



Segurança de Redes

FootPrint Levantando Informações

■ Tipos de Hackers

- hacker
- cracker
- ethical hacker
- white hat
- black hat
- gray hat

■ Fraquezas de segurança

- script kiddie
- hacktivismo
- vulnerabilidade
- Exploit / 0day
- Empregados mal preparados / descontentes
- Administradores imprudentes
- Espionagem industrial
- Wardriving

- Levantamento de informações
 - footprint
 - fingerprint
 - varreduras
- Explorações
 - força bruta
 - exploits
 - sql injection, etc.
- Elevação de privilégios
- Instalação de backdoor e ferramentas
- Obtendo as informações privilegiadas

- Levantamento de informações sobre o sistema “alvo”;
- É o início para se traçar uma estratégia de ataque;
- Sun Tzu (A arte da guerra)
 - "O que possibilita ao soberano inteligente e seu comandante conquistar o inimigo e realizar façanhas fora do comum é a previsão, conhecimento que só pode ser adquirido através de homens que estejam a par de toda movimentação do inimigo"

Por que garimpar informações ?

- Sistemas são feitos por pessoas, e cada pessoa é diferente (comportamento, humor, caráter, fidelidade, etc...)
- Os ataques são feitos contra uma organização e não contra um único equipamento
- Suas chances diminuem muito devido a medidas de segurança. (Exemplo: descobrir um 0day para explorar um WebServer)

■ Requisitos

- Gestão de pessoas
- Boa Memória
- Agradável
- Simpático

Comunicação

Pro Ativo

Persuasível

Postura de “Chefe”

■ Interações com as pessoas

- Reciprocidade
- Modelo a ser seguido

Amável

Herói

■ Meios

- Instante Messenger
- Forum
- Second Life
- E-Mail
- Cara-a-Cara

Lista de Emails / Grupos

Comunidades Virtuais

Telefone

Web

■ Métodos

- Pesquisas email/web
- Ouvidos atentos
- Escuta telefônica
- Happy Hour

“Passeios” pela empresa

Empregados externos

Sala do café

- Informações sobre a empresa
 - **Aquisições / Fusões recentes**
 - maturidade no nível de segurança diferentes
 - migrações / integrações de sistemas / infra
 - **Aquisições de novos equipamentos**
 - **WebSite**
 - muitas informações escondidas
 - Possui extranet?
 - **DNS lookup**
 - servidor de nomes
 - faixa de endereços
 - **Whois**
 - informações sobre o registro do domínio
 - **Blogs / Vagas de emprego / Forums / Orkut / secondlife**

Garimpando informações

- Webpage da empresa
- Histórico dos sites da empresa
 - <http://www.archive.org>

INTERNET ARCHIVE
WayBackMachine

Enter Web Address: All [Adv. Search](#) [Compare Archive Pages](#)

Searched for <http://www.uol.com.br> 2148 Results

Note some duplicates are not shown. [See all](#)
 * denotes when site was updated.
 Material typically becomes available here 6 months after collection. [See FAQ](#)

Search Results for Jan 01, 1996 - Sep 24, 2008												
1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
1 pages	4 pages	7 pages	22 pages	109 pages	460 pages	26 pages	63 pages	208 pages	541 pages	160 pages	358 pages	28 pages
Dec 23, 1996 *	Jun 07, 1997 *	May 17, 1998 *	Jan 16, 1999 *	Feb 29, 2000 *	Feb 28, 2001 *	Feb 20, 2002 *	Jan 28, 2003 *	Jan 15, 2004 *	Jan 01, 2005 *	Jan 01, 2006 *	Jan 01, 2007 *	Jan 01, 2008
	Jun 08, 1997	May 26, 1998	Jan 17, 1999	Feb 29, 2000	Mar 01, 2001	May 23, 2002	Jan 28, 2003	Jan 25, 2004	Jan 03, 2005	Jan 01, 2006	Jan 01, 2007	Jan 01, 2008
	Oct 08, 1997 *	Dec 01, 1998 *	Jan 25, 1999 *	Feb 29, 2000	Mar 03, 2001	May 27, 2002	Feb 01, 2003	Feb 12, 2004	Jan 04, 2005	Jan 03, 2006	Jan 02, 2007	Jan 04, 2008
	Oct 21, 1997	Dec 05, 1998	Feb 08, 1999	Mar 01, 2000	Mar 03, 2001	Jun 01, 2002	Feb 09, 2003	Mar 21, 2004	Jan 04, 2005	Jan 04, 2006	Jan 03, 2007	Jan 06, 2008
		Dec 06, 1998	Feb 09, 1999	Mar 01, 2000	Mar 03, 2001	Jun 03, 2002	Feb 10, 2003	Mar 23, 2004	Jan 05, 2005	Jan 04, 2006	Jan 04, 2007	Jan 07, 2008
		Dec 12, 1998	Feb 18, 1999	Mar 02, 2000	Mar 03, 2001	Jun 03, 2002	Feb 18, 2003	Mar 26, 2004	Jan 07, 2005	Jan 05, 2006	Jan 05, 2007	Jan 09, 2008
		Dec 12, 1998 *	Feb 20, 1999	Mar 02, 2000	Mar 04, 2001	Jul 20, 2002	Feb 19, 2003	Apr 04, 2004	Jan 08, 2005	Jan 05, 2006	Jan 05, 2007	Jan 09, 2008
			Apr 17, 1999	Mar 02, 2000	Mar 04, 2001	Aug 02, 2002	Mar 20, 2003	Apr 29, 2004	Jan 09, 2005	Jan 07, 2006	Jan 06, 2007	Jan 10, 2008
			Apr 23, 1999	Mar 02, 2000	Mar 05, 2001	Aug 07, 2002	Mar 20, 2003	May 10, 2004	Jan 11, 2005	Jan 08, 2006	Jan 07, 2007	Jan 11, 2008
			Apr 27, 1999	Mar 02, 2000	Mar 05, 2001	Aug 12, 2002	Mar 24, 2003	May 13, 2004	Jan 12, 2005	Jan 10, 2006	Jan 08, 2007	Jan 12, 2008
			Apr 27, 1999	Mar 03, 2000	Mar 06, 2001	Aug 19, 2002	Mar 27, 2003	May 19, 2004	Jan 14, 2005	Jan 10, 2006	Jan 09, 2007	Jan 13, 2008
			Apr 27, 1999	Mar 03, 2000	Mar 06, 2001	Aug 26, 2002	Mar 27, 2003	May 21, 2004	Jan 15, 2005	Jan 10, 2006	Jan 10, 2007	Jan 15, 2008
			Apr 30, 1999	Mar 03, 2000	Mar 07, 2001	Sep 02, 2002	Mar 28, 2003	May 23, 2004	Jan 15, 2005	Jan 11, 2006	Jan 10, 2007	Jan 15, 2008
			May 08, 1999	Mar 04, 2000	Mar 07, 2001	Sep 23, 2002	Mar 30, 2003	May 25, 2004	Jan 16, 2005	Jan 11, 2006	Jan 11, 2007	Jan 16, 2008
			Oct 02, 1999	Mar 06, 2000	Mar 07, 2001	Sep 28, 2002	Mar 31, 2003	May 27, 2004	Jan 17, 2005	Jan 12, 2006	Jan 13, 2007	Jan 17, 2008
			Oct 13, 1999	Apr 07, 2000	Mar 07, 2001	Sep 28, 2002	Apr 06, 2003	Jun 03, 2004	Jan 18, 2005	Jan 12, 2006	Jan 13, 2007	Jan 19, 2008
			Oct 13, 1999	Apr 07, 2000	Mar 07, 2001	Sep 30, 2002	Apr 19, 2003	Jun 06, 2004	Jan 19, 2005	Jan 12, 2006	Jan 14, 2007	Jan 20, 2008
			Oct 13, 1999	Apr 08, 2000	Mar 07, 2001	Sep 30, 2002	Apr 23, 2003	Jun 06, 2004	Jan 20, 2005	Jan 12, 2006	Jan 14, 2007	Jan 23, 2008
			Oct 13, 1999	Apr 15, 2000	Mar 07, 2001	Oct 22, 2002	Apr 23, 2003	Jun 07, 2004	Jan 20, 2005	Jan 13, 2006	Jan 15, 2007	Jan 25, 2008
			Oct 23, 1999	Apr 16, 2000	Apr 05, 2001	Nov 02, 2002	Apr 24, 2003	Jun 08, 2004	Jan 22, 2005	Jan 14, 2006	Jan 15, 2007	Jan 28, 2008
			Nov 18, 1999	Apr 18, 2000	Apr 17, 2001	Nov 21, 2002	Apr 25, 2003	Jun 09, 2004	Jan 23, 2005	Jan 15, 2006	Jan 16, 2007	Jan 29, 2008
			Nov 27, 1999	May 02, 2000	Apr 17, 2001	Nov 21, 2002	May 01, 2003	Jun 09, 2004	Jan 24, 2005	Jan 16, 2006	Jan 17, 2007	Feb 03, 2008
				May 10, 2000	Apr 21, 2001	Nov 21, 2002	May 23, 2003	Jun 09, 2004	Jan 25, 2005	Jan 17, 2006	Jan 18, 2007	Feb 04, 2008
				May 10, 2000	May 03, 2001	Nov 25, 2002	May 26, 2003	Jun 10, 2004	Jan 26, 2005	Jan 17, 2006	Jan 18, 2007	Feb 07, 2008
				May 10, 2000	May 03, 2001	Nov 29, 2002	Jun 03, 2003	Jun 10, 2004	Jan 27, 2005	Jan 18, 2006	Jan 19, 2007	Feb 08, 2008
				May 10, 2000	May 03, 2001	Nov 30, 2002	Jun 06, 2003	Jun 10, 2004	Jan 29, 2005	Jan 18, 2006	Jan 20, 2007	Feb 10, 2008
				May 10, 2000	May 03, 2001		Jun 08, 2003	Jun 10, 2004	Jan 30, 2005	Jan 18, 2006	Jan 20, 2007	Feb 11, 2008
				May 10, 2000	May 03, 2001		Jun 10, 2003	Jun 11, 2004	Feb 04, 2005	Jan 26, 2006	Jan 21, 2007	Feb 13, 2008
				May 10, 2000	May 04, 2001		Jun 10, 2003	Jun 11, 2004	Feb 04, 2005	Jan 26, 2006	Jan 21, 2007	
				May 10, 2000	May 04, 2001		Jun 10, 2003	Jun 12, 2004	Feb 05, 2005	Jan 27, 2006	Jan 22, 2007	
				May 11, 2000	May 04, 2001		Jun 11, 2003	Jun 12, 2004	Feb 05, 2005	Jan 27, 2006	Jan 24, 2007	
				May 11, 2000	May 04, 2001		Jun 12, 2003	Jun 14, 2004	Feb 06, 2005	Jan 27, 2006	Jan 24, 2007	
				May 11, 2000	May 05, 2001		Jun 23, 2003	Jun 14, 2004	Feb 06, 2005	Jan 27, 2006	Jan 25, 2007	

- <http://www.dogpile.com>
- Grupos de E-mail
 - <http://groups.google.com/> - pesquisar @alvo.com.br
- Sites
 - Tribunais (Ex: <http://www.tj.sp.gov.br>)
 - Telefônica
- Livros sobre investigações (investigador particular)
 - www.crimetime.com

- Google (<http://johnny.ihackstuff.com/ghdb.php>)
 - “@alvo.com.br”
 - Arquivos do excel em determinado site
 - `site:www.alvo.com.br filetype:xls`
 - `intitle:"extranet"`
 - Procurando arquivos do word
 - `intitle:"index of" -inurl:htm -inurl:html docx`
 - Estatísticas do site
 - `intitle:"Usage Statistics for" "Generated by Webalizer"`
 - VNC
 - `intitle:"vnc" inurl:5800`
 - Cópias de arquivos importantes
 - `filetype:bak inurl:"htaccess | passwd | shadow | htuser"`
 - Video server
 - `intitle:"live view" intitle:axis · intitle:axis intitle:"video server"`
- Yahoo
 - Sites que apontam para a empresa
 - `linkdomain:alvo.com.br -alvo.com.br`

- Câmeras

- `inurl:"/view/viewer_index.shtml"`

- Arquivo padrão texto que é colocado no site da empresa para “dizer” o que não deve ser indexado pelos mecanismos de busca
 - Google hacks
 - "robots.txt" "Disallow:" filetype:txt

```
User-agent: *  
Disallow: /WEB-INF/  
Disallow: /_private/  
Disallow: /_vti_bin/  
Disallow: /_vti_cnf/  
Disallow: /_vti_log/  
Disallow: /_vti_pvt/  
Disallow: /_vti_txt/  
Disallow: /cgi-bin/  
Disallow: /images/  
Disallow: /tmp/
```

- whois
 - whois alvo.com.br
- registro.br

```
domínio:          grvsoftware.com.br
entidade:         GRV Informática de Vinhedo LTDA ME
documento:        005.107.093/0001-71
responsável:      Gabriel Omizollo
ID entidade:      GAO38
ID admin:         GAO38
ID técnico:       HIS5
ID cobrança:      GAO38
servidor DNS:     ns1.locaweb.com.br
status DNS:       27/02/2008 AA
último AA:        27/02/2008
servidor DNS:     ns2.locaweb.com.br
status DNS:       27/02/2008 AA
último AA:        27/02/2008
servidor DNS:     ns3.locaweb.com.br
status DNS:       27/02/2008 AA
último AA:        27/02/2008
criado:           13/11/2002 #1013625
expiração:        13/11/2017
alterado:         30/01/2008
status:           publicado
```

```
ID:              GAO38
nome:            Gabriel Omizollo
e-mail:          omizollo@terra.com.br
criado:          12/11/2002
alterado:        03/01/2008
```

```
ID:              HIS5
nome:            Hostmaster HostNet Networks
e-mail:          registro@hostnet.com.br
criado:          14/12/1998
alterado:        03/09/2007
```

- ping
 - Verifica se o host responde a uma requisição ICMP
- traceroute / tracert
 - Mostra a rota até chegar no host destino
- On Line
 - <http://network-tools.com>
 - <http://visualroute.visualware.com/>
 - <http://ping.eu/>

- Domínios

- <http://whois.registro.br>
 - <http://whois.domaintools.com>
- <http://allwhois.org>

- Informações do que roda

- <http://netcraft.com>

- Tools

- <http://centralops.net/co>
 - <http://www.yougetsignal.com/>
 - (*) <https://hackertarget.com>
- <http://ping.eu/>
<http://network-tools.com>

- E-Mail

- <http://mxtoolbox.com>

- DNS

- (*) <http://dnsdumpster.com>

- Redes Sociais

- <http://keyhole.co/>

- “blackhat”

- (*) <http://www.shodanhq.com/>

- Não intrusivo
- Ex: www.netcraft.com
 - Whats that site running



The screenshot shows a web browser window with the address bar displaying <http://uptime.netcraft.com/up/graph?site=bolinhabolinha.com>. The browser's address bar also shows the Netcraft logo and a search bar. The browser's tab bar shows several tabs, including 'localhost:8000 / localhost | phpMyA...', 'Netcraft What's That Site Runnin...', and 'Site report for www.bolinhabolinha....'. The main content area of the browser shows the Netcraft website interface. At the top, it says 'New York Internet'. Below that, there is a search bar with the text 'Whats that site running?' and the input field containing 'bolinhabolinha.com'. A 'Search' button is next to the input field. Below the search bar, there is a table titled 'OS, Web Server and Hosting History for bolinhabolinha.com'. The table has five columns: 'OS', 'Server', 'Last changed', 'IP address', and 'Netblock Owner'. The table contains one row of data for 'Linux', 'Apache/2.2.11 (Unix) mod_auth_passthrough/2.1 FrontPage/5.0.2.2635 mod_perl/2.0.4 Perl/v5.8.8', '23-Mar-2009', '207.182.135.7', and 'eNET Inc.'. To the right of the table, there is a link to 'FAQ'.

http://uptime.netcraft.com/up/graph?site=bolinhabolinha.com

Últimas notícias OCOMON1.40 SpeedyZone

localhost:8000 / localhost | phpMyA... x Netcraft What's That Site Runnin... x Site report for www.bolinhabolinha.... x

New York Internet

Site Search

Whats that site running? bolinhabolinha.com Search

OS, Web Server and Hosting History for bolinhabolinha.com

<http://bolinhabolinha.com> was running Apache on Linux when last queried at 23-Mar-2009 12:57:20 GMT - refresh now Site Report
Try out the Netcraft Toolbar! [FAQ](#)

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache/2.2.11 (Unix) mod_auth_passthrough/2.1 FrontPage/5.0.2.2635 mod_perl/2.0.4 Perl/v5.8.8	23-Mar-2009	207.182.135.7	eNET Inc.

- **Olhando o cabeçalho**
- Logar via telnet no servidor
 - telnet pop3.servidor.com.br 110
- Autenticando
 - user nome_do_usuario
 - pass senha_do_usuario
- Comandos
 - Mostra a quantidade de mensagens e o espaço ocupado
 - stat
 - Mostrar lista das mensagens
 - list
 - Mostrar uma mensagem
 - retr numero_mensagem
 - Mostra o cabeçalho mais “n” linhas
 - top numero_mensagem numero_linhas
 - Marcar para deleção
 - dele numero_mensagem
 - Sair
 - quit

- Fazendo download do site inteiro
 - wget -r www.alvo.com.br

```

CA: Administrator: C:\Windows\system32\cmd.exe
C:\Users\Softpedia\Desktop>wget --help
GNU Wget 1.10.2, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -U, --version           display the version of Wget and exit.
  -h, --help             print this help.
  -b, --background       go to background after startup.
  -e, --execute=COMMAND  execute a '.wgetrc'-style command.

Logging and input file:
  -o, --output-file=FILE  log messages to FILE.
  -a, --append-output=FILE append messages to FILE.
  -d, --debug            print lots of debugging information.
  -q, --quiet            quiet (no output).
  -v, --verbose          be verbose (this is the default).
  -nv, --no-verbose      turn off verboseness, without being quiet.
  -i, --input-file=FILE  download URLs found in FILE.
  -F, --force-html       treat input file as HTML.
  -B, --base=URL         prepends URL to relative links in -F -i file.

Download:
  -t, --tries=NUMBER     set number of retries to NUMBER (0 unlimits).
                        retry even if connection is refused.
  -O, --output-document=FILE write documents to FILE.
  -nc, --no-clobber      skip downloads that would download to
                        existing files.
  -c, --continue         resume getting a partially-downloaded file.
  -P, --progress=TYPE    select progress gauge type.
  -N, --timestamping     don't re-retrieve files unless newer than
                        local.
  -S, --server-response  print server response.
  -spider                don't download anything.
  -T, --timeout=SECONDS  set all timeout values to SECONDS.
                        --dns-timeout=SECS  set the DNS lookup timeout to SECS.
                        --connect-timeout=SECS set the connect timeout to SECS.
                        --read-timeout=SECS  set the read timeout to SECS.
  -w, --wait=SECONDS     wait SECONDS between retrievals.
                        --waitretry=SECONDS wait 1..SECONDS between retries of a retrieval.
                        --random-wait       wait from 0..2*WAIT secs between retrievals.
  -Y, --proxy            explicitly turn on proxy.
  -nY, --no-proxy        explicitly turn off proxy.
  -Q, --quota=NUMBER     set retrieval quota to NUMBER.
                        --bind-address=ADDRESS bind to ADDRESS (hostname or IP) on local host.
                        --limit-rate=RATE   limit download rate to RATE.
                        --no-dns-cache      disable caching DNS lookups.
  
```

- Extrai metadados de arquivos em determinados sites
 - Google
 - Site:alvo.com filetype: pdf

```
root@bt:/pentest/enumeration/google/metagoofil# python metagoofil.py
```

```
*****  
*MetaGooFil Ver. 1.4a                *  
*Coded by Christian Martorella       *  
*Edge-Security Research              *  
*cmartorella@edge-security.com       *  
*****
```

```
MetaGooFil 1.4
```

```
usage: metagoofil options
```

```
-d: domain to search  
-f: filetype to download (all,pdf,doc,xls,ppt,odp,ods, etc)  
-l: limit of results to work with (default 100)  
-o: output file, html format.  
-t: target directory to download files.
```

```
Example: metagoofil.py -d microsoft.com -l 20 -f all -o micro.html -t mi  
cro-files
```

- Coletar informações do DNS
 - Tenta fazer transferência de zonas

```
root@bt:/pentest/enumeration/dnsenum# ./dnsenum.pl bolinhabolinha.com
dnsenum.pl VERSION:1.2


----- bolinhabolinha.com -----

-----
Host's addresses:
-----
bolinhabolinha.com. 10705 IN A 207.182.135.7

-----
Name servers:
-----
ns2.byethost15.org. 9956 IN A 207.182.135.8
ns1.byethost15.org. 9014 IN A 207.182.135.7

-----
MX record:
-----
bolinhabolinha.com. 10705 IN A 207.182.135.7

-----
Trying Zonetransfers:
-----
```



■ NMAP

- Host
 - `nmap 192.168.0.1`
- Rede
 - `nmap 192.168.0.1-100` (range)
 - `nmap 192.168.0.*` (caractere curinga)

■ Opções

- **-v** Verbose (Mais informações)
- **-O** ou **-A** (Detectar o Sistema Operacional)
- **-sP** (Verifica por ping)
- **-F** ou **-T5** (análise rápida)
- **-p porta** (analisa determinada portas – separar por vírgula ou range)
- **--top-ports n** (analisa as n portas mais comuns)
- **-sV** (tenta descobrir as versões dos programas/serviço daquela porta)
- **-D ip1,ip2,...** (Decoy, isca, finge se passar por outros IP's)
- **-oN** arquivo (cria um log da varredura)

- Em Grupo:
 - Levante as seguintes informações sobre a sua máquina. Quais comandos você utilizou:
 - Endereço IP
 - Máscara
 - Classe da Rede (A,B ou C)
 - Servidor de DNS
 - Servidor DHCP
 - Gateway
- Faça uma lista de 5 sites famosos e descubra qual sistema operacional está rodando neles.

Escolha um site e levante todas as informações que puder (Exemplo: SO,IP, registros, DNS, etc...) utilizando de técnicas não intrusivas.

- Site:
 - Informações apuradas e como foram conseguidas:
-
- Quais as formas de “tentar” minimizar o processo de obtenção de informações descritos nesta aula.

■ Livro texto

- THOMAS, Tom. **Segurança em Redes - Primeiros Passos**. 1.ed. São Paulo: Ciência Moderna, 2007.
- MAURO, Douglas R.. **SNMP Essencial**. 1.ed. São Paulo: CAMPUS, 2001.

■ Complementar

- NORTHCUTT, S.. **Desvendando Segurança em Redes**. 1.ed. São Paulo: CAMPUS, 2002, v.1.