione alla porta e completa un handshaking a tre vie (SYN, SYN/ACK, ACK) tipico di TCP. Questo tipo di scansione comporta la possibilità di essere rilevato e registrato nei log, ma non richiede nessun tipo di autorizzazione particolare.
* Scansione SYN TCP: chiamata scansione semiaperta perché non viene stabilita una connessione TCP completa ma ci si limita ad inviare un pacchetto SYN alla porta. Se si riceve un SYN/ACK dalla porta si deduce che la porta è in Listening mentre se si riceve un RST/ACK significa che la porta non è in ascolto. Questa tecnica comporta il fatto che non è facile per il bersaglio rilevare la scansione
* Scansione FIN TCP: invio di un pacchetto FIN alla porta. Il bersaglio dovrebbe restituire RST per tutte le porte chiuse. Di solito funziona su stack TCP/IP basati su UNIX
* Scansione Xmas Tree TCP: invio di un pacchetto FIN, URG, PUSH verso la porta. Dovrebbe essere il ritorno di un messaggio RST per tutte le porte chiuse
* Scansione NULL TCP: disattivazione di tutti i flag. Ci si aspetta un RST per tutte le porte chiuse.
* Scansione ACK TCP: utilizzata per mappare i ruleset dei firewall per comprendere se il firewall è un semplice filtro di pacchetti che consente solo connessioni con il bit ACK impostato oppure è un firewall con controllo sullo stato che opera su un filtro avanzato.
* Scansione di Finestre TCP: rilevare porte aperte anche filtrate/non filtrate su alcuni sistemi a causa di un’anomalia nel modo in cui è riportata la dimensione delle finestre TCP.
* Scansione RPC TCP: specifica per UNIX viene usata per rilevare ed individuare le porte RPC e programmi associati con il loro numero di versione
* Scansione UDP: invio di un pacchetto UDP alla porta. Se risponde con un messaggio di porta ICMP irraggiungibile, significa che è chiusa. Se non riceve questo messaggio la porta potrebbe essere aperta. Dato che UDP è inaffidabile, non si può avere certezza di ciò che si sta facendo.

### Individuare servizi TCP ed UDP in esecuzione

Nmap fornisce anche delle scansioni di SCTP INIT e TCP Maimon, cioè la scansione delle porte dopo aver discoverato quelli che sono gli host attivi nella rete. La più semplice delle scansioni è quella delle porte SYN TCP. È possibile effettuare delle scansioni civetta in modo da sommergere un sito bersaglio con informazioni superflue tramite l’opzione -D. Queste scansioni vanno lanciate in contemporanea ad una scansione reale, falsificando l’indirizzo di origine dei messaggi per indicare server leggittimi mescolando alla scansione di porte reale.  
Superscan è un’alternativa a Nmap per Windows. Fornisce scansione ping, TCP ed UDP con diverse tecniche. Fornisce la ricerca

Le contromisure del port scanning vede l’utilizzo di SNORT, Scanlogd, Firewall che rilevanno messaggi SYN e ignorano i FIN, Attacker.

La prevenzione del port scanner può essere svolta in linux contrassegnando come commenti i servizi non necessari nel file etc/inetd.conf e disabilitando l’avvio dei servizi negli script di startup.  
In windows si dovrebbero disattivare tutti i servizi non necessari.

## Rilevamento del sistema operativo

Nella ricerca delle vulnerabilità è utile conoscere il sistema operativo in uso.

Esistono due modalità: attiva e passiva.

### Modalità attiva

In modalità attiva abbiamo: banner grabbing, scanning porte, stack fingerprinting.

#### Banner

Per svolgere questo compito si possono utilizzare tecniche di cattura dei banner che ottengono informazioni da servizi come FTP, telnet, SMTP, http, POP.

#### Scanning delle porte

Oppure è possibile fare lo scanning delle porte disponibili dato che è noto che alcune porte sono specifiche per alcuni sistemi operativi. In particolare, i sistemi windows sono in ascolto sulle porte 445, 139 e 135. Alcuni servizi sono specifici di alcuni sistemi operativi come la porta TCP 3389 utilizzata per il protocollo RDP, tipico di windows.

Per quanto riguarda i sistemi UNIX, un buon indicatore è costituito dalla porta TCP 22 riguardante l’SSH, oppure dalla porta TCP/111 riguardante servizi come portmapper, servizi Berkeley TCP/512-514, NFS TCP/2049.

#### Fingerprinting dello stack

Il fingerprinting dello stack è una tecnologia che consente di determinare rapidamente il sistema operativo di un host. Analizzando le implementazioni dello stack IP dei vari produttori è possibile notare le varie differenze di interpretazione delle indicazioni RFC ed ipotizzare il tipo di sistema operativo in uso. Per funzionare si ha necessità di una porta in ascolto.

Nmap viene usato per effettuare il fingerprinting specificando l’opzione -O utilizzando tecniche quali:

FIN probe (Windows 7/200x/Vista respond with FIN/ACK), Bogus flag probe, Initial Sequence Number sampling, “Don’t fragment bit” monitoring, TCP initial window size, ACK value (+0 or +1), ICMP message quenching, ICMP message quoting, ICMP message echoing integrity, TOS, fragmentation handling, TCP options

Le contromisure contro il rilevamento del sistema operativo sono il rilevamento attraverso la scansione delle porte e la prevenzione andando a modificare il codice sorgente del sistema operativo o qualche parametro in modo da cambiare caratteristiche pecuriali del fingerprint dello stack.

### Modalità passiva

#### Fingerprinting dello stack

Simile a quello attivo ma invece di inviare pacchetti ad un sistema bersaglio, l’hacker controlla in modo passivo il traffico di rete per determinare il sistema operativo in uso. Questa tecnica richiede di trovarsi in una posizione centrale della rete e su una porta che consenta la cattura di pacchetti.  
Il funzionamento è tale per:

* Segnature passive, limitandoci ad una sessione TCP/IP.   
  Valutare che valore di TTL imposta il sistema operativo sul pacchetto in uscita.  
  Valutare il valore della dimensione della finestra che imposta il sistema operativo.  
  Valutare il bit di non frammentazione che imposta il sistema operativo  
    
  Analizzando i dati ottenuti con alcuni noti è possibile determinare il sistema operativo.

Elaborazione e memorizzazione dei dati di una scansione

La gestione della grande quantità di dati che sono stati raccolti può essere fatta da Metasploit.

È un framework di exploit utilizzato per modularizzare exploit e payload. L’installazione di Metasploit attiva un server PostgreSQL che consente la realizzazione di query specifiche sul database dei dati di scansione.   
Per funzionare bisogna indicare al programma i parametri di connessione e il database desiderato.

Metasploit viene richiamato tramite “msfconsole”.

I comandi sono:

* db\_connect, per fornire i parametri di connessione e il database.
* db\_nmap, effettua scansioni nmap ed importa nel database tramite db\_import (metasploit effettua scansioni come nmap ma con tempistiche lunghe, quindi sfrutta direttamente nmap)
* hosts ritorna gli host trovati con nmap
* servicesm ritorna i servizi e le porte aperte sugli host trovati da nmap
* filtri particolari tramite -s

# Enumerazione – Chapter 3

L’enumerazione è il processo che avviene dopo lo scanning per identificare eventuali punti deboli nei servizi prima osservati.

La differenza tra le tecniche di raccolta delle informazioni dello scanning e la enumerazione sta nel livello di intrusività. L’enumerazione comporta l’utilizzo di connessioni attive ai sistemi bersaglio e di interrogazioni dirette che potrebbero essere registrate nei file di log e quindi notate.  
In generale, i principali dati che gli hacker cercano sono nomi di account utente, risorse condivise mal configurate e vecchie versioni software con note vulnerabilità.

## Fingerprinting di servizi

Il fingerprinting rivela i servizi associati a ciascuna porta, andando più avanti della solita scansione. Richiede ovviamente più tempo ed è facilmente rilevabile perché genera più traffico.

Attraverso l’utilizzo di nmap possiamo mappare i servizi con le porte associate, informazioni che sono ottenute da un file chiamato nmap-services.

Attraverso il comando “-sV” interroga le porte cercando un feedback da queste e facendo un mapping con informazioni note presenti in un file nmap-service-probe. Per esempio, solitamente nmap tornerebbe il servizio che fa uso di una porta specifica. Ma forzandolo con -sV potremmo ottenere informazioni diverse, come l’utilizzo di quella porta da parte di un servizio nascosto diverso.

## Scanner di vulnerabilità

L’utilizzo di uno scanner di vulnerabilità automatizzato può essere utile quando non si hanno preoccupazioni sul farsi individuare dal bersaglio.

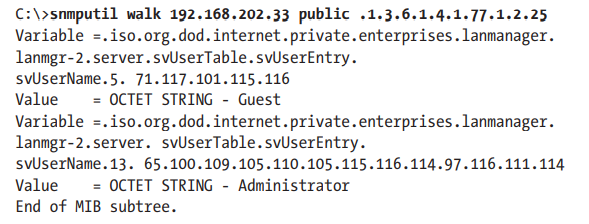
Il prodotto Nessus è lo standard di riferimento per gli scanner di vulnerabilità.  
Nmap fornisce anche attività di enumerazione tramite degli script NSE, estendendo le funzionalità di nmap tramite script personalizzati dagli utenti.

La cattura dei banner, come visto nello scanning, permette di ottenere informazioni dall’output di questi servizi. Può essere fatta in maniera manuale tramite una telnet sulla porta conosciuta.

In modalità automatica si può usare netcat connettendosi ad una porta TCP/IP e catturando il banner del servizio.

Oppure è possibile usare netcat e cercare di forzare i server a inviare più informazioni

### Enumerazione dei servizi di rete comuni

* FTP: analizzare il contenuto dei siti ftp che forniscono l’accesso pubblico e consentono l’accesso anonimo. È possibile farlo puntando alla porta 21 usando una connessione TCP. Questi servizi dovrebbero essere disattivati e dovrebbe essere usato sempre un SFTP o FTPS che utilizzando SSH o SSL. Inoltre dovrebbe essere vietato l’upload illimitato di contenuti.
* Telnet: era molto utilizzato in quanto forniva l’accesso remoto ma trasmetteva i dati in chiaro, quindi qualunque sniffer aveva la possibilità di vedere la comunicazione client-server, inclusi username e password. Adesso è stato cifrato, sostituito dal SSH. Viene testato sulla porta 23, connessione TCP. Telnet può offrire informazioni dell’host dato che prima della fase di login mostra sempre un banner che riporta sistema operativo e versione. Altri banner invece sono tipici di alcuni dispositivi, che sono quindi facilmente riconoscibili. L’enumerazione dell’account invece consiste nell’osservare i messaggi restituiti dal server in caso tentato login. In certi casi si può sapere se l’utente che stiamo cercando di usare per il login sia corretto o meno dal fatto che se sbagliamo password ma non l’utente, ritorna solo l’errore della password. Per prevenire tutto ciò è consigliato modificare i codici di errore rendendoli generici oppure modificare le informazioni del banner.
* SMTP: protocollo eseguito su porta 25 con connessione TCP. Fornisce due comandi interni per enumerare gli utenti: VRFY che conferma i nomi di utenti validi e EXPN che rivela gli effettivi indirizzi di recapito di alias e mailing list. La prevenzione consiste nel disattivarlo. Le versioni moderne forniscono una sintassi che si può incorporare nel file mail.cf per disabilitare questi comandi.
* DNS: usato sulla porta 53 con connessione UDP ma può usare anche TCP. Una delle tecniche di enumerazione è il trasferimento di zona DNS che si può implementare su server DNS mal configurati tramite TCP 23. Consiste nel visualizzare l’intero contenuto del file di zona di un dato dominio ricavando informazioni come le associazioni tra host e indirizzo ip. Viene utilizzato il comando nslookup, ls -d e il dominio oppure il comando dig in linux.  
    
  I server DNS mantengono una cache per risolvere più velocemente gli host.é possibile quindi interrogare un server cache DNS in modo da controllare quale siti sono stati frequentati di più. Si parla in questo caso di snooping. Se il server DNS non ha mai elaborato tale richiesta, risponde con flag “Answer” impostato a 0. Attraverso nslookup si può capire chi è il proprio dns server, ed effettuare attraverso la dig di un sito questa ricerca.
* TFTP: su porta 69 con connessione TCP,UDP. È un protocollo basato su UDP per eseguire trasferimenti rapidi senza autenticazione. È necessario conoscere il nome del file. In questa maniera, se un file è mal protetto, è molto facile impossessarsene. Spesso gli stessi dispositivi di rete come router e switch offrono la possibilità di effettuare la configurazione come server TFTP.  
  Se possibile è meglio disattivare questo servizio ed eventualmente usare una protezione degli accessi con un wrapper, limitare l’accesso alla directory ed assicurarsi che sia impostato un blocco presso il firewall.
* Finger: enumerare gli utenti utilizzando l’utility finger su porta 79 con TCP/UDP.
* HTTP: ricavare produttore e versione di un server web usando la porta 80 e TCP. Usando netcat si può interrogare un server web, leggere la response head di http ed eventualmente reindirizzare il traffico ad un proxy SSL in grado di negoziare una connessione SSL. Il modo migliore per prevenire questi attacchi è modificare i banner.
* MSRPC: alcuni sistemi microsoft eseguono un servizio endpoint mapper RPC sulla porta TCP 135. Interrogando questo servizio si ottengono informazioni sulle applicazioni e servizi disponibili sulla macchina, usando lo strumento epdump. Evitare questo tipo di interrogazioni sulla porta TCP 135.
* NetBios: è un servizio nomi distribuito per reti basate su Microsoft Windows. È stato sostituito da altri servizi ma è ancora presente in tutte le distribuzioni windows. L’enumerazione è semplice perché gli strumenti e le tecniche per tenere d’occhio la connessione NetBios sono disponibili e integrati nel sistema operativo. Il comando netview da riga di comando elenca i domini disponibili sulla rete e poi tutte le macchine di un dominio. Funziona solamente sul segmento di rete locale. Se NBNS è instradato su TCP/IP può enumerare gruppi di lavoro, domini e host Windows di un’intera rete aziendale, elencandone la struttura dell’intera organizzazione.  
  Tutte le tecniche netBios lavorano su UDP 137. Basta limitare l’accesso tramite firewall o bloccando il protocollo nei router di rete. Per evitare che i dati degli utenti possano apparire nella visualizzazione delle tabelle dei nomi basta disabilitare servizi Avvisi e Messenger sui singoli host.
* NetBIOS: su connessione TCP 139/445. Quando si accede ad un file o ad una stampante di rete associata ad una macchina windows si fa uso del protocollo SMB (server Messagge block) che può fornire tante informazioni se non protette. Uno dei metodi è quello di connettersi al servizio tramite “sessione null”  
    
  In questa maniera ci si sta connettendo alla condivisione “di comunicazione interprocesso nascosta (IPC$) all’indirizzo IP con utente anonimo (/u:) e password nulla. Se il comando ha successo si ha un canale aperto sul quale ottenere informazioni.
* Registro: visualizzare il contenuto del registro di Windows sul bersaglio. Alcune applicazioni lasciano informazioni nel registro di sistema. Windows blocca gli accessi ad utenti non amministratori tranne quando viene specificato una cosa diversa.
* Utenti: alcune macchine windows diffondono informazioni sugli utenti su sessioni null. Utilizzando DumpSec dalla riga di comando si può generare un file contenente tali informazioni da un computer remoto.  
  Altri strumenti di enumerazione sono sid2user e user2sid che cercando di determinare i SID della famiglia NT dall’input del nome utente e viceversa. Il SID è il Security Identifier, valore numerico di lunghezza variabile attribuito ad un sistema della famiglia NT al momento dell’installazione. Conoscendo il SID è possibile definire i RID dei vari administrator e guest e trovare il nome degli account degli amministratori.
* SNMP: connessione UDP 161. È un protocollo (Simple Network Management Protocol) concepito per la gestione e monitoraggio della rete, for fornire informazioni sui dispositivi, software e sistemi di rete che sono vittime di attacchi.  
  I dati SNMP sono protetti da un sistema di autenticazione mediante password, ma sfortunatamente esistono diverse password di default ormai ben note. Generalmente la password più comune è “public” e viene cercata di indovinare usare wireshark cercando la stringa nella scansione delle porte.  
    
  Una variabile di questi comandi è OID (object identifier) che indica uno specifico ramo del MIB di Microsoft, un namespace gerarchico simile ai registri windows all’interno dei quali i vendors inseriscono dati.  
  I dati disponibili dall’enumerazione SNMP sono i servizi in esecuzione, i nomi condivisi e le cartelle condivise oltre ai nomi di dominio e username.  
  Chi riesce ad ottenere informazioni, come se nel caso peggiore fosse abilitato il nome di comunità di default per la scrittura, potrebbe modificare parametri per tentare un attacco Dos.  
  Per prevenire l’enumerazione SNMP bisogna disabilitare gli agenti SNMP sulle singole macchine o almeno assicurarsi che la configurazione con nomi di comunità vengano scelti in modo da non essere indovinati. Bloccare le porte TCP UDP 161 e limitare l’accesso agli agenti SNMP.
* BGP: TCP 179. Il border gateway protocol è un protocollo di routing utilizzato dai router per propagare informazioni necessarie per instradare pacchetti ip. Osservando le tabelle di routing ci si può fare un idea di come sono le reti associate a quelle aziendali. BGP viene usata solo da aziende medio grandi con più uplink.  
  Per enumerare BGP bisogna determinare l’ASN (Autonomus system number) dell’organizzazione bersaglio ed eseguire una query sui router per individuare tutte le reti in cui l’AS path termina con l’ASN dell’organizzazione.  
  Questo sistema non ha contromisure e non può essere bloccato.
* LDAP Windows Active Directory: TCP.UDP 389 e 3268. É un servizio di directory basato sul protocollo LDAP progettato per contenere una rappresentazione logica unificata di tutti gli oggetti relativi all’infrastruttura tecnologica aziendale, quindi fonte primaria di informazioni. Un hacker potrebbe utilizzare ldp.exe su un host con windows 2000 ed enumerare tutti i gruppi e gli utenti esistenti con una query. Come contromisura utilizzare il filtro sulle porte 389 e 3268 e non fornire la possibilità di accesso senza autenticazione.

# Hacking Windows – Chapter 4

## Attacchi senza autenticazione

I principali vettori per compromettere sistemi Windows da remoto sono:

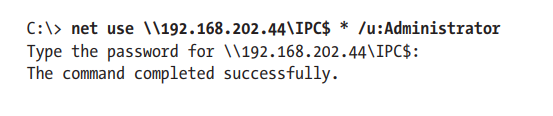
* Falsificazione dell’autenticazione (spoofing)
* Servizi di rete
* Vulnerabilità dei client
* Driver di periferica

### Spoofing

Tecniche che prevedono di indovinare o falsificare le credenziali di autenticazione per ottenere l’accesso non autorizzato a windows.

La via tradizionali per violare da remoto è quella di attaccare il servizio di condivisione file e stampanti SMB attraverso porta TCP 445 e 139.   
Altri servizi vittima di attacchi che puntano all’indovinare la password sono MSRPC su porta TCP 135, TS su porta TCP 3389, SQL su porta TCP 1433 e UDP 1434 e altri come Sharepoint su http/s.

Un altro metodo è quello di connettersi ad una condivisione enumerata (IPC$ o C$) e tentare combinazioni di utenti e password tramite riga di comando:



Attraverso uno script ed un ciclo for, usando file di test con una lista di utenti e password, è possibile iterare il processo.



Questo codice cattura dal file txt i primi due elementi di ciascuna riga inserendo il primo come variabile per password e l’altro per l’utente.  
  
Metodi per difendersi sono: l’utilizzo di un firewall per limitare l’accesso ai servizi vulnerabili, sia firewall di rete che firewall su host; disabilitare servizi non necessari; imporre password forti; registrare nei log tentativi di accesso falliti.

Il firewall di rete bloccherà gli accessi a tutte le porte TCP e UDP (139 e 445 di SMB) se il sistema non è interessato a rispondere a delle richieste di condivise.

La disabilitazione dei servizi di rete non necessari come NetBios e SMB è importante.

I criteri della password possono essere impostati dal pennello di controllo per gestire lunghezza e utilizzo di caratteri speciali, oppure usare secpol.msc da terminale.

Il controllo dei log può essere fatto attraverso strumenti di analisi e manipolazione dei file da riga di comando come Dumpel.

Le password possono essere spiate attraverso tre attacchi: **LM, NTLM e Kerberos**.  
Gli attacchi verso il protocollo di autenticazione Lan Manager (LM) sfruttano un punto debole nell’implementazione del meccanismo di richiesta/risposta di Windows. È facile individuare l’hash LM originale che equivale ad una password, usata per decodificare le password in chiaro. Lo strumento più usato per questo è Cain. Integra funzioni di sniffing delle password e decodifica di tutti i dialetti Windows disponibili con tecniche di attacco brutto, dizionario e rainbow cracking. È possibile fare lo spoofing ARP reindirizzando il traffico sulle proprie reti.

Kerberos è un protocollo di autenticazione. È previsto l’invio di un pacchetto di preautenticazione che contiene un testo in chiaro (timestamp) cifrato con una chiave derivata dalla password dell’utente. Se si riesce a decifrare il pacchetto tramite forza bruta o dizionario, si avrà accesso alla password.

Per difendersi, quindi, è utile disabilitare l’autenticazione LM o al massimo usare un dialetto NTLM che è molto difficile da violare.

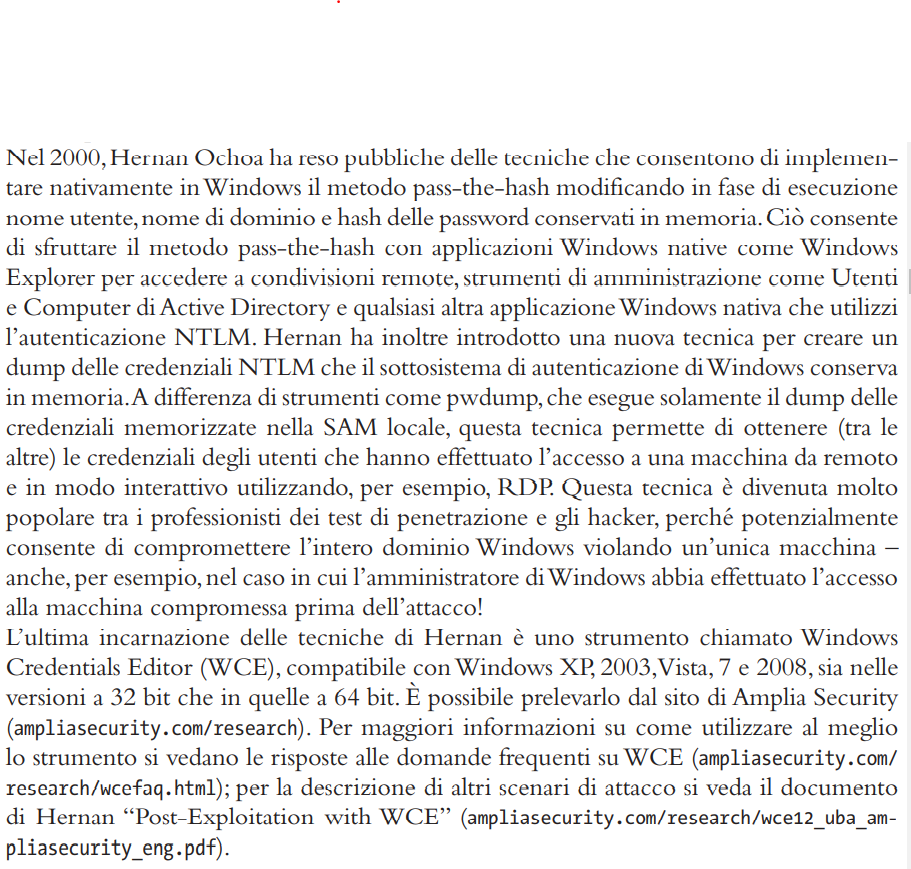
Attacchi **Man in the Middle** compromettono l’integrità del canale di comunicazione tra client e server impedendo lo scambio di informazioni sicuro. Inserendosi nella comunicazione tra client e server. Se il client possiede dei privilegi, l’hacker può autenticarsi come client e godere dei privilegi avendo accesso alla shell. I primi attacchi sono stati fatti su server SMB. Generalmente si spinge un cliente a connettersi ad un server SMB malevolo ed autenticarsi.

Tool capaci di effettuare attacchi simili sono Squirtle, che consente di intercettare autenticazione NTLM in connessioni SMB e anche http, IMAP, POP3 e SMTP.

Altri sono CAIN e SMBRelay3.  
Gli attacchi di questo tipo richiedono che l’hacker si trovi vicino al sistema bersaglio, esempio come LAN locale. In questo caso è difficile contrastare un attacco simile.  
Si fa uso di comunicazioni autenticate e cifrate per ostacolare client o server fittizzi. In SMB è stata inserita la firma smb per autenticare la connessione.

Disabilitare anche il servizio nomi NetBios in quanto basandosi su UDP è facilmente violabile.

**Pass the Hash** è una tecnica che consente ad un hacker di autenticarsi su di un server remoto utilizzando l’hash LM e/o NTLM della password di un utente.  
Nel caso di autenticazione NTLM, gli hash delle password di windows sono equivalenti alle password in chiaro, quindi possono essere utilizzate per ottenere l’accesso.



**Pass the ticket** quando si usa l’autenticazione Kerberos, i client si autenticano per servizi remoti su sistemi remoti utilizzando dei ticket, e all’accesso creano nuovi ticket con TGT fornito dal KDC (key distribution Center) che fa parte del controller di dominio.Il pass the ticket permette ad un hacker di eseguire il dump dei ticket windows kerberos e riutilizzarli assieme al TFT. Una volta aperta una falla, l’hacker può eseguire il dump dei ticket kerberos esistenti.

**Exploit senza autenticazione da remoto**

Le tecniche di exploit senza autenticazione da remoto puntano a difetti o errori di configurazione del Windows.

Strumenti che effettuano exploit è Metasploit.

Gli exploit degli utenti è un ottimo bersaglio per gli hacker a causa del fatto che l’ambiente del client è pieno di software anche mal configurato. Questo ha portato la Microsoft a concentrarsi tanto sulla sicurezza lato client con continue patch. Una delle applicazioni più attaccate è Adobe flash player.

Le contromisure per queste cose sono l’utilizzo di un firewall persone, eseguire scansioni antivirus e aggiornarsi alle patch rilasciate.

Anche i driver periferici vengono presi di mira come per esempio quando i driver di rete wireless di windows potevano essere attaccati semplicemente passando vicino ad un access point violato che inviava pacchetti beacon sospetti. La problematica principale è che queste periferiche eseguono in modalita kernel con privilegi elevati, interfacciandosi a basso livello con l’hardware.

## Attacchi con autenticazione

### Privilegi

Ottenuto un account utente in Windows, si cerca di ottenere i privilegi di amministratore o SYSTEM.

Il primo attacco simile fu fatto tramite getadmin, che è un attacco a scalata dei privilegi contro Windows NT4 tramite la DLL injection. Per evitare attacchi di questo tipo bisogna installare tutte le patch di aggiornamento poiché getadmin sfrutta difetti del sistema operativo e finchè non viene risolta a livello codice, è indifendibile.

I privilegi di SYSTEM sono i massimi privilegi che si possono avere su di una macchina.

Bisogna inoltre limitare i privilegi di accesso interattivo, controllando il menù Criterilocali\ Assegnazione diritti utente e verificando se il diritto accesso locale è assegnato a qualcuno.

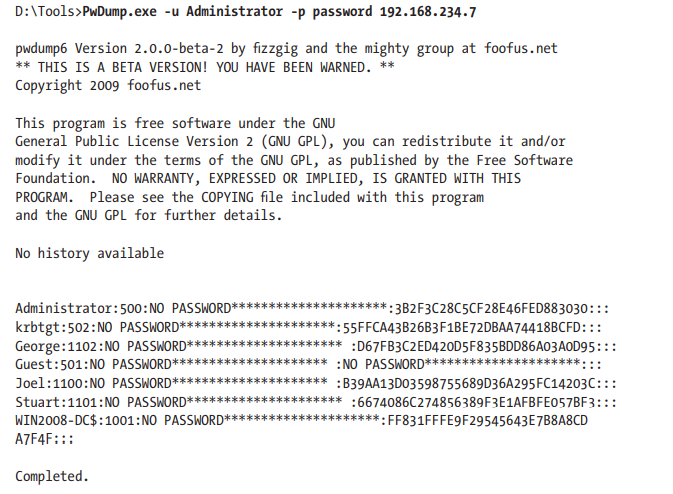
Il primo passo, una volta ottenuto lo status di amministratore, è quello di sottrarre informazioni dal sistema come le password e gli utenti.

Per attaccare gli hash delle password, si fa riferimento al SAM (security account manager) che è l’equivalente di etc/password in unix per utenti locali e in Active directory sul controller di dominio.

Per ottenere gli hash delle password ci sono diversi metodi a seconda della versione di Windows. Generalmente sono memorizzati in %sistemroot%\system32\config\SAM che normalmente è bloccato durante l’esecuzione del SO. Questo file è anche rappresentato come uno dei cinque sottorami principali del registro di Windows sotto la chiave HKEY\_LOCAL\_MACHINE\SAM anche se non è facile da essere modificata anche dall’amministratore stesso.

Sui controller di dominio gli hash si trovano in Active directory in %windir%\WindowsDS\ntds.dit.

L’estrazione degli hash avviene tramite il dump degli hash direttamente dal registro in un formato adatto per l’analisi offline. Un tool adatto è ciò è pwdump. Questo utilizza la DLL injection per inserirsi in una serie di processi in esecuzione con privilegi (Isass.exe) al fine di estrarre gli hash. Anche Cain funziona allo stesso modo.



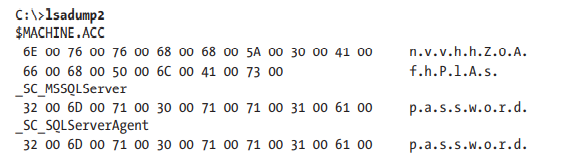
### Cracking delle password

Quello che è stato ottenuto è l’hash della password che però rende difficile il ricavare la password in chiaro. Il processo che porta a fare questo viene chiamato **cracking delle password** che consiste nell’ indovinare la password facendo delle esecuzioni offline. Una volta noto l’algoritmo di hashing, si cerca di calcolare la password usando per esempio le parole del dizionario, facendo anche dei confronti. Tendenzialmente il crack delle password cerca di scovare degli algoritmi di hash deboli:

* L’algoritmo di hashing di LAN Manager (LM) presenta gravi vulnerabilità che permettono di violarlo. La password è suddivisa in due parti di 7 caratteri e tutte le lettere sono trasformate in maiscuolo, il che riduce le 2^84 possibili password alfanumerica ottenibili con 14 caratteri a soli 2^37 hash diversi.   
  Il nuovo hash NTLM non presenta più questi punti deboli.  
  Tutti gli hash di Windows soffrono di un altro punto debole: mancano di un salt. Gli altri sistemi operativi aggiungono un valore casuale denominato salt ad una password, prima dell hashing e della memorizzazione. Il Salt è memorizzato insieme all’hash in modo da verificare la corrispondenza. Essendo randomico come valore, l’hacker farebbe molta difficoltà a precalcolare le tabelle di hash per ogni salt.

Windows inoltre mantiene i dati delle password memorizzati anche in varie cache. È utile quindi andare a cercare questo tipo di dati con i privilegi ottenuti. La cache di LSA (local security authority), specificata nella sottochiave HKLM\SECURITY\ Policy\ Secrets del registro di sistema contiene:

* Password di account di servizio in chiaro
* Cache contenenti gli hash delle password
* Password in chiaro di utenti FTP e web
* Nomi di account e password del servizio di accesso remoto
* Account e passowrd per l’accesso al dominio



Nel tempo windows ha spostato alcuni elementi e reso LSADump2 utilizzabile solo da SYSTEM.

### Backdoor

Ottenuti i privilegi e le password, si possono abilitare i servizi che permettono il **controllo remoto e backdoor**.

Una della più facili da impostare è netcat mettendolo in ascolto su una certa porta rendendo possibile la connessione da remoto e l’esecuzione di un programma quando un sistema remoto si connette.

Attraverso il comando:



Si ottiene la shell dell’host sotto attacco nel proprio sistema remoto.

Un altro tool quando si accede a SMB (tcp 139 o 445) è psexec.

Un altro ancora è metasploit.

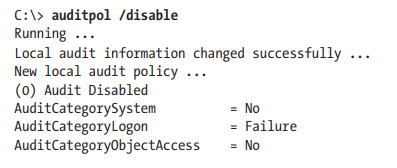
È possibile anche ottenere una shell orientata alla grafica. Se si ha accesso a terminal server si può tentare di collegarsi ad un sistema remoto che è in ascolto sulla porta tcp 3389. Un servizio simile è VNC.

### Reindirizzamento delle porte

Quando un hacker tenta l’accesso ad un sistema può essere bloccato dal firewall. Attraverso il reindirizzamento delle porte è possibile raggirare il firewall.  
Il reindirizzamento permettete a tutti i pacchetti di essere reindirizzati verso una destinazione specifica attraverso l’utilizzo di un programma che è messo in ascolto su una determinata porta. Un programma che fa questo è fpipe. è in grado di creare un flusso TCP con una porta di origine opzionale, una porta in ascolto e una porta di destinazione: è utile per oltrepassare i firewall che permettono il passaggio di certi tipi di traffici.

### Coprire le tracce

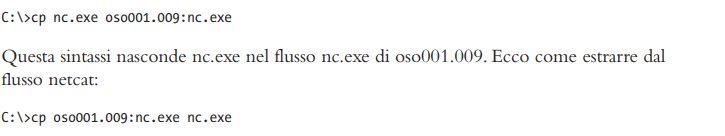
Una volta ottenuti i privilegi di sistema, l’hacker cerca di non lasciare tracce.  
Viene tentato di disabilitare il controllo di windows (auditing). Attraverso lo strumento auditpol viene tentata disabilitazione.



Inoltre, è possibile cancellare le proprie tracce nel registro degli eventi di windows attraverso il visualizzatore eventi.

Un hacker potrà anche lasciare un toolkit sul sistema bersaglio per degli attacchi futuri. Questi devono essere nascosti in alcune cartelle. Basta copiare i file in una directory ed utilizzare DOS attrib per impostare l’attributo di file nascosto. Ciò nasconde i file dagli strumenti da riga di comando ma non da GUI.

Se invece il sistema bersaglio utilizza NTFS, gli hacker possono inserire più flussi di informazioni in un file. Permette quindi di nascondere i toolkit in flussi che stanno dietro dei file. Questa tecnica è chiamata ADS (alternate data streams). Per eliminare un file inserito in un flusso si possono usare utility oppure copiare il file in una partizione FAT e ricopiarlo in un file system NTSF.



Le contromisure da prendere in caso di violazione della procedura di autenticazione non sono semplici dato che chi riesce ad ottenere i privilegi può camuffare tutto ciò che fa in tanti modi.

Innanzitutto, cercare diversi programmi che potrebbero richiamare la shell sotto falso nome in varie posizioni del disco. Controllare con fare sospettoso i file contenuti in PROGRAMS\STARTUP\ dato che presenta file che vengono eseguiti all’avvio del SO.

Dare un’occhiata anche alle chiavi di registro HKEY\_USERS\.DEFAULT\Software\ORL\WINVNC3 ed eventualmente eliminare le chiavi tramite REG.EXE del Resource kit.

Gli hacker utilizzano valori del registro di sistema sotto chiavi di avvio standard di Windows, in HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run e RunOnce.

Controllare periodicamente lo stato delle porte in LISTENING ed ESTABLISHED con netstat -aon.

# Hacking Unix – Chapter 5

## Accesso Remoto

L’accesso remoto comporta l’accesso attraverso una rete o altri canali di comunicazione ad un sistema UNIX.

I tipi di attacchi in accesso remoto sono:

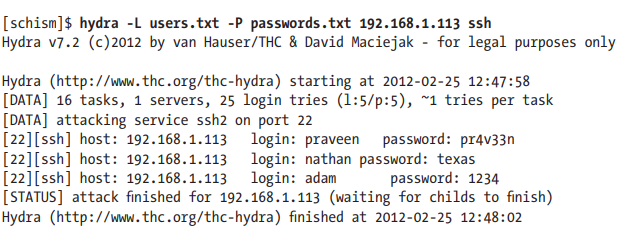
* Exploit di un servizio in ascolto.
* Routing attraverso un sistema UNIX
* Esecuzioni di programmi in remoto avviata dall’utente
* Attacchi in modalità promiscua

### Brute Force Attack

È un attacco utilizzato per scovare la password di un sistema attaccato e sono molto efficaci. Consiste nell’individuare una combinazione user ID/ password su un servizio che richiede l’autenticazione dell’utente prima di concedergli l’accesso.  
I servizi che vengono attacchi sono: telnet, FTP, comandi “r” (RLOGIN,RSH), secure Shell (SSH), SNMP, POP, http, CVS, Postgres e simili.

I servizi che vengono utilizzati per scovare gli account utenti sono finger, ruscrs e sendmail.  
Ottenuto l’account con la password possono provare ad ottenere una shell di sistema.

Per ottenere una password si fa uso di due utility quali **THC Hydra** e **Medusa.**



In questo caso vengono forniti due file ad Hydra che utilizzerà per tentare l’accesso via SSH in questo caso. Data la quantità di combinazioni possibili fra user e password, sono stati riscontrati i seguenti account con user e password forniti.

Le contromisure contro gli attacchi simili consiste nell’usare password molto forti e complesse e tutto ciò che contorna il concetto di password complessa.

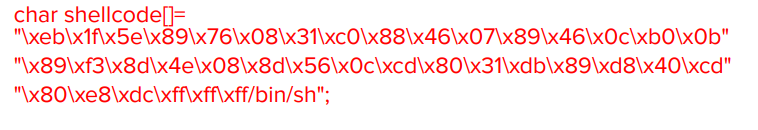
### Attacchi data-driven

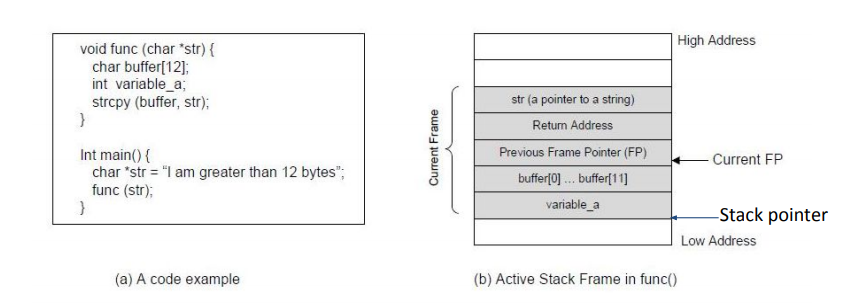
Gli attacchi data-driven servono ad ottenere l’accesso remoto. Inviano dati ad un servizio attivo per causare risultati inattesi o sgraditi.  
Attacchi di questo tipo sono i buffer overflow e attacchi di convalida dell’input.

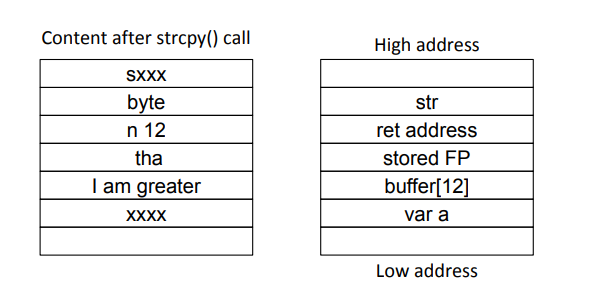
Un attacco di buffer overflow si verifica quando un utente o un processo tenta di inserire in un buffer una quantità di dati superiore a quella precedente allocata. Questo comportamento è associato a specifiche come strcpy(), strcat() e sprintf().

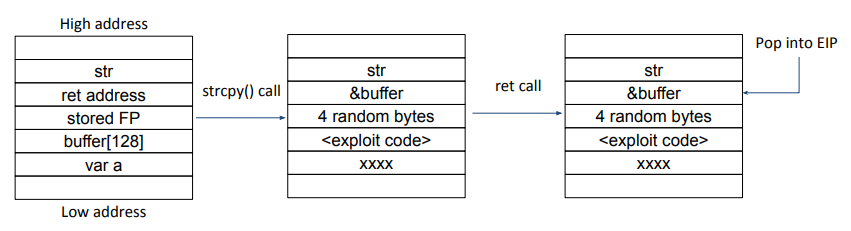
Un buffer overflow causerebbe un errore di segmentazione ma viene sfruttato in maniera differente per ottenere l’accesso ad un sistema.

Ipotizzando di avere un buffer allocato con una lunghezza fissa di 12 byte, durante l’esecuzione del programma l’hacker immette una stringa molto più lunga tramite un servizio avviato con set User ID (SUID) root e che quindi sia in esecuzione con i permessi di root. Il buffer in questa maniera traboccherà e causerà il blocco del servizio. Se invece di inviare del test a caso più lungo dei 12byte viene inviato un codice preciso, l’hacker causerà quello che viene chiamato Buffer Overflow. Infatti questo codice preciso che andrà a posizionarsi in quell’area di memoria destinata al “return address” farà partire, per esempio, il comando di /bin/sh. Impostando questo codice specifico in quell’area di memoria, l’hacker imposta l’indirizzo di ritorno della funziona alterando il flusso di esecuzione del programma. In questa maniera la funzione non tornerà alla locazione corretta ma eseguirà /bin/sh









Se invece il buffer può contenere tutto il nostro codice malevolo, quello che può essere fatto è di impostare come indirizzo di ritorno non quello della funzione ma l’indirizzo del buffer contenente il codice.

Contromisure contro il buffer overflow sono l’utilizzo della SSP (stack smashing protector) fornita dal compilatore gcc. Cerca di individuare gli overflow dello stack nel tentativo di ridurre al minimo l’attacco.  
Poi validare tutto l’input modificabile dall’utente, quindi verificando i limiti per ogni variabile. Utilizzare routine più sicure come fgets(), strncpy() e strncat() e soprattutto ridurre il codice eseguito con privilegi di host.  
Alcuni suggeriscono di disabilitare l’esecuzione dello stack che consente di proteggere da questo tipo di attacco in parte anche se questo non difende dagli overflow sull’heap.

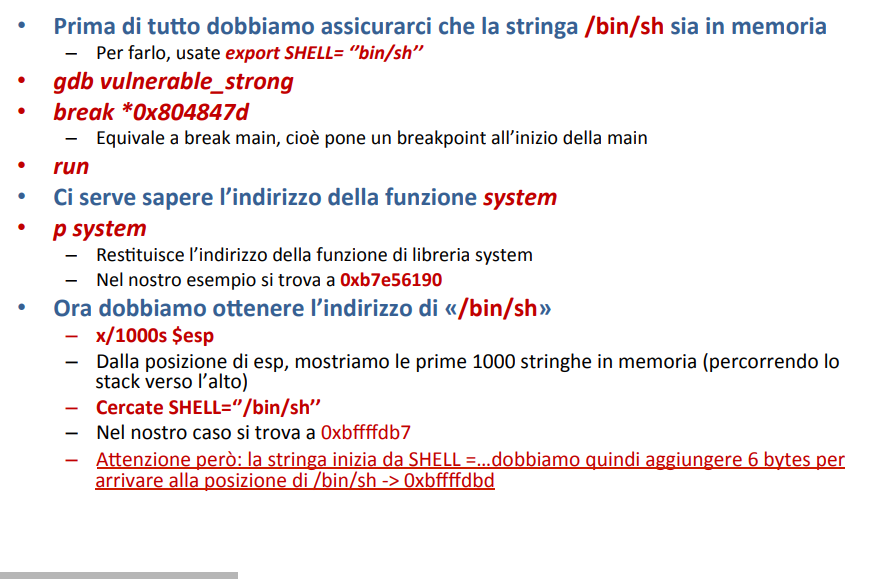
Per difendersi è stato pensato di randomizzare lo spazio degli indirizzi (ASLR) in modo da complicare all’hacker il tentativo di attacco ad indirizzi chiave.

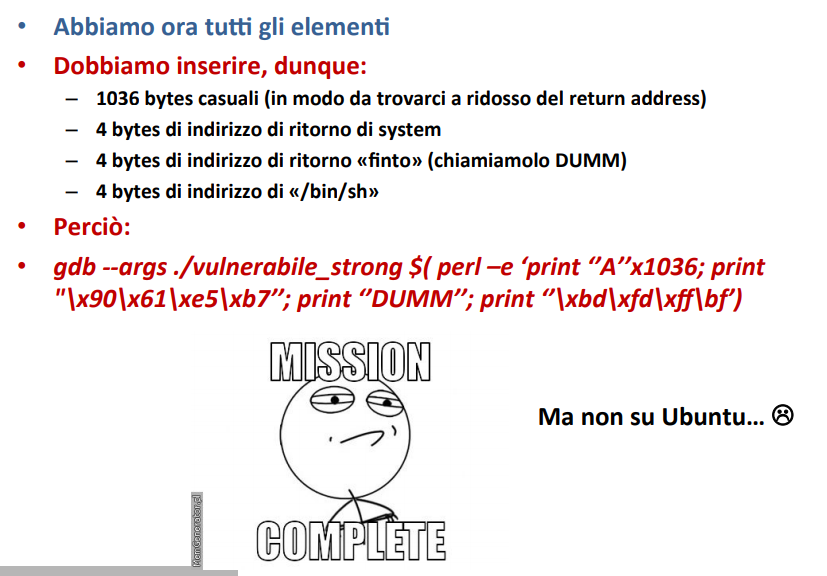
#### Return to libc

Questo tipo di attacchi è in sostituzione ai buffer overflow quando è attiva la protezione dell’esecuzione dello stack, impedendo l’iniezione di codice nello spazio degli indirizzi di un processo.  
L’attacco return to libc consiste nell’impostare come ritorno la libreria libc di C anziché verso il codice arbitrario inserito nello stack. In questa maniera viene scavalcato il controllo di esecuzione dello stack chiamando del codice esistente che non risiede sullo stack.

Viene sfruttata durante l’esecuzione del programma di quelle funzioni della libreria come system(), exit(), execl().

Mentre nel buffer overflow si va a riempire lo stack fino a raggiungere l’indirizzo di ritorno nel frame e poi sostituire l’indirizzo di ritorno con l’indirizzo del buffer, adesso voglio eseguire la funzione system con argomento (/bin/sh) ed ottenere la shell





#### Attacchi con stringhe di formato

Le vulnerabilità a stringa di formato nasce da errori di programmazioni presenti nella famiglia di funzioni per output con possibilità di formattazione come printf() o sprintf().  
Un hacker può sfruttare questi errori passando stringhe di testo realizzate in modo da contenere direttive di formattazione per fare eseguire al computer bersaglio alcuni comandi arbitrari.

Nel comando printf() viene cercato nella stringa di formato la presenza di un carattere % e quando la trova, recupera un argomento tramite la famiglia di funzioni stdarg. I caratteri che seguono % sono considerati come direttive che determinano il modo in cui la variabile sarà formattata come stringa di testo.  
Si verificano problemi quando il numero di direttive non corrisponde al numero di argomenti forniti.

Altri problemi si verificano quando un programmatore utilizza direttamente una stringa fornita dall’utente come stringa di formato, stampando tramite printf(buf) la variabile buf memorizzata dal passaggio di valori di un utente. I dati che buf potrebbe contenere direttive di formato come %x che permettono all’utente di leggere i dati memorizzati nello spazio di memoria del processo.

#### Attacchi a validazione dell’input

Un attacco a validazione dell’input si verifica a seguito di queste condizioni:

* Un programma non riconosce un input sintatticamente errato
* Un modulo accetto un input estraneo
* Un modulo non gestisce correttamente dei campi di input
* Si verifica un errore di correlazione campo-valore

La vulnerabilità che bypassa l’autenticazione è il risultato di problemi nella validazione dell’input. Il daemon telnet, in.telnetd, non effettua correttamente il parsing dell’input prima di passarlo al programma di login. Questo effettua delle ipotesi errate sui dati che deve ricevere. In questa maniera un hacker è in grado di autenticarsi senza conoscere la password utente. Necessita solamente di un nome utente valido che possa accedere al sistema via telnet. Affinche funzioni il daemon telnet deve essere in funzione e senza patch risolutive.



Quando si esegue la validazione dell’input si possono utilizzare due approcci fondamentali: validazione con blacklist che confronta l’input dell’utente con un insieme di dati considerati errati o pericolosi. Se l’input corrisponde ad un elemento della blacklist viene rifiutato sennò viene accettato.

Oppure una validazione con white list in cui viene accettato soltanto l’input che corrisponde a dei dati considerati corretti.

#### Attacchi integer overflow e integer sign

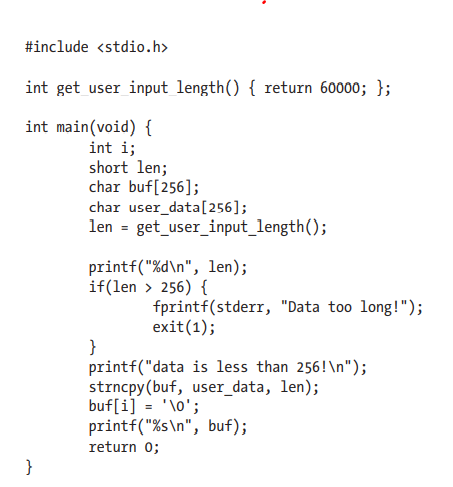
Simile al buffer overflow ma il colpevole oltre al programmatore è il compilatore.

Un numero intero è un tipo di dato positivo o negativo registrato in binario con un valore 0 o 1 nel bit più significativo del loro primo byte (1 negativo, 0 positivo). Gli interi senza segno non utilizzano questo bit perciò sono tutti positivi.

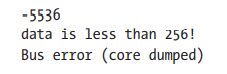
Un dato intero numerico ha una dimensione limitata. Un tipo di dato intero a 16 bit può memorizzare un valore massimo di 32767 mentre uno a 32 bit un valore di 2147483647.

Se si assegna un tipo di dati intero con segno il valore 60000 si verifica un integer overflow e il valore memorizzato nella variabile sarà -5536. Ogni compilatore può decidere la modalità di gestione di quel dato.

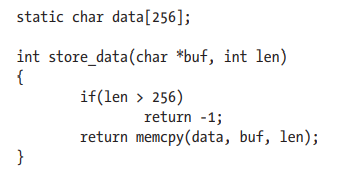
In un esempio in cui un programmatore deve copiare i dati forniti da utente, che possono essere molto grandi, se il programmatore tenta di assegnare la lunghezza di questi dati ad un tipo di dati troppo piccolo si verifica un overflow



In questo caso, dato che il valore di 60000 viene cercato di far rientrare in un tipo di dati intero a 16bit, il calcolatore leggerà quel valore come -5536. Questo valore dal programma non viene visto come un errore ma nel frattempo lo stesso valore sta creando un overflow



Gli attacchi con segno sono simili. SI verifica quando un intero senza segno è assegnato ad uno con segno. Dato che il computer non conosce la differenza tra byte con segno e senza segno, spetta al compilatore assicurarsi che sia generato un codice in grado di distinguere queste variabili.



Se si passa un valore negativo a len (intero con segno), si bypassa il controllo del buffer overflow. Dato che memcpy() richiede un intero senza segno per il parametro della lunghezza, la variabile con segno len viene promosso ad intero senza segno perdendo il segno negativo, e si verifica un wrapping ottenendo un numero positivo molto grande per cui memcpy() prosegue la lettura oltre i limiti di buf.

Gli attacchi integer overflow fanno di miccia per attacchi di buffer overflow, quindi le stesse contromisure vanno bene.

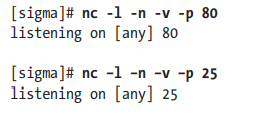
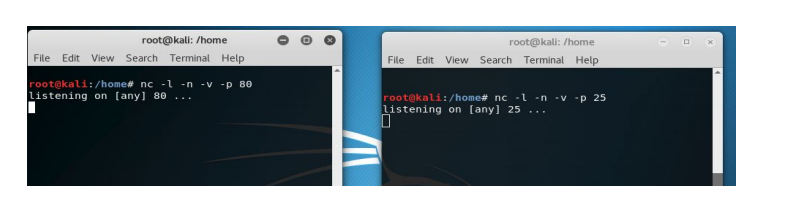
## Accesso alla shell

L’accesso alla shell in modalità interattiva si ottiene con un login remoto in un server Unix via Telnet, rlogin o SSH. In modalità non interattiva si può fare attraverso comandi rsh, ssh o rexec.

Ipotizzando che il server sia coperto da firewall che non funge da proxy per alcun servizio, sappiamo che gli unici pacchetti che possono passare sono http porta 80, HTTPS porta 443.

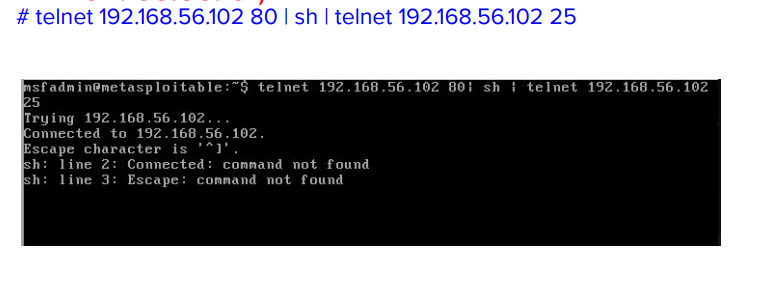
Viene un usato il back channel attack, cioè un meccanismo in cui il canale di comunicazione ha origine dal sistema bersaglio anziché dal sistema che porta l’attacco. Dato che non possiamo ottenere la shell in modo tradizionale avendo solo la 80 e la 443 come porte disponibili, dobbiamo sfruttare il canale di ritorno a seguito della sessione avviata col server.

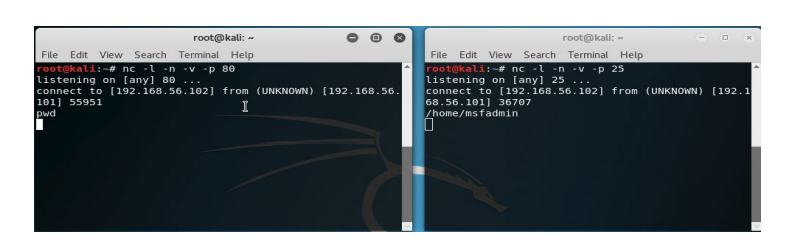
Il metodo è quello del telnet inverso. Un client telnet è generalmente disponibile sulla maggior parte dei server e raramente il suo utilizzo è riservato.  
L’hacker avvia telnet sul sistema bersaglio, e deve attivare anche netcat sul proprio sistema (listener nc) che accetti le connessioni di telnet inverso, eseguendo i comandi sul proprio sistema in due finestre separate per ricevere connessioni di telnet inverso.

Viene effettuato un attacco exploit tramite metasploitable richiedendo telnet sul sistema bersaglio.

In questa maniera metasploitable connette gli input da effettuare sul sistema bersaglio tramite la finestra relazionata alla porta 80 e riceve le risposte sulla finestra della porta 25.





Per proteggersi bisognare disabilitare tutti i servizi non necessari e applicare le patch rilasciate e fornire a Telnet una lista di utenti leggittimi che possono accedere alla shell.

Altri attacchi remoti sono:

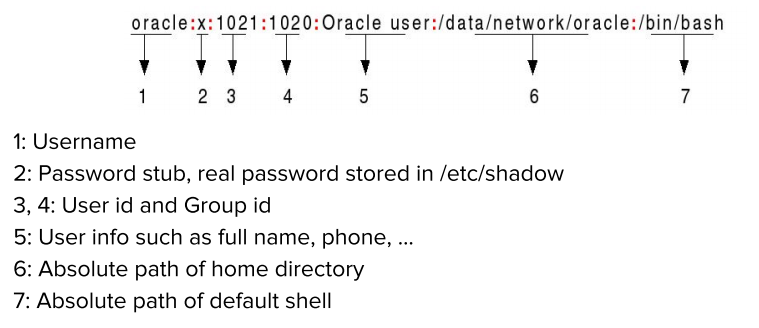
* **FTP** effettuare upload e download di file in sistemi remoti anche tramite accesso anonimo che riesce ad ottenere l’intera directory.
* **Sendmail** è un Mail Transfer Agent usato in linux che possiede tante vulnerabilità. Se configurato male invia spam tramite il server
* **DNS** l’hacker cerca la vulnerabilità più comune nel pacchetto BIND. I buffer overflow in BIND possono portare a delle risposte a query DNS malformate. Gli attacchi di avvelenamento della cache del DNS fanno si che i client contattino un server maligno, reindirizzando le loro richieste.
* **SSH** ha un difetto nel codice di individuazione degli attacchi CRC-32 in SSH1. Portava all’esecuzione di codice arbitrario nei server e clienti ssh.

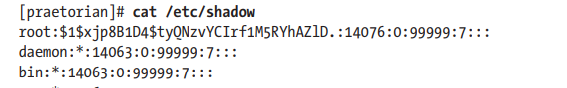
## Accesso locale

Una volta ottenuta una shell di comandi interattiva, si viene considerati interni al sistema. Si ottiene quindi un accesso utente per poi scalare di privilegi fino al root.

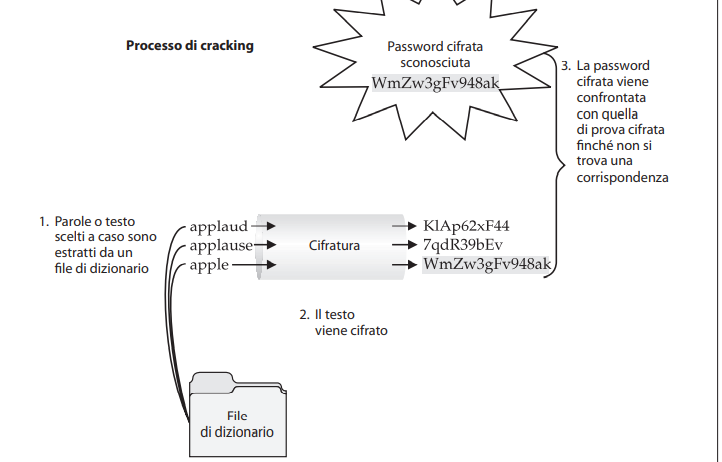
### Vulnerabilità della password

L’utilizzo di password deboli mette a rischio il sistema. Il cracking delle password è noto come attacco di dizionario automatizzato. Mentre l’attacco di forza brutta è considerato di tipo attivo, il cracking delle password può essere fatto in maniera offline ed è per natura passivo.





Bisogna avere accesso al file /etc/passwd o al file della password cifrate (etc/shdw). Viene tentato di determinare la password per un account eseguendo la cifratura di una parola o di un testo generato in modo causale e confrontando l’hash di password cifrato ricavato dal file delle password. Per Unix è necessario un input ulteriore chiamato “salt”, che funge da input ulteriore per l’hash al fine di garantire che due utenti con la stessa password non producano lo stesso hash di password. Questo evita anche l’attacco con tabelle precalcolate.



Il programma migliore per farlo è John the Ripper.

Il formato del file shadw presente tre campi separati da “$”, cioè il OS supporta il formato MCF.

La stringa composta specifica che l’hash è stato creato utilizzando MD5, il secondo campo contiene il seme usato per genere l’hash e il terzo contiene l’hash effettivo.

### Race Condition

Per race condition si intende lo sfruttamento di programmi o processi che stanno eseguendo in modalità privilegiata durante la finestra temporale a loro disposizione.

Le più comuni race condition sono quelle che riguardano la gestione dei segnali. I segnali vengono usati per notificare ad un processo che si è verificata una certa condizione, e fornire un meccanismo che consenta di gestire eventi asincroni. La capacità di alterare un flusso di esecuzione è un problema di sicurezza. Viene sfruttato un processo che ha problemi con la gestione dei segnali durante la modalità privilegiata, come accadde a FTP con i segnali SIGPIPE e SIGURG. Infatti, un utente accede a FTP con uid diverso da 0. Può decidere di chiudere la connessione inaspettatamente e il segnale SIGPIPE viene quindi inviato a FTP. Il server FTP allora chiama la funzione per il logout() con uid 0 in root. Gli hacker sfruttano questo arco temporale per cercare di connettersi a FTP con privilegi di root cercando di interrompere le sue attività con il segnale SIGURG.

### Manipolazione file core

Una vulnerabilità per la manipolazione dei file core è stata trovata in vecchie versione di FTPD che consentiva ad un hacker di fare in modo che il FTP server scrivesse un file core accessibile in scrittura nella directory root del file system, se si inseriva il comando PASV prima di accedere al server.  
Il file core conteneva porzioni del file di password shadow e gli hash.

### Librerie condivise

Le librerie condivise consentono ai file eseguibili di richiamare porzioni di codice da una libreria comune quando sono eseguiti. Questo codice è collegato ad una libreria condivisa host durante la compilazione. Il vantaggio di usarle sta nel risparmio di spazio e memoria e maggiore manutenzione del codice. Se gli hacker fossero in grado di modificare la libreria, possono ottenere accesso root.

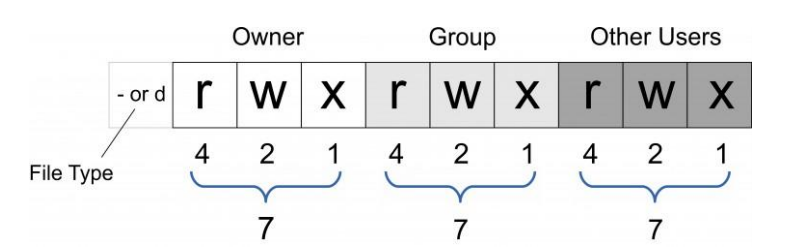
### Difetti del kernel

I difetti del kernel si riversano poi su tutto ciò che riguarda la sicurezza del sistema. Il difetto di verifica dei permessi può essere sfruttato per modificare la memoria di un processo nel kernel.

### Permessi su file e directory

In Unix ogni cosa è un file con i relativi permessi. I principali abusi vengono effettuati sui file SUID root e sui file accessibili a tutti in scrittura.

Attraverso il comando “ls -l” è possibile avere la lista dei file con i relativi permessi



I permessi sono di tre tipi: lettura, scrittura ed esecuzione. Identificati da un numero. Le classi di accesso al file sono il proprietario, il gruppo o gli altri utenti.

Ogni file presente 3 permessi speciali per ogni classe che consentono di impostare determinate funzioni avanzate sui file: SUID (set user id), SGID (set group id), Sticky.

Impostando SUID su un file si fa in modo che chiunque esegua quel file ottenga gli stessi privilegi dell’utente proprietario. Il problema sorge quando il proprietario è root.  
Impostando SGID il permesso impostato sulla directory invece che sul file. Qualsiasi file creato all’interno della stessa cartella erediterà lo stesso gruppo di appartenenza della cartella.

La modalità sticky viene applicata ad una directory e consente la cancellazione dei file solo ai legittimi proprietari.

I file con SUID e SGID root sono letali.

Un altro difetto si ha quando i file riservati sono accessibili a tutti in scrittura, quindi qualsiasi utente può modificarli.



### Trojan

Una volta ottenuto l’accesso di root, gli hacker possono inserire dei trojan per tutti i comandi del sistema. Uno può essere quello che fa da versione alterata di login che fa accedere in maniera normale gli utente mentre traccia in un file nome utente e password. Altri trojan potrebbero creare delle backdoor eseguendo dei listener TCP.

I trojan sono difficili da individuare. Le tecniche migliori si basano su firme univoche per ogni file da controllare.

### APT Sniffer

Quando un hacker installa uno sniffer di rete hanno la possibilità di attaccare qualsiasi sistema che invia del traffico all’host attaccato. All’interno dei pacchetti passano tantissimi dati riservati compresi password e utente. Lo sniffer si mette in ascolto sulle interfacce della scheda di rete. Generalmente una scheda di rete rifiuta il traffico non indirizzato alla scheda stessa quindi è necessario portare la scheda in modalità promiscua

### Cancellazione dei log

I log contengono le informazioni riguardo tutte le attività del sistema. Gli hacker per far notare la presenza cancellano i log tramite dei rootkit.

# Crimini cibernetici e minacce avanzate persistenti (APT) – Chapter 6

APT è un termine che fa riferimento ad un hacker fa uso di strumenti avanzati per compromettere un sistema con lo scopo di ottenere l’accesso al sistema e portare via informazioni necessarie. Sta per advanced persistent threat cioè minacce avanzate persistenti e descrive praticamente i tre aspetti che compongono il profilo dell’hacker, lo scopo e la struttura dell’attacco:

* Avanzata perché l’hacker ha un’ottima conoscenza dei metodi di intrusione e delle tecniche di amministrazione
* Persistente perché l’obiettivo è a lungo termine
* Minaccia perché l’hacker possiede finanze e motivazioni per portare l’attacco.

Gli apt si differenziano da malware perché usano normali funzioni quotidiane del sistema operativo e si nascondono nel file system. Gli hacker non volendosi fare scoprire cercano di non interrompere le normali operazioni del sistema operativo.

La tecnica più popolare utilizzata per ottenere l’accesso alle reti è lo spear-phishin che si basa sulla posta elettronica. Viene mantenuto un record (in più luoghi) del messaggio, del metodo di exploit usato e degli indirizzi e protocolli di comunicazione usati per corrispondere con i computer controllati dagli hacker. La mail può contenere del malware che tenta di sfruttare il software della vittima o può portare l’utente ad un server che consegnerà il malware.

Altre tecniche diffuse sono l’SQL injection di siti web, i meta exploit dei software che girano sui server web, lo sfruttamento di vulnerabilità nelle applicazioni di social network, chiavette usb infette o hardware infetto.

L’apt si compone di fasi:

1. Scelta dell’obiettivo: la raccolta delle informazioni da fonti pubbliche o private per cercare vie di accesso. Uso della scansione delle vulnerabilità, ingegneria sociale e spear-phishing.
2. Accesso / compromissione: gli hacker ottengono l’accesso e determinano i metodi efficienti o efficaci per sfruttare i sistemi informativi.
3. Riconoscimento: Gli hacker scoprono l’architettura di rete, i server dei nomi, i controller del donimio e verificano i permessi degli utenti.
4. Movimento laterale: movimento verso altri host relazionati alla rete
5. Raccolta e trasporto di dati all’esterno
6. Amministrazione e mantenimento: mantenere l’accesso alla rete nel tempo

## Operazione Aurora

Nel 2009 aziende americane del comparto tecnologia e difesa sono state oggetto di intrusione e compromissione dei sistemi di gestione e configurazione del software. Come risultato si ebbe il furto di informazioni riservate.

Gli hacker hanno acquisito acceso alle reti delle vittime utilizzando email di spear-phishing mirate agli impiegati delle aziende. La mail conteneva un link a un sito web di taiwan, con all’interno un javascript maligno. Quando l’utente cliccava sul collegamento e accedeva al sito web, lo script sfruttava una vulnerabilità di IE che consentiva l’esecuzione di codice remoto puntando ad una zona di memoria parzialmente deallocata e lo script non veniva rilevato dagli antivirus. Quello che veniva trasferito nei computer target era un trojan download che sfruttava i privilegi del browser per scaricare e installare e configurare un trojan backdoor, cioè uno strumento di amministrazione remota (RAT). Questo RAT forniva accesso a comunicazioni crittografate via SSL. Gli indirizzi relativi a chi ha inviato l’email erano legati a Taiwan ma i veri comandi di controllo e comunicazioni sono stati ricondotti a due scuole cinese, che avevano interessi a competere con le aziende attaccate. Si pensa il tutto fosse anche supportato dal governo cinese.

## Anonymous

Gruppo di hacker del 2011. Hanno condotto attacchi DoS contro banche, agenzie governative rendendo pubbliche le informazioni che riguardavano identità dei vari funzionari e relazioni tra aziende ed enti pubblici. Le varie tecniche di hacking prevedevano la SLQ injection, cross-site scripting e altri exploit per vulnerabilità dei servizi in rete. Il loro principale obiettivo non era ottenere vantaggi competitivi o finanziari ma era un gruppo di interesse sociale: dimostrare che in pochi possono influenzare il destino di molti, interrompendo i servizi.

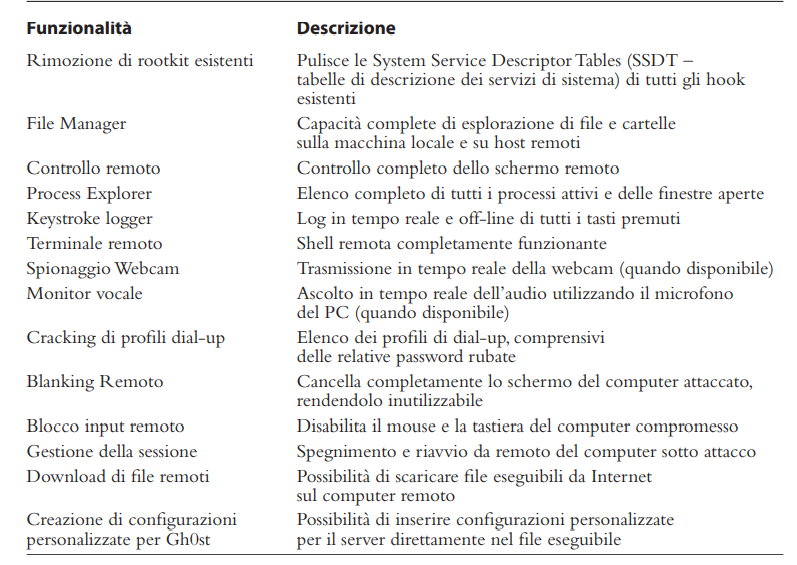
## RBN

Russian Business Network è un’organizzazione criminale russa del 2007. Gestisce diverse reti botnet conducendo campagne di spamming, fishing, distribuzione di malware. Hanno come scopo quello di lucrare su truffe finanziarie e di identità ed usano malware per restare in modo persistente sui computer target.

## Strumenti e tecniche APT

### Ghost

Ghost RAT è uno strumento utilizzato negli attacchi Ghostnet. Il principale obiettivo furono i servizi informatici del Dalai Lama. Gli attacchi provenivano dalla Cina.

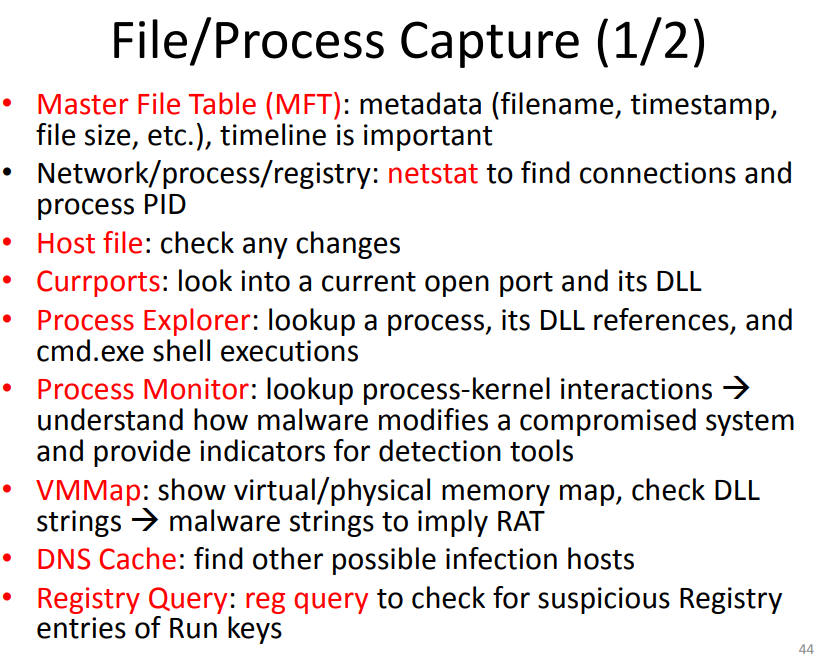


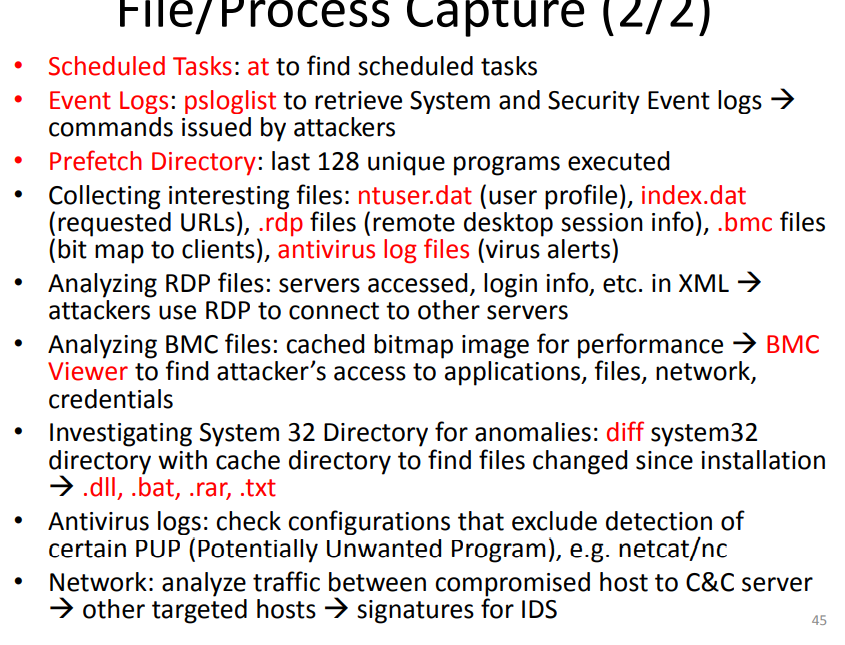
L’attacco si è composto di diverse fasi: è stata inviata una email malevole, il contenuto prevedeva una transazione finanziaria, con un collegamento all’interno. La transazione però aveva un dominio tedesco che niente aveva a che fare con l’azienda attaccata, dominio risultato poi in una black list per campagne di spam.

La connettività di rete mostrava l’apertura di una sessione con indirizzo IP sconosciuto. Analizzando i registri degli eventi, è risultato chiaro che gli hacker stavano perlustrando il dominio interno, creando account e utilizzo desktop remoto per saltare da un client all’altro. È stata notata la creazione di account per l’uso di FTP e la creazione di un job giornalieri di pulizia dei log.

Il malware fa di tutto per sopravvivere ad un riavvio del computer usando diversi meccanismi come: uso di chiavi di registro, creazione di un servizio, collegamento ad un servizio esterno, sovrascrittura del master boot record, sovrascrittura del BIOS del computer.

L’analisi della memoria fornisce il dettaglio sul fatto che i dati siano stati decriptati. Viene usato un tool Volatility Framework Tool che analizza processi, connessioni, DLL.





Per analizzare un sistema sospetto si controllano: memoria, file di paginazione o swap, informazione sui processi in esecuzione, dati di rete come porte in ascolto, registro di sistema, file di log.

Gli hacker si aprono diverse connessioni di rete, quindi è necessario controllare con netstat -aon.

Il process monitor consente di visualizzare le interazioni a livello kerner del processo con il filesystem e sistema operativo.

Può essere anche utile salvare l’elenco delle richieste DNS rimaste nella cache del sistema sospetto.

Un modo per cercare modifiche alla cartella System32 è quello di confrontarla con “diff” con la cache della medesima cartella. Si ottiene un elenco dei file modificati a partire dall’installazione.   
Netcat presente nella cartella %Temp% per essere usato come servizio per creare una backdoor su un sistema compromesso.

Sempre nella cartella %temp% ci possono essere stringhe che identifica l’utilizzo di un file ZIP contenente password o informazioni utili.

## Linux APT

# Remote Connectivity and VoIP Hacking – Capitolo 7

L’approccio per l’hacking dial-up si compone sempre di footprinting, scansione, enumerazione e attacco. Esistono degli strumenti, i war dialer o daemon dialer, che compongono da programma una serie di numeri telefonici e quando rilevano una linea dati, cercano di identificare il sistema che si trova dall’altra parte della linea telefonica per tentare un approccio di login con utente e password di uso comune.

Il tutto, quindi, inizia con l’individuazione di blocchi di numeri da fornire ai war dialer tramite l’utilizzo di rubriche pubbliche o con l’ingegneria sociale.

La scelta dell’hardware specifico per il wardialing è molto importante: utilizzo di più modem, la modalità in cui sono collegati e la configurazione delle porte COM.

Il wardialing ha a che fare con gli aspetti burocratici e legali di ogni paese riguardo l’attività di identificazione di linee telefoniche, registrazione e uso di numeri falsi.

## Script di forza bruta

Una volta ottenuti dall’output di uno dei programmi di wardialing si procede con la classifica dei domini. La scelta di quale sistema attaccare dipende da tanti fattori che è necessario conoscere e classificare. Ottenute le informazioni necessarie, vengono inserite in questi domini di penetration wardialing. Esistono quattro domini che vengono scelto in base al numero di meccanismi di autenticazione e sul numero di tentativi di accesso consentiti:

Immagine che contiene testo

Descrizione generata automaticamente

## Hacking centralini telefonini

Esistono ancora connessioni dial-up a centralini telefonici (PBX). Data la scarsa cura con cui vengono gestiti dalle aziende, vengono hackerate.

Immagine che contiene tavolo

Descrizione generata automaticamente

Vengono violati anche i sistemi voicemail tramite forza bruta con Voicemail Box Hacker 3.0 oppure con VrACK 0.51.  
Vengono attaccati in maniera simile alle connessioni dial-up ma usando il metodo degli script di forza bruta.

## Hacking reti VPN

Le connessioni dial-up con accesso remoto sono state in parte sostituite tramite reti VPN che offre cifratura e tunnelling dei dati attraverso internet.

Prendendo in considerazione IPSEC come suite di protocolli a livello di rete per la cifratura ed autenticazione dei dati, questo usa IKE per la gestione delle chiavi della sessione. IKE possiede due fasi:

1. Scopo della fase 1 è di autenticare le parti ed impostare una comunicazione sicura per la fase due. Viene fatto in:
   1. Main mode: 3 handshaking separati a due vie (messaggi) per autenticare entrambe le parti
   2. Aggressive mode: 3 soli messaggi che autenticano le due parti in modo più veloce ma meno sicuro. Non fornisce un canale sicuro per proteggere le informazioni di autenticazione
2. La fase due stabilisce il tunnel a seguito dell’autenticazione.

La modalità aggressive può essere vittima di attacchi dato che non fornisce una sicurezza elevata. Tramite IKE-PROBE viene testato se il server usa l’aggressive mode. Successivamente con IKECrack viene avviata una connessione al server VPN per catturare i messaggi di autenticazione e tentare attacchi di forza bruta.

Google può fornire informazioni per un attacco VPN come il **filetype:pcf.** L’estensione pcf è usata per identificare un profilo per un client vpn cisco. Cercando su internet file di questo tipo si possono ottenere profili del bersaglio e cercare di connettersi al server. Le password possono essere riutilizzate per ulteriori attacchi, dato che sono salvate nel file.

Quando si attacca un server VPN si deve controllare se la porta di attacco è disponibile, generalmente la **UDP 500.**

Immagine che contiene testo

Descrizione generata automaticamente

Un altro tool è **ike-scan**  focalizzato su IKE che riporta sia l’host in ascolto per connessioni VPN ma anche identifica il supporto della modalità IKE fase1, fornendo informazioni hardware del server.

Immagine che contiene testo

Descrizione generata automaticamente

## Attacchi VoIP

VoIP è una tecnologia che sfrutta la comunicazione vocale su rete IP. Utilizza due protocolli almeno, uno per la segnalazione e uno per la trasmissione del traffico voce cifrato che sono H.323 e SIP (session initation protocol) che praticamente gestiscono le impostazioni, le modifiche e la chiusura delle chiamate. Le porte usate sono TCP/UDP 5060.

Data la complessità e il numero elevato di protocolli da utilizzare VoIP è sottoposto a numerosi attacchi.

### Scansione SIP

Il primo passo è quello di fare una scansione SIP per puntare a trovare altri proxy o dispositivi SIP tramite **SiVuS.**

### Saccheggio TFTP

Quando i dispositivi SIP attivano il processo di boot, si appoggiano ad un server tftp per recuperare i dati di configurazione quali username/password.

Basta conoscere il nome del server tftp e provare ad indovinare il file di configurazione, che generalmente hanno una nomenclatura specifica in base al produttore. In questa maniera viene svolto un attacco bruteforce con una lista di nomi.

Basterebbe limitare l’accesso a TFTP per evitare brutte sorprese.

### Enumerazione Utenti SIP

Oltre ai metodi di wardialing manuali e automatizzati, gli interni VoIP possono essere enumerati tramite osservazione della risposta di un server dato che il protocollo di comunicazione è di facile lettura e quindi di facile analisi.

L’enumerazione automatizzata è fornita da alcuni tool quali **svwar.py, SIPScan e sipsak.**  A questi tool è possibile passare una serie di opzioni quali un file dizionario oppure un intervallo di numeri interni. Inoltre supportano le tecniche di enumerazione con OPTIONS, REGISTER e INVITE che sono i metodi supportati dal protocollo.

## Attacco di intercettazione

Consiste nell’intercettare il flusso del protocollo di segnalazione (SIP, SKYNNY,UNIStim) ed RTP tramite lo spoofing ARP dato che la maggior parte degli switch aziendali non hanno funzioni di sicurezza attivati.

Sul server di intercettazione viene attivato il routing, consentito il passaggio del traffico, disattivo il reindirizzamento ICMP ed incrementato il TTl tramite iptables

Immagine che contiene testo

Descrizione generata automaticamente

Dopodichè viene corrotta la cache ARP del client tramite arpspoof di dsniff, in modo da accedere al flusso di dati VoIP tramite uno sniffer.

Un altro metodo è quello di seguire gli scambi SIP e ottenere le informazioni sulle perte dal campo MEDIA PORT di media Description. Una volta identificato il flusso RTP, occorre identitificare il codec usato per la codifica della voce che si trova nel campo Payload Type del flusso UDP o nel media format dello scambio sip. Dopodichè viene convertita la conversazione da un formato a WAV tramite vomit.

## Dos

Il denial of service è molto facile da compiere anche se non offre un elevato tasso di successo inviando un gran numero di configurazioni di chiamata false che segnalino traffico (SIP INVITE) oppure sommergendo un singolo telefono con traffico indesiderato. I tool utilizzati sono **inveteflood** o **hack\_library.**

# Hacking di reti Wireless – Capitolo 8

Esistono due tipi di reti wireless:

* **Infrastruttura**: necessitano di un access point per le comunicazioni tra client e tra rete cablata e wireless
* **Ad** **hoc**: lavorano con uno schema peer to peer senza access point.

Per comunicare il client avvia una sessione con l’access point tramite un messaggio chiamato **probe request,** con l’SSID della rete ricercata su tutti i canali disponibili attendendo una risposta chiamata **probe response.** Una volta che l’access point risponde, il client invia una richiesta di autenticazione. I due tipi di autenticazione disponibili sono: **autenticazione** **aperta**, dove l’access point accesso qualsiasi tentativo di connessione; **autenticazione** con **chiave** **condivisa** in caso la rete sia cifrata con chiave WEP.

A seguito dell’autenticazione vi è **l’association** **request** da parte del client con cui l’access point risponde con un **association** **response** con cui terrà traccia della comunicazione col client.

## Meccanismi di sicurezza

* **Filtro sugli indirizzi MAC**: gli access point hanno la capacità di verificare l’indirizzo MAC del Client durante la fase di autenticazione, confrontandolo con una lista di MAC.
* **Reti Wireless nascoste**: Gli access point, ad intervalli regolari, inviano dei segnali beacon che contengono l’SSID dell’access point. È possibile nascondere l’SSID all’interno dei beacon rendendo difficile gli attacchi in quanto l’SSID è necessario per potersi connettere ad una rete.
* **Non rispondere a messaggi probe request diffusi pubblicamente**: i client possono diffondere pubblicamente probe request senza alcun SSID all’interno per scoprire quali reti wireless sono disponibili. Se sia i client che gli access point sono preconfigurati, gli access point ignorano queste probe request.

## Autenticazione

L’autenticazione ha come obiettivo non solo quello di definire l’identità del client che si vuole connettere ma anche di creare una chiave di sessione per cifrare i messaggi che vengono scambiati. L’autenticazione avviene al livello 2, ancora prima che il client riceva l’indirizzo IP dall’access point.

La WPA (Wifi protected access) è una certificazione che identifica il livello di compatibilità di un determinato apparecchio con la specifica IEEE 802.11i. WPA conferma se un apparecchio è compatibile con TKIP mentre WPA2 se è compatibile con TKIP e AES.

WPA presenta due forme:

* WPA pre-shared key: utilizza una chiave precondivisa come parametro di input di una funzione crittografica che genera chiavi di cifratura per la protezione della sessione. È composta da 8-63 caratteri ASCII
* WPA Enterprise: utilizza IEEE 802.1x, standard usato per l’autenticazione delle porte degli switch. In questa configurazione, l’access point veicola le comunicazione di autenticazione tra client e server RADIUS sulla rete cablata 802.1x.

In entrambi i casi, client e server eseguono un processo di handshake a 4 vie per generare due chiavi di cifratura: chiave ptk per comunicazione unicast, chiave gtk per comunicazioni multicast e broadcast.

## Cifratura

La cifratura avviene a livello 2 dello stack. Le informazioni riguardo: indirizzo MAC, frame di gestione (probe, beacon.. ) non sono cifrati.

Esistono tre tipi di cifratura:

* WEP: predecessore di WPA, non prevede una fase di autenticazione obbligatoria. In questo modo, ogni partecipante alla rete conosce la chiave di cifratura. Utilizza RC4.
* TKIP: successore di WEP, basato su RC4 (rivest cipher 4). Utilizzato per essere compatibile anche con hardware di vecchia data. Era molto sicuro
* AES – CCMP: (Advanced encryption standard with cipher block chaining messagge authentication code protocol) molto sicuro e consigliato

## Equipaggiamento

È molto importare avere un equipaggiamento completo di tutto:

* Chipset
* Sistema operativo adatto
* Antenne omnidirezionali
* Supporto di entrambe le bande
* Interfaccia adattatore wireless

## Ricerca e monitoraggio di reti wireless

Vengono sfruttate le informazioni all’interno dei frame 802.11 dato che non vengono cifrate. In questa maniera è possibile individuare delle relazioni all’interno dei dati trasmessi e stabilire quali client siano connessi a quali access point.

Esistono due metodi di **ricerca** **wireless**:

* **Attiva**: vengono inviati messaggi probe request in broadcast e prendono nota delle risposte che ricevono dagli access point. Se gli access point sono settati bene, ignorano queste richieste.
* **Passiva**: i client ascoltano le informazioni in modo passivo su tutti i canali per raccogliere dati da analizzare per capire quali reti wireless sono presenti. Anche se gli access point nascondo il SSID, nei beacon viene inviato cmq l’indirizzo MAC. Quando un client si connette ad una rete, lo strumento di ricerca passiva sniffa i messaggi, legge l’SSID e collega il MAC al SSID. La ricerca passiva non è individuabile.

Gli strumenti di ricerca principali sono sviluppati su Linux e sono Kismet e airodump-ng, utilizzati molto spesso da persone che muovendosi per strada vanno alla ricerca di access point wireless dando vita alla pratica di war-driving.

## Sniffing del traffico wireless

Alcune reti sono prive di cifratura per motivi tecnici o per negligenza. Spesso un client utilizza una cifratura a livelli più alti del secondo dato che in caso di mancanza di cifratura, un attacco Man in the Middle è molto semplice. Lo sniffing del traffico è illegale in alcuni stati, come gli USA.

Gli strumenti che sniffano il traffico hanno la possibilità di salvare tutto il traffico in formato PCAP per poi analizzarlo con strumenti quali Wireshark, il quale mostra i pacchetti dei diversi livelli con i diversi protocolli. Se i pacchetti vengono coperti da cifratura, il contenuto risulta illeggibile anche da Wireshark. Oppure utilizzando una VPN anche se si trova in una rete wireless aperta.

## Attacchi Dos (Denial of Service)

Lo standard 802.11 prevede out of the box la possibilità di avere degli attacchi Dos in cui l’access point, per alcuni motivi quali chiavi di cifratura non corretta o sovraccarico, termina la connessione con il client. Situazioni di questo tipo quindi sono già previste e i client devono accettarle. Ovviamente sono presenti anche attacchi Dos non previsti.

Attacchi Dos previsti sono: **attacco di deautenticazione (deauth)** dove vengono creati dei frame di deautenticazione fasulli per indicare al client che l’access point intende chiudere la connessione o per indicare all’access point che il client intende scollegarsi.

Un tool che eseguo un attacco di deautenticazione è **aireplay-ng**  il quali invia un totale di 128 frame, 64 verso l’AP e 64 verso il client.

Viene specificato il canale, il livello, il bSSID, il client e l’interfaccia.

Immagine che contiene testo

Descrizione generata automaticamente

Quello che può succedere è che nel tentativo di riconnessione da parte di un client, lo sniffing delle probe request fornisce dettagli quali l’SSID nascosto, il quale mettendolo in collegamento con i messaggi di deautenticazione forniscono una panoramica completa della rete.

Si può fare poco contro chi abusa degli attacchi Dos dato che sono previsti dalla specifica 802.11.

## Encryption attack

Gli attacchi sulla cifratura avvengono se gli algoritmi di cifratura possiedono delle falle che mettono in pericolo la sicurezza dei dati.

Il meccanismo di cifratura WPA dipende dalla fase di autenticazione, quindi se esiste un bug in TKIP o in AES-CCMP si ha la possibilità di cifrare i dati. Ciò accade fino a che le chiavi di cifratura non vengono cambiate, dato che in WPA le chiavi sono temporanee.

In WEP non vi è una fase di autenticazione ne una rotazione delle chiavi quindi in caso di attacco riuscito si ha pieno potere.

### Attacchi contro WEP

Quando vengono inviati i dati su una rete cifrata con WEP, è richiesta la chiave WEP e un vettore di inizializzazione (IV) che viene generato in modo pseudocasuale per ogni frame ed inserito alla fine dell’header 802.11. La chiave e il vettore vengono usati per creare il keystream che viene usato per convertire il testo semplice in testo cifrato e viceversa. In fase di decriptazione viene usata la propria chiave, viene estratto il IV dal frame e viene creato il proprio keystream da usare. Inoltre viene effettuato un controllo checksum per validare il contenuto.

La problematica sta nel fatto che l’IV è un valore di 24 bit, molto breve e quindi vi è la possibilità di avere dei doppioni all’interno della rete. Se si individua un duplicato, si controlla il testo cifrato per indovinare il keystream che l’ha prodotto.

Il keystream può essere indovinato anche facendo dei confronti tra più frame particolari cercando di indovinare il contenuto. Se viene indovinato, è possibile cifrare tutti i frame e anche produrne di nuovi. Inoltre se si riesce a identificare la keystream si può anche scoprire la chiave wep.

**L’attacco passivo** prevede la cattura di un numero elevato di frame per esaminare gli IV e tentare di indovinare la chiave WEP. Per registrare i frame si può usare airodump:



Oppure anche aircrak-ng per effettuare analisi statistica dei dati WEP di un file PCAP per scoprire la chiave: fornisce la quantità di dati che si necessitano per ottenere la WEP, in base al numero di IV.



**ARP replay con falsa autenticazione** abusa di una serie di difetti di WEP per generare traffico su una rete wireless, fornendo ad aircrack-ng dei dati necessari per scoprire la chiave.

WEP non è in grado di capire il replay arp, quindi l’hacker colleziona i frame cifrati e li ritrasmette come nuovi. I frame collezionati sono tutti frame ARP di tipo broadcast che vengono modificati riguardo l’indirizzo e vengono ritrasmessi all’access point. Quando l’access point li riceve, li decifra, elabora il frame che indica di essere inviato in broadcast, lo cifra nuovamente con un nuovo IV e lo invia. In questa maniera l’access point è costretto a creare sempre più IV dato il numero elevato di frame che riceve. Nell’attacco con falsa autenticazione viene sfruttata l’autenticazione aperta dell’access point senza però inviare ad esso nessuno dato dopo la connessione in modo da non farsi espellere.

## Attacchi contro i sistemi di autenticazione

L’attacco prende di mira il processo con il quale l’utente fornisce le credenziali che vengono controllate per verificare la sua identità.

### WPA

La chiave WPA è una chiave precondivisa con tutti gli utenti di una rete wireless, viene usata per generare le chiavi di cifratura da usare durante la sessione utente. Le chiavi generate sono 2 attraverso la fase di 4 way handshake e, forzando queste, si potrebbe risalire alla WPA. È difficile in quanto la chiave PSK è sottoposta ad hash 4096 volte ed lunga fino a 63 caratteri utilizzando anche l’SSID della rete.

La metologia di attacco a forza bruta sull’handshake a 4 vie viene fatta captando passivamente le fasi di autenticazione del client oppure forzando lo scollegamento cercando di captarlo quando si riconnette.

Gli strumenti utilizzati sono airodump:



Una volta intercettato il traffico scambiato nell’handshake si passa all’attacco di forza bruta per forzare la chiave, generalmente basato su un attacco a dizionario.



Un altro attacco è l’uso delle **tabelle arcobaleno** le quali contengono degli hash precalcolati per alcuni algoritmi. Quando si esegue l’attacco il programma prende una stringa, la crittografa con l’algoritmo appropriato producendo un hash che poi andrà a confrontare con l’hash che si sta tentando di forzare. Se corrispondono, la stringa era la password cercata. Se no il programma passa alla stringa successiva.Le tabelle quindi contengono degli hash e delle password corrispondenti. Quando viene fatta la decriptazione si controlla l’hash trovato con quello della tabella. In questo modo si elimina il processo di creazione degli hash che è molto pesante per il computer. Un tool che usa attacco dizionario e tabella arcobaleno è coWPAtty la quale possiede una tabella di circa 40 GB generata da 1000 SSID recenti e dizionario di 172000 parole.

**Cracking con GPU**

Dato che le GPU presentato piu core, vengono usate per le operazioni di forzatura delle password velocizzando il processo. Un programma che sfrutta le GPU si chiama pyrit.

## Attacco alla WPA Enterprise

Attaccare la WPA Enterprise significa attaccare lo specifico tipo di EAP usato dalla rete. Bisogna quindi scoprire il tipo di EAP utilizzato tramite wireshark.

EAP è un framework di autenticazione usato dagli access point per autenticare il client.

### LEAP

Leap sta per Lightweight extensible authentication protocol. Possiede delle vulnerabilità: utilizza una challenga ed una risposta MSCHAPv2 e li trasmette in chiaro sulla rete wireless. Data la chiarezza dei dati, basta l’osservazione dei pacchetti e l’attacco di forza bruta utilizzando **asleap:**

Immagine che contiene testo

Descrizione generata automaticamente

### EAP-TTLS e PEAP

Sono due tipi di EAP che operano in modo simile. Istituiscono un tunnel RLA tra il client non autenticato e il server RADIUS. L’access point non ha visibilità all’interno del tunnel tls e quindi si limita solo a veicolare il traffico. Viene definito un tunnel affinche il protocollo di autenticazione all’interno passi le credenziali in maniera meno sicura, essendo TLS sicuro di natura. L’obiettivo è quello di accedere al tunnel per leggere i dati. TLS è sicuro ma le reti wireless lo sono un po’ meno, quindi si tenta di impersonificare l’access point con cui il client sta parlando per agire come terminale del tunnel TLS. Se il client è configurato male non verificherà l’identità del server RADIUS.

Per rendere sicuri questi EAP basta utilizzare un casella di controllo e compilare un campo di input. Inoltre bisogna controllare che i client verifichino il certificato del server. In questo modo vengono ignorati tutti i server RADIUS che non sono autorizzati.

# Hacking Hardware – Capitolo 9

## Accesso fisico

L’attacco ai dispositivi hardware richiede l’accesso fisico agli stessi. Uno dei metodi di elusione dei meccanismi di controllo dell’accesso è quello della porta chiusa a chiave.

Si parla di lock bumping quando una singola chiave può aprire ogni serratura dello stesso tipo. Per far fronte a questa pratica si utilizzano dispositivi più sicuri e moderni come tastierini numerici o letteri di impronte digitali.

Alcune strutture usano le carte di accesso: a banda magnetica o RFID (di prossimità). È possibile, però, clonare queste carte.

Carte magnetiche   
Alcune carte magnetiche non posseggono misure di sicurezza per proteggere i dati memorizzati su tre tracce definite dalla standard ISO 7810,7811 e 7813. Attraverso dei lettori/registratori è possibile leggere, scrivere e clonare queste carte che contengono anche dati personali. Questo strumenti dotato di interfaccia visualizza i dati in chiaro in vari formati. Analizzando più carte è possibile acquisire tanti dati da fare statistica per ottenere informazioni utili.

La fase di scrittura è facile se non per l’uso eventuale di un checksum da conoscere prima di poterlo riapplicare.

### Carte RFID

Le carte RFID opera su due gamme di frequenza tramite segnale radio: 135 kHz o 13,56 MHz. Anche queste peccano di sicurezza e possono essere facilmente clonate, con l’aggiunta che possono essere lette a distanza. Le nuove carte RFID stanno adottando dei sistemi custom di crittografia.

Gli strumenti utilizzati per leggere e imitare le carte RFID sono dati openpcd.org. Una versione più avanzata di lettore e registratore è il proxmark3 il quale incorpora una scheda che consente la decodifica di vari protocolli RFID.

Una terza opzione per l’intercettazione e la decodifica del traffico RFID è l’USRP che è in grado di intercettare le onde radio grezze, le quali devono essere poi decodificate dall’utente. Un USRP correttamente configurato può inviare e ricevere segnali grezzi sulle normali frequenze RFID, consentendo di intercettare e imitare le carte.

Le contromisure adoperato sono l’utilizzo di soluzioni crittografiche per prevenire di clonare e il replay. Quando una carta viene alimentata dal lettore, viene inviato un segnale di challenge alla carta RFID crittografata e firmata mediante chiave privata memorizzata sulla carta. Tale segnale viene restituito al lettore. Il lettore convalida la risposta prima di consentire al possessore della carta l’accesso alle risorse.

## Hacking Devices

L’hacking dei dispositivi che memorizzano informazioni è importante.

### Bypass della sicurezza con password ATA

L’ATA è un metodo di salvaguardia adottato dalle società come deterrente dall’uso di pc rubati. Il meccanismo comprende l’inserimento di una password per ottenere l’accesso al disco rigido dal BIOS. Questa cosa fornisce solo sicurezza sull’accesso ma non codifica e protezione. Questa soluzione viene bypassata tramite lo scambio a caldo dell’unità in un sistema con sicurezza ATA disabilitata. Bisogna trovare un computer in grado di impostare le password ATA e un’unita sbloccata. Avviare il computer con l’unità sbloccata, entrare nel BIOS. Impostare la password del BIOS, rimuovere delicatamente l’unità ed inserire quella bloccata. Una volta inserita quella bloccata, impostare la password del disco fisso con l’interfaccia bios. L’unità accetterà la nuova password. In questo modo l’unità dovrebbe accettare la nuova password.

### U3 USB

Una chiavetta USB è uno dei modi più semplici per entrare in un sistema, soprattutto se usa lo standard U3. Il sistema U3 è una partizione secondaria inclusa all’interno delle unità in modalità di sola lettura e contiene un software gratuito per gli utenti da provare o scaricare. Il menù della partizione è configurato per essere eseguito automaticamente non appena si inserisce la chiavetta nei PC.

Lo standard utilizza la funzione di avvio automatico integrata in Windows che quando viene inserita viene enumerata e vengono installati due dispositivi distinti: la partizione U3 e la periferica di memorizzazione. La partizione si esegue immediatamente qualunque sia il programma configurato. Quindi sovrascrivendo questo programma si può eseguire del programma pirata, per esempio, per leggere gli hash delle password dal file windows, disattivare firewall oppure installazione di trojan per accesso remoto.

Per fare questo si usa un programma, **Universal\_Customizer,** che impacchetta il programma di avvio automatico, gli eseguibili e gli script creati, nella cartella U3CUSTOM in un file ISO da scrivere nella partizione.

Per contrastare questo attacco va disattivato l’avvio automatico di Windows e degli altri OS. Un altro metodo è quello di tenere premuto MAIUSC prima dell’inserimento di una chiavetta USB in modo da impedire lo start del programma predefinito.

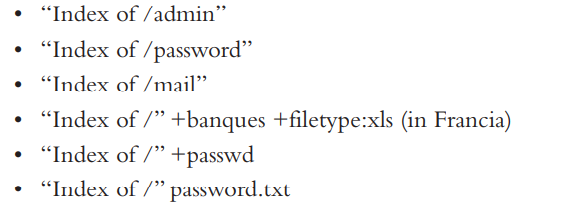
### Bluetooth

Alcuni modelli di telefono vengono forniti con la modalità di scoperta abilitata per impostazione predefinita, consentendo a qualsiasi hacker di scoprire e connettersi al cellulare. Uno strumento è **Ubertooth** che consente di sniffare e riprodurre frame bluetooth su 80 canali bluetooth nella banda ISM 2,4 GHz

# Hacking web application – Capitolo 10

L’hack delle web application si focalizza sul codice dell’applicazione custom e non di un programma già pronto.

Per trovare applicazioni web vulnerabili si possono usare i motori di ricerca attraverso delle query specifiche. Con google è possibile avere la lista di alcune pagine accessibili su un sito web oppure le directory /admin, /password e /mail non protette e il relativo contenuto.



Il web crawling invece è la tecnica di attacco ad un’applicazione web scaricando l’intero contenuto di un sito web alla ricerca di obiettivi facili da attaccare, in modo da familiarizzare col sito e tutto ciò che lo riguarda.

Vengono cercati commenti sul codice, path, server response header, nomi dei server ed inditizzi IP, librerie, codice sorgente e cookie. Strumenti che fanno questo sono wget e HTTrack.

Wget scarica file attraverso protocolli http e HTTPS e FTP.



A seguito dell’analisi viene fatta una valutazione su come è stata implementata l’applicazione per cercare le vulnerabilità e corrompere la logica di risposta dell’applicazione. Gli attacchi da questo punto di vista si basano su: autenticazione, gestione delle sessioni, interazione con i database, validazione degli input e logica dell’applicazione. Spesso vengono usati dei plugin per svolgere questi attacchi.

I plugin permettono di visualizzare e modificare i dati che si inviano al server remoto in tempo reale durante la navigazione. L’idea di base è quella di installare un software nel browser che monitora le richieste a mano a mano che vengono inviate al server. Quando osserva una nuova richiesta, la mette in pausa e la mostra all’utente permettendone la modifica prima dell’invio.

Le suite di strumenti sono basate su dei proxy tra client e server e sono molto più potenti dei plugin in quanto invisibili agli host. Il client stesso può non essere un browser ma qualsiasi applicazione.

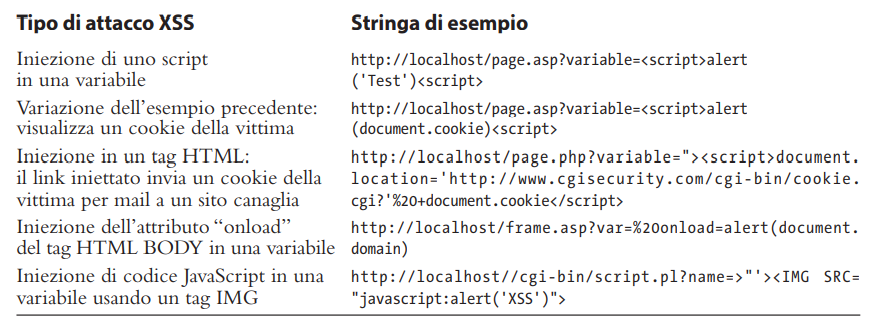
## Attacchi Cross-site Scripting XSS

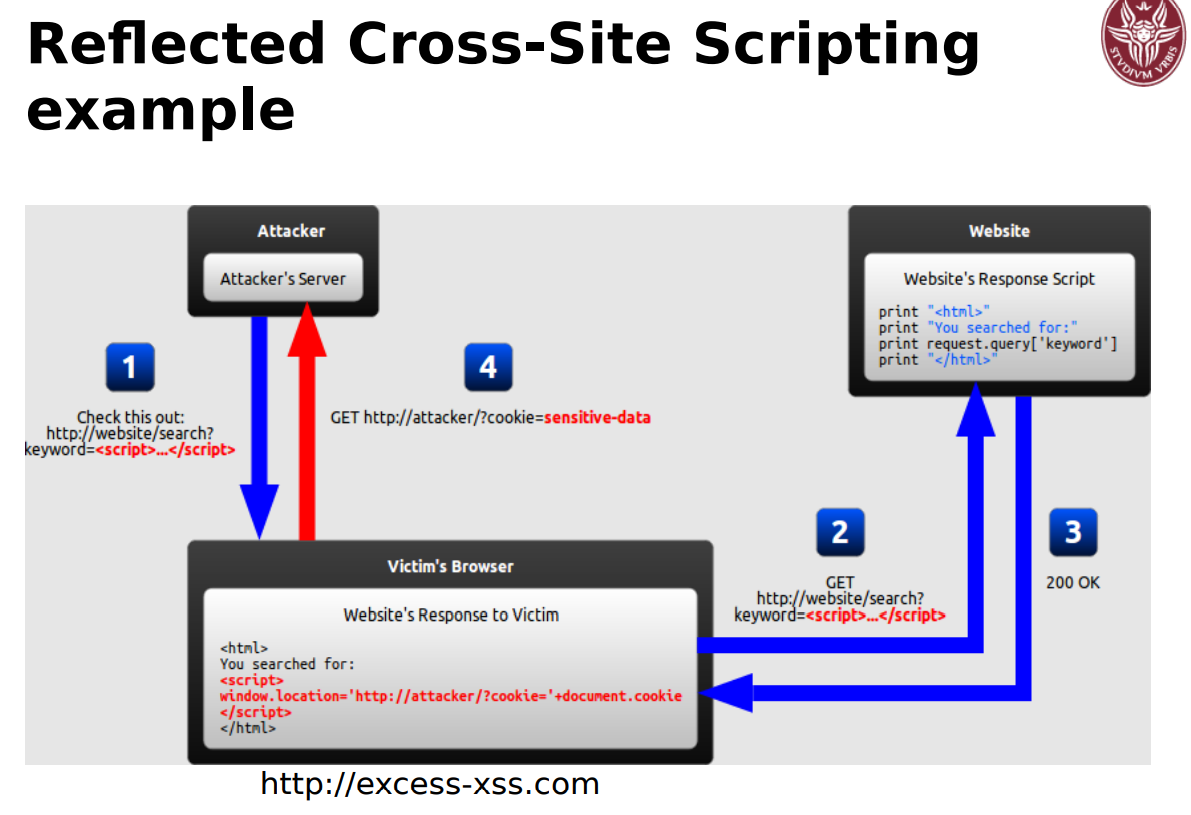
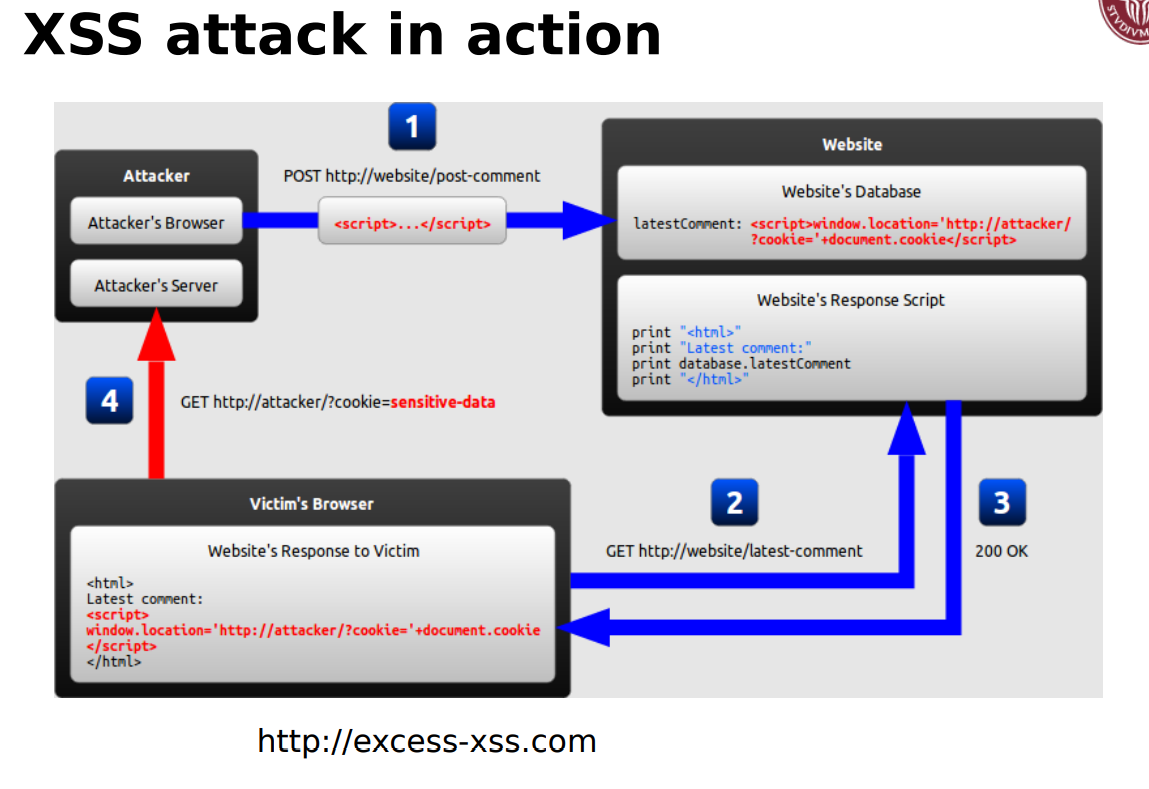
Gli XSS sono degli attacchi che sfruttano le deficiente nelle routine di validazione dell’input/output delle applicazioni. Non viene diretto applicazione ma agli altri utenti dell’applicazione vulnerabile. Un esempio può essere la presenza di codice malevolo lasciato in una parte del sito che può essere letto ed eseguito dal browser di un utente normale fornendo privilegi all’hacker. Possono dirottare sessioni, rubare credenziali o cookie, reindirizzare su altri siti creando problemi sia all’utente che all’azienda. L’attacco più classico consiste nel rubare cookie di sessione di un utente, inaccessibile altrimenti.

In genere gli attacchi XSS nascono da applicazioni che non sanno gestire con sicurezza l’input e output HTML, in particolare i tag HTML racchiusi tra <> o “ ed & che racchiudono codice eseguibe degli script.

I tipi di XSS sono:

* Reflected: l’injection avviene in un parametro usato dalla pagina per mostrare dinamicamente informazioni all’utente
* Stored: l’injection è salvato in una pagina dell’applicazione, tipicamente DB, e poi mostrato agli utenti quando accedono alla pagina
* Dom-based: l’injection avviene in un parametro usato da una script in esecuzione nella pagina.



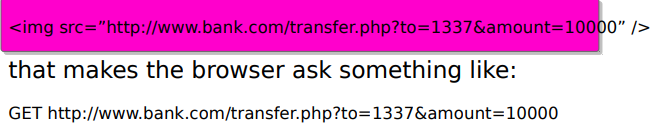


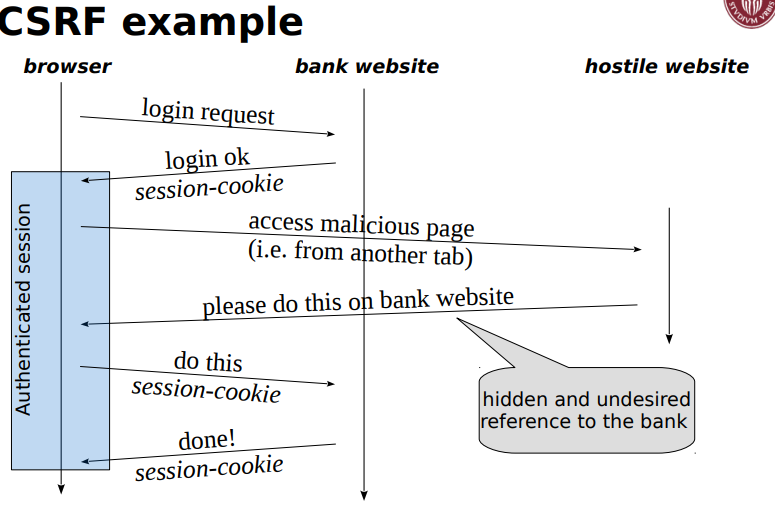
Le contromire contro questi tipi di attacchi sono quelle di codificare l’output in html, di usare dei cookie che non siano disponibili agli script.

## Cross site request forgery

Le vulnerabilità di questo tipo sfruttano il fatto che le applicazioni web assegnano ai propri utenti delle sessioni autenticate persistenti in modo che non debbano riautenticarsi ogni volta che richiedono una pagina. L’hacker può convincere il browser di un utente ad inviare una richiesta al sito web utilizzando la persistenza della sessione per effettuare azioni con le credenziali della vittima. Il sito non riesce a distinguere l’utenza reale da quella a seguito di un attacco. Tramite questi attacchi possono essere cambiate password, fatti bonifici, acquisti online e cose di questo tipo. Spesso viene anche usato per cambiare configurazioni al router o modem.

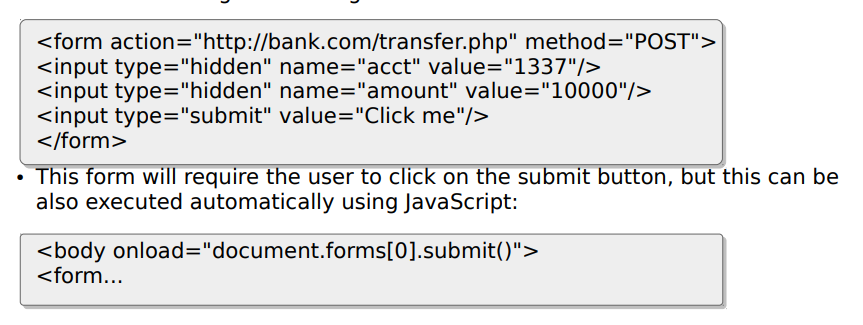
La vittima visita il sito della banca ed ottiene il token di sessione autenticandosi in maniera corretta. Nel frattempo apre un’altra tab visitando un sito sospetto. Quel sito contiene del codice malevolo come anche un’immagine che in realtà quando viene scaricata dal browser si rivela essere del codice che esegue qualcosa. In questo caso potrebbe chiedere di effettuare un trasferimento di denaro. La richiesta fatta dal browser sfrutta però il cookie di sessione avuto in precedenza e quindi effettivamente il trasferimento viene svolto correttamente





Nell’eventualità che invece la banca non usa una GET per effettuare questa operazione ma una POST, la richiesta con la POST non soddisfa i criteri e non possono essere usati tag o immagini in tal senso.

A questo punto viene creato un form nascosto precompilato che nel momento in cui l’utente spingerà il tasto submit, il codice con la richiesta verrà inviato ad uno script in javascript.



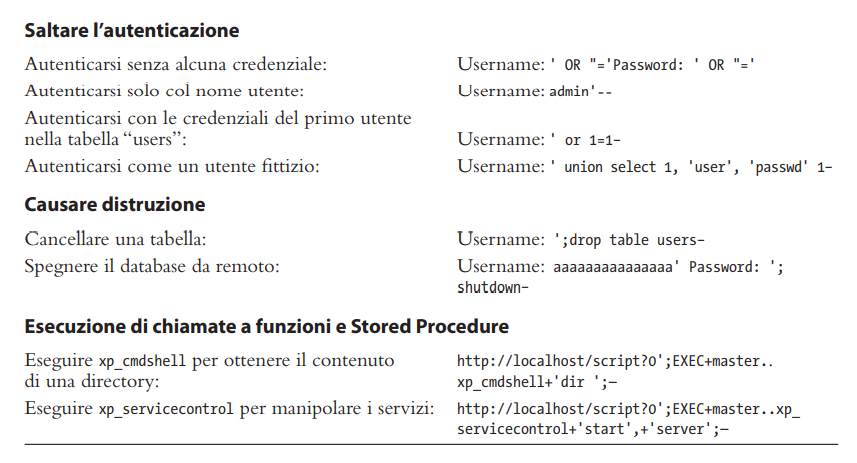
È possibile inoltre evitare che il tasto submit venga cliccato da un utente ma automatizzato dal codice javascript stesso all’apertura della pagina.

Per prevenire questi attacchi, il token di sessione deve essere richiesto ogni volta, randomizzato e composto da valori sicuri

## SQL injection

La maggior parte delle applicazioni web moderne si basano su contenuti dinamici per richiamare l’aspetto dei consueti programmi desktop. Questo dinamismo è ottenuto tramite dati presi da un database o servizio esterno. In risposta ad una richiesta di una pagina web, l’applicazione genera una query. Se non vi è attenzione alla costruzione della query, l’hacker può modificarla creando compromissioni per il database anche se dietro firewall.

La sql injection consiste nell’inerire query SQL grezze all’interno di una applicazione per ottenere azioni inattese. Alcuni dei caratteri utilizzati sono (‘) oppure (--) e il (;). In questa maniera si possono anche ottenere dati non autorizzati o anche arrivare ad ottenere il controllo completo sul server web.



I risultati non sono sempre visibili all’hacker ma le query vengono ugualmente eseguite. Spesso i database vengono forzati per inviare dati ad un server controllato da un hacker attraverso http,DNS o anche email.

Le SQL injection vengono inserite nelle user input tramite get/post o negli http header. Altri posti in cui inserire la SQLi sono i cookies o il database stesso.

