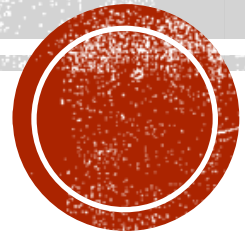
ATTACCHI INFORMATICI



SICUREZZA DOCUMENTALE

A.A. 2017-2018

LE FASI DI UN ATTACCO INFORMATICO

- Footprinting
- Scansione
- Enumerazione
- Exploit
- Controllo del sistema

FASE1: FOOTPRINTING

- Raccolta di informazioni sull'obbiettivo da attaccare.
- Determinare il profilo di protezione della struttura target.
- Riuscire ad ottenere uno specifico intervallo di nomi di dominio, blocchi di rete e indirizzi IP direttamente collegati ad internet

FASE1: FOOTPRINTING

- **Passaggio 1: Delimitare l'ambito di azione**
- Stabilire i cofini per l'attività di footprinting (tutta l'azienda o solo una determinata sede).
- Creare una copia locale del sito (Es. Teleport Pro o wget) alla ricerca di informazioni nascoste (ad esempio nei commenti HTML).
- **Passaggio 2: Enumerazione della rete**
- Identificare i nomi di dominio collegati ad una specifica organizzazione.
- Utilizzo di whois (specificando differenti server whois)
- **Passaggio 3: Interrogazione del DNS**
- Effettuare un trasferimento di zona non autorizzato. Un server master secondario allinea le proprie informazioni con il server master primario. In alcuni casi I trasferimenti di zona vengono concessi a chiunque.
- Comandi: nslookup, host, dig,Sam Spade, etc.

FASE1: FOOTPRINTING (PASSAGGIO 3)

- **Ad esempio il comando:**

nslookup

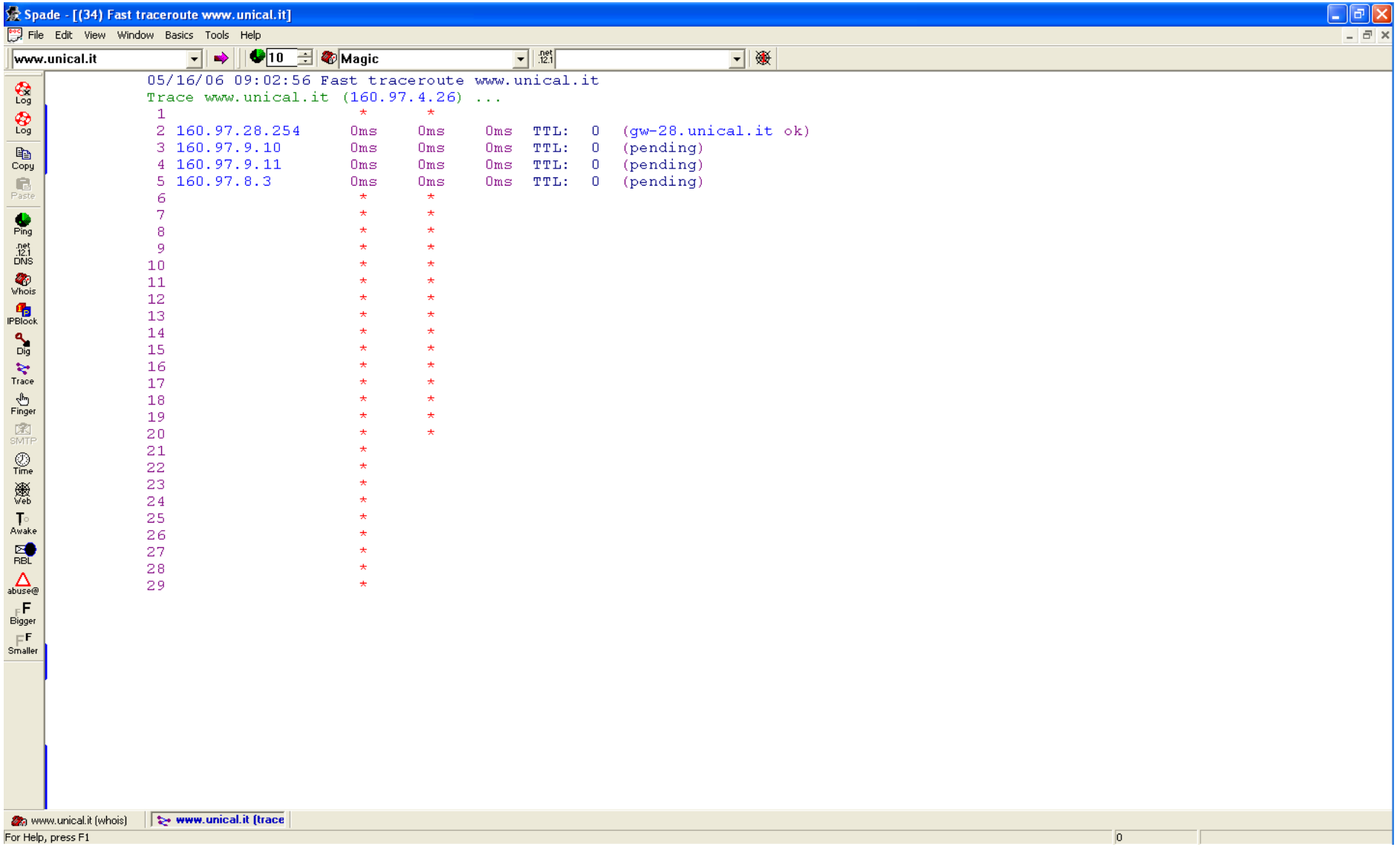
>> ***server x.y.z.w (DNS predefinito)***

>> ***set type=any***

>> ***ls –d mydomain.x >>tmp/zone_out***

- **Nel caso in cui il server DNS oggetto non fosse opportunamente configurato mi restituisce tutti i record associati ad un dominio.**
- **Con comandi come grep potrei filtrare questi record alla ricerca di particolari valori (es. tipo di sistema operativo,etc.)**

FASE1: FOOTPRINTING (PASSAGGIO 3)



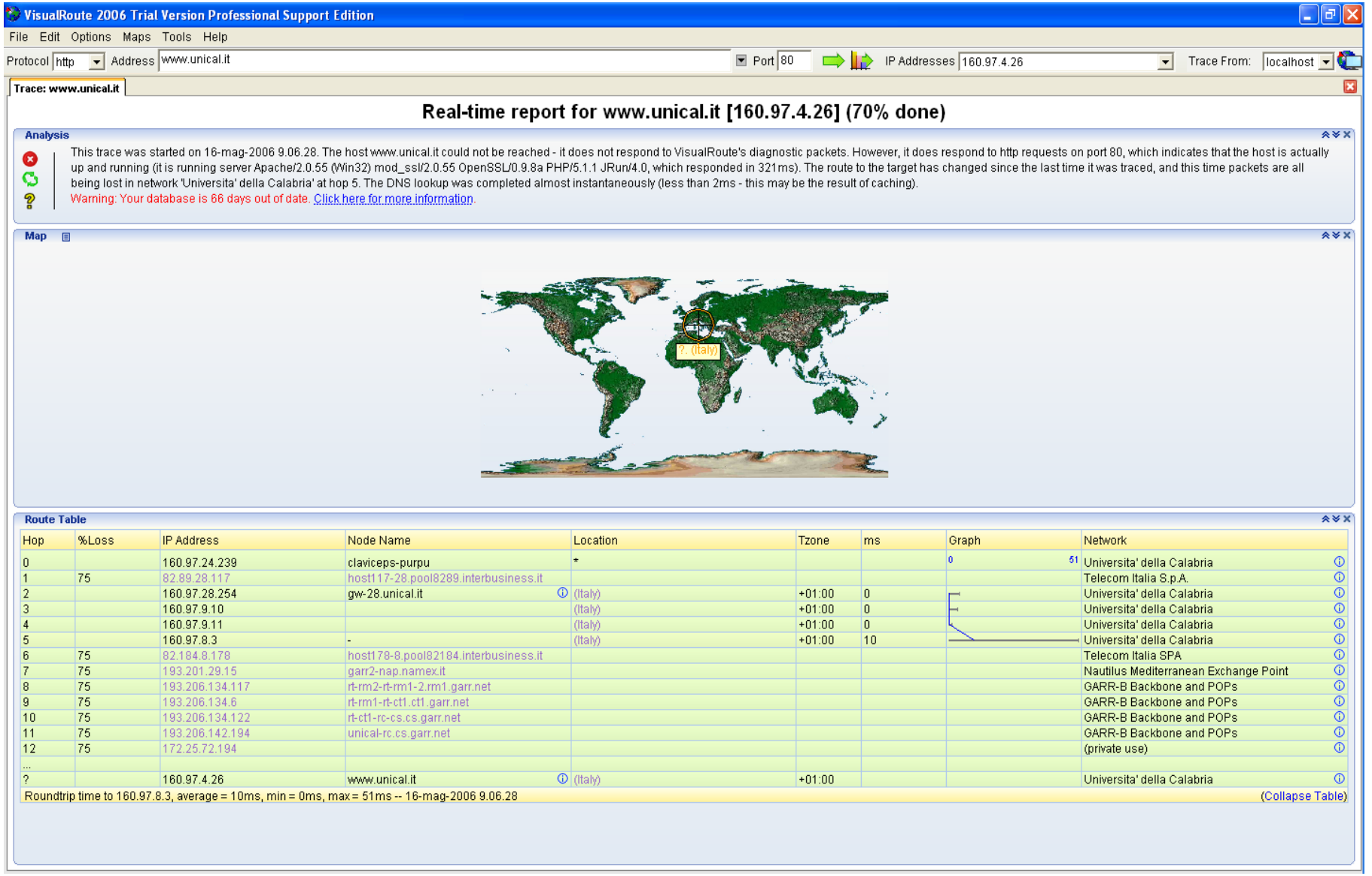
TRASFERIMENTI DI ZONA (CONTROMISURE)

- **Limitare i trasferimenti di zona solo a chi autorizzato.**
- **Configurare i firewall affinché rifiutino connessioni sulla porta TCP 53 (usata per i trasferimenti).**
- **Limitare l'utilizzo di record HINFO.**

FASE1: FOOTPRINTING

- **Passaggio 4: Perlustrazione della rete**
- Individuare possibili percorsi di accesso.
- Comando **traceroute**: sfrutta le proprietà TTL del pacchetto IP per ottenere un messaggio di tipo ICMP TIME_EXCEEDED da ogni router. In questo modo si possono individuare i dispositivi di controllo dell'accesso (firewall software o router con filtraggio sui pacchetti).
- Tuttavia i pacchetti alcune volte vengono respiti.
- Con l'opzione *–S –pN* possiamo specificare la porta sulla quale inviare la sonda.
- Ad esempio si potrebbe utilizzare la porta UDP 53 destinata alle interrogazioni DNS

PERLUSTRAZIONE DELLA RETE (VISUAL ROUTE)



PERLUSTRAZIONE DELLA RETE (CONTROMISURE)

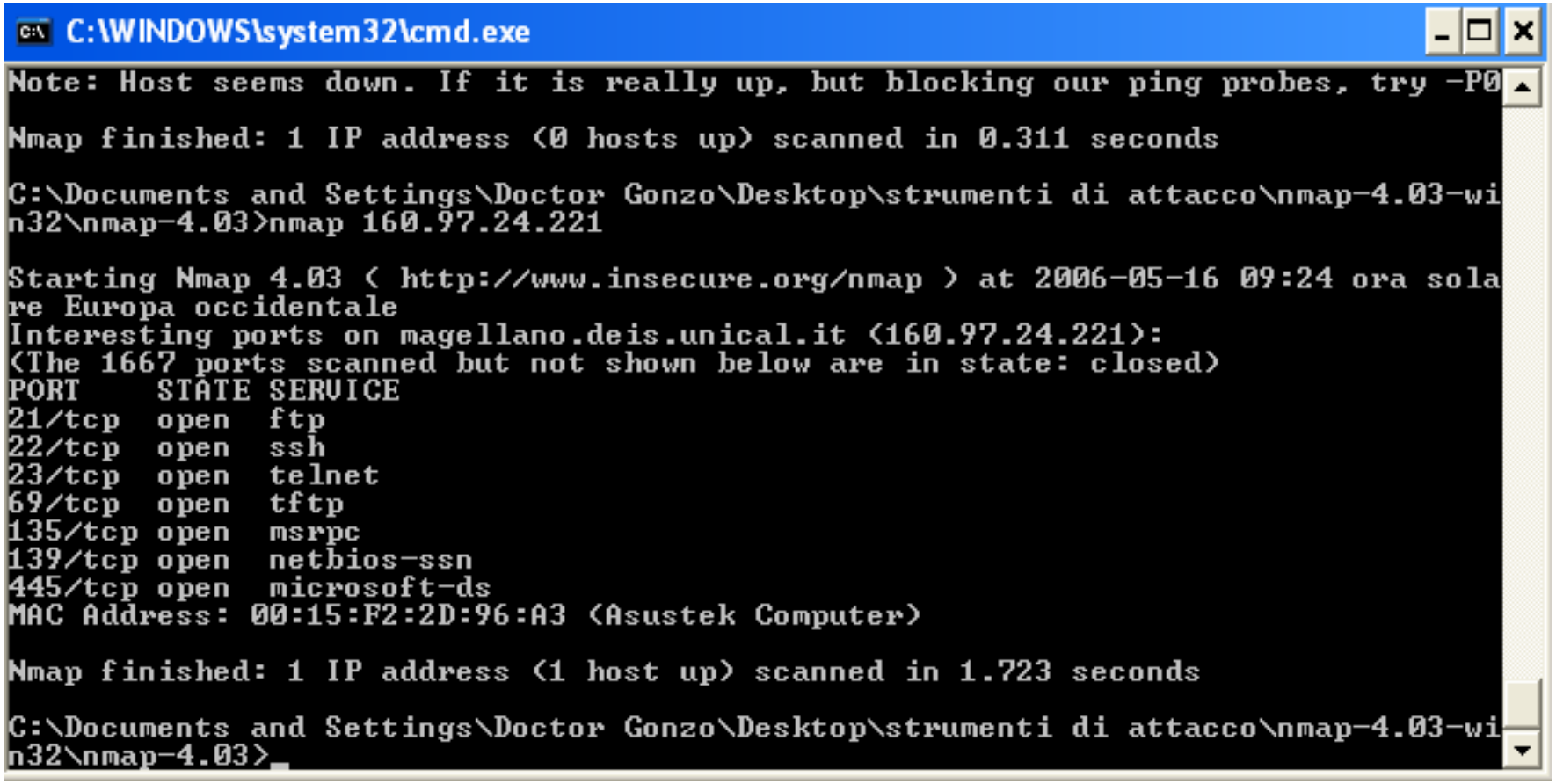
- **Utilizzo di IDS (Intrusion Detection Systems)**
- **Tool Snort**
- **Tool RotoRouter (contrattacco): genera risposte non valide.**
- **Ridurre il traffico ICMP e UDP a sistemi specifici.**

FASE 2: SCANSIONE

- Questa fase ha lo scopo di "bussare" su tutte le pareti per trovare porte e finestre.
- Stabilire quali sistemi siano effettivamente raggiungibili.
- Un indirizzo IP ottenuto attraverso un trasferimento di zona non è detto che sia attivo.
- Ping su un intervallo di indirizzi IP
- Nmap (es. nmap –sP 192.168.0.1/254)
- Nel caso in cui vengano bloccati i pacchetti sulla porta di default, nmap consente di specificare la porta: nmap –sP –PT80 192.168.9.1/24

FASE 2: SCANSIONE DELLE PORTE

- Identificazione dei servizi TCP e UDP attivi.
- Strumenti (strobe, udp_scan,netcat,nmap)



FASE 2: TIPO DEL SISTEMA OPERATIVO

- **Fingerprint attivo dello stack: tecnica che consente di identificare con precisione il sistema operativo di un host.**
- **Le differenti implementazioni TCP/IP differiscono per piccoli aspetti dovuti ad una differente interpretazione della RFC.**
- **Sulla base di queste differenze può essere identificato il sistema operativo.**
- **Es. nmap –o 192.168.0.1**
- **In assenza di porte aperte, nmap effettua una previsione.**

RILEVAMENTO DEL SISTEMA OPERATIVO (CONTROMISURE)

- **Si dovrebbero settare delle politiche in grado di riconoscere le impostazioni del flag SYN.**
- **Scartare i pacchetti SYN+FIN**
- **Tuttavia: Fingerprint passivo dello stack:**
- **Si analizzano gli attributi di una sessione TCP/IP sniffando il traffico di rete:**

  TTL, Dimensione della finestra, DF, ToS
- **Ogni S.O ha delle caratteristiche quasi univoche.**
- **Strumento Cheops**

FASE 3: ENUMERAZIONE

- **Individuazione di account validi e/o di risorse condivise poco protette.**
- **La differenza è che l'enumerazione richiede connessioni dirette ai sistemi e interrogazioni esplicite e per questo dovrebbe o potrebbe essere intercettata.**
- **Le tecniche di enumerazione dipendono fortemente dal sistema operativo.**

FASE 3: ENUMERAZIONE IN WINDOWS

- **Sessioni nulle**
- **Comando net view /domain**
- **Comando nbtstat (lettura dei nomi netbios)**
- **Enumerazione dei controllori di dominio**
- **Enumerazione delle condivisioni netview \\nomehost**
- **Strumenti: Legion, Nat,**

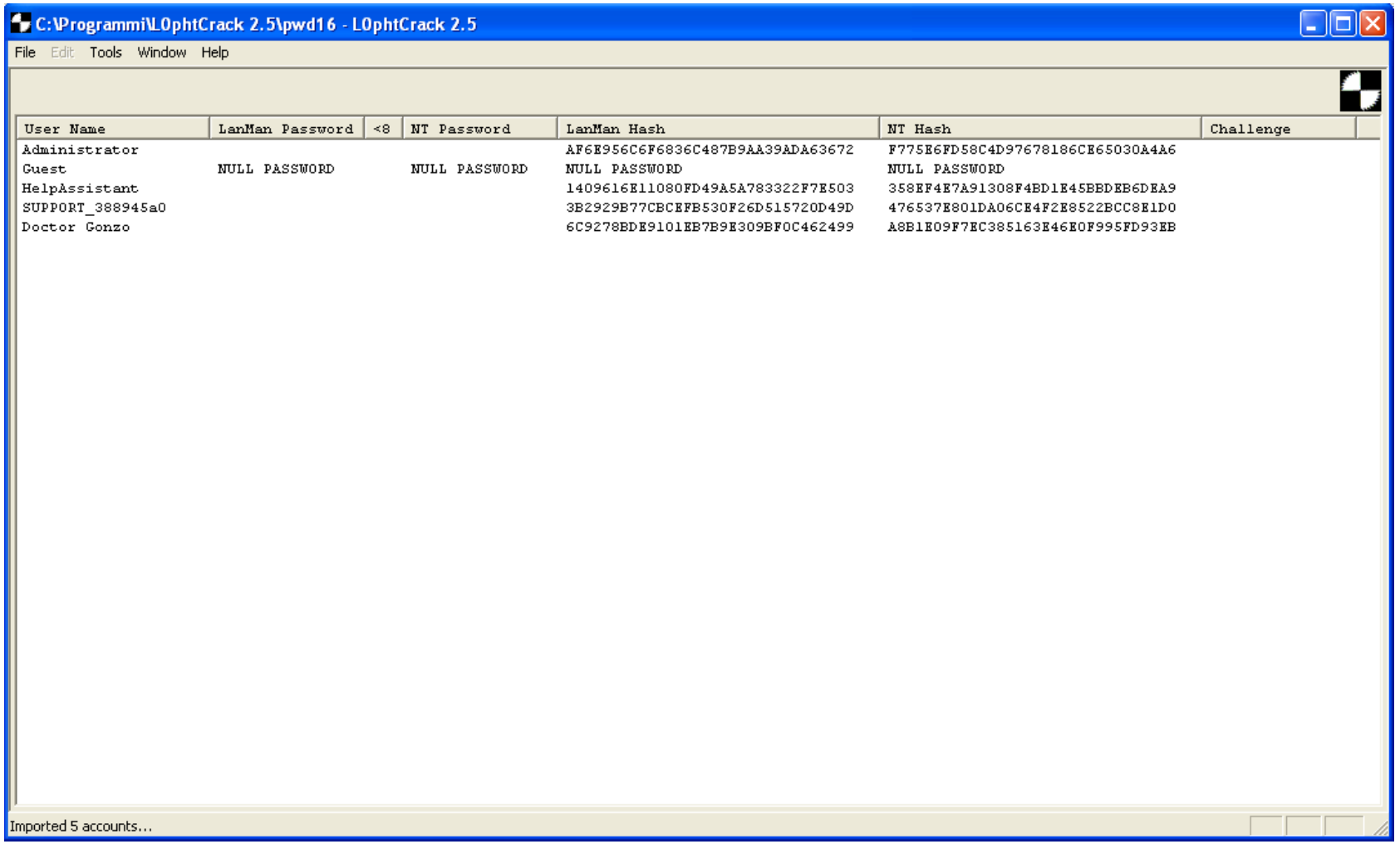
FASE 3: ENUMERAZIONE IN WINDOWS

- **Chiusura delle porte TCP e UDP da 135 a 139.**
- **Tuttavia enumerazione SNMP (Simple Network Management Protocol).**
- **Tool: IP network browser.**

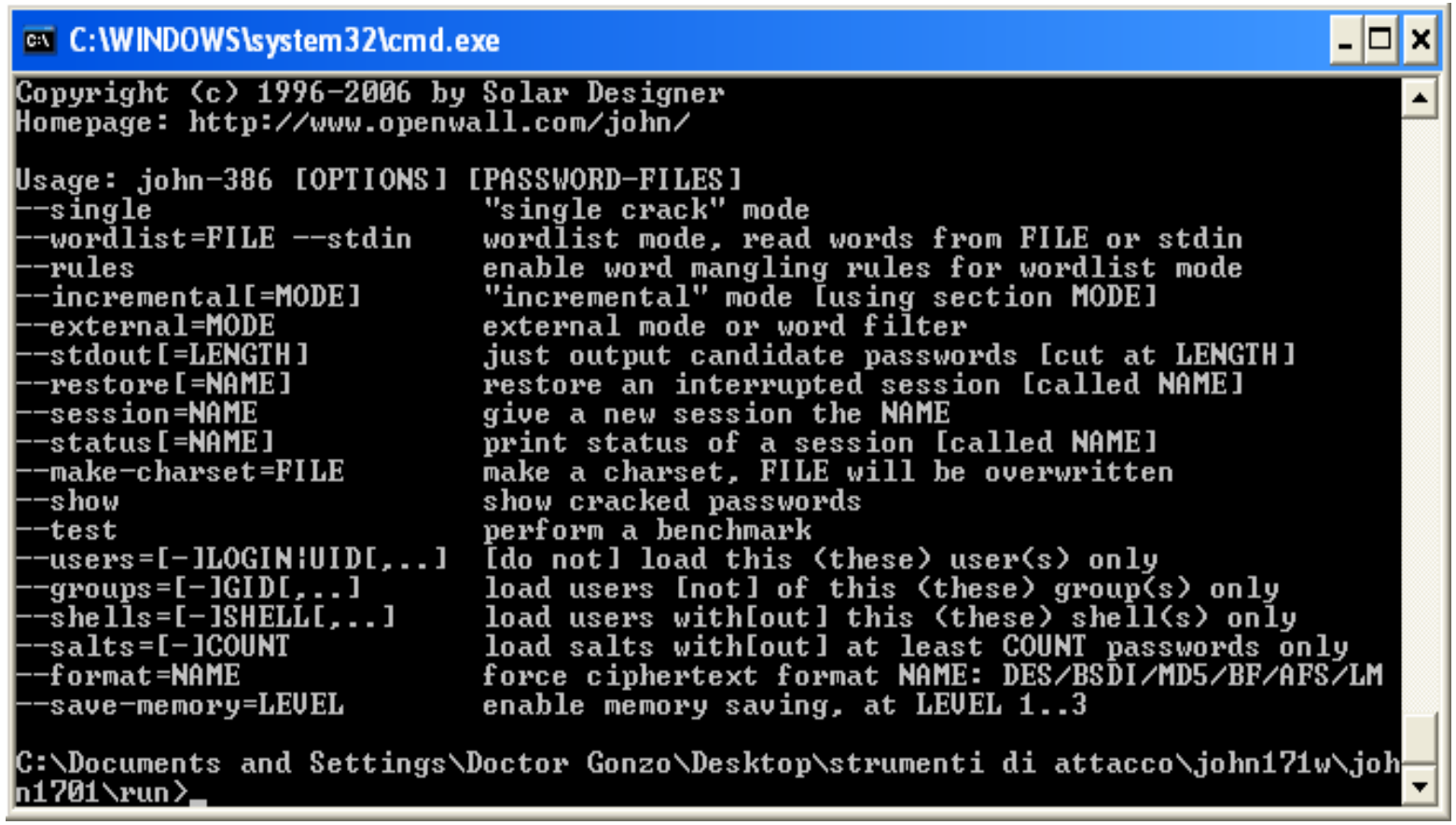
HACKING DELLE PASSWORD

- **Windows NT: L0pht Crack**
- **Linux/UNIX: John the Ripper, CrackerJack**
- **Attacco Forza Bruta**
- **Attacco del dizionario**

LOPHT CRACK


C:\Programmi\LOphtCrack 2.5\pwd16 - LOphtCrack 2.5
File Edit Tools Window Help
User Name | LanMan Password | <8 | NT Password | LanMan Hash | NT Hash | Challenge
Administrator AF6E956C6F6836C487B9AA39ADA63672 F775E6FD58C4D97678186CE65030A4A6
Guest NULL PASSWORD NULL PASSWORD NULL PASSWORD NULL PASSWORD
HelpAssistant 1409616E11080FD49A5A783322F7E503 358EF4E7A91308F4BD1E45BBDEB6DEA9
SUPPORT_388945a0 3B2929B77CBCEFB530F26D515720D49D 476537E801DA06CE4F2E8522BCC8E1D0
Doctor Gonzo 6C9278BDE9101EB7B9E309BF0C462499 A8B1E09F7EC385163E46E0F995FD93EB
Imported 5 accounts...

JOHN THE RIPPER



DEFINIZIONE

Con Intrusion Detection si identificano arti e tecniche per scoprire attività anomale, scorrette o non appropriate nei sistemi.

Intrusion Detection Systems

Host-based, Network-based, Stack-based.

Statistical detection, pattern-matching detection.

NIDS

Network-based Intrusion Detection Systems

Catturano il traffico che passa sulla rete.

Filtro di primo livello --> identifica il traffico da analizzare

Secondo livello --> analizzatore di attacchi

Terzo livello --> modulo di intervento

NIDS

Punti di forza:

- Costi modesti
- Analizzatore di pacchetti
- Registrano gli attacchi
- Evidenziano gli attacchi
- Identificazione e risposta real-time
- Usi complementari e verifiche di policy
- Indipendenza da OS

HIDS

Host-based Intrusion Detection Systems

Fanno un auditing sistematico dei log di sistema.

Real-time vs scheduled auditing

Tracciano I/O, Process, Port e Network activity

Modulo di analisi, modulo di intervento

INTEGRITY CHECKERS

Un tipo di host-based IDS è l'*integrity checker*.

tripwire

Falsi positivi

SIDS

Un ibrido dei precedenti due sistemi è costituito dagli

Stack-based Intrusion Detection Systems

Analizzano il traffico di rete pertinente a un singolo sistema

Vi è un solo modulo di filtro+analisi realizzato come estensione dello stack TCP/IP (si aggancia agli *hook* dello stack)

Inbound, outbound & local activity

E' piuttosto leggero, ma occorre una console centralizzata per la gestione di sistemi multipli

{H,S}IDS

Punti di forza:

- Verifica degli attacchi
- Verifica di attività specifiche del sistema
- Reti *switched*
- Crittografia
- Monitoraggio di componenti chiave
- Identificazione e risposta in near real-time o real-time
- Nessun hardware aggiuntivo

CONFIGURAZIONI MISTE

Una soluzione particolarmente efficace consiste nell'adottare una miscela delle tipologie di IDS descritte, che consentirebbe di identificare attacchi complessi correlando nel tempo eventi separati. Esempi:

- Telnet (N), su root (H), kill syslog (H)
- Port scan (N), cgi-bin attack (N), HTML defacement (H)
- port scan (N), sendmail attack (N), rootkiit install & exec (H)

NETWORK MEDIA

Nelle reti switched occorrono soluzioni per installare i NIDS

Per esempio si può inserire un HUB tra il sistema da analizzare e lo switch. All'hub si collega il NIDS.

Pros:

- Semplice ed economico

Cons:

- Interferisce troppo con il sistema analizzato: il management dell'IDS genera collisioni sull'HUB
- Gli HUB sono a basso costo → failures
- Poco o non applicabile per sistemi multipli, su GbE o dove il traffico complessivo è elevato

NETWORK MEDIA

SWITCH: si usa un TAP a cui si collega il NIDS

Pros:

- Fault tolerant
- Nessun impatto sul traffico
- Disaccoppia la rete dal NIDS
- Nessun degrado di prestazioni

Cons:

- Costoso
- Non si può collegare dappertutto e l'applicabilità dipende sostanzialmente dalla topologia dei collegamenti

NETWORK MEDIA

SWITCH: si usa la SPAN, una porta a cui viene rediretto il traffico dello switch e a cui si collega il NIDS

Pros:

- Nessuna modifica fisica alla rete

Cons:

- Una sola SPAN per ogni switch, di solito
- Monitorando le (molte) altre porte la SPAN (e il NIDS) si sovraccarica
- Sovraccarico dello switch

Configurazione *stealth* a due porte: il NIDS ha una porta di cattura senza protocolli bound e un'altra di gestione

SNORT

E' un NIDS "leggero" capace di effettuare analisi e logging del traffico IP in tempo reale.

Ha tre modi: sniffer, logger o NIDS.

L'analisi si basa sulla tecnica del *pattern matching*. Quando analizza un pacchetto contenente certi *pattern* specificati nelle sue regole esegue l'azione ad essi associata (logging, alert…).

http://www.snort.org

INTRUSION PREVENTION

Nel tempo gli IDS si sono rivelati poco utilizzabili.

- NIDS sono come guardiani all'ingresso di una Banca, cui è consegnato un pacco di fotografie di delinquenti: quando ne vedono uno suonano l'allarme

- HIDS sono come guardiani all'interno della cassaforte della Banca, che controllano che il contenuto sia ancora lì

Il danno non si può evitare, finché non si dotano i guardiani di armi per impedire l'intrusione.

INTRUSION PREVENTION

Gli IDS sono poco efficaci anche per motivi legati alla complessità dei fenomeni controllati.

- Le regole di *matching* cambiano continuamente
- Per funzionare in modo utile, il riconoscitore ha bisogno di *statefulness*
- Servono tecniche di riconoscimento di anomalie a livello di protocolli continuamente aggiornate
- Servono tecniche di riconoscimento di anomalie su base statistica continuamente aggiornate
- Impegnano il team a essere "pronto all'azione"

INTRUSION PREVENTION

Gli IDS sono nati senza pensare alla prevenzione dell'intrusione, ma solamente all'identificazione, essenzialmente perché limitazioni hw e sw imponevano scelte di compromesso.

- Iniziano gli HIDS
- I NIDS nascono come IDS "estratti" dagli host
- Manca la potenza elaborativa necessaria

La possibilità di prevenzione era negata dalla posizione nella rete.

INTRUSION PREVENTION

La tendenza dei NIPS è stata:

- sfruttare la crescente potenza elaborativa dei processori dedicati e degli ASIC ecc
- mettere la logica di *detection* negli switch di rete
- associare ad essa una (buona) logica di *prevention* (analisi + intervento)

Quando un pacchetto entra nel sistema si prende una decisione "*go/no-go*", nel caso più semplice, oppure si possono realizzare soluzioni più sofisticate implementando servizi di alto livello (content filtering, web o email)

INTRUSION PREVENTION

La tendenza dei HIPS è stata:

- sfruttare la crescente potenza elaborativa dei processori dei computer
- agganciarsi a ogni *hook* che il sistema operativo (kernel, stack, ecc) fornisce
- associare logiche di *prevention* (analisi + intervento) appropriate, modulari, aggiornabili e monitorabili

Per gestire una molteplicità di sistemi con queste caratteristiche occorre un sistema centrale di gestione

Esempi tipici: antivirus e anti-malware in genere

LIDS

E' un HI**P**S per Linux: http://www.lids.org

Oltre alla identificazione delle intrusioni e alla loro notifica, protegge anche il sistema modificando le chiamate del kernel che sovrintendono le operazioni di I/O su directory, files e dispositivi fisici e che controllano i processi e applicandovi politiche di Mandatory Access Control. Include:

- un port scan detector
- protezione dei file
- protezione dei processi
- Access Control Lists

Riferimenti

- **www.unife.it/ing/lm.tlcele/.../060-b80-intrusion-detection.ppt**
- **Intrusion Detection Systems**
  ISS Howto Guide
  B. Laing, J. Alderson
- **Intrusion Detection FAQ**
  SANS
- **Intrusion Detection is dead. Long live Intrusion Prevention!**
  SANS GIAC Certification Practical
  T. D. Wickham

http://www.snort.org

http://www.lids.org

http://www.foundrynet.com/solutions/appNotes/ironShieldSecurity.html