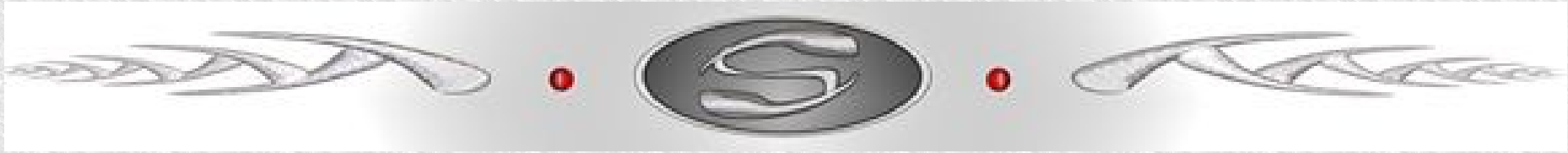


Rischi e insicurezze dei sistemi informativi aziendali

Relatori:

Marco Balduzzi, Michele Marchetto

Vicenza, 30 Settembre 2004

Rischi di un sistema informativo

- Furto di informazioni riservate
- Furto d'identità
- Accesso con privilegi non autorizzati
- Accesso non autorizzato
- Denial Of Service (DOS)
- Esecuzione di software non autorizzato (virus e worm)
- Guasto hardware
- Furto fisico

Sicurezza software

- Bug di sicurezza
  - Errori di programmazione che permettono l'esecuzione di istruzioni arbitrarie
  - L'attaccante è in grado di ottenere
    - accesso remoto non autorizzato
    - accesso con privilegi non autorizzati (“privilege escalation”)
- Codici replicanti
  - Software che in modo trasparente eseguono istruzioni non autorizzate e si replicano su dispositivi rimuovibili o via internet. Fan parte di questa categoria virus e worm.

Sicurezza software

- Aggiramento delle protezioni software
  - Cracking: procedura di disassemblamento del codice eseguibile al fine di ricostruire particolari strutture, procedure ed algoritmi del programma.
  - L'attaccante è in grado di evadere protezioni software come le password.
- Attacco diretto alle password (brute-force)
  - Metodo per decriptare tentando in sequenza tutte le possibili combinazioni.

Sicurezza software

- Intercettazione dell'attività di un utente
  - Intervenendo sul codice di un programma o del sistema operativo stesso è possibile catturare il comportamento di un utente, realizzando un furto di identità e di informazioni riservate.
- Trojan e backdoor
  - Programma specifico o modificato utilizzato dall'attaccante per accedere nuovamente (e con i privilegi desiderati) alla macchina vittima.

Sicurezza sociale

- Social engineering
  - Tecniche psicologiche (non informatiche!) utilizzate da un attaccante per recuperare dati personali e codici di accesso.
  - Caso Kevin Mitnick

Sicurezza di rete

- Denial Of Service
  - Permette all'attaccante di saturare la disponibilità di banda o di risorse della macchina vittima provocando un “mancamento di servizio”.
  - 7 febbraio 2000: Distributed DoS contro Yahoo.
- Occultamento della propria identità (spoofing)
  - Per mezzo di server malconfigurati e debolezze note del TCP/IP è possibile falsificare e nascondere la propria identità.
  - Un attaccante può far ricadere la colpa verso un'altra persona!

Sicurezza di rete

- Avvelenamento delle informazioni di rete (poisoning)
  - L'attaccante falsifica il contenuto delle cache di rete a proprio piacimento (ARP, DNS, Tabella di Routing).
  - E' in grado di dirottare il traffico.
- Raccolta di informazioni dalla rete (sniffing)
  - L'attaccante intercetta il traffico di rete accedendo ad informazioni riservate.
  - Può intervenire sul flusso dati modificandolo (hijacking), dirottandolo, distruggendolo...

Sicurezza di rete

- Attacchi specifici delle reti wireless
  - Associazione non autorizzata all'AP
  - Furto della chiave WEP
  - Dirottamento delle associazioni dei dispositivi
- E bluetooth
  - Utilizzo non autorizzato dei servizi bluetooth (per es. furto della rubrica e dei messaggi di un cellulare)
- Molto altro...

Un attacco informatico

- Ricercare l'obiettivo
- (Mascherare la propria identità)
- Raccogliere informazioni sul sistema
- Guadagnare l'accesso
- Realizzare il lavoro prefissato (furto d'informazioni e quant'altro..)
- Installare backdoor/trojan
- Cancellare le proprie tracce
- Abbandonare il sistema o utilizzarlo come “proxy”

Raccolta delle informazioni

- Information gathering
  - Obiettivo: ottenere il maggior numero di informazioni sulla macchina vittima
  - Tipologia di informazioni
    - Tipologia di sistema [router, client, server, ...]
    - Architettura hardware [i386, sparc, macppc, ...]
    - Infrastruttura di rete
    - Sistema operativo
    - Servizi abilitati (tipo) [ftp, ssh, http, ...]
    - Servizi abilitati (software e versione) [ProFTPD 1.2.9, Apache/2.0.52, ...]
    - Vulnerabilità note
    - Relazioni (di fiducia) con altre macchine

Raccolta delle informazioni

- Modalità
  - Esistono numerosi strumenti che automatizzano questa attività
  - L'attaccante confronta e integra i risultati manuali con quelli automatici
  - Vediamo i più famosi strumenti di information gathering:
    - whois
    - host
    - nmap
    - nessus

whois

- Strumento per l'accesso al database delle registrazioni internet (RFC-812)
- A chi appartiene il dominio satexpo.it?

```
$ whois satexpo.it
domain:      satexpo.it
x400-domain: c=it; admd=0; prmd=satexpo;
org:         promospace srl.
descr:       servizi pubblicitari e di marketing
nserver:     193.43.2.1  dns.nettuno.it
remarks:     Delegated to NETTuno
mnt-by:      NETTUNO-MNT
created:     19971120
expire:      20041120
```

host

- Strumento di gestione delle richieste DNS

```
$ host -a www.satexpo.it dns.nettuno.it
Trying "www.satexpo.it"
Using domain server:
Name: dns.nettuno.it
Address: 193.43.2.1#53
;; QUESTION SECTION:
;www.satexpo.it.                IN      ANY
;; ANSWER SECTION:
www.satexpo.it.         86400   IN      A       193.207.41.36
;; AUTHORITY SECTION:
satexpo.it.             86400   IN      NS      dns.nettuno.it.
satexpo.it.             86400   IN      NS      dns2.nextra.it.
satexpo.it.             86400   IN      NS      dns2.nic.it.
```

host

- Quali sono i mail-server autoritativi per satexpo.it?

```
$ host -t MX satexpo.it dns.nettuno.it
Using domain server:
Name: dns.nettuno.it
Address: 193.43.2.1#53

satexpo.it mail is handled by 0 mail.satexpo.it.
satexpo.it mail is handled by 10 mx2.nettuno.it.
```

nmap

- E' uno strumento di esplorazione della rete e di scansione delle porte (portscan)

- E' possibile trovare le macchine attive di una rete

```
$ nmap -sP 192.168.1.0/24
Starting nmap 3.50 at 2004-09-25 12:11 CEST
Host zeus.too.fun (192.168.1.2) appears to be up.
Host puzzle.too.fun (192.168.1.4) appears to be up.
Host 192.168.1.10 appears to be up.
Host router.too.fun (192.168.1.254) appears to be up.
Nmap run completed -- 256 IP addresses (4 hosts up) scanned in 7.931
seconds
```

nmap come portscanner

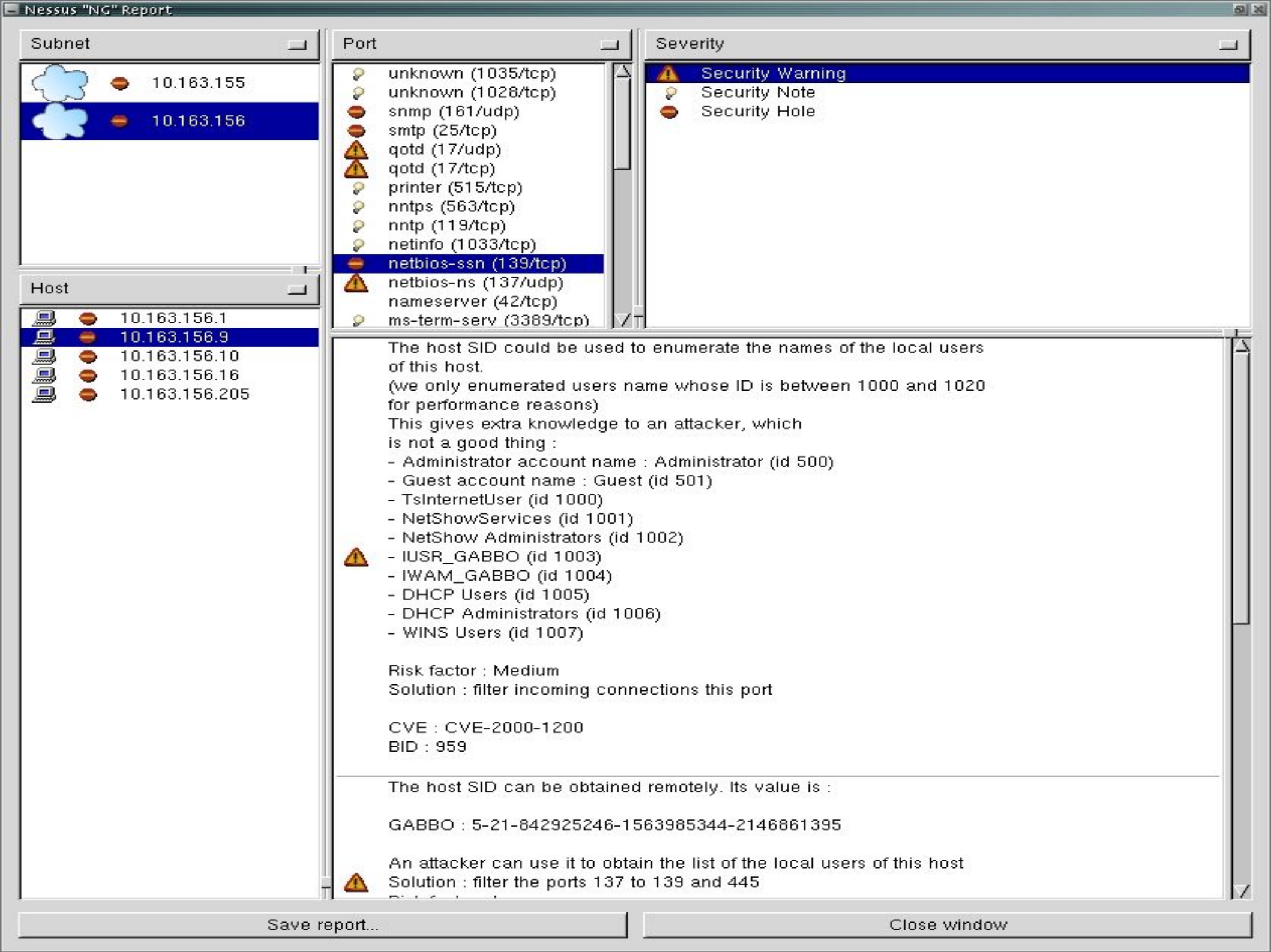
```
# nmap -A www.satexpo.it

Interesting ports on www.open-sky.it (193.207.41.36):
(The 1654 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE    VERSION
21/tcp   open     ftp?
22/tcp   open     ssh        OpenSSH 3.4p1 (protocol 2.0)
80/tcp   open     http       Apache httpd 1.3.26 ((Unix) Debian GNU/Linux
PHP/4.1.2)
135/tcp  filtered msrpc
5432/tcp open     postgresql PostgreSQL DB
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 134.831 days (since Thu May 13 16:04:42 2004)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3834808 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 146.166 seconds
```

nessus

- Cos'è?
  - Famoso e aggiornato scanner remoto di vulnerabilità offerto dalla comunità opensource
  - Architettura client-server
  - Interfaccia grafica user-friendly
  - Lista dei test estremamente personalizzabile
  - Report multi-formato


Nessus "NG" Report
Subnet
10.163.155
10.163.156
Host
10.163.156.1
10.163.156.9
10.163.156.10
10.163.156.16
10.163.156.205
Port
unknown (1035/tcp)
unknown (1028/tcp)
snmp (161/udp)
smtp (25/tcp)
qotd (17/udp)
qotd (17/tcp)
printer (515/tcp)
nntps (563/tcp)
nntp (119/tcp)
netinfo (1033/tcp)
netbios-ssn (139/tcp)
netbios-ns (137/udp)
nameserver (42/tcp)
ms-term-serv (3389/tcp)
Severity
Security Warning
Security Note
Security Hole
The host SID could be used to enumerate the names of the local users
of this host.
(we only enumerated users name whose ID is between 1000 and 1020
for performance reasons)
This gives extra knowledge to an attacker, which
is not a good thing :
- Administrator account name : Administrator (id 500)
- Guest account name : Guest (id 501)
- TsInternetUser (id 1000)
- NetShowServices (id 1001)
- NetShow Administrators (id 1002)
- IUSR_GABBO (id 1003)
- IWAM_GABBO (id 1004)
- DHCP Users (id 1005)
- DHCP Administrators (id 1006)
- WINS Users (id 1007)
Risk factor : Medium
Solution : filter incoming connections this port
CVE : CVE-2000-1200
BID : 959
The host SID can be obtained remotely. Its value is :
GABBO : 5-21-842925246-1563985344-2146861395
An attacker can use it to obtain the list of the local users of this host
Solution : filter the ports 137 to 139 and 445
Save report...
Close window

Sicurezza

- Sicurezza esterna
- Sicurezza interna
- Sicurezza wireless
- Sicurezza sociale
- Spesso non basta nemmeno questo...

Sicurezza Esterna (1)

- Riguarda tutti quegli attacchi che provengono dall'esterno della vostra LAN aziendale
- Gli attacchi piu' comuni si svolgono sfruttando vulnerabilita' note nei servizi offerti al pubblico (HTTP, FTP, ...)
- Spesso questi attacchi sono automatizzati, e vengono lanciati su range IP a scopo di mass deface
- Talvolta gli attacchi possono essere piu' mirati e intelligenti
- Possono provenire da fuori e svilupparsi dentro, come nel caso di e-mail contenti troyan, virus, tunnel...
- Possono mirare a rendere il tale servizio o la tale macchina indisponibile

Sicurezza Esterna (2)

- Firewall, IDS e Honeypots **NON** sono la soluzione a tutti i problemi, ma possono dare un contributo importante alla sicurezza se configurati a dovere
- Spesso il problema principale e' la collocazione
- Un firewall puo' aiutarci anche in caso di attacchi DdoS e puo' limitare il numero di informazioni ottenibili con tool come nmap filtrando non solo le porte ma anche mascherando l'OS fingerprint
- Sensori IDS possono informarci di eventuali tentativi di attacco, ma sono ancora una tecnologia abbastanza sperimentale e il numero di falsi positivi puo' essere spesso molto alto

Sicurezza Esterna (3)

- Essere sicuri al 100% che tutti i nostri servizi siano inattaccabili è impossibile, possiamo solo adottare delle contromisure per limitare i danni in caso di breaking in
- Limitare il numero di servizi usufruibili da tutti
- Rimanere sempre aggiornati sui nuovi buchi di sicurezza ed applicare le relative patch con tempestività
- Nel caso di webserver prestare estrema attenzione a contenuti dinamici, interazioni con i database (PHP, SQL...)
- Chroot, privilege separation, systrace e simili possono spesso essere di aiuto
- Limitare al minimo trust relationship tra host “esterni”

Sicurezza Esterna (4)

- E' importante educare i propri dipendenti in modo che siano attenti ad utilizzare in maniera sicura strumenti come client di posta, browser...
- L'utilizzo della firma digitale è **FONDAMENTALE** per garantire che l'autenticita' di una e-mail.
- Filtri spam che bloccano virus e troyan possono essere d'aiuto
- Virus, troyan, tunnel, ssh inversi possono compromettere i nostri duri sforzi per rendere l'infrastruttura sicura

Sicurezza Interna (1)

- Spesso l'errore più grave è supporre che gli attacchi possano provenire esclusivamente dall'esterno...
- Un utente interno alla LAN e' potenzialmente più pericoloso di uno esterno
- Può attaccare gli apparati godendo di una posizione favorita, magari al di fuori della portata dei sensori IDS
- Può sniffare il traffico di rete, password e dati sensibili
- La possibilita' di infezione di worms costruiti ad-hoc e' notevolmente più alta
- Può modificare il routing della LAN se quest'ultimo non e' abbastanza protetto

Sicurezza Interna (2)

- Attraverso tecniche come l'arp poisoning un attaccante è in grado di agire da proxy trasparente, potenzialmente con tutte le connessioni che avvengono in LAN anche su reti switchate
- Può quindi portare un attacco MITM, compromettendo qualsiasi dato sensibile che passi per la LAN
- Una soluzione intelligente è quella di criptare il traffico sensibile attraverso algoritmi a chiave pubblica con pre-shared keys memorizzate nei vari host
- Entry ARP statiche ove possibile
- Utilizzare switch con politiche di sicurezza resistenti come ad esempio arp inspection + dhcp snooping

Sicurezza Interna (3)

- Come nel caso “esterno” sarebbe bene sempre utilizzare la firma digitale anche quando le e-mail sono intra-aziendali
- L'accesso a dati sensibili dovrebbe utilizzare schemi di autenticazione/criptazione forte e essere limitato solo a chi ne ha veramente bisogno, limitando al massimo le trust relationship basate su hostname/IP
- Firewall e IDS dovrebbero controllare e limitare anche il traffico interno in modo da limitare e avvertire eventuali tentativi di azioni illecite

Sicurezza Interna (4)

- I protocolli di routing dinamico sono spesso, nella modalità di default, altamente insicuri
- Protocolli basati su broadcast e multicast come RIP e RIPv2 se non usati nella modilità di autenticazione keyed MD5 sono altamente vulnerabili
- Anche protocolli basati su TCP ereditano tutte le insicurezze di ques'ultimo e sono quindi insicuri
- In alcune circostanze è possibile agendo sui protocolli di routing locale andare ad influenzare il routing extra-aziendale
- In qualunque caso, sarebbe bene costituire dei tunnel criptati fra i vari apparati che regolamentano il routing dell'intranet aziendale

Sicurezza Interna/Esterna

- Tools interessanti:

  Ettercap

  (http://ettercap.sf.net)

  Ripper

  (http://www.spine-group.org/tools/ripper-1.4.tar.gz)

  Nast

  (http://nast.berlios.de)

Sicurezza Wireless

- La tecnologia wireless è sicuramente comoda, ma porta con se numerosi buchi di sicurezza...
- Se non criptato a dovere il traffico può essere comodamente sniffato dall'esterno
- Schemi di criptazione basati su WEP sono stati dimostrati assolutamente inefficienti
- Il controllo sul MAC address può aiutare, ma il MAC di una scheda si può cambiare
- WPA2 è tutt'ora lo schema di criptazione più sicuro sulla piazza

Sicurezza Sociale (1)

- L'anello più debole della catena è sempre l'uomo. Un comportamento poco attento di qualsiasi utente nell'intranet può compromettere i nostri sforzi per rendere l'infrastruttura sicura
- Sarebbe bene insegnare ai dipendenti alcuni piccoli accorgimenti per evitare spiacevoli sorprese
- Controllare **sempre** l'autenticità di qualsiasi tipo di messaggio; se questa non è verificabile e il messaggio ha contenuti potenzialmente dannosi, scartare il messaggio
- Autorizzare l'installazione di programmi con firma digitale solo se assolutamente sicuri della validità e credibilità della signing authority

Sicurezza Sociale (2)

- Anche per quanto riguarda telefonate, fax, lettere controllare sempre la loro validità, in quanto un attacker preparato utilizza tutti i metodi possibili per guadagnare informazioni
- Controllare anche ciò che si cestina, poichè c'e' una pratica molto comune, chiamata trashing che consiste nell'andare a rovistare nei documenti scartati dalle aziende per riuscire a scoprire informazioni
- Bisogna rimanere sempre attenti a ciò che si fa anche nel mondo fisico, non solo in quello virtuale

Sicurezza delle infrastrutture esterne (1)

- Non basta essere sicuri della propria porzione di rete per raggiungere un buon grado di sicurezza, bisogna anche controllare che le infrastrutture esterne su cui poggia la nostra rete siano sicure
- DNS e router BGP di frontiera possono essere dei punti deboli che un attaccante può compromettere per portare attacchi DDoS o MITM
- Vedremo come whois, traceroute e dig/host possano essere fidi alleati dei nostri nemici, ma anche utili tools per condurre penetration test

DNS (1)

- Un possibile attacco da portare ad un DNS consiste nello sporcare la sua cache e inserire coppie hostname/IP fasulle
- L'autenticità di una risposta DNS si basa semplicemente su un numero a 16 bit chiamato transaction ID
- Un tempo questo ID seguiva un andamento incrementale per ogni richiesta di risoluzione, mentre dal 1997 a questa parte è (per fortuna!!) casuale
- E' comunque possibile portare un attacco ai DNS per sporcare la loro cache con conseguente attacco MITM
- Conseguentemente verrebbe sporcata tutta la cache dei DNS non autoritativi per quella zona che interrogano il DNS

DNS (2)

- Fino allo scorso anno era possibile nei DNS BIND, sfruttando il così detto “Birthday Paradox”, riuscire con una probabilità del 100% a sporcare la cache inviando ~ 700 pacchetti spoofati
- Un altro aspetto a cui bisogna prestare attenzione è il così detto trasferimento di zona, che deve essere permesso solo ai DNS di backup

DNS (3)

```
bash-2.05b$ hostx -l mit.edu BITSY.mit.edu
[...]
MIT.EDU.                    A       18.7.22.69
W92-171-AP-1.MIT.EDU.       A       18.18.0.45
LEIFERICSSON.MIT.EDU.       A       18.33.1.133
BEYOND.MIT.EDU.             A       18.250.0.185
HERMANN-ONE-THIRTY-NINE.MIT.EDU.        A       18.171.5.139
BHANUM.MIT.EDU.             A       18.251.1.98
NORTHWEST-TWENTYTWO-SIX-SIXTY-THREE.MIT.EDU.    A       18.161.7.152
GOURETTE.MIT.EDU.           A       18.58.2.241
MAIN-TWELVE-FOUR-FIFTY-NINE.MIT.EDU.    A       18.19.6.204
NORTHEAST-FORTYSIX-SIX-EIGHTY-FIVE.MIT.EDU.     A       18.126.7.174
SIMMONS-SIX-O-SEVEN.MIT.EDU.    A       18.96.7.96
RANDOM-FIVE-FOURTY-NINE.MIT.EDU.        A       18.243.7.38
AA.MIT.EDU.                 A       18.250.1.207
NEXT-ONE-FORTY-FOUR.MIT.EDU.    A       18.242.5.144
MCCORMICK-THREE-SEVENTY-THREE.MIT.EDU.  A       18.240.6.118
AI.MIT.EDU.                 NS      MINTAKA.LCS.MIT.EDU.
MINTAKA.LCS.MIT.EDU.        A       18.26.0.36
AI.MIT.EDU.                 NS      OSSIPEE.LCS.MIT.EDU.
[...]
```

Router BGP (1)

- I router BGP di frontiera sono quei router che gestiscono il routing tra gli AS (Autonomous Systems)
- Esistono alcuni accorgimenti per renderli sicuri
- Se attaccati con successo possono portare alla variazione del routing verso un dato AS con possibilità di distribuzione delle rotte maligne per tutti i router di internet
- In alternativa è possibile un attacco DoS sfruttando le insicurezze del TCP

Router BGP (2)

- Attacchi al TCP

  DDos, Resource Saturation, RST Attack

- Attacchi a BGP

  Pacchetti malformati, Packet injection

- Attacchi a MD5

  Dictionary attack, brute force

- Attacchi alle configurazioni

  Acl troppo permissive

- Attacchi agli IGP

  Injectare rotte negli IGP per influenzare BGP

Router BGP (3)

- Testare la sicurezza dei router BGP del proprio AS è spesso una buona abitudine
- Dovrebbero filtrare qualsiasi pacchetto proveniente da sorgente sconosciuta
- Dovrebbero appoggiarsi a IGP **sicuri**
- Dovrebbero comunicare tra di loro attraverso tunnel criptati (IPSec)
- MD5 è tutto sommato una buona protezione

  Signature formata con un MD5 tra il TCP pseudo header, TCP data e una password **MAI** trasmessa on the wire
- S-BGP fornisce un OTTIMO grado di sicurezza

  PKI, attestations, IPSec (ESP)

Esempi BGP (4)

```
bash-2.05b$ whois -h whois.radb.net 80.180.0.0
route:          80.180.0.0/16
descr:          INTERBUSINESS
origin:         AS3269
notify:         network@cgi.interbusiness.it
[...]

bash-2.05b$ whois -h whois.radb.net AS3269
[...]
import:         from AS6762
+               action pref=100; accept ANY
import:         from AS6664
+               action pref=100; accept ANY
import:         from AS1913
+               action pref=100; accept AS1913
[...]
export:         to AS1913
+               announce ANY
export:         to AS2162
+               announce ANY
export:         to AS2164
```

Esempi BGP (5)

```
bash-2.05b$ whois -h whois.radb.net AS3327
aut-num:      AS3327
as-name:      DATATELECOM
descr:        Data Telecom Autonomous System
remarks:      ----------------------------------------
remarks:      Tallinn Internet Exchange (TIX-LAN)
remarks:      ----------------------------------------
remarks:      *** Uninet ***
import:       from AS2586  193.40.149.3    action pref=140; accept AS2586
export:       to   AS2586  193.40.149.3    announce AS3327
import:       from AS2586  193.40.149.132  action pref=140; accept AS2586
export:       to   AS2586  193.40.149.132  announce AS3327
remarks:      *** EENet ***
import:       from AS3221  193.40.149.18   action pref=140; accept AS3221
export:       to   AS3221  193.40.149.18   announce AS3327
remarks:      *** Estpak Data ***
import:       from AS3249  193.40.149.99   action pref=140; accept AS3249
export:       to   AS3249  193.40.149.99   announce AS3327
import:       from AS3249  193.40.149.136  action pref=140; accept AS3249
export:       to   AS3249  193.40.149.136  announce AS3327
```

Esempi BGP (6)

```
bash-2.05b# traceroute www.velug.it
traceroute to 195.78.200.2 (195.78.200.2), 30 hops max, 40 byte packets
[...]
10 host4-9.pool81118.interbusiness.it (81.118.9.4)
11 host194-48.pool81116.interbusiness.it (81.116.48.194)
12 host194-48.pool81116.interbusiness.it (81.116.48.194)
13 151.6.0.145 (151.6.0.145)
14 151.6.0.122
[...]
18 195.78.192.3
[...]
20  195.78.200.2 (195.78.200.2)

bash-2.05b# nmap -sS -p 179 151.6.0.145

Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-09-28 13:33 CEST
Interesting ports on 151.6.0.145:
PORT    STATE SERVICE
179/tcp open  bgp
```

BGP/DNS

- Alcuni papers / siti interessanti

  Insicurezze dei protocolli di routing dinamico
  http://www.spine-group.org/slides/secdate04.pdf
  http://www.spine-group.org/slides/secdate_html/index.html
  http://www.spine-group.org/slides/secdate04.sxi

  The Netlantis Project
  http://www.netlantis.org/

  DNS Cache Poisoning – The Next Generation
  http://www.securityfocus.com/guest/17905

Contatti e riferimenti

- La presentazione sarà disponibile sul sito dello S.P.I.N.E. Group

  http://www.spine-group.org

- Potete contattarci via mail
  - Marco Balduzzi <embyte@spine-group.org>
  - Michele Marchetto <mydecay@spine-group.org>

- Domande?