Fingerprinting

ed attacco ad un sistema informatico

"Ci sono più cose tra cielo e terra..."

Angelo Dell'Aera - Guido Bolognesi

Free Advertising

Name lookup

- Strumenti:

  nslookup, host, dig

- Risoluzione da nome host a indirizzo IP e viceversa
- Panoramica dell'obiettivo
- Reti con servizi esposti

Whois

- Whois sui domini e sulle reti
- Richieste rivolte alla tcp/43 ad un whois server
- ARIN, RIPE, APNIC
- Un client “intelligente” sceglie il server “giusto”

whois $dominio

- Data di creazione
- Data di “scadenza” :)
- Nameserver autoritativi

nic-handle

- Dipendente dal registrar, per un dominio
- registrant
- admin-c
- tech-c

nic-handle, registrar

- Proprietario del dominio
- Indirizzo, città, codice postale
- Telefono, fax
- Email

nic-handle, admin-c

- La “segretaria” per il dominio
- Indirizzo, città, codice postale
- Telefono, fax
- Email

nic-handle, tech-c

- Il "tecnico" per il dominio
- Indirizzo, città, codice postale
- Telefono, fax
- Email

whois $rete

- Provider a cui appartiene
- Dimensione
- A volte l’uso a cui è destinata

Nota di colore

- Ricordarsi l'Evil Bit!
- RFC 3514

  The Security Flag in the IPv4 Header
  (S. Bellovin, AT&T Labs Research, I April 2003)

- Nel momento in cui si genera traffico a scopi potenzialmente malvagi bisogna ricordarsi di attivarlo!

whois $rete

inetnum: 130.cc.xx.0 - 130.cc.yy.255

netname: CINECA-NON-GARR-NET

descr: CINECA-NON-GARR

country: IT

admin-c: ADF1-RIPE

tech-c: AA107

status: ASSIGNED PI

remarks: CINECA - Connettivita' Non Garr

mnt-by: CINECA-MNT

source: RIPE # Filtered

DNS

- Domain Name System / Service
- Directory distribuita
- Gerarchia organizzata
- I nomi simbolici ci servono!
- Ottimo strumento di information gathering

Query NS

- Name server autoritativi per il dominio

```
$ dig sikurezza.org NS

sikurezza.org.      2813    IN      NS      ns1.sikurezza.org.
sikurezza.org.      2813    IN      NS      ns2.sikurezza.org.

;;ADDITIONAL SECTION:
ns1.sikurezza.org.  78242   IN      A       130.186.88.33
ns2.sikurezza.org.  78242   IN      A       84.18.145.17
```

- Per quali altri dominii è autoritativo?

Query MX

- Server SMTP delegati alla gestione della posta del dominio

```
$ dig sikurezza.org MX

sikurezza.org.          86400   IN      MX      10 ns1.sikurezza.org.

sikurezza.org.          86400   IN      MX      20 ns2.sikurezza.org.
```

Query PTR

- Risoluzione di un indirizzo IP in un Fully Qualified Domain Name
- Enumerazione del ruolo degli host
- FQDN particolarmente significativo (es. vpn.domain.com, oracle.domain.com...)

```
$ dig 33.88.186.130.in-addr.arpa PTR

33.88.186.130.in-addr.arpa. 43200 IN    PTR     sikurezza.org.
```

Query A

- Risoluzione da FQDN in un indirizzo IPv4
- Enumerazione di host attivi senza PTR attivo risolvendo XXX.domain.com (con XXX preso da un dizionario)
- Da notare il TTL dei record (e zone)

Query AAAA

- Risoluzione di un FQDN in un IPv6 (se esiste)
- Enumerazione di host attivi

$ dig www.kame.net AAAA

www.kame.net. 86400 IN AAAA

2001:200:0:8002:203:47ff:fea5:3085

- Nota di colore: chi ha mai visto ACL su IPv6?

Query SRV

- RFC 2782 “per l’host HOST, per il servizio X con protocollo Y, chiedere il record _X._Y.HOST IN SRV”
- _ldap._tcp.dc._msdcs.esempio.it
- _sip._tcp.esempio.it (RFC 3263)

Query AXFR

- Utilizzata per trasferire i file di zona
- Solitamente utilizzata dai nameserver secondari
- Solitamente con ACL (ma a volte no)
- Di solito molto "rumorosa" viene segnalata dagli IDS come “attività sospetta”

Google? I feel lucky!

- Il motore di ricerca più utilizzato per efficacia nell'indicizzazione di contenuti e per performance
- Una miniera di informazioni a portata di mano di chiunque
- Ricerche molto specifiche e granulari grazie ad API molto ben pensate e quasi sconosciute alla massa degli utenti

Chi cerca trova...

- Usando le API è possibile reperire qualsiasi tipo di informazione su una rete target indicizzata più o meno incidentalmente
- Non è raro trovare file di configurazione, di servizi, di password o persino file dimenticati contenenti informazioni sensibili o addirittura numeri di carte di credito

Il passato che torna...

- Un file cancellato resta indicizzato da Google Cache a meno che non venga esplicitamente rimosso
- L'accesso a un contenuto indicizzato da Google Cache è assolutamente anonimo ed è quindi una tecnica molto stealth per fare information gathering
- Ricordate: non è pensato per questo (ACL)

Dimmi che database usi...

- ...e ti dirò chi sei
- Spesso molti sysadmin poco prudenti alle prese con dubbi di configurazione chiedono aiuto su mailing list inviando notizie dettagliate sulle tecnologie utilizzate
- Google Groups indicizza mail
- Una ricerca su Google Groups può fornire risultati piuttosto interessanti in maniera assolutamente anonima

SNMP

- Spesso (ab)usato per gli apparati di confine
- A volte accade che la community "public" sia un po' troppo pubblica
- Lista interfacce, contenuto delle acl e a volte configurazione completa...
- E se trovassi una community con accesso read-write al MIB?!

SMTP

- Banner grabbing: server, firewall (proxy applicativi)

```
220 nomehost.dominio.it ESMTP Sendmail 8.13.6/8.13.6;
    Wed, 1 Oct 2003 12:57:56 +0200 (CEST)
```

- Non esponete informazioni superflue!

SMTP

- Si può fare application fingerprint (amap, nmap -sV)
- Mandare mail informativa (o per i bounce)
- Software dei server e indirizzi interni
- Mandare mail in HTML con immagine di 1x1 a indirizzi validi (exit point, OS)

HTTP

- Ottenere i banner è la cosa più semplice

```
$ telnet server 80
GET / HTTP/1.0<enter><enter>
```

- L'ottimo Netcraft.com tiene addirittura lo storico...

Facile capire cosa gira?

- Server: Apache/2.0.59 (FreeBSD) DAV/2 SVN/1.3.2 mod_ssl/2.0.59 OpenSSL/0.9.8b
- Server: Microsoft-IIS/6.0
  X-Powered-By: ASP.NET
  X-AspNet-Version: 2.0.50727

Facile capire cosa gira?

- Server: Apache
- Server: Microsoft-IIS/6.1
  ETag: "3347c8-8a0-450ac792"
- Server: HTTPd-WASD/7.2.1
  OpenVMS/AXP SSL

HTTP: navigazione

- Tool per mappare un sito navigando (webscarab)
- Servizi di urlcount
- URI curiosi
- Altri dominii? (docs.dominio.com, images.altrodominio.it)

HTTP: navigazione

- I cookies! Di cosa si tiene traccia?
- robots.txt

  User-agent: *

  Disallow: /private-data # Progetti segreti!

- IDS/IPS? (cosa succede se richiedo /cmd.exe?)

HTTP: metodi

- Enumerazione del server HTTP utilizzato mediante il metodo HEAD
- Tecnologie dinamiche (HEAD)
- Funzionalità offerte dal server (OPTIONS)... e se offrisse la CONNECT?!
- Bilanciatori (clock skew)

HTTP: errori

- Enumerazione del server HTTP utilizzato mediante la generazione di errori
- Eventuali database di backend mediante query SQL sintatticamente invalide
- Funzionalità offerte dal server HTTP mediante la generazione di errori

Traceroute

- Consente di individuare informazioni relative al router del fornitore di connettività e sulla distanza dalla rete in termini di hop (utile per firewalking)
- Strumenti:

  traceroute/tcptraceroute

Traceroute

$ tcptraceroute www.sikurezza.org

[...]

9 81-208-106-226.ip.fastwebnet.it (81.208.106.226) 46.012 ms 44.104 ms 43.702 ms

10 gwnb-a.cineca.it (130.186.84.36) 46.482 ms 49.221 ms 46.592 ms

11 sikurezza.org (130.186.88.33) 46.103 ms 46.937 ms 49.390 ms

12 sikurezza.org (130.186.88.33) [open] 47.236 ms 47.042 ms 50.213 ms

Firewalking?

- Enumerazione delle ACL di un firewall ed eventualmente di host e servizi che protegge
- Si basa sul field TTL dell'header IP
- Strumenti:

  firewalk, hping2

IPSec?

- Individuare un concentratore VPN richiede tool appositi
- Un pacchetto UDP non fa primavera e spesso non viene neanche loggato...
- Strumenti:

  ike-scan

IPSec?

$ ike-scan -M XXX.XXX.XXX.XXX

Starting ike-scan 1.8 with 1 hosts (http://www.nta-monitor.com/ike-scan/)

XXX.XXX.XXX.XXX Main Mode Handshake returned

HDR=3D(CKY-R=3D39ac0d108dfd249c)

SA=3D(Enc=3D3DES Hash=3DSHA1 Group=3D2:modp1024 Auth=3DPSK
LifeType=Seconds LifeDuration=3D28800)

VID=3D4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

Ending ike-scan 1.8: 1 hosts scanned in 0.141 seconds (7.09 hosts/sec). 1 =

returned handshake; 0 returned notify

OS Fingerprinting

- Identificazione di un sistema operativo mediante differenze nell'implementazione dello stack TCP/IP
- Fingerprint attivo: effettuato mediante probing dell'host da analizzare (nmap)
- Fingerprint passivo: effettuato analizzando il traffico naturalmente generato dall'host nell'erogazione dei suoi servizi (paketto, p0f)

Food for mind

- Michal Zalewski

  "Silence on The Wire"

- W. Richard Stevens

  "TCP/IP Illustrated Volume 1: The Protocols"

Q&A

buffer@s0ftpj.org

guido@kill-9.it