Part I - Gathering WHOIS Information

Exercise 1: **command-line WHOIS queries**: in the following exercise you will use a Linux system to perform WHOIS lookups from a command-line. This requires outbound TCP port 43 access.

As mentioned in the lecture discussion, ICANN is the authoritative registry for all top-level domains (TLDs) and is a great starting point for all manual WHOIS queries. NOTE: in practice, the Internet Assigned Numbers Authority (IANA) handles the day-to-day operations, which is located online at www.iana.org.

1. Start your BackTrack VM

2. Make sure you are connected to the Internet

3. Open a Linux shell

4. At the prompt, type the following (only type what's in **bold**):

user1@bt:~$ **whois net -h whois.iana.org | less**

Syntax breakdown:
whois: command name
net: search the .net TLD
-h whois.iana.org: connect to server whose hostname is whois.iana.org (which is the authoritative registry for all TLDs)
| less: send the output to the less paging program so you can view the results one page at a time. Use your up/down arrows to scroll text on the screen.

5. Who is the authoritative registry for .net? What is their WHOIS server domain name?

6. At the Linux prompt, type the following (only type what's in **bold**):

user1@bt:~$ **whois intermedia.net -h whois.verisign-grs.com | less**

Syntax breakdown:
whois: command name
intermedia.net: target domain you're interested in finding out registrar information on
-h whois.verisign-grs.com: connect to server whose hostname is VeriSign Global Registry Services (which is VeriSign's WHOIS server)
| less: send the output to the less paging program so you can view the results one page at a time

7. Who is the registrar for intermedia.net? What is the registrar's WHOIS server domain name?

8. Record the target organization's nameserver names and/or IP addresses:

9. At the Linux prompt, type the following (only type what's in **bold**):

user1@pentest:~$ **whois intermedia.net -h whois.godaddy.com | less**

10. Record the target organization's address (does this compare with the information you collected in Lab #4?):

11. Record the target organization's Administrative and Technical contact information:

Exercise 2: Domain-related WHOIS searches: in this exercise, you will use a web browser to perform a domain-related WHOIS lookup.

Because it has public information regarding Internet domain name registration services, the **InterNIC** (**www.internic.net**) is a great place to start for all domain-related searches. In addition, it provides web-based WHOIS lookups.

1. Open a web browser

2. Go to **www.internic.net**

3. Click Whois in the list of options available at the top of the page

4. In the Whois text box, enter **intermedia.net**. Make sure the Domain radio button is selected

5. Click the Submit button

6. How does this information compare with what you gathered in Exercise 1, steps #7-11?

7. Leave your browser open for the next exercise

Another web-based WHOIS engine resides at **ARIN** (**www.arin.net**). ARIN is the Regional Internet Registry (RIR) responsible for IP number resources in Canada, many Caribbean and North Atlantic islands, and the US. When trying to find IP-related information for a target organization, ARIN is an excellent place to start, even if the target organization is outside ARIN's internet numbers resource scope.

Exercise 3: IP-related WHOIS searches: in this exercise, you will use a web browser to perform an IP-related WHOIS lookup for the target domain.

1. From a web browser, go to **www.arin.net**

2. In the SEARCH WHOIS text box in the upper right-hand corner of the site, enter **intermedia.net**. Press Enter

3. What is the address block(s) assigned to the target organization?

4. Is the address listed the same as the one you collected in Lab #4? If not, record it here:

5. Leave your browser open for the next exercise

Exercise 4: IP-related WHOIS searches: in this exercise, you will use a web browser to perform an IP-related WHOIS lookup:

The following process can be used to trace back any IP address in the world to its owner, or at least a point of contact. It can also be used to find out IP ranges and Border Gateway Protocol (BGP) autonomous system (AS) numbers that an organization "owns" by searching the RIR WHOIS servers for the organization's literal name.

1. From a web browser, go to **www.arin.net**

2. In the SEARCH WHOIS text box in the upper right-hand corner of the site, enter the following IP address: **61.0.0.2**. Press Enter

3. Who is managing this IP address?

4. In your web browser, go to **www.apnic.net** (which happens to be the RIR that manages the 61.0.0.2 address) and type in the **61.0.0.2** address in the WHOIS Search text box

5. Who is managing this IP address?

Part II - Manual DNS Zone Transfers

The name *nslookup* means **name server lookup**. Nslookup is a command-line administrative tool for testing and troubleshooting DNS servers. On most OSes, the tool is installed along with the TCP/IP protocol stack.

You can also use Nslookup from a *NIX machine, but the *ls* command is not supported. In that case, you can use the dig or host commands. In the following exercise, you will use the latter.

Exercise 1: using Dig to perform a zone transfer from a misconfigured DNS server: in this exercise, you will use the Dig utility in BackTrack to pull a copy of the misconfigured DNS server's *forward* zone file:

1. From your backtrack VM, open a shell (only type what's in **bold**):

user1@bt:~#**cd /root/ceh**
user1@bt:~#**pwd**
/root/ceh

Syntax breakdown:
cd /root/ceh: change into the directory called /root/ceh
pwd: program name to print current directory

2. From your shell type (only type what's in **bold**, on one line):

user1@bt:~#**dig @ns4.intermedia.net intermedia.net AXFR > /root/ceh/dns_enum1**

Syntax breakdown:
dig: program name
@ns4.intermedia.net: the nameserver to query (which you determined via WHOIS queries)
intermedia.net: the target domain
AXFR: perform a full zone transfer (transferring all records)
> /root/ceh/dns_enum1: redirect the output to a file called dns_enum1 in the /root/ceh directory

3. Because the DNS server is misconfigured to allow any host to request a copy of its zone file, you should see the entire contents of the forward zone file; that is, all name-to-IP mappings, any mail servers (MX records), who the name servers are for the domain (NS records), etc.

3. Examine your results:

user1@bt:~#**cat /root/ceh/dns_enum1 | less**

Exercise 2: using Dig to perform a zone transfer from a misconfigured DNS server: in this exercise, you will use the Dig utility in BackTrack to pull a copy of the misconfigured DNS server's *reverse* zone file:

1. To get a copy of the reverse lookup file type (only type what's in **bold**, on one line):

user1@bt:~#**dig @ns4.intermedia.net intermedia.net AXFR 22.78.64.in-addr.arpa > /root/ceh/dns_enum2**

Syntax breakdown:
dig: program name
@ns4.intermedia.net: the nameserver to query
interedia.net: the domain to query records for
AXFR 22.78.64.in-addr.arpa: perform a full zone transfer (transferring all records) of the reverse address space

> /root/ceh/dns_enum2: redirect the output to a file called dns_enum2 in the /root/ceh directory

2. Examine your results:

user1@bt:~#**cat /root/ceh/dns_enum2 | less**

Part III - Network Reconnaissance

Exercise 1: using tracert from a Windows system: in this exercise, you will use the tracert program in Windows to identify any of the target organization's perimeter devices:

1. From your Windows XP system, open a command shell and type the following (only type what's in **bold**):

C:\>**tracert www.intermedia.net**

Syntax breakdown:
tracert: program name
intermedia.net: the target domain

2. Examine the results

3. Identify potential entry points into the target organization here:

http://network-tools.com/

Part IV - Network Ping Sweeps Using nmap

Nmap ("Network Mapper") is a free and open source utility for network exploration and/or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and both console and graphical

versions are available.

Although nmap is discussed in more detail later in this chapter, it is worth noting that it does offer ping sweep capabilities with the -sP option:

Exercise 1:

1. From a BackTrack shell, type the following (only type what's in **bold**):

   user1@bt:~# **nmap -sP -v class_IP_range/24 | grep up > /root/ceh/ps1**

   Syntax breakdown:
   nmap: program name
   -sP: program option for ping sweep
   -v: verbose mode
   class_IP_range/24: network block to scan (e.g., 10.10.10.0/24)
   | grep up: show just the target systems that are “alive”
   > /root/ceh/ps1: redirect the output to a file called ps1 in the /root/ceh directory

2. Examine your results:

   user1@bt:~#**cat /root/ceh/ps1 | less**

3. Record the “alive” systems: