Global Information Assurance Certification Paper

The Flat Footed Hacker

You have a firewall protecting your resources from the Internet. You operate a proxy server for your users to access the Internet without them having to directly touch the Internet. You are diligent with the latest system patches. Even through your efforts, are you still leaking too much information out to the bad guys?

Nowadays, most of the system compromises come from script kiddies 'who got lucky'. Your company may be hit with the latest worm/virus/exploit of the day, but was it really targeted at you? Probably not, but if a system cracker really wanted access to your company's assets, there is very little you can do to stop them, but you can make the job a little tougher. You are probably leaking information all over the Internet without your knowledge. Even though you run the latest Intrusion Detection systems and diligently log all data traversing to and from your location, an attacker can find out all sorts of key information about your company without even touching your resources.

When your company registered for a domain name, certain pieces of information were gathered:

Administrative Contact name/address/phone number/email address
Technical Contact name/address/phone number/email address
Billing Contact name/address/phone number/email address
DNS server names and IP addresses for the domain name
Record creation date
Record last modified date

How do we get this information? A utility included with most Unix systems, and available via web queries on the Internet is the WHOIS command. Taken from a WHOIS help file: *'WHOIS is a tool that is used to look up records in the Registrar database. Each record within the Registrar database has a "handle" (a unique identifier assigned to it), a name, a record type, and various other fields. The WHOIS service provides a means for searching on these specific fields. To use WHOIS for a domain search, simply type in the domain you are looking for. This domain must be a second-level domain, for example "example.com". Domains with a "www" or third-level domains like "my.example.com" are not contained within WHOIS. The default action for WHOIS is to only search for domain records, however you can do other types of searches by using specific keywords. If the domain you are searching for is not contained within the Registrar WHOIS database, WHOIS will access the Shared Registry System and the WHOIS services of other remote Registrars to satisfy the domain name search. The following description applies ONLY to the Registrar WHOIS service and NOT to either the Shared Registry System or any other Registrars.'*

In short, the WHOIS command allows you to lookup the registration information about a specific domain, but WHOIS goes beyond that. WHOIS allows you to find a domain name given a complete or partial company name, will identify key name servers for a given domain, and will also give up some email addresses.

In this exercise, we are trying to gather information about a potential target that provides computer security training programs. We know the company is named SANS, but we do not have their Internet address. We could try to type in http://www.sans.com, but it does not resolve to anything. We could try different combinations: sans.net, sans.org, sanstraining.com, etc., but that could take a lot of time, and if we do stumble upon the real location, our IP address is probably logged in the http access log file somewhere. There is an easier way, without ever touching the destination using the WHOIS NAME command:

 # whois "name *Sans*"@whois.networksolutions.com

Juan Segura Piera (SANS3-DOM)	SANS.NET
SANS Consulting Services, Inc. (SANS2-DOM)	SANS.COM
SANS Institute (GIAC5-DOM)	GIAC.ORG
SANS Institute (GIAC4-DOM)	GIAC.NET
SANS Institute (V19377-OR) alanpaller@aol.com	301-229-0777
SANS Institute (INTERNETSTORMCENTER-DOM)	INTERNETSTORMCENTER.ORG
SANS Institute (INTERNETSTORMCENTER2-DOM)	INTERNETSTORMCENTER.NET
SANS Institute (INTERNETSTORMCENTER3-DOM)	INTERNETSTORMCENTER.COM
The SANS Institute (SANS-DOM)	SANS.ORG

*Please note that the output from the WHOIS command is limited to the first 50 entries found.

Given this output, we can probably rule out the SANS.NET and SANS.COM entries, but the GIAC.*, INTERNETSTORMCENTER.* and SANS.ORG entries look interesting. Also notice the entry with the email address and phone number. I now wonder if these are all related to target that we are after. A few more WHOIS queries will determine that:

 # whois "domain sans.org"@whois.networksolutions.com

```
Registrant:
The SANS Institute (SANS-DOM)
   15235 Roller Coaster Rd.
   Colorado Springs, CO 80921
   US

   Domain Name: SANS.ORG

   Administrative Contact:
      Paller, Alan  (AP160)  alanpaller@AOL.COM
      Escal
      4610 Tournay Road
      Bethesda, MD 20816
      301-229-1062
   Technical Contact:
      Polk, Jeff  (JP232)  polk@DELOS.COM
      Delos Enterprises
      15235 Roller Coaster Rd.
      Colorado Springs, CO  80921
      US
      719-481-6541 719-481-6551
   Billing Contact:
      Paller, Marsha  (MP1458)  mmpaller@AOL.COM
      The SANS Institute
      4610 Tournay Road
      Bethesda, MD 20816
      301-951-0102

   Record last updated on 19-Jul-2000.
   Record expires on 05-Aug-2009.
   Record created on 04-Aug-1995.
   Database last updated on 17-Sep-2001 02:17:00 EDT.

   Domain servers in listed order:
```

SERVER1.SANS.ORG 167.216.133.33
NS.BSDI.COM 206.196.44.241
DELOS.COM 192.65.171.1

 # whois "domain internetstormcenter.org"@whois.networksolutions.com

Registrant:
SANS Institute (INTERNETSTORMCENTER-DOM)
5410 Westbard
Bethesda, MD 20816
US

Domain Name: INTERNETSTORMCENTER.ORG

Administrative Contact, Billing Contact:
SANS Institute (V19377-OR) alanpaller@aol.com
SANS Institute
5410 Westbard
Bethesda, MD 20816
US
301-229-0777
Technical Contact:
WorldNIC Name Host (HOST-ORG) namehost@WORLDNIC.COM
Network Solutions, Inc.
505 Huntmar Park Drive
Herndon, VA 20170-5142
1-888-642-9675

Record last updated on 02-May-2001.
Record expires on 02-May-2002.
Record created on 02-May-2001.
Database last updated on 17-Sep-2001 02:17:00 EDT.

Domain servers in listed order:

NS54.WORLDNIC.COM 216.168.225.194
NS53.WORLDNIC.COM 216.168.225.193

whois "domain giac.org"@whois.networksolutions.com
Registrant:
SANS Institute (GIAC5-DOM)
Suite 1501 5401 Westbard Ave.
Bethesda, MD 20816
US

Domain Name: GIAC.ORG

Administrative Contact:
Paller, Alan (AP160) alanpaller@AOL.COM
Escal
4610 Tournay Road
Bethesda, MD 20816
301-229-1062
Technical Contact:
Brenton, Chris (CB8949) cbrenton@SOVER.NET
Geek-Speak
7 Spring Rd
Tunbridge, VT 05077
802-889-3569
Billing Contact:
Paller, Marsha (MP1458) mmpaller@AOL.COM
The SANS Institute
4610 Tournay Road
Bethesda, MD 20816
301-951-0102

```
Record last updated on 20-Jun-2001.
Record expires on 29-Dec-2010.
Record created on 29-Dec-1999.
Database last updated on 17-Sep-2001 02:17:00 EDT.

Domain servers in listed order:

NS1.ALTENET.COM          12.33.246.130
MAIL.ALTENET.COM         12.33.246.131
```

It looks like Alan Paller is the administrative contact for each of these domains, and the addresses seem to point to Bethesda. MD. Look a little closer at the entry for the SANS.ORG listing and you will see the domain servers listed, in particularly the SERVER1.SANS.ORG listing. We may have found our target company: SANS.ORG. We wonder who is hosting the IP range for the SANS name server SERVER1.SANS.ORG?

```
# whois 167.216.133.33@whois.arin.net
whois.arin.net]
[No name] (SERVE34-HST)        SERVER1.SANS.ORG              167.216.133.33
Digital Island, Inc. (NETBLK-MIC-DIGISLE-A) MIC-DIGISLE-A
                                167.216.128.0 - 167.216.143.255
Manoa Innovation Center (NET-MIC) MIC          167.216.0.0 - 167.216.255.255
```

It looks like Digital Island, Inc controls the IP range that the SANS name server is using. In later exercises, we will see that there are a few others hosting the SANS domain as well.

By looking at these examples, we now have the names of a few people we could impersonate with social engineering attempts. Look at the WHOIS man page for additional flags that can be used to query the WHOIS databases, and try these lookups against your own company. You may be surprised as what information may be disclosed. There are a few ways to make the information returned less useful. First, log into the registrars database system (or send an update request) to change the contact information to a generic name (such as Billing Admin). Change the email address to either a generic mailbox within your domain, or better yet, a generic mailbox within another email domain not related to your company. If you company has a PO box, change the address to that PO box.

A whole other suite of information is also cataloged within the Internet news archives. A few creative searches on the various Internet search engines and financial news sites may produce a wealth of useful data to an information gatherer. Be wary of announcements about company financials and new products that are not yet public knowledge. One example would be the speculation of a takeover of another company. An attacker could use this knowledge to enumerate both your company and the 'partner' company, looking for any type of privileged connectivity options available between them to make the transition as smooth as possible (lax firewall rules, combining data centers, etc). Another good source for information gathering is the USENET archives at Google (http://groups.google.com). A search for email addresses in the '@sans.org' domain could bring up a wealth of information regarding hobbies of employees that could be the

source of a social engineering attempt, or actual infrastructure problem questions. It is very popular to post a question regarding product XYZ along with the configuration and often a network connectivity diagram to a newsgroup in hopes of someone assisting with a resolution. It is suggested to encourage employees to use a personal email account when posting to USENET, and administrators should follow the same practice, and take care not to indulge any information about their company or their architecture in these public forums. While on this topic, I would like to also stress that a lot of administrators fall victim to indulging too much information to vendors as well. In a recent bug report to a vendor on a firewall appliance, I was instructed to run a tech support utility that gathered the system configurations to be sent to technical support for analysis. Being curious and security minded, I extracted the archive file before sending it on and looked at the contents. In this archive were SNMP community strings, usernames with group memberships, IP routing tables, ARP cache entries, currently logged in users, listening processes and even the contents of the password and shadow password file! Needless to say, every file was inspected and either removed or altered to hide the crown jewels of the system before I forwarded the archive on. Every administrator should double-check the files for any proprietary information and passwords before sending them to a vendors tech support.

Getting a little 'Touchy-Feely'

Now that we have our target domain and have gathered email addresses from the USENET groups, we may want to start to touch the company's resources in a discretionary manner. First, one could try to get a listing of all the machines in the domain. If you are lucky, you will get an entire listing of all machines registered in the company's DNS servers, but most often, you will only get the machines visible to the Internet. This information can be gathered with the NSLOOKUP command:

```
# nslookup sans.org
Server:  localhost
Address:  127.0.0.1

Name:    sans.org
Address:  167.216.133.33
```

This gave us the IP address of SERVER1.SANS.ORG, which we already know. By running NSLOOKUP in interactive mode, we can get a lot more information:

```
#nslookup
> set type=any
> sans.org
Server:  fnsrv0.fnal.gov
Address:  131.225.8.120

Non-authoritative answer:
sans.org
        origin = sans.org
        mail addr = hostmaster.sans.org
        serial = 200108130
        refresh = 7200 (2H)
        retry   = 3600 (1H)
        expire  = 1728000 (2w6d)
        minimum ttl = 7200 (2H)
sans.org        nameserver = server1.sans.org
sans.org        nameserver = ns.BSDI.COM
```

```
sans.org        nameserver = ns.DELOS.COM
sans.org        internet address = 167.216.133.33

Authoritative answers can be found from:
sans.org        nameserver = server1.sans.org
sans.org        nameserver = ns.BSDI.COM
sans.org        nameserver = ns.DELOS.COM
server1.sans.org        internet address = 167.216.133.33
ns.BSDI.COM     internet address = 206.196.44.241
ns.DELOS.COM    internet address = 192.65.171.1
```

This NSLOOKUP query (with the 'set type=any' command) not only lists the authoritative name servers for the SANS.ORG domain, but also tells us when the DNS records were last updated and another email address (hostmaster.sans.org), but there is still more information to be had. This time, we will run the NSLOOKUP command directly against SERVER1.SANS.ORG name server:

```
#nslookup
> server 167.216.133.33
<TIMEOUT>
```

This host seems to be down. Lets try the next DNS server in the list:

```
#nslookup
> server 206.196.44.241
> set type=any
> sans.org
sans.org        internet address = 167.216.133.33
sans.org        preference = 10, mail exchanger = iceman.giac.ORG
sans.org        preference = 0, mail exchanger = server1.sans.org
sans.org        nameserver = server1.sans.org
sans.org        nameserver = ns.BSDI.COM
sans.org        nameserver = ns.DELOS.COM
sans.org
        origin = sans.org
        mail addr = hostmaster.sans.org
        serial = 200108130
        refresh = 7200 (2H)
        retry   = 3600 (1H)
        expire  = 1728000 (2w6d)
        minimum ttl = 7200 (2H)
sans.org        nameserver = server1.sans.org
sans.org        nameserver = ns.BSDI.COM
sans.org        nameserver = ns.DELOS.COM
iceman.giac.ORG internet address = 12.33.247.3
server1.sans.org        internet address = 167.216.133.33
ns.BSDI.COM     internet address = 206.196.44.241
ns.DELOS.COM    internet address = 192.65.171.1
```

We now have the IP address of the mail exchangers for SANS.ORG (iceman.giac.org, server1.sans.org). If the mail exchangers allowed, we could possibly make connections to the SMTP port and try to enumerate valid email addresses using the VRFY and EXPN commands. Any more information available?

```
> ls -d sans.org
[[206.196.44.241]]
$ORIGIN SANS.ORG.
@                       2H IN SOA       @ hostmaster (
                                        200108130       ; serial
                                        2H              ; refresh
```

```
                                1H              ; retry
                                2w6d            ; expiry
                                2H )            ; minimum

                        1H IN NS        server1
                        1H IN NS        ns.BSDI.COM.
                        1H IN NS        ns.DELOS.COM.
                        1H IN A         167.216.133.33
                        1H IN MX        10 iceman.giac.ORG.
                        1H IN MX        0 server1
server1                   1H IN A         167.216.133.33
registration              1H IN A         12.33.247.7
server2                   1H IN A         167.216.198.40
forum                     1H IN A         12.33.247.7
defiant                   1H IN A         208.255.174.6
localhost                 1H IN A         127.0.0.1
www                       1H IN CNAME     maverick.giac.ORG.
conference                  1H IN CNAME     intrepid
oldwww                    1H IN A         38.209.4.166
intrepid                  1H IN A         208.255.174.5
ftp                     1H IN A         167.216.133.33
@                       2H IN SOA       @ hostmaster (
                                200108130       ; serial
                                2H              ; refresh
                                1H              ; retry
                                2w6d            ; expiry
                                2H )            ; minimum
```

This looks like a DNS table. The **'ls –d sans.org'** command attempts to perform a zone transfer of the SANS.ORG domain (if allowed). In this case, the DNS server ns.BSDI.COM allows zone transfers. We now have a list of potential hosts to target our host enumeration (port scanning) upon. Unlike the previous enumeration attempts with WHOIS, this attempt is running queries against the actual servers hosting the SANS.ORG domain. While these queries are benign in nature, some alert administrators may take notice to zone transfers taking place and question your attempts. However, there are some ways to thwart this attempt as well. First, do not include comments or any other unneeded records in your external DNS servers (HINFO, TXT records). These record entries may give away more information about a host than you wish. Second, there are two ways to limit DNS zone transfers. Usually, the DNS server has some configuration settings to either disable all zone transfers, or limit zone transfers to specific hosts, such as secondary DNS servers. Also, since zone transfers utilize port 53/TCP (unlike normal DNS queries on 53/UDP), you may want to consider blocking 53/TCP at your firewall as well. Since 53/TCP is used legitimately in very long DNS response queries, blocking it at the firewall may have adverse effects to some users, so keep that in mind.

A dedicated system cracker determined to get into your company's assets usually does not do it on a whim. Many companies that have proprietary information stolen from their systems wonder how an attacker could easily gain specific knowledge about their systems in just a few minutes. In reality, the intruder may spend months gathering information about your company and identification of potential targets. They may try to impersonate an employee to a less-knowledgeable employee to get information such as accounts, passwords and computer architecture. Even something that seems innocent, such as a survey noting the number and types of firewalls installed, types on operating systems, etc), could lead a would-be attacker one step closer to their goal. You cannot stop them,

but you can make it that much more difficult.

Sources

Update/Change Domain Listing Information:
http://www.networksolutions.com

IP Address block allocation lookup:
http://www.arin.net

Online WHOIS search engines:
http://www.allwhois.com
http://www.network-tools.com
http://www.networksolutions.com/cgi-bin/whois/whois

Information about BIND – the Berkeley Internet Name Domain:
http://www.isc.org/products/BIND/
DNS and BIND, 4th Edition ,By Paul Albitz & Cricket Liu, O'Reilly Press, April 001

Securing BIND:
http://www.enteract.com/~robt/Docs/Articles/secure-bind-template.html
http://www.sans.org/infosecFAQ/DNS/sec_BIND.htm

Using NSLOOKUP:
http://uw7doc.sco.com/NET_tcpip/dnsC.nslook.html

Network Enumeration:
Hacking Exposed, by J.Scambray, S.McClure, G.Kurtz, McGraw-Hill Publishing