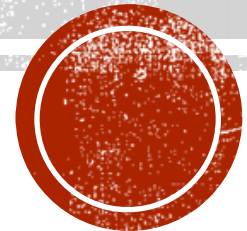


# **ATTACCHI INFORMATICI**

**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'obiettivo 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 confini 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)

The screenshot shows the Spade application window titled "Spade - [(34) Fast traceroute www.unical.it]". The interface includes a menu bar (File, Edit, View, Window, Basics, Tools, Help), a toolbar with icons for Log, Copy, Paste, Ping, net 121 DNS, Whois, IPBlock, Dig, Trace, Finger, SMTP, Time, Web, Awake, FBL, and abuse@, and a status bar at the bottom with "For Help, press F1".

The main window displays the following text:

```
05/16/06 09:02:56 Fast traceroute www.unical.it
Trace www.unical.it (160.97.4.26) ...
1 * *
2 160.97.28.254 0ms 0ms 0ms TTL: 0 (gw-28.unical.it ok)
3 160.97.9.10 0ms 0ms 0ms TTL: 0 (pending)
4 160.97.9.11 0ms 0ms 0ms TTL: 0 (pending)
5 160.97.8.3 0ms 0ms 0ms TTL: 0 (pending)
6 * *
7 * *
8 * *
9 * *
10 * *
11 * *
12 * *
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 * *
22 * *
23 * *
24 * *
25 * *
26 * *
27 * *
28 * *
29 * *
```

The status bar at the bottom shows "www.unical.it (whois)" and "www.unical.it (trace)".



# 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 **tracert**: 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)

VisualRoute 2006 Trial Version Professional Support Edition

File Edit Options Maps Tools Help

Protocol http Address www.unical.it Port 80 IP Addresses 160.97.4.26 Trace From: localhost


Trace: www.unical.it

### Real-time report for www.unical.it [160.97.4.26] (70% done)

**Analysis**

This trace was started on 16-mag-2006 9.06.28. The host www.unical.it could not be reached - it does not respond to VisualRoute's diagnostic packets. However, it does respond to http requests on port 80, which indicates that the host is actually up and running (it is running server Apache/2.0.55 (Win32) mod\_ssl/2.0.55 OpenSSL/0.9.8a PHP/5.1.1 JRun/4.0, which responded in 321 ms). The route to the target has changed since the last time it was traced, and this time packets are all being lost in network 'Universita' della Calabria' at hop 5. The DNS lookup was completed almost instantaneously (less than 2ms - this may be the result of caching).  
**Warning: Your database is 66 days out of date. [Click here for more information.](#)**

**Map**



**Route Table**

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		160.97.24.239	claviceps-purpu	*			0	51 Universita' della Calabria
1	75	82.89.28.117	host117-28.pool8289.interbusiness.it	(Italy)	+01:00	0		Telecom Italia S.p.A.
2		160.97.28.254	gw-28.unical.it	(Italy)	+01:00	0		Universita' della Calabria
3		160.97.9.10		(Italy)	+01:00	0		Universita' della Calabria
4		160.97.9.11		(Italy)	+01:00	0		Universita' della Calabria
5		160.97.8.3	-	(Italy)	+01:00	10		Universita' della Calabria
6	75	82.184.8.178	host178-8.pool82184.interbusiness.it					Telecom Italia SPA
7	75	193.201.29.15	garr2-nap.nameix.it					Nautilus Mediterranean Exchange Point
8	75	193.206.134.117	rt-rm2-rt-rm1-2.rm1.garr.net					GARR-B Backbone and POPs
9	75	193.206.134.6	rt-rm1-rt-ct1.ct1.garr.net					GARR-B Backbone and POPs
10	75	193.206.134.122	rt-ct1-rc-cs.cs.garr.net					GARR-B Backbone and POPs
11	75	193.206.142.194	unical-rc.cs.garr.net					GARR-B Backbone and POPs
12	75	172.25.72.194						(private use)
...								
?		160.97.4.26	www.unical.it	(Italy)	+01:00			Universita' della Calabria

Roundtrip time to 160.97.8.3, average = 10ms, min = 0ms, max = 51ms -- 16-mag-2006 9.06.28 (Collapse Table)



# 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)

```
C:\WINDOWS\system32\cmd.exe
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap finished: 1 IP address (0 hosts up) scanned in 0.311 seconds
C:\Documents and Settings\Doctor Gonzo\Desktop\strumenti di attacco\nmap-4.03-win32\nmap-4.03>nmap 160.97.24.221
Starting Nmap 4.03 ( http://www.insecure.org/nmap ) at 2006-05-16 09:24 ora solare Europa occidentale
Interesting ports on magellano.deis.unical.it (160.97.24.221):
(The 1667 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
69/tcp    open  tftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:F2:2D:96:A3 (Asustek Computer)
Nmap finished: 1 IP address (1 host up) scanned in 1.723 seconds
C:\Documents and Settings\Doctor Gonzo\Desktop\strumenti di attacco\nmap-4.03-win32\nmap-4.03>
```



# 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.**

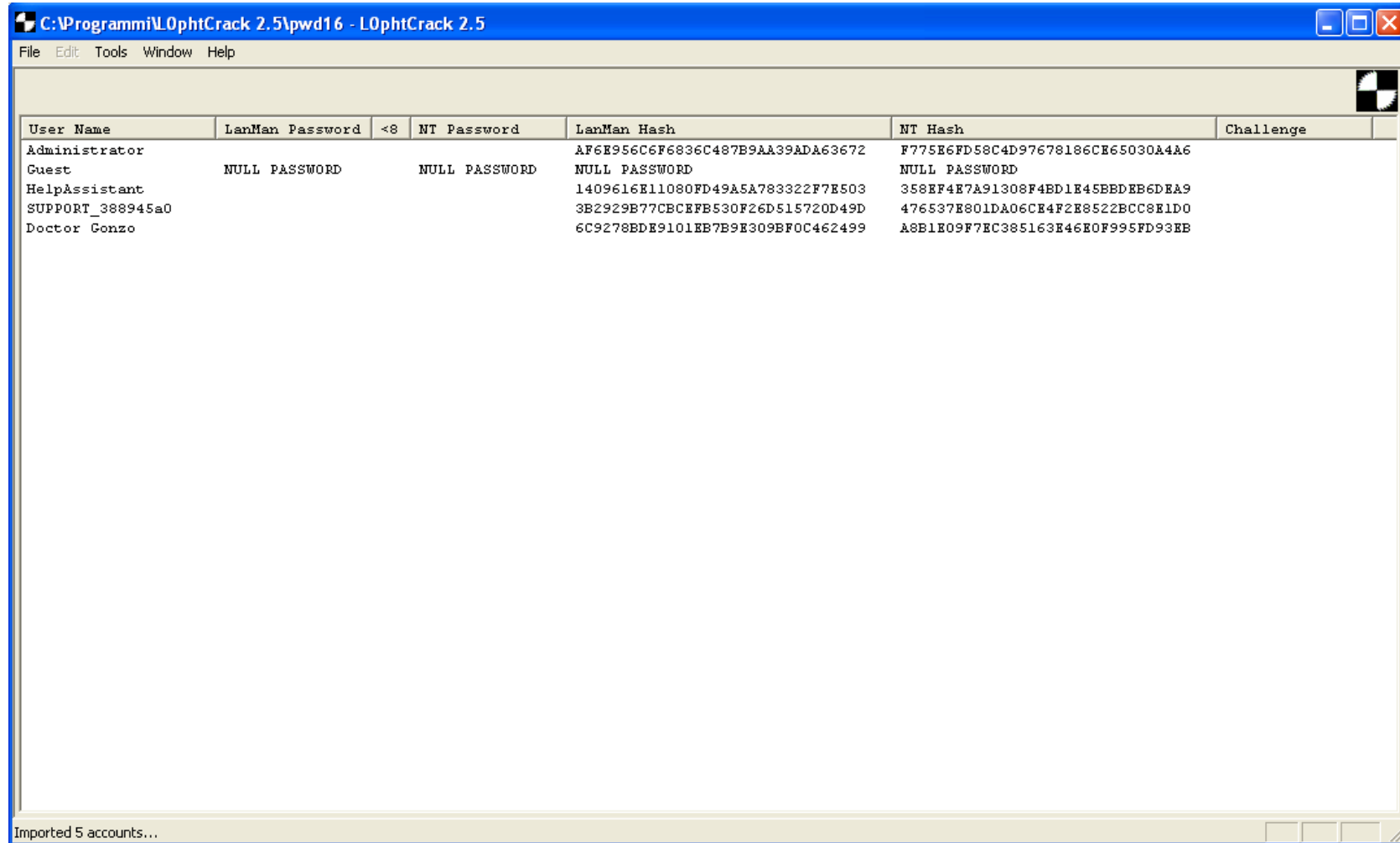


# HACKING DELLE PASSWORD

- **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			3B2929B77CCEFB530F26D515720D49D	476537E801DA06CE4F2E8522BCC8E1D0	
Doctor Gonzo			6C9278BDE9101EB7B9E309EF0C462499	A8B1E09F7EC385163E46E0F995FD93EB	

Imported 5 accounts...



# JOHN THE RIPPER

```
C:\WINDOWS\system32\cmd.exe
Copyright (c) 1996-2006 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john-386 [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules                 enable word mangling rules for wordlist mode
--incremental[=MODE]    "incremental" mode [using section MODE]
--external=MODE         external mode or word filter
--stdout[=LENGTH]      just output candidate passwords [cut at LENGTH]
--restore[=NAME]       restore an interrupted session [called NAME]
--session=NAME         give a new session the NAME
--status[=NAME]        print status of a session [called NAME]
--make-charset=FILE    make a charset, FILE will be overwritten
--show                 show cracked passwords
--test                 perform a benchmark
--users=[-]LOGIN!UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]   load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..] load users with[out] this (these) shell(s) only
--salts=[-]COUNT     load salts with[out] at least COUNT passwords only
--format=NAME          force ciphertext format NAME: DES/BSDI/MD5/BF/AFS/LM
--save-memory=LEVEL    enable memory saving, at LEVEL 1..3

C:\Documents and Settings\Doctor Gonzo\Desktop\strumenti di attacco\john171w\john1701\run>
```



# 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), rootkit 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 HIPS 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/Im.tlcele/.../060-b80-intrusion-detection.ppt](http://www.unife.it/ing/Im.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>

