Ethical Hacking

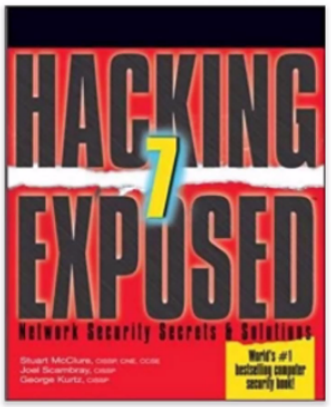
22/02/2022

Hacking Exposed 7: Network Security Secrets and Solutions 7th Edition

by Stuart McClure (Author), Joel Scambray (Author), George Kurtz (Author)

76 customer reviews

Look inside



ISBN-13: 978-0071780285
ISBN-10: 0071780289
Why is ISBN important?

Have one to sell? Sell on Amazon

Add to List

Share <Embed>

Kindle $34.44 | **Paperback** $29.32 | Other Sellers See all 3 versions

Buy new

In Stock.
Ships from and sold by Amazon.com. Gift-wrap available.

This item ships to **Italy**. **Want it Monday, March 5?** Order within **6 hrs 25 mins** and choose **AmazonGlobal Priority Shipping** at checkout. Learn more

More Buying Choices

31 New from $24.19 | 44 Used from $7.76 | 1 Collectible from $28.99

prime student College student? Get FREE shipping and exclusive deals LEARN MORE

Student Assessment Criteria

- Homework/Lab assignments: 50%
- Students will have to complete their Homework and Laboratory Assessments.
- Final Written Exam: 50%
- Students will take a writing exam at the end of the course. The final exam covers all material for the semester.
- If for serious reasons a student does not deliver the majority of the Lab assignments, then for these students the Final Written Exam = 100%.

2 o 3 assignment durante questo semestre

Caso di studio

L'anonimato è fondamentale per un hacker. Non basta runnare nmap ma bisogna anche nascondere la propria identità. L'hacker utilizzerà

- Tor (The Onion Router)
  Rete composta da nodi volontari che runnano un proxy server e permette di effettuare connessioni anonime TCP, utilizza crittografia e un sistema a strati sovrapposti. Grande vantaggio: indipendente dall'applicazione e opera a livello di flusso TCP. E' compatibile con proxy SOCKS, browser web e Internet Relay Chat (IRC).
- Vidalia (Gui per Tor) con Torbutton (estensione firefox)
- Privoxy (proxy web)

Tor in ascolto sulla 9050 e privoxy sulla porta 8118.

Con Google cerca:

intitle:Test.Page.for.Apache "It worked!" "this Web site!"

cerca server web Apache con installazione di default.
L'hacker ora conosce il server web e il nome di dominio associato. Vuole trovare l'ip ma non può utilizzare il comando *host* altrimenti la sua posizione sarebbe rilevata. Utilizza quindi:

tor-resolve

L'hacker non vuole assolutamente inviare pacchetti ICMP e UDP direttamente al sistema di destinazione. Deve utilizzare sempre la rete Tor.

tor-resolve www.esempio.com

Riceve quindi l'ip (10.10.10.100). Adesso vuole conoscere quali sono i servizi attivi e vuole utilizzare Nmap ma deve far passare il suo traffico all'interno della rete tor. Utilizza quindi:

- Proxychain → forza qualsiasi connessione TCP effettuata da qualsiasi applicazione, in questo caso Nmap, ad utilizzare la rete Tor.

proxychains nmap -sT -PN -n -sV -p 21,22,54,…,443 10.10.10.100

Specifica un range di porte interessanti per evitare una scansione completa in quanto richiederebbe troppo tempo.
Adesso l'hacker conosce i servizi attivi e che la macchina runna un'installazione di default di Apache. Vuole quindi approfondire e vuole scoprire l'esatta versione di apache e quindi utilizza:

- socat → gli permette di realizzare una connessione persistente con il server web della vittima ed eseguire qualsiasi numero di verifiche attraverso il relay di socat.

Il seguente comando imposta un proxy socat in ascolto sul sistema locale dell'hacker (127.0.0.1 porta 8080) e inoltra tutte le richieste TCP a 10.10.10.100 porta 80 tramite il proxy TOR SOCKS in ascolto su 127.0.0.1 porta 9050.

socat TCP4-LISTEN:8080, fork

Per determinare la versione di Apache:

1. *nc 127.0.0.1 8080*
2. *HEAD / HTTP/1.0*

Riesce a scoprire che il sistema runna una versione di Apache vecchia (2.2.2) e che presenta diverse vulnerabilità.

Il libro consiglia di tornare su questo caso di studio una volta letto tutto il libro.

Capitolo 1 : footprinting

Il footprinting permette agli hacker di creare un profilo quasi completo dello stato di sicurezza dell'organizzazione in questione attraverso attività metodiche e sistematiche. Le tecniche in questione cercano di ricavare informazioni relative ai seguenti ambienti: internet, intranet, accesso remoto ed extranet.

Conoscendo ciò che l'hacker può vedere si possono conoscere le potenziali falle presenti nel proprio ambiente. Questo capitolo tratta in particolare il footprinting delle connessioni Internet di un'organizzazione.

Di seguito sono presenti i passi base per effettuare un'analisi di footprinting esaustiva.

Passo 1: determine the scope of your activities

Si sceglie l'ambito delle proprie attività di footprinting.

- intera organizzazione?
- solo alcune sedi?
- consideriamo anche i partner commerciali?(extranet)

Passo 2: get proper authorization

Bisogna considerare ciò che gli esperti considerano come il livello 8 e 9 del modello OSI a sette livelli: politica e finanziamenti.

- abbiamo l'autorizzazione per procedere con le nostre attività?
- quali sono esattamente le nostre attività?
- E' stata concessa dalla persona giusta?

Prima di iniziare con l'attività di footprinting bisogna informare i superiori.

Passo 3: Publicly available information

- Pagine web aziendali
- Organizzazioni correlate
- Informazioni sul personale

- Motori di ricerca

Company web pages

Può tornare utile effettuare le seguenti attività:
Consultare il codice HTML, soprattutto i commenti (<!-- --!>). E' buona norma effettuare l'analisi relativa al codice html mediante una copia locale del sito bersaglio. Il website mirroring tools for offline viewing sono:

- wget - Unix
- teleport pro per windows

enumerate hidden files and directories recursively:

- OWASP DirBuster - bruteforce

Questa attività attira l'attenzione perciò conviene utilizzare una funzione apposita di DirBuster per gestire il traffico mediante privoxy.

Look for other sites beyond the main:

- www, www1., www2.
- vpn → vpn.esempio.com (è possibile trovare informazioni sul fornitore della vpn e dettagli sulla versione)

Remote access to internal resources via browser: (proxy to internal servers)
Un esempio comune è quello di Microsoft Outlook Web Access, che opera come proxy per i server Microsoft Exchange interni da Internet. URL tipici di questa risorsa sono https://owa.esempio.com o https://outlook.esempio.com.

Related Organizations and Location Details

Qui dobbiamo cercare eventuali collegamenti dell'azienda target con altre aziende, spesso lo sviluppo e la progettazione dei siti web avviene mediante aziende esterne. (Esempio: in un commento CSS potremmo trovare informazioni riguardanti l'azienda che ha scritto quel CSS).

- Partners might not be security-minded
- Social engineering attack

I dettagli riguardanti la posizione dell'azienda permettono di:

- Dumpster-diving
  cercare nella spazzatura informazioni riguardanti l'azienda
- social engineering
- unauthorized access
  Tramite un accesso non autorizzato è possibile accedere a reti cablate e wireless, computer e dispositivi mobili.

Strumenti di supporto: Google Earth e Google Maps. Le macchine di google tengono traccia anche delle reti Wi-Fi che incontrano e il loro indirizzo MAC.
Tramite Google Locations e Skyhook è possibile trovare informazioni di località utilizzando solo un indirizzo MAC. (shodan.io)

Employee Information

Spesso nelle aziende si utilizza una struttura comune per formare le mail aziendali:

matteo.santini@syrus.it

Conoscendone uno è possibile risalire ad altre email. Sono tutte informazioni utili per l'ingegneria sociale.

Esistono siti per risalire al numero di telefono di una persone:

phonenumber.com, 411.com e yellowpages.com.

Altre informazioni come social security number e address:

blackbookonline.online e peoplesearch.com

Per informazioni di social/professional networking:

facebook, twitter, linkedin e flickr

Business directory services:

jigsaw.com

Sito a pagamento utilizzati da team di vendita per ottenere dati di contatto di potenziali clienti. Generalmente i dati sono aggiornati in quanto la piattaforma ricompensa tramite dei punti chi li aggiorna. Mantengono i dati delle persone che lavorano nelle aziende.

job posting and resumes

- "Checkpoint firewalls and Snort IDS" tells much!
  Tramite questo annuncio di lavoro sappiamo che l'azienda utilizza snort come IDS e magari hanno bisogno di un profilo professionale in grado di utilizzarlo in quanto ora stanno avendo dei problemi con il sistema. Per chiarire i nostri dubbi potremmo chiamare per fingerci interessati alla posizione lavorativa.

- Google "company resume firewall" to get resumes from current and past employees
  Dai CV dei dipendenti passati possiamo ricevere informazioni sulle tecnologie che l'azienda utilizza o ha utilizzato. Per ricercare i curriculum possiamo utilizzare siti come careerbuilder.com.

- Watch disgruntled and ex- employees: revenge!
  Chi è insoddisfatto del proprio lavoro e vuole vendicarsi potrebbe lasciare aperte backdoor.

- Employee's home computers
  Invece che studiare firewall, IDS e IPS l'hacker può utilizzare un keylogger per poi effettuare attività di spoofing di un utente fidato.

current events

Gli eventi attuali di maggior interesse sono:

Mergers, acquisitions, scandals, layoffs, rapid hiring, reorganization, outsourcing, temporary contractors

Quando avvengono delle fusioni è solito che le reti aziendali vengano unite e i tempi imposti per essere messi insieme siano brevi. Può succedere che per effettuare questo merge in tempi rapidi la sicurezza venga meno.

Human factor:
Un morale basso potrebbe far concentrare il lavoratore ad aggiornare il proprio cv piuttosto che eseguire l'update di patch di sicurezza.

Informazioni sugli eventi in corso possono essere facilmente reperibili da internet tramite i periodical report e gli annual report per quanto riguarda le aziende americane quotate in borsa (sec.gov). Altre informazioni utili possono essere prese tramite Yahoo Finance.

privacy or security policies archived information

Sono informazioni utili per l'hacker quelle relative alla privacy e alla sicurezza aziendale o dettagli tecnici relativi a hardware e software utilizzati per la protezione dell'organizzazione. Per accedere a vecchie informazioni che sono state rimosse direttamente dall'azienda possiamo usare servizi come wayback machine o le cache di google.

search engines and data relationships

Possibili search engines: google, yahoo e bing. Esistono stringhe da utilizzare sul motore di ricerca per rimediare informazioni importanti (GHDB - google hacking database). Esempio di stringa:

"allinurl:tsweb/default.htm"

Restituisce i server con Microsoft windows che hanno attiva la connessione web desktop remoto.

Altri tool: Athena, sitedigger e Wikto che ricercano vulnerabilità, informazioni proprietarie e informazioni sulla configurazione nelle cache di google.
SiteDigger utilizza GHDB.

Per analizzare i metadati dei web file possiamo utilizzare FOCA che prima ricerca i documenti con specifiche estensioni e poi i metadati al loro interno.
FOCA utilizza shodan che è un motore di ricerca per trovare dispositivi connessi ad internet che utilizzano meccanismi potenzialmente non sicuri per autenticazione e autorizzazione.

Altro tool online di data mining che permette di tracciare mappe relazionali sulla base dei dati forniti riguardanti un soggetto → Maltego.

Altro metodo che potrebbe utilizzare un hacker è quello di controllare nei forum chi ha avuto dei problemi con specifiche configurazioni, spesso nei messaggi lasciano in chiaro l'ip oppure tramite ingegneria sociale potrebbe approcciarsi al creatore del thread per "aiutarlo" personalmente.

public database security countermeasures

Periodically review tramite la risorsa Site Security Handbook: RFC 2196. E' importante rimuovere i dati pubblici sensibili e di utilizzare pseudonimi quando si utilizzano mailing list o forum pubblici.

Passo 4: WHOIS and DNS Enumeration

Domain name, IP addresses & port numbers sono gestiti centralmente da ICANN (Internet Corporation for Assigned Names and Numbers). ICAN è composta da diverse organizzazioni, le tre più importanti sono:

- ASO: alloca blocchi di indirizzi IP a vari registri regionali RIR. I RIR poi allocano gli indirizzi IP ad organizzazioni come ISP, NIR E LIR.
- GNSO: responsabile dei nomi di dominio generici di primo livello (.com, .edu …)
- CCNSO: gestisce le politiche relative ai nomi di dominio di primo livello.

Tre R per WHOIS: Registry, Registrar, Registrant

To lookup keyhole.com, start from whois.iana.org

- Find the registry and registrar for .com (Registry: verisign-grs.com) and then keyhole.com (Registrar: markmonitor.com)
- Find the registrant details of keyhole.com (for later spoofing)
- Web whois or command-line whois
- Automatic tools (allwhois, uwhois) and GUI tools (superscan, netscan tools pro)

Se dovessimo conoscere un indirizzo IP possiamo utilizzare whois tramite arin per sapere chi gestisce l'intervallo di IP corrispondente.
To lookup 61.0.0.2, start from arin.net

- Find apnic.net, then find National Backbone of India
- But keep in mind the IP address might be spoofed/masqueraded. E' semplice mascherare il proprio indirizzo ip.

Public Database Security Countermeasures

Bisogna aggiornare i propri contatti amministrativi oppure utilizzare le funzioni di anonimizzazione proposte dal provider (ad esempio GoDaddy). In questo modo andremo a limitare gli attacchi di ingegneria sociale.

Authenticate updates rigidly to avoid domain hijacking
Tre metodi per aggiornare i dati di dominio: campo FROM email, password e una chiave PGP. La più debole riguarda il campo FROM dell'e-mail che permette di effettuare hijacking (dirottamento) cambiando informazioni sul dominio.

Passo 5: DNS Interrogation

DNS è un database distribuito utilizzato per assegnare indirizzi IP a nomi di host e viceversa. Se il DNS ha un basso livello di sicurezza potrebbe rilasciare informazioni importanti sul bersaglio. Problemi più seri di configurazione:

- DNS zone transfer by untrusted users

  Un trasferimento di zona consente a un server master secondario di aggiornare il proprio database di zona dal master primario. (Il primario manda a tutti i server secondari una copia della sua zona così tutti i secondari faranno un mirroring dei dati che hanno ricevuto).
  Se il DNS è configurato male chiunque può richiedere una copia della zona. Un meccanismo di DNS pubblico/privato permette di separare i dati esterni (ip pubblici) da quelli interni (nomi di host e indirizzi ip interni). Se un'azienda non utilizza questo meccanismo chiunque può accedere ai dati interni. Per effettuare un trasferimento di zona si può utilizzare il comando *nslookup*.

  Possibili tipologie di record nslookup:
  - A indirizzo ip
  - HINFO la piattaforma o il tipo di sistema operativo in esecuzione

  Possiamo salvare l'output di nslookup in un file per poi analizzare con comandi tipo grep, sed o perl. Tramite questi strumenti è possibile vedere quali host stanno eseguendo dei sistemi operativi specifici.

  Script per enumerare le voci DNS di un dominio:
  - dnsenum, dsnmap e dsnrecon.

  alcuni DNS impediscono di effettuare query se non si è autorizzati, questi tool utilizzano dei metodi di brute force su più dns per ricavare le informazioni.

DNS Security Countermeasures

L'obiettivo è limitare la quantità di dati disponibili su internet. Bisogna → Restrict zone transfer to only authorized servers. Per farlo:

- Su BIND utilizziamo la direttiva *allow-transfer* nel file named.conf.
- DNS Microsoft Windows 2008 è possibile specificarlo.
- Bloccare sul firewall la porta TCP 53 (utilizzata per zone transfer), questo non preclude il funzionamento del DNS dato che la ricerca di domini avviene in UDP.
- Il DNS deve essere configurato per non divulgare informazioni riguardanti la rete interna
- Avoid HINFO, rilascia dati sensibili come OS.

PASSO 6: Network Reconnaissance

Obiettivo Network Reconnaissance: determinare potenziali reti, topologie e percorsi di ingresso.
Strumento che si può utilizzare: traceroute (sfrutta il campo TTL per sollecitare il pacchetto ICMP TIME_EXCEEDED da ciascun router). Con -p 53 possiamo specificare la porta a cui fa riferimento il pacchetto, in questo caso 53 - DNS. Può succedere che alcuni firewall bloccano i pacchetti senza la specifica sulla porta in quanto potrebbero avere un numero diverso da 53. Il campo TTL si trova nell'header IP quindi possiamo provare a fare dei traceroute tramite TCP (tcptraceroute), UDP e ICMP.

Thwarting Network Reconnaissance Countermeasures

- NIDS (snort, bro-ids) e IPS
- configurare i router per limitare il traffico ICMP e UDP solo a sistemi specifici.

Capitolo 2: Scanning

Dopo fingerprint abbiamo raccolto informazioni utili sul bersaglio adesso con lo scanning vogliamo vedere gli eventuali punti di accesso.

Determining If the System is Alive

In questa fase andiamo a controllare se ad un indirizzo ip corrisponde un host attivo. Per farlo utilizzeremo un ping sweep sugli indirizzi ottenuti.

ARP: host discovery on the same subnet

ARP traduce l'indirizzo fisico MAC di un sistema nell'indirizzo IP che gli è stato assegnato. Un host viene considerato vivo se riceve una risposta ARP.

Possibili strumenti:

- ARP-Scan
  permette di effettuare ping ARP e fingerprint, si deve runnare come sudo.
- Network Mapper (Nmap)
  Supporta scansione ARP con il parametro -PR. Conviene mettere opzione -sn per evitare di effettuare la scansione delle porte.
- Cain
  Offre funzionalità per windows. Permette di effettuare una ricerca host ARP.

ICMP host discovery: remote host/router

ICMP ECHO REQ invio pacchetti a un sistema bersaglio, ICMP ECHO REPLY risponde a request.
ICMP TIMESTAMP serve per identificare l'ora di sistema del bersaglio.
ICMP ADDRESS MASK identifica la maschera di sottorete locale.

Possibili strumenti:

- Sistemi operativi hanno il comando ping che invia ICMP ECHO REQUEST.
- Nmap
  Permette di inviare ECHO REQUEST, TIMESTAMP e ping TCP.
- hping3 e nping
  Permettono il packet-crafting con ogni tipo di combinazione di flag e tipologie di pacchetto. Consentono di inviare pacchetti ICMP ECHO REQUEST e tutti gli altri.
- Superscan
  Invia ICMP ECHO REQUEST in parallelo. Tool di windows.

TCP/UDP host discovery: when internal and/or external ICMP is not permitted

Se ICMP dovesse essere bloccato sull'host target tramite un firewall possiamo determinare se è vivo o meno cercando di accedere ai suoi servizi (http sulla porta 80 ad esempio).

Possibili strumenti:

- Nmap

Cerca i servizi attivi tramite le porte logiche. Per evitare di creare rumore conviene provare le porte di utilizzo più comuni. Con -Pn evitiamo la ricerca di host. Con -p 22 indichiamo di cercare gli host che hanno la porta 22 aperta.

- Superscan e nping
  Scan sulle porte.

Ping Sweeps Countermeasures

- Detection
  IDS snort all'interno di una rete.
  Utility UNIX nei sistemi host (protolog, scanlogd).
  I firewall riescono a rilevare ping sweep con pacchetti ICMP, TCP e UDP.
  In questo caso abbiamo sempre bisogno di una persona che controlli e che sia pronta a reagire.

- Prevention
  Tramite ACL limitiamo il traffico all'interno della nostra rete o sistema.
  Approccio minimalista: consentiamo solo ICMP ECHO_REPLY, HOST_UNREACHABLE e TIME_EXCEEDED nella rete DMZ e soltanto verso indirizzi specifici IP del proprio ISP.
  - Loki2 hackers use it to backdoor the OS and tunnel data in ICMP ECHO
  - Pingd: move ICMP from kernel to user space

Determining which services are running or listening

Dopo aver determinato quali sono i sistemi attivi dobbiamo scoprire quali porte hanno aperte e quali servizi hanno in esecuzione.

Port Scanning

Adesso l'obiettivo è quello di determinare:

- Servizi TCP e UDP in esecuzione sul sistema bersaglio
- il tipo di SO sul target
- applicazioni specifiche o versioni di un particolare servizio

Scan Types

TCP connect scan (3-way handshake),

1. TCP connect scan (3-way handshake)
   Si effettua la connessione alla porta bersaglio e completa un handshaking a tre vie (SYN, SYN/ACK, ACK). E' facilmente rilevabile e richiede tempo.

2. Scansione SYN TCP
   E' chiamata half-open scan (scansione semi-aperta) in quanto ci si limita ad inviare un pacchetto SYN. Se si riceve SYN/ACK si può dedurre che tale porta si trova nello stato LISTENING. Se si riceve invece un RST/ACK solitamente significa che la porta non è in ascolto.

3. TCP FIN scan
   Si invia un FIN e il target dovrebbe restituire un RST per tutte le porte chiuse.

4. TCP Xmas Tree scan
   Sistema invia FIN, URG e PUSH e il target dovrebbe rispondere con RST per le porte chiuse.

5. TCP null scan
   Tutti i flag del pacchetto sono disattivati, per le porte chiuse il target dovrebbe rispondere con RST.

6. TCP ACK scan
   Permette di valutare se il firewall è un semplice filtro di pacchetti oppure se effettua controlli sullo stato della connessione.

7. TCP RPC scan
   Permette di individuare le porte RPC e i programmi associati con i numeri di versione.

8. Scansione UDP
   Metodo inaffidabile. Si invia un pacchetto UDP alla porta bersaglio e se il sistema risponde con un ICMP port unreachable significa che è chiusa, se non lo riceve si può dedurre che è aperta.

Determining TCP and UDP running services

- Nmap
  Port scanning after host discovery. Prima esegue una ricerca di host e poi effettua la scansione di porte soltanto per gli host individuati come attive. Opzione -o per salvare l'output in un file, -oN per salvarlo in un formato human-readable. Opzione -f l'header TCP viene frammentato e potrebbe permettere di non essere rilevati dagli IDS. Opzione -D intermix decoy and real scans, per evitare di essere rilevati il sistema invia pacchetti superflui, che possono presentare anche indirizzi IP di origine falsificati, in contemporanea con i pacchetti di scan.

- Superscan
  Alternativa GUI di nmap per windows.

- Scanline
  Windows-based with command-line

- Netcat
  Windows e Linux. minimize your footprint on a compromised system, Swiss Army knife of security. Default utilizza porte TCP, per UDP bisogna utilizzare l'opzione -u.

Port Scanning Countermeasures

- Detection
  IDS di rete come Snort.
  scanlogd su UNIX detect and log scansioni di porte TCP.

Configurare il firewall per rilevare i tentativi di scansione delle porte, ad esempio possiamo ignorare le scansioni FIN e rilevare quelle SYN.
Infine il tool Attacker che su windows si mette in ascolto sulle porte e invia un messaggio di avviso quando rileva un tentativo di scansione

- Prevention
  Disabling all unnecessary services/ports.

Detecting the Operating System

Il sistema operativo ci permette di capire se ci sono potenziali vulnerabilità da sfruttare sul target.

Active Operating System Detection

- Banner grabbing
- Nmap (active stack fingerprint)

Making guess from available ports:

- 445, 139 e 135 probabilmente il sistema è windows.
- 3389 utilizzata per il protocollo RDP (remote desktop protocol) comune in windows.
- 22 SSH - UNIX
- 3277x RPC in UNIX Solaris

Active stack fingerprinting (Phrack Magazine)
Fingerprint dello stack è una tecnologia che consente di determinare rapidamente il sistema operativo di un host. Le implementazioni dello stack IP dei vari produttori variano per molti dettagli. Esempio:

- FIN PROBE
  Un pacchetto FIN viene inviato a una porta aperta, l'RFC 793 stabilisce che il comportamento corretto è di non rispondere. Molte implementazioni dello stack (come windows 7) rispondono con FIN/ACK.

- Bogus Flag Probe (Prova flag contraffatto)
  Si imposta un flag TCP undefined nell'header TCP di un pacchetto SYN. Alcuni SO rispondono con il flag impostato nel pacchetto di risposta (Linux)
- Initial Sequence Number Mapping
  Bisogna trovare un pattern nella sequenza iniziale scelta dall'implementazione TCP in risposta a una richiesta di connessione.

- "Don't fragment bit" monitoring
  Alcuni SO per migliorare le prestazioni utilizzano questo bit.

- TCP initial window size
  Si tiene traccia della dimensione della finestra iniziale sui pacchetti restituiti. Per alcune implementazioni dello stack, questa dimensione è unica e tale informazione è molto utile per la precisione del meccanismo di fingerprinting.

- ACK value

Alcune implementazioni restituiscono il numero che abbiamo inviato nel campo ACK, altre restituiscono un numero di sequenza +1.

- ICMP message quenching (Limitazione dei messaggi di errore ICMP)
  Alcuni SO possono limitare la frequenza con cui sono inviati i messaggi di errore. Si inviano molti pacchetti UDP ad alcune porte e si contano i messaggi di HOST UNREACHABLE.

- ICMP message quoting
  I sistemi operativi si distinguono per la quantità di informazioni citate quando si incontrano errori ICMP. Esaminando il messaggio con la citazione, è possibile ipotizzare quale sia il sistema operativo.

- ICMP message echoing integrity (integrità di messaggio di errore restituito)
  Alcuni SO alterano gli header IP quando restituiscono messaggi di errore ICMP.

- TOS (Type of service)
  Per i messaggi di tipo “ICMP PORT UNREACHABLE” si esamina il TOS: la maggior parte delle implementazioni dello stack utilizzano il tipo 0, ma non è sempre così.

- fragmentation handling
  Alcuni stack sovrascrivono i dati vecchi con quelli nuovi e viceversa, al momento di riassemblare i frammenti. Osservando il modo in cui sono riassemblati dei pacchetti di prova, è possibile fare delle ipotesi sul sistema operativo bersaglio.

- TCP options
  Inviando un pacchetto con più opzioni impostate, per esempio quelle di nessuna attività, massima dimensione del segmento, fattore di scala finestra e timestamp, è possibile fare delle ipotesi sul sistema operativo bersaglio.

Nmap utilizza queste metodologie tramite l’opzione -O (tranne frammentazione e limitazione dei messaggi di errore ICMP).

Countermeasures

- Detection
  Snort, scanlogd…
- Prevention
  Secure proxy or firewall. Anche se gli hacker sono in grado di identificare il sistema operativo in uso, è necessario fare in modo che abbiano difficoltà a ottenere l’accesso al sistema bersaglio.

Passive operating system detection

Per un sistema è facile rilevare un tentativo di identificazione del sistema operativo in quanto richiede di inviare dei pacchetti al target. Per rimanere nascosti agli occhi dell’IDS dobbiamo utilizzare una metodologia passiva.

- Passive Stack Fingerprint

At a central location or a port with packet capture by port mirroring.
Non inviamo più i pacchetti ma analizziamo quelli presenti nella rete.
Tool:
Siphon: a passive port-mapping, OS identification, and network topology tool.

- Passive Signature
  Analizziamo caratteristiche degli attributi associati a una sessione TCP/IP:
  - TTL
    Che valore imposta il so come TTL sul pacchetto in uscita?
  - Window size
    Che valore imposta il so come dimensione della finestra?
  - DF.
    Il sistema operativo imposta il bit di non frammentazione?

L'insieme di signatures sono presenti in Siphon tramite il file osprints.conf
Questa metodologia presenta i seguenti limiti:

1. applications build their own packets (come nmap)
2. not able to capture packets (dobbiamo per forza trovarci nella rete interna)
3. a remote host changes the connection attributes.

Countermeasures

- Same as OS detection countermeasures

Processing and Storing Scan Data

La mappatura di una rete bersaglio può tradursi in una grande quantità di dati. Soprattutto per reti molto grandi è opportuno ottimizzare il processo di gestione dei risultati delle scansioni. Efficiency in managing scan data → speed to compromise a large number of systems

Managing scan data with Metasploit

Metasploit permette di eseguire le scansioni e inviare i dati al programma per ulteriori elaborazioni. Utilizza un server PostgreSQL.

- db_connect: tells metasploit how to connect to database and which database to use
- db_nmap (root required): run Nmap scans e salva i dati direttamente nel db (è più lento)
- db_import, importiamo i risultati di nmap direttamente nel db di metasploit.

Dopo che il db è stato popolato possiamo effettuare diverse query al db, ad esempio:

- hosts restituisce l'elenco di tutti gli host presenti nel db.
- services show all available ports and services
- services -s ssh | mostra tutti gli host con ssh. Oppure mediante altre query possiamo visualizzare i sistemi windows 2008.

Capitolo 3: Enumeration

Dopo aver individuato gli host attivi e i relativi servizi in esecuzione l'hacker esamina in dettaglio i servizi identificati cercando eventuali punti deboli in un processo chiamato enumerazione. Rispetto alla raccolta di informazioni (scanning) questo step prevede l'utilizzo di connessioni attive e di interrogazioni dirette che potrebbero essere registrate nei file di log. Tramite l'enumerazione possiamo trovare nomi di account utente, risorse condivise mal configurate e vecchie versioni di software con note vulnerabilità.

Service Fingerprinting

Metodi manuali risultano più stealthy rispetto ai metodi automatici.

nmap version scanning

nmap-services è un file di testo che mette in corrispondenza i servizi con le porte comunemente associate.
Con il flag -sV interroga le porte e dopo aver ricevuto un feedback lo va a comparare con il contenuto del file nmap-service-probe, quest'ultimo contiene le informazioni sulle risposte fornite dai servizi noti. In questo modo è possibile trovare servizi esposti su porte non note. Ad esempio tramite un semplice syn scan (-sS) potremmo trovare sulla porta 141 7 il servizio Timbuktu mentre utilizzando -sV potremmo rilevare che in realtà su quella porta è presente SSH.

amap version scanning

Alternativa ad nmap che utilizza un sistema di pattern-matching.

Vulnerability Scanner

Utilizzano un database di known vulnerability signatures. Sono più utili quando non è richiesta attenzione nel farsi individuare. Ne esistono diversi tipi: Nessus, OpenVas, McAfee, Rapid7…

Nessus

E' considerato lo standard di riferimento per gli scanner. Permette di scrivere plug-in tramite il linguaggio NASL - Nessus Attack Scripting Language.

Nessus countermeasures

Audit yourself regularly. Effective patch and configuration management. Il self audit deve essere fatto utilizzando tool simili in modo tale da poter patchare le vulnerabilità prima che vengano trovate da hacker esterni. Gli IDS/IPS hanno un insieme di signature che rilevano i tipici comportamenti di Nessus.

Script NSE di Nmap

Nmap può essere esteso mediante script scritti in Lua che possono essere richiamati mediante -sC o –script. Questi script permettono di eseguire attività quali network discovery, rilevamento di versione, rilevamento di backdoor e perfino di sfruttare vulnerabilità. Nmap provvede una libreria apposita comprendente questi script.

Basic Banner Grabbing

Catturare un banner significa semplicemente connettersi a servizi remoti e osservarne l'output, e può offrire utili informazioni agli hacker che operano da remoto e, come minimo, con queste tecniche possono identificare il produttore e la versione del servizio in esecuzione, cosa che in molti casi è sufficiente per avviare il processo di ricerca delle vulnerabilità.

Le basi per la cattura di banner: telnet e netcat

Metodo manuale: telnet.

telnet www.example.com 80

e da terminale vedremo la risposta html di questa pagina. Questa metodologia funziona sulle porte standard come 80 HTTP, 25 SMTP e 21 FTP.

Metodo automatico: netcat.

nc –v www.example.com 80

Si collega alla porta TCP/IP indicata e cattura la risposta. Per catturare più risposta possiamo passargli un file in input. Ad esempio consideriamo un file nudge.txt che contiene solamente la riga GET / HTTP/1.0.

nc –nvv -o banners.txt 10.219.100.1 80 < nudge.txt

A seconda del servizio che stiamo analizzando possiamo utilizzare il file a nostro favore: "head / HTTP/1.0 <cr><cr>", "HELP <cr>", "ECHO <cr>".

Banner grabbing countermeasures

Shut down unnecessary services or limit their access with ACL. Audit yourself regularly. Try to disable the presentation of vendor and version in the banners.

Enumerating Common Network Services

FTP Enumeration, TCP 21

FTP is still popular for web content uploading. Esempio di connessione FTP mediante windows:

ftp ftp.example.com

Molte configurazioni permettono di effettuare il login tramite l'accesso anonimo (User: anonymous) che non necessità di password per il login. Bisogna anche stare attenti a questo protocollo in quanto la password è inviata in chiaro. Per trovare FTP server tramite google bisogna effettuare la seguente ricerca:

intitle:"Index of ftp://"

FTP enumeration countermeasures

Data la password in chiaro bisogna utilizzare metodi alternativi come:

- SFTP (SSH)
- FTPS (SSL)

Questi permettono l'autenticazione e sono protetti da password. Bisogna controllare l'accesso anonimo e non consentire l'upload di file senza limitazione di memoria. Public content should be served over HTTP, not FTP.

Enumerating Telnet, TCP 23

E' stato uno dei primi servizi in rete in uso che permette di effettuare l'accesso remoto. Il suo principale difetto è: It sends passwords+data in cleartext. Questo servizio è stato superato tramite SSH.

Enumeration del sistema tramite banner telnet:
Prima del login telenet mostra un banner in cui spesso riporta il sistema operativo e la versione in uso sull'host. Se non dovesse mostrarli direttamente potremmo risalire alla tipologia di sistema che il target sta utilizzando mediante la schermata che ci viene proposta:

```
User Access Verification.
Password:
```

oppure:

```
User Access Verification.
Username:
```

Tramite questi due banner ad esempio possiamo scoprire mediante una rapida ricerca che l'host sia un dispositivo CISCO.
Nel caso in cui venga richiesta solamente la password è molto probabile che l'hacker possa lanciare un brute force attack.

Enumeration dell'account tramite telnet:
attempt login with a particular user and observe error messages. Grazie ai messaggi di errore possiamo stilare una lista di nomi di user validi e non. Ad esempio per capire se un user esiste, ma la password inserita è sbagliata, su un sistema AS/400 questo deve rispondere con

"CPF1107 – Password not correct for user profile"

Telnet countermeasures

- Telnet should be eliminated if possible, Use SSH instead
- If you must use Telnet, restrict it to proper source IP addresses or run it through a VPN.
- Limitare l'accesso in base all'host o al segmento di rete.
- Modify banner info

- Reconnect between failed login attempts (così rallenti un eventuale brute force)

Enumerating SMTP, TCP 25

SMTP can be enumerated with Telnet or netcat, using these commands

- VRFY confirms names of valid users
- EXPN reveals the actual delivery addresses of aliases and mailing lists

```
[root$]telnet 10.219.100.1 25
Trying 10.219.100.1...
Connected to 10.219.100.1.
Escape character is '^]'.
220 mail.example.com ESMTP Sendmail Tue, 15 Jul 2008 11:41:57
vrfy root
250 root <root@mail.example.com>
expn test
250 test <test@mail.example.com>
expn non-existent
550 5.1.1 non-existent… User unknown
quit
221 mail.example.com closing connection
```

Un tool automatico è vrfy.pl che prende in input un indirizzo di un server SMTP e una lista di utenti da controllare.

SMTP countermeasures

Disable the EXPN and VRFY commands, or restrict them to authenticated users

Enumerating DNS, TCP/UDP 53

- Normally on UDP 53; TCP 53 for zone transfer

Un metodo antico di enumerazione consiste nel effettuare un trasferimento di zona su server DNS miscofingured. Per effettuare l'enumerazione possiamo utilizzare nslookup oppure dig. I dati che possiamo ricavare sono i record A, le informazioni HINFO e altri dati importanti come servizi/server e porte corrispettive in esecuzione (karberos, ldap)

Enumerazione di BIND:
BIND è un noto DNS per sistemi UNIX. Bind presenta un record nella classe CHOAS che contiene la versione dell'installazione caricata sul server bersaglio. Tramite il comando dig e version.bind possiamo risalire a tale versione.

DNS Cache snooping

Le cache per i dns sono utili per risolvere velocemente i nomi di host utilizzati più spesso. Quando viene richiesta la risoluzione di un nome di host che non rientra nel suo dominio il server utilizza la ricorsione e interroga un altro server DNS. Tramite:

dig … … +norecurse

l'hacker può determinare se il DNS ha già fatto richiesta per un dominio specifico. Se non ha mai elaborato tale richiesta questo comando tornerà il flag answer settato a 0 altrimenti 1.

DNS Enumeration Tools

Due tools:

- dnsenum
  ricerca i subdomain, effettua bruteforce ai subdomain, enumeration of the network interval in a domain and execution of whois queries on such intervals.
- Fierce
  Effettua zone transfer, dictionary attack and enumeration with reverse lookup.
- Web resources
  Servizi gratuiti online comprendo l'enumerazione WHOIS

DNS Enumeration Countermeasures

Se DNS non è necessario conviene disabilitarlo. Oltre alle tecniche descritte precedentemente conviene:

- Use separate internal and external DNS servers (do not expose internal targets)
- block or restrict DNS zone transfers only to authorized machines
- Restrict DNS queries to limit cache snooping

Enumerating TFTP, TCP/UDP 69

TFTP = Trivial File Transfer Protocol. Basato su UDP per eseguire trasferimenti di file rapidi, senza autenticazione sulla porta UDP 69.

- Runs in cleartext
- Have to know the exact file name.
- Anyone can grab any file (no auth) like /etc/passwd
- Used in routers and VoIP Telephones to update firmware. Look for config files

TFTP Enumeration Countermeasures

TFTP è un protocollo di per sé insicuro, poiché opera in chiaro, non offre un meccanismo di autenticazione e può lasciare aperti a eventuali abusi gli elenchi di controllo d'accesso del sistema, nel caso di una configurazione non ottimale. Per questi motivi è meglio non utilizzarlo, e se si ha la necessità di farlo:

- attuare una protezione degli accessi con un wrapper (mediante uno strumento come TCP Wrapper), is like a software firewall.
- limitare l'accesso alla directory /tftpboot e assicurarsi che sia impostato un blocco presso il firewall sul margine della rete.

Enumerating finger, TCP/UDP 79

Shows users on local or remote systems, if enabled. I dati più pericolosi sono i nomi degli utenti che hanno effettuato il login e i tempi di inattività, che possono consentire a un hacker di farsi un'idea di chi sta osservando il sistema (root?) e dell'attenzione con cui lavora.

- Useful for social engineering

finger Countermeasures

- stop finger execution
- block udp port 79
- use TCP Wrappers

Enumerating HTTP, TCP 80

Banner grabbing with telner or netcat inviando HEAD. Se il server utilizza SSL è possibile utilizzare un sslproxy oppure openssl. Un tool automatico che ci permette di effettuare enumerazione è il grendel-scan. Questo ci permette di prelevare tutti i commenti di un sito web, analizzare il codice HTML e controllare robots.txt e directories.

HTTP Enumeration Countermeasures

- Change the banner on the website
- Use MS URLScan for IIS v4, permette di bloccare attacchi a IIS

Microsoft RPC Endpoint Mapper (MSRPC), TCP 135

Querying this service can yield information about applications and services available on the target machine. Per effettuare tale enumerazione possiamo utilizzare lo strumento epdump che interroga l'endpoint mapper MRSPC e mostra i servizi associati a indirizzi IP e numeri di porta. Su UNIX possiamo utilizzare rpcdump.

MSRPC Countermeasures

- Block port 135 at the firewall, if you can
  Se bisogna fornire servizi mail a client Internet tramite Microsoft Exchange Server bisogna esporre il servizio MSRPC. Soluzione:
- Use VPN
- Usare Microsoft Outlook Web Access (OWA). E' un front-end web per mailbox e funziona su HTTPS.

NetBIOS Name Service, UDP 137

Servizio Microsoft per Name Service, like DNS. Windows needs to change a computer name to an IP address to send data packets.

enumerazione di gruppi di lavoro e domini windows con net view

NET VIEW can list the domains, or the computers in each domain.
net view richiede l'accesso a NBNS su tutte le reti da enumerare quindi funziona solo su rete locale. It is possible to route NBNS over TCP/IP, allowing enumeration from a remote

system. Se un host riceve tramite DHCP un indirizzo IP di una rete locale può enumerare, tramite una query non autenticata, i domini e host di un'intera rete aziendale.

enumerazione di controller di dominio windows

nltest e netdom permettono di identificare i domain controller. I domain controller provvedono a gestire le credenziali di autenticazione delle reti windows.

enumerazione di servizi di rete con netviewx

Simile a netview ma in aggiunta alle funzionalità di net view elenca i server con servizi specifici.

dumping della tabella di nomi NetBIOS con nbtstat e nbtscan

nbtstat si connette a singole macchine anziché enumerare l'intera rete. It dumps the whole NetBIOS name table. Questa tabella contiene informazioni come l'indirizzo MAC della scheda di rete, ogni servizio in esecuzione ed eventuali utenti connessi.

nbtscan applica nbtstat all'intera rete facendo il dump di tutte le NetBIOS name table.

strumenti di enumerazione NetBIOS per linux

Il tool è NMBscan.

NetBIOS countermeasures

- Block UDP 137 at the firewall, or restrict it to only certain hosts
- To prevent user data from appearing in NetBIOS name table dumps, disable the Alerter and Messenger services on individual hosts
- Blocking UDP 137 will disable NBNS name resolution, and stop some applications that uses NBNS

NetBIOS Session, TCP 139/445

Over a NetBIOS session (TCP 139) it is possible to enumerate SMB. SMB (Server Message Block) di Microsoft sta alla base della condivisione di file e stampanti. E' possibile accedere a questo servizio mediante una sessione nulla:

```
C:\>net use \\192.168.202.33\IPC$ "" /u:""
```

se il comando ha successo l'hacker può ricavare informazioni di rete, utenti, chiavi di registro, password policy e molto altro.

enumerazione delle condivisioni di file

Dopo una null session risulta facile enumerare i nomi delle condivisioni di file tramite net view. Oppure tramite DumpSec è possibile enumerare:
file permission, services ecc… Questi sono strumenti manuali, se volessimo utilizzare tool automatici dovremmo optare per:

- ShareEnum e NetworkScanner

registry enumeration

To check if a remote registry is blocker the most suited tools are reg and DumpSec. Per default Windows è configurato in modo da consentire l'accesso al registro soltanto agli amministratori; l'enumerazione non funziona con null session.

trusted domain enumeration

after null session + nltest è possibile enumerare i trusted domain.

enumerazione di utenti

sessione null + DumpSec puoi ottenere informazioni sugli utenti e gruppi. Oppure utilizzando sid2user e user2sid sempre su windows NT. SID is a unique, immutable identifier of security principal: a user, user group,...
Gli ultimi tre numeri del SID sono il RID - Relative IDentifier. E' un numero predefinito per untenti e gruppi (500 rappresenta admin, 501 Guest).
Per esempio si utilizza prima user2sid per determinare il sid dell'admin e poi tramite sid2user per trovare il nome dell'account dell'amministratore. Gli account generati ricevono RID 1000,1001 … così facendo è possibile enumerare anche gli utenti. Funziona su windows NT ma non su Win XP SP2.

all-in-one null session enumeration tools

winfingerprint (single/multihost), NBTEnum (HTML output + bruteforce), winfo

SMB Null Session Countermeasures

- Le sessioni null richiedono l'accesso alla porta TCP 139 e/o 445 su Windows 2000 e versioni successive, perciò il modo più prudente per bloccarle è quello di filtrare tali porte su tutti i dispositivi perimetrali di accesso alla rete.
- Set the RestrictAnonymous registry key to 1 (or 2 on Win 2000 and later)
- Audit yourself with dumpsec

SNMP, UDP 161

Simple Network Management Protocol (Security Not My Problem). SNMP is intended for network management and monitoring It provides inside information on net devices, software and systems. Administrators use SNMP to remotely manage routers and other network devices

I dati sono protetti da autenticazione tramite password ma esistono diverse password di default ben note. Esempio di password per accedere ad SNMP in sola lettura è "public" oppure "private" per la scrittura, queste sono chiamate SNMP Community Strings. Tool per enumerare SNMP sono:

- snmputil in windows
- snmpget/snmpwalk (intero MIB) per linux.
- IP Network Browser browser grafico

Le informazioni rilasciate da SNMP sono salvate in una struttura gerarchica chiama MIB.

Tra le informazioni che vengono rilasciate da SNMP abbiamo:

- Running services
- Share names
- Share paths
- Comments on shares
- Usernames
- Domain name
- Running OS

scanner SNMP

SNScan permette di specificare una community string e un intervallo per la scansione oppure si può specificare un file contenente un elenco di community strings.

SNMP Enumeration Countermeasures

- Remove or disable unneeded SNMP agents (Rimuovere gli agenti SNMP sulle singole macchine)
- Change the community strings to non-default values (rimuovere public e private)
- Block access to TCP and UDP ports 161 (SNMP GET/SET) at the network perimeter devices
- Restrict access to SNMP agents to the appropriate management console IP address

BGP, TCP 179

BGP = Border Gateway Protocol, is the de facto routing protocol among Autonomous Systems.
Osservando le tabelle di routing di BGP è possibile determinare le reti associate a una particolare azienda. Organizations with more than one uplink use BGP.

Enumerazione BGP:

1. Determinare ASN (unique IP-like for a large organization) dell'organizzazione bersaglio
2. Eseguire una query sui router per individuare tutte le reti in cui l'AS path termina con l'ASN dell'organizzazione

Se si conosce il nome dell'organizzazione si può determinare l'ASN tramite una ricerca WHOIS sull'ARIN. Se si conosce l'IP si può interrogare un router e utilizzare l'ultimo elemento dell'AS path come ASN.

Non esistono contromisure.

LDAP Windows Active Directory, TCP/UDP 389 e 3268

LDAP = Lightweight Directory Access Protocol
Active Directory è un servizio di directory basato su LDAP.
ldp.exe permette di connettersi a un server AD e navigare nel contenuto della directory.
L'unico requisito per poter eseguire questa enumerazione è quello di creare una sessione autenticata via LDAP. Le informazioni che possono essere prese sono gli utenti e i gruppi e altre informazioni presenti sui Windows Domain Controller.

Active Directory Enumeration Countermeasures

- Filter access to ports 389 and 3268 at the net perimeter devices
- Legacy-compatible mode vs. Native Win 2000. Selezionare la modalità nativa in quanto la legacy aggiunge il gruppo everyone (chiunque sia autenticato) ai gruppi che possono accedere all'AD.

RPC UNIX, TCP/UDP 111/32771

Protocollo che permette la comunicazione tra due applicazioni in rete. rpcinfo è l'equivalente di finger per enumerare le applicazioni RPC in ascolto su host remoti. Anche nmap permette l'enumerazione di servizi RPC.

RPC Countermeasures

- Utilizzare un sistema di autenticazione per RPC
- Secure RPC permette di utilizzare l'autenticazione a chiave pubblica
- Filtro su firewall delle porte 111 e 32771

rwho (UDP 513) e rusers (RPC Program 100002)

Sono due programmi simili a finger. rwho restituisce gli utenti attualmente connessi a un host remoto che eseguono il daemon rwho. rusers è simile con l'aggiunta del tempo trascorso dall'ultima volta che l'utente ha digitato qualcosa alla testiera.

rwho and rusers Countermeasures

Come finger, questi servizi andrebbero semplicemente disattivati.

NIS, RPC program 100004

Fonte di informazioni di rete UNIX è NIS → Network Information System.
Una volta che si conosce il nome di dominio NIS di un server si può risalire alle informazioni fondamentali per ciascun host del dominio come il contenuto del file passwd.

NIS Countermeasures

- Passare a NIS+ che supporta autenticazione e cifratura dei dati

SQL, UDP 1434

SQL runna di default sulla porta 1434. Da SQL Server 2000 è possibile utilizzare più istanze SQL sullo stesso computer. Il problema è che solo un'istanza può utilizzare la porta 1434. SQL Server Browser Service permette di utilizzare più istanze contemporaneamente mettendosi in ascolto sulla porta 1434 e gestendo le chiamate in ingresso.

Tramite SQLPing è possibile scansionare un intervallo di indirizzi IP interrogando la porta 1434. Permette di effettuare anche attacchi brute force.

SQL Enumeration Countermeasures

- Limitare l'accesso mediante firewall

Oracle TNS, TCP 1521/2483

Il listener Oracle TNS (Transparent Network Substrate) gestisce il traffico del database client/server.
TNS ha due funzioni: tnslsnr e lsnrctl. Il primo gestisce le comunicazioni mentre il secondo gestisce l'amministrazione di tnslsnr. Da questo servizio è possibile ricavare informazioni come il SID del database, la versione, il sistema operativo. Conoscendo il SID del database un hacker potrebbe lanciare un brute force.

Oracle TNS Countermeasures

- Project Lockdown aiuta a migliorare la sicurezza di TNS andando a configurare permessi e password.

NFS, TCP/UDP 2049

L'utility showmount permette di enumerare file system esportati con NFS (Network File System). (sostanzialmente vedi le directory presenti su un server)

```
[root$] showmount -e 192.168.202.34
export list for 192.168.202.34:
```


```
/pub                    (everyone)
/var                    (everyone)
/usr                    user
```

NFS Countermeasures

- NFS bloccato sul firewall, porta 2049

IPSec/IKE, UDP 500

L'hacker può utilizzarla per infiltrarsi nella rete tramite VPN. Per violare IPSec, l'hacker deve prima enumerare IKE (Internet Key Exchange) che gestisce le negoziazioni di chiave, al fine di determinare dove si trovi esattamente IPSec e dove colpirlo. Non basta effettuare una scansione di porta standard della porta UDP 500 dato che i pacchetti formattati in modo errato dovrebbero essere ignorati in modo silente da qualsiasi servizio IPSec. E' possibile mediante lo strumento ike-scan.

Le informazioni rilasciate da ike-scan sono se il server VPN esegue l'autenticazione con chiavi o tramite certificati, quali protocolli di cifratura utilizza e se è in modalità Main Mode o Aggressive Mode. Se il server utilizza un sistema tramite chiavi ed è in modalità aggressiva allora è possibile ricevere un hash della chiave dal server VPN.

Se si ha una chiave hash rilasciata dal server, tramite psk-crack, è possibile eseguire un attacco brute force o dictionary per scoprire la chiave originale.

IPSec/IKE Countermeasures

- Bloccare indirizzi IP di origine non validi, poco scalabile
- Scegliere Main Mode rispetto ad Aggressive Mode, più sicura e non rilascia informazioni come l'hash della chiave precondivisa
- Utilizzo di certificati

Capitolo 4: Hacking Windows

Unauthenticated Attacks

I principali vettori utilizzati per compromettere sistemi Windows da remoto sono i seguenti:

1. Authentication Spoofing
   dictionary, brute force & mitm
2. Network Services
   penetration di servizi vulnerabili in ascolto sulla rete
3. Client Software Vulnerabilities
   Internet Explorer, Outlook, Office & Acrobat … Tramite le vulnerabilità software l'hacker può ottenere accesso ai dati degli utenti finali
4. Device Drivers
   Aree di attacco relative alle periferiche come network adapters e USB.

Authentication Spoofing Attacks

remote password guessing

La via tradizionale per violare i sistemi Windows da remoto è quella di attaccare il servizio di condivisione di file e stampanti che opera su un protocollo denominato SMB (Server Message Block). 2 porte per SMB che sono la porta TCP 445 e 139. Altri servizi soggetti ad attacchi sono:

- MSRPC (Microsoft RPC)
  TCP 135
- TS (Terminal Services)
  TCP 3389
- SQL
  TCP 1433 e 1434
- Web services like SharePoint (HTTP & HTTPS)
  TCP 80 e 443

Generalmente SMB è disabilitato nella configurazione standard dei sistemi windows che non sono Windows Server (ad esempio Windows Vista/Windows 8
). Per effettuare un dictionary attack ad un servizio SMB possiamo utilizzare questo file (credentials.txt):

```
[file: credentials.txt]
password        username
""""            Administrator
password        Administrator
admin           Administrator
administrator   Administrator
secret          Administrator
```

E applicare la seguente FOR nella shell di windows:

```
C:\>FOR /F "tokens=1, 2*" %i in (credentials.txt) do net use \\target\IPC$ %i /u:%j
```

Nella for su %i verrà inserita la password e su %j l'username (dictionary attack).
Tool automatici cli:

- enum, brutus, venom.

Tool automatici termial:

- TSGrinder, Rdesktop

password-guessing countermeasures

1. Use a network firewall to restrict access to SMB services on TCP 139 and 445
2. Use host firewall to restrict access to SMB
3. Disable SMB services (TCP 139 and 445)
4. Enforce the use of strong/long passwords using policy
5. Set an account-lockout threshold and ensure that it applies to the built-in Administrator account. (impostare una soglia per il blocco degli account e assicurarsi che valga per l'accont Administrator interno)
6. Log every failed attempt and audit regularly the event register

Use all of them for defense in depth.
Per impostare dei criteri sulle password da utilizzare possiamo utilizzare Local Security Policy direttamente in windows. (SECPOL.MSC) Possiamo impostare una lunghezza minimi e altri requisiti di complessità.

Tramite Local Security Policy è possibile impostare l'audit sugli eventi del sistema e mediante Dumpel possiamo estrarre i tentativi di accesso falliti sul sistema locale:

```
C:\> dumpel -e 529 -f seclog.txt -l security -m Security -t
```

Per migliorare ancor di più la sicurezza dei sistemi windows bisognerebbe utilizzare IDS e/o IPS.

Eavesdropping on Network Password Exchange

Tre tipologie di attacco per per spiare lo scambio di dati di accesso:

1. LM - Lan Manager (hash)
2. NTLM - NT LAN Manager (with encryption)
3. Kerberos (private or optional public key)

Il vecchio protocollo di autenticazione LAN Manager permette di individuare con facilità l'hash LM originale (equivalente di una password). Tool per attaccare l'autenticazione LM è Cain. Cain lavora anche su sessioni NTLM e permettendo di runnare algoritmi di password cracking sugli hash delle password trovati.

Kerberos sends a preauthentication packet which contains a timestamp encrypted with a key derived from the user's password.

- Offline attack on that exchange (dictionary attack) can reveal a weak password
- Anche qui Cain dispone di uno sniffer integrato MSKerb5-PreAuth

Windows Authentication Sniffing Countermeasures

1. Disable LM authentication. NT LAN Manager (NTLM) hashes are harder to crack.
2. Pick good passwords (complexity features)

3. Do not allow dictionary password
4. Use public key encryption
5. Use built-in Windows IPsec to authenticate and encrypt traffic.

Man In The Middle Attacks

SMBRelay è un server SMB in grado di ricavare nomi utente e hash di password dal traffico SMB in ingresso. Questi hash possono essere importati in strumenti di cracking. Consente all'hacker di introdursi tra client e server per intercettare la legittima comunicazione di autenticazione del client e di ottenere accesso al server con gli stessi privilegi del client stesso.

Quando utilizza questa tecnica, l'hacker può intercettare la connessione e riconnettersi sia al client che l'ha originata (metodo noto come SMB Credential Reflection) sia a qualsiasi altro server che accetti le credenziali fornite dal client (SMB Credential Forwarding)

Anche CAIN permette MITM SMB, combinando APR (ARP Poison Routing) con il downgrade dell'auth version dei client.

- Cain: redirect local traffic to itself with ARP spoofing, then downgrade clients to easier authentication dialects (sniffed, unencrypted, recorded)

MITM Countermeasures

- Very hard to block MITM if the attacker is already inside your LAN
- Use authenticated and encrypted protocol
- Disable NetBIOS Name Services - use DNS

Pass-the-Hash

E' una tecnica che consente a un hacker di autenticarsi presso un server remoto utilizzando l'hash della password di un utente eliminando così la necessità di violare gli hash per ottenere le password in chiaro. In un contesto NTLM gli hash sono equivalenti alle password in chiaro.

1. Compromise a machine
2. Dump password hashes stored in RAM
3. Use them as credentials for network services without cracking them

Questo sistema permette di ottenere anche le credenziali degli utenti che hanno effettuato l'accesso a una macchina da remoto. Esempio: admin che si è collegato alla macchina prima che venisse compromessa. Tool per fare il dump delle credenziali in memoria → WCE - Windows Credentials Editor.

Pass-the-hash countermeasures

- Pass-the-hash è intrinseca al protocollo di autenticazione NTLM. SMB, FTP, HTTP possono utilizzare NTLM e di conseguenze sono vulnerabili a questo attacco.
- Prevent intrusions in the first place, since this is a post-exploitation technique. E' una tecnica "post-violazione" in quanto, per poter compiere l'attacco, l'hacker deve prima entrare in possesso degli hash

- If possible, use two-factor auth

Pass the ticket

L'autenticazione Kerberos permette ai client di autenticarsi utilizzando dei ticket e all'accesso creano nuovi ticket con TGT (Ticket Granting ticket) fornito dal KDC (Key Distribution Center), che fa parte del controller di dominio.

Anche qui utilizzando WCE possiamo effettuare il dump dei ticket Windows di Kerberos e utilizzarli assieme al TGT per crearne nuovi per altri servizi.

Remote Unauthenticated Exploits

A differenza delle tecniche descritte finora sull'attacco ai protocolli di autenticazione Windows, le tecniche di exploit senza autenticazione da remoto puntano a difetti o errori di configurazione del Windows vero e proprio.

1. Exploit dei servizi di rete
2. End-user Application Exploits

Exploit dei servizi di rete

Metaxploit

- Framework plus archive of exploit modules
- Locate/search the exploit module
- Customize exploit parameters (vendor and model of victim software), payloads (remote command shell) and options (target IP address)

Network Service Exploit Countermeasures

- Apply patches quickly
- Use workarounds for unpatched vulnerabilities like disabling weak services
- Audit, Log and monitor traffic
- Have an incident response plan: Computer Security Incident Response Team (CSIRT), a group including information security and general IT staff, representatives legal, human resources and public relations departments. Produce plan with the organization's response to a cyberattack.

End-user Application Exploit

Il tipico ecosistema del client, mal gestito e stracolmo di software, fornisce un ottimo bersaglio di attacco per i malintenzionati.
Applicazioni più bersagliate:

- Adobe Flash Player
- Adobe PDF Reader

end-user application countermeasures

1. Use a firewall to limit outbound connections. Limitiamo quindi i tentativi di connessione in uscita.
2. Tenersi aggiornati su tutte le patch attinenti alla sicurezza.

3. Eseguire un Antivirus con scansione automatica e che si mantenga aggiornato. Possibilmente con utility controllo email (pishing).
4. Run with least privilege; if browsing Internet, never as Administrator
5. Use software security options, such as read email in plaintext
6. Configure MS Office to very high macro security

Device Driver Exploits

Oltre agli exploit di servii di rete remoti anche le vulnerabilità dei driver di periferica sono altrettanto esposte ad attacchi esterni. Esempio di attacco:
Windows wireless: within physical proximity to a rogue access point beaconing malicious packets → i driver di rete wireless Winws potevano essere attaccati semplicemente passando vicino, fisicamente, a un access point violato.

L'aspetto forse più grave di questi exploit è che in genere consentono di ottenere l'esecuzione in una modalità kernel con privilegi elevati, poiché i driver di periferica si interfacciano a basso livello per accedere in modo efficiente ai livelli di astrazione hardware primitivi.

Metaexploit WIFI exploit modules: e.g. oversized wireless beacon frame remote code execution

Driver Exploit Countermeasures

- Apply vendor patches
- Disable wireless networking at high concentration of Aps (Access points), and other high-risk environments
- Nel futuro: User-Mode Driver Framework. L'idea è quella di fornire un'API dedicata attraverso la quale i driver che operano in modalità utente con bassi privilegi possano accedere al kernel in modi ben definiti.

Authenticated Attacks

Qui vediamo cosa succede una volta che l'hacker è riuscito a entrare nel sistema.

Privilege Escalation

Once a user can log on to a Windows machine as a Guest or Limited User, the next goal is to escalate privileges to Administrator or SYSTEM

- getadmin.exe was an early exploit. (Utilizzava DLL Injection)

L'account SYSTEM ha più privilegi rispetto all'account Administrator. Esistono dei metodi che consentono agli amministratori di ottenere i privilegi di SYSTEM, uno è quello di utilizzare il servizio Windows Scheduler.

Preventing Privilege Escalation

- Keep Win machines patched
- Restrict interactive logon to trusted accounts (Strumento "Local Security Policy" di Windows)

Extracting and Cracking Passwords

Una volta ottenuto lo status di amministratore, gli hacker fanno di tutto per sottrarre tutte le informazioni possibili, da sfruttare per ulteriori conquiste. Una delle prime attività degli hacker, dopo aver ottenuto l'accesso, consiste nel raccogliere altri nomi utente e password→ in order to penetrate deeper into the network.

Grabbing the Password Hashes

Gli hash delle password di sistema sono memorizzate in:

- SAM (Security Account Manager) per utenti locali
- Active Directory per account di dominio

SAM sarebbe la controparte di /etc/passwd di UNIX in quanto contiene gli usernames e gli hash delle password corrispettive.

Obtaining the hashes

Sui sistemi windows gli hash delle password sono memorizzati in:

- %systemroot%\ system32\config\SAM (Sistemi NT4 e precedenti)
- o come valore della chiave: HKEY_LOCAL_MACHINE\SAM
- sui controller di dominio: %windir%\WindowsDS\ntds.dit

Ora sappiamo dove sono salvati i file, dobbiamo scoprire come prendere questi hash.

How to get the hashes

Con l'accesso di amministratore è facile effettuare il dump degli hash tramite strumenti come pwdump, Cain and Ophcrack. Questi utilizzano DLL injection e permette di estrarre le password. Non ci sono contromisure contro pwdump, fortunatamente per funzionare necessità dei privilegi di amministratore.

Cracking Passwords

Una volta noto l'algoritmo di hashing, l'hacker può utilizzarlo per calcolare l'hash per un elenco di possibili valori di password (per esempio, tutte le parole contenute in un dizionario di italiano o di inglese) e confrontare i risultati con un hash recuperato utilizzando uno strumento come pwdump.

Da un punto di vista pratico, l'attività di crack delle password si riduce a individuare algoritmi di hashing deboli (se ve ne sono), fare delle ipotesi in modo intelligente, utilizzare gli strumenti appropriati e, naturalmente, utilizzare tempo di elaborazione.

Algoritmi di hash deboli

Algoritmo di hashing di LAN Manager presenta gravi vulnerabilità che permettono di violarlo rapidamente: la password è suddivisa in due parti di 7 caratteri e tutte le lettere sono trasformate in maiuscolo, il che riduce le 2^284 possibili password alfanumeriche ottenibili con 14 caratteri a soli 2^237 hash diversi.

NTLM non è vulnerabile come LM e utilizza l'hashing MD5 a 128bit.

Generalmente per rendere gli hash più forti i sistemi operativi aggiungono un “random salt” prima di effettuare l’hash della password. Windows non lo implementa.
→ Two accounts with the same password hash to the same result, even in Windows 7 Beta!
→ This makes it possible to speed up password cracking with precomputed Rainbow Tables

Strategie per ipotizzare le password

- Brute Force
  Tries all possible combinations of characters
- Dictionary
  Tries all words in a word list.
- PreCalculated Hash Table
  In questo modo si riduce notevolmente il tempo necessario per generare gli hash da confrontare. → Rainbow tables

Tools:
- CLI: John the ripper jumbo
- GUI: Cain, Ophcrack

Cracking Password Countermeasures

L’entropia della password è proporzionale al tempo necessario per craccarla quindi la miglior difesa contro questa attività è la scelta di una password forte. Requisiti windows:
- non possono contenere il nome dell’account dell’utente,o parti del nome completo dell’utente, che superino due caratteri consecutivi
- devono essere lunghe almeno sei caratteri;
- lettere maiuscole inglesi (da A a Z);
- lettere minuscole inglesi (da a a z);
- cifre in base 10 (da 0 a 9);
- caratteri non alfabetici (per esempio !, $, #, %).

Consigliano di aumentare l’entropia della password aumentando la lunghezza minima da 6 a 8 caratteri. Con 8 caratteri si ha l’entropia maggiore.
- Configurare scadenza password anche di diversi mesi
- Disabilitare memorizzazione hash LM

Dumping Cached Passwords

Local Security Authority (LSA) Secrets è una cache contenente:
- password degli account di servizio in chiaro
- hash di password degli ultimi dieci utenti che hanno effettuato il login
- password in chiaro di utenti FTP
- RAS (Remote Access Services) names and passwords
- Encrypted when the machine is off, but decrypted and retained in memory after login

Tool per estrazione di queste info:
- Cain
- LSADump
- Windows Credential Editor (WCE)

- Extracts cleartext login password from RAM
- No hash-cracking required
- BUT you only get currently logged-on users

Logon Cache Dump Countermeasures

La miglior difesa è quella di evitare che un hacker possa ottenere i privilegi di amministratore. Solo tramite l'account amministratore (o SYSTEM) è possibile prendere questi hash. You can change the Registry value to eliminate the cached credentials (da 10 a 1).

Dumping di hash registrati in memoria

Tramite accesso remoto RDP, Windows salva in memoria la password degli utenti che hanno effettuato il login. Domain Admin should avoid RDP connections. Basterebbe utilizzare WCE per risalire a queste password.

Remote Control and Back Doors

Back door: services enabling remote control.
Tool per remote CLI: netcat.

```
C:\TEMP\NC11Windows>nc -L -d -e cmd.exe -p 8080
```

Avvia un listener sulla porta 8080 e restituisce una shell di comandi remota a chiunque si connetta a quella porta. Per connettersi al listener possiamo utilizzare anche telnet o nuovamente netcat.

Graphical Remote Control

Due tool:

- Windows built-in terminal services (aka Remote Desktop) listens on port 3389. It's not on by default
- VNC (Virtual Network Control) is free and can be installed remotely

Port Redirection

Una volta che un sistema è stato violato è possibile utilizzare il reindirizzamento delle porte per inoltrare tutti i pacchetti a una destinazione specifica. Il meccanismo di reindirizzamento funziona in questo modo: un programma si mette in ascolto su determinate porte e inoltra i pacchetti a una destinazione secondaria specificata.

Tool redirection: fpipe d McAfee. Si specifica una porta per l'ascolto e una porta di destinazione remota. Appena il viene stabilita una connessione sulla porta in ascolto viene effettuata una nuova connessione alla macchine e alla porta di destinazione creando un circuito completo.

Esempio di utilizzo:
abbiamo un host compromesso che ha in esecuzione telnet (porta 23) dietro un firewall che blocca la porta 23. La porta 53 (DNS) del firewall invece è aperta. Se impostiamo un port

redirection sull'host che manda i pacchetti dalla porta 53 alla 23 saremo in grado di superare il firewall e utilizzare telnet.

Covering Tracks

Once intruders have Administrator or SYSTEM equivalent privileges, they will:

- Hide evidence of intrusion
- Install backdoors
- Hide a toolkit to use for regaining control in the future and to use against other systems

Disabling Auditing

Generalmente l'auditing può rallentare le prestazioni sui server windows e per questa ragione generalmente è un opzione disabilitata. Dal resource kit è possibile utilizzare:

```
auditpool /disable
```

per disabilitare l'auditing sul sistema remoto. In questo modo le attività dell'hacker passeranno inosservate all'interno del sistema. Una volta finite le proprie attività attiveranno l'auditing:

```
auditpool /enable
```

Clearing the event log

Per eliminare i log e quindi eliminare ulteriori tracce lasciate dall'hacker è possibile utilizzare l'utility ELsave che ci permette di eliminare le nostre tracce dai log.

Hiding Files

Per mantenere dei file/toolkit sul sistema bersaglio e tenerli nascosti dagli occhi degli amministratori possiamo utilizzare l'attributo +h (hidden) per nascondere la directory:

```
attrib +h [directory]
```

In questo modo la directory sarà nascosta dal cli ma sarà visibile nel file explorer se è presente la spunta "Visualizza cartelle e file nascosti".

Alternate Data Streams (ADS)

Se il sistema utilizza NTFS (Windows NT File System) allora è possibile inserire più flussi di informazioni in un file. Permette quindi di nascondere un file all'interno di un file. Questa feature è stata inserita per motivi di compatibilità con sistemi Macintosh. Per creare flussi si utilizza POSIX cp che è un utility del Resource Kit.

```
C:\>cp nc.exe oso001.009:nc.exe
```

Questa sintassi nasconde nc.exe nel flusso di oso001.009.
Per estrarre dal flusso netcat:

```
C:\>cp oso001.009:nc.exe nc.exe
```

a cambiare è solo la data di modifica di oso001.009 ma non la sua dimensione.

- To delete an ADS, copy the file to a FAT partition and then back to NTFS

Per eseguire il flusso bisogna utilizzare il comando start:

```
start oso001.009:nc.exe
```

ADS Countermeasures

Per scoprire i flussi nei file NTFS bisogna utilizzare sfind di Foundstone.

Rootkits

Sono strumenti utili per sfuggire al rilevamento delle intrusioni. Se ne parlerà meglio nel capitolo 6. Rootkits are the best way to hide files, accounts, backdoors, network connections, etc. on a machine.

General Countermeasures to Authenticated Compromise

Once a system has been compromised with administrator privileges, you should just reinstall it completely. You can never be sure you really found and
removed all the backdoors. But if you want to clean it, cover four areas:
Files, Registry keys, Processes and Network ports.

Suspicious Files

Bisogna cercare i nomi di strumenti comunemente utilizzati come:

- nc.exe, fpipe.exe e psexec.exe
- controllare se all'interno del sistema è stata copiata la shell in diverse directory e con nomi diversi da cmd.exe
- controllare i programmi che runnano all'avvio di windows e che sono quindi presenti come valore della chiave Start Menu\PROGRAM\STARTUP di windows
- Utilizzare antivirus
- Use Tripwire or other tools that identify changes to system files

Suspicious Registry Entries

Bisogna controllare se sono presenti programmi di backdoor o altri programmi pericolosi nei seguenti registri:

1. HKLM\SOFTWARE
2. HKEY_USERS\.DEFAULT\Software

Una volta trovati programmi sospetti bisogna utilizzare *reg delete* per eliminare tali entry.

ASEP (Autostart Extensibility Points)

Le chiavi :

1. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
3. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
4. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

possono presentare dei comandi da terminale che vengono eseguiti ad ogni avvio del sistema windows. Ad esempio è possibile impostare netcat per avere una backdoor attiva sul sistema in questione.

Suspicious Processes

I processi maligni possono essere individuati dal task manager. Generalmente sono quelli che consumano più CPU e possono essere fermati direttamente da task manager. Un altro sistema utilizzato dagli hacker è il Task Scheduler di Windows che permette di avviare dei processi. Bisogna quindi controllare anche il task scheduler per i processi.

Suspicious Ports

Se un listener nc è stato rinominato l'utility netstat permette di identificare le sessioni in stato LISTENING o ESTABLISHED. Comando per vedere le network connections:

```
netstat -aon
```

Windows Security Features

- Windows Firewall

- Automated Updates

- Security Center (punto centrale per windows firewall, update, antivirus e internet options). E' indicato per i consumer ma non per gli esperti IT in quanto mancano funzioni di sicurezza più avanzate (come i group policy)

- Group Policy Tool
  → Allows security policy settings in domains

- Microsoft Security Essentials
  → Free antivirus, included in Win 8 by default

- EMET (Enhanced Mitigation Experience Toolkit)
  → Allows the user to configure DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization)

- Bitlocker and Encrypting File System (EFS)
  One of the major security-related centerpieces released with Windows 2000 is the Encrypting File System (EFS). EFS is a public key cryptography-based system for transparently encrypting file-level data in real time so attackers cannot access it without the proper key. EFS can encrypt a file or folder with a fast, symmetric, encryption algorithm using a randomly generated file encryption key (FEK) specific to that file or folder. The randomly generated FEK is then itself encrypted with one or more public keys, including those of the user and a key recovery agent (RA). Key recovery is implemented in case employees who have encrypted some sensitive data leave an organization or their encryption keys are lost. Although EFS can be useful in

many situations, it probably doesn't apply to multiple users of the same workstation. That's what NTFS Access Control List (ACL) are for.

- Bitlocker Drive Encryption (BDE)
  With Windows Vista, Microsoft introduced Bitlocker Drive Encryption (BDE). Although BDE was primarily designed to provide greater assurance of operating system integrity. Rather than association data encryption keys with individual user accounts, BDE encrypts entire volumes and stores the key in ways that
  are much more difficult to compromise. Researchers at Princeton University published a paper on so-called cold boot that bypasses BDE. Essentially, the researchers cooled DRAM chips to increase the amount of time before the loaded OS was flushed from volatile memory. This permitted enough time to harvest an image of the running OS, from which the master BDE decryption keys could be extracted, since they obviously had to be available to boot the system into a running state. The only real mitigation for cold-boot attacks is to separate the key physically from the system it is designed to protect.

  Contromisure Attacco di avvio a freddo
  Tenere la chiave fisicamente separata dal sistema che si deve proteggere.

- Windows Resource Protection (WRP)
  Tenta di garantire che i file critici e i valori critici del registro di sistema del sistema operativo non siano modificati, intenzionalmente o meno.
  WRP utilizza ACL. Il punto debole è che gli amministratori possono cambiare il valore alle ACL.

- Integrity Levels, UAC e PMIE
  Mandatory Integrity Control (MIC) is an extension of the windows architecture that permits the implementation of mandatory controls in certain situations. It implements four security principles that are called Integrity Level (IL) that are: low, medium, high, system which can be added to access tokens and ACLs.

  Example: a process with a medium level of integrity could be blocked to read, write or execute a process with a high level of integrity. It follows the Biba model ("no write up no read down").

  ILs are implemented as SIDs. MIC represents the base for UAC (User Access Control) and PMIE (Protected Mode Internet Explorer)
  se vuoi approfondire PAGINA 229 del pdf.

- Data Execution Prevention
  Mark portions of memory as non executable to prevent buffer overflow attacks. Making the stack non-executable, for example, shuts down one of the most reliable mechanisms for exploiting software available today: the stack-based buffer overflow.

- Windows Service Hardening

Introdotto per prevenire la compromissione dei servizi. Questa tecnologia include:

1. Service resource isolation
   Many services execute in the context of the same local account, such as LocalService. If any one of these services is compromised, the integrity of all other services executing as the same user are
   effectively compromised as well. To address this, Microsoft meshed two technologies:
   - Service-specific SIDs;
   - Restricted SIDs;

   By assigning each service a unique SID, service resources, such as a file or Registry key, can be ACLed to allow only that service to modify them.

2. least privilege services
   Before Vista the service's privileges were only linked to the user's privilege. With Vista the services are now capable of providing the SCM (Service Control Manager) with a list of specific privileges that they require. Upon starting the service, the SCM removes all the privileges from the services process that are not explicitly requested. For services that share a process, like svchost, the process token contains an aggregate of all privileges required by each individual service in the group, making this process an ideal attack point. Removing the unnecessary privileges the attack surface will be reduced.

3. service refactoring
   Il refactoring di servizi indica l'esecuzione di servizi con account dotati di privilegi più ridotti, in sostanza è un modo per eseguire i servizi con privilegi minimi.

4. restricted network access
   With the new version of the Windows Firewall network restriction policies can be applied to service as well. The firewall permit to create new connection based rules such as:
   - directionality. Rules that check the incoming and outgoing network traffic
   - Protocol: Checks the type of protocol
   - Principal: Rules related to a specific user
   - Interfaces: Rules that are related to a set of interfaces such as wireless, LAN and so on.

5. session 0 isolation
   In 2002, Chris Paget introduced a new Windows attack technique coined the "Shatter Attack" (Attacco Distruttore). The technique involved using a lower privileged attacker sending a window message to a higher- privileged service that causes it to execute arbitrary commands, elevating the attacker's privileges to that of
   the service. By design every service inside the interactive desktop is on the same level and each service can impose requests on each other. This design allowed attackers to send window messages to privileged services because

they shared the default login session, Session 0. By separating user and service sessions, Shatter-type attacks are mitigated.

- Compiler-based Enhancements
  Some of the worst exploits result from memory corruption attacks like the buffer overflow. Microsoft imple-mented some features to deter such attacks, including:
  1. GS
  2. SafeSH
  3. ASLR

  These are mostly (low-level) compile-time under-the-hood features that are not configurable by administrators or users.

  GS is a compile-time technology that aims to prevent the exploitation of stack-based buffer overflows on the Windows platform. GS achieves this by placing a random value (or cookie) on the stack between local variables and the return address.

  A hacker can override the Exception Manager in order to run code in a more reliable way with respect to overriding the return address. SafeSH was introduced for resolving this problem. SafeSEH is a compile-time security technology. Unlike GS, instead of protecting the frame pointer and return address, the purpose of SafeSEH is to ensure the exception handler frame is not abused.

  ASLR is designed to mitigate an attacker’s ability to predict locations in memory where helpful instructions and controllable data are located. Before ASLR every image such as DLL and EXE were loaded in the same address space at every run. DEP + ASLR permits to achieve a high level of security.