3 Information Gathering

Lab Scenario

As a Pen Tester, you have proven yourself to management and they trust you with more tasks. During this engagement, you will be performing the second part in Recon – Port Scanning. This is a vital aspect, just like all others, and you will need to verify all the results with more than one tool. You are performing a Pen Test on an internal network and all proper documentation and approvals have been taken care of by your team leader.

Lab Objectives

1. Port scanning the target network with the following tools:
    a. NMAP – Command line and Front End Gui (Linux and Windows)
    b. Hping3
    c. Look@LAN
2. Prioritize the attack targets from least secure to most secure and record your results.
3. Learn how to create a grepable file with NMAP.
4. Learn how to search the grepable file with basic Linux commands.
5. Learn how to use Unicornscan.
6. Document every task you perform in such a way that a thorough report can be compiled.

Lab Resources

1. Look@lan
2. Zenmap
3. Hping3
4. Nmap

Lab Tasks Overview

1. Use Firefox with security extensions.
2. Use online tools to gather information.
3. Use nslookup.
    a. View MX records for a domain.
4. Use Google queries to gather information.
5. Run nmap from the command line.
    a. Create grepable output with NMAP.
6. Perform collection and analysis with Maltego.
7. Use Look@Lan to scan your network.

8. Use Zenmap (nmapfe) to scan your network.
9. Use Hping3 to scan a target:
    a. half-open SYN scan
    b. UDP scan and FIN scan

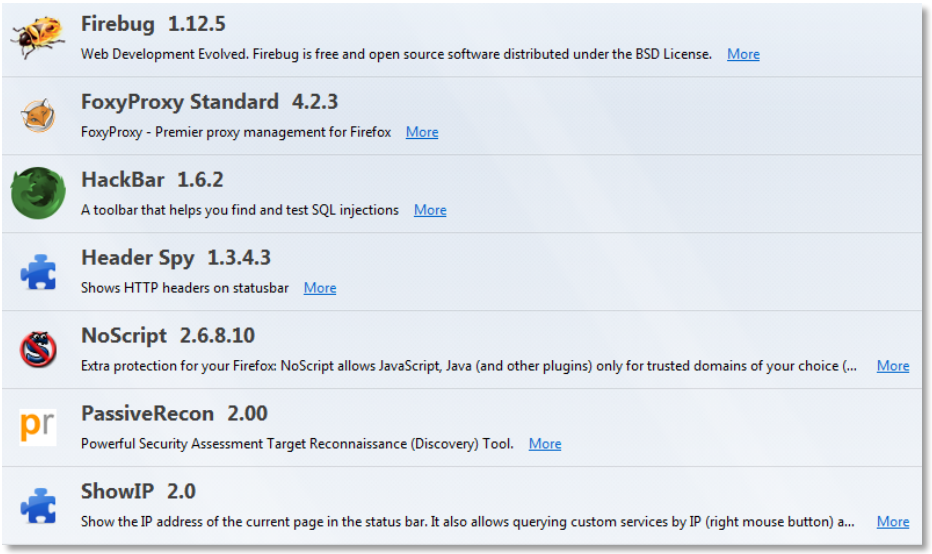
Lab Details - Step-by-Step Instructions

3.1 Passive Reconnaissance

1. On your Windows 7 VM, open Firefox and check out the installed extensions. Each time you open a web page, there is important information that you don't normally have access to. Click on the "More" link for each Firefox extension to see how it might be useful during a Pen Test.

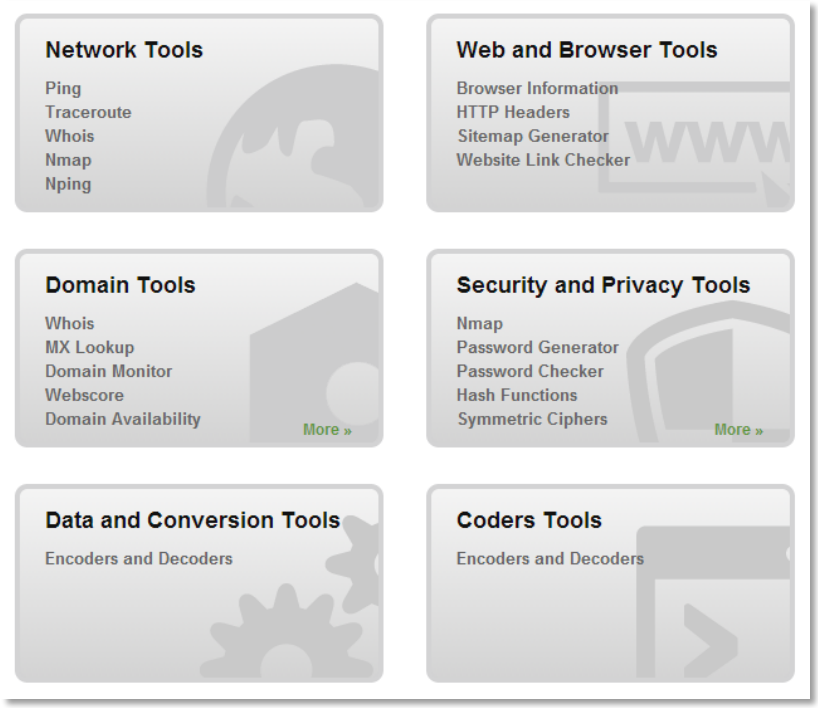
    Tools/Add-ons

    Note: If there are any missing add-ons, simply do a Google search to download the add-ons. At some point after looking at the add-ons, disable the Hackbar toolbar.



2. During a Pen Test, you'll need to use several online tools to gather information on your targets. From your base computer or the Kali Linux VM, browse to http://online-domain-tools.com to see some of the free tools available.

http://online-domain-tools.com/



3. Using Nslookup – A command line tool installed on the Kali Linux VM

   a. At a command prompt, type nslookup.

   b. You are now in nslookup interactive mode, and so there will be a “>” prompt.

```
root@kali:~# nslookup
> 
```

   c. Often, you will have a timeout issue since the default for nslookup is 2 seconds. Change the timeout by typing set timeout=10 – this will give you a 10 second timeout.
   Note: There cannot be spaces on either side of the equal sign.

```
root@kali:~# nslookup
> set timeout=10
> 
```

   d. Use nslookup to query for the host records of a domain. To do this, type in a domain name (FQDN) and press Enter. The results of your queries should be the associated host IP address. Try several queries.

```
root@kali:~# nslookup
> set timeout=10
> google.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 65.196.188.55
Name:   google.com
Address: 65.196.188.53
Name:   google.com
Address: 65.196.188.59
```

   e. You will now query the DNS server for Mail Exchanger (MX) records, which list who the SMTP servers are for a particular domain. To do this type:
   set type=MX

```
> set type=MX
> 
```

f. Now enter a domain name. You should receive a reply indicating that domain's mail

```
> set type=MX
> box.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
box.com mail exchanger = 20 ALT1.ASPMX.L.GOOGLE.com.
box.com mail exchanger = 30 ASPMX2.GOOGLEMAIL.com.
box.com mail exchanger = 10 ASPMX.L.GOOGLE.com.
box.com mail exchanger = 30 ASPMX3.GOOGLEMAIL.com.
box.com mail exchanger = 20 ALT2.ASPMX.L.GOOGLE.com.

Authoritative answers can be found from:
ASPMX2.GOOGLEMAIL.com   internet address = 74.125.24.26
ASPMX2.GOOGLEMAIL.com   has AAAA address 2a00:1450:400b:c02::1b
ASPMX.L.GOOGLE.com      internet address = 74.125.141.27
ALT1.ASPMX.L.GOOGLE.com internet address = 74.125.24.26
ALT1.ASPMX.L.GOOGLE.com has AAAA address 2a00:1450:400b:c02::1b
```

g. Type: set type=ANY

h. Now enter a FQDN. You should receive a reply including most of the zone file data.

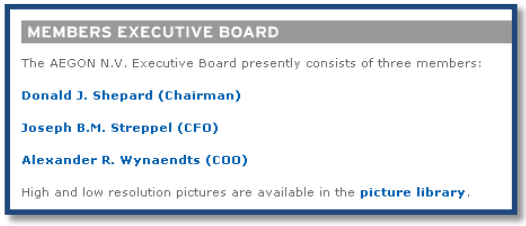
i. Type exit when finished with nslookup.

3.2 Google Queries

This is to be done on your Kali Linux VM or Base System.

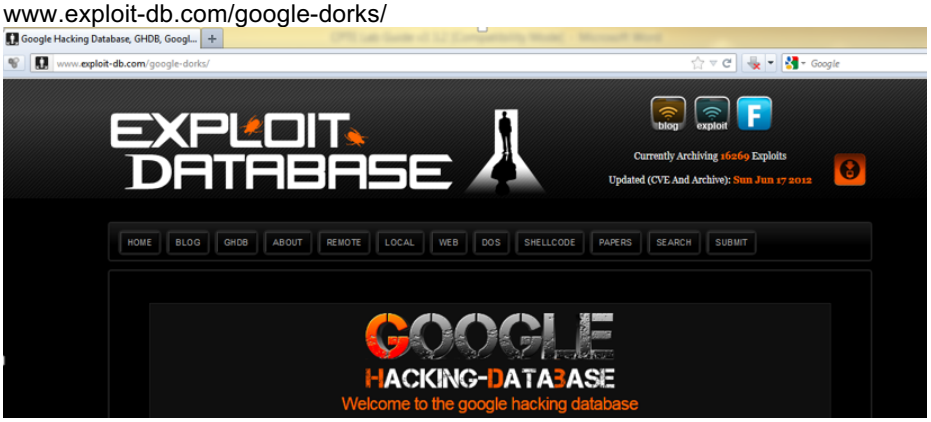
1. Gather the information from Aegon, using the Internet. Aegon - www.aegon.com
   a. Refer to the CPEH student workbook for examples of information that a hacker would look for.
   b. Information gathered will ideally include:
      i. Members of the Executive Board of AEGON N.V. and AEGON USA.
      ii. Educational Background of the Executive Members Board and contact information.
      iii. Name of the Chairman's Wife.
      iv. Find out the office location, telephone and name of the CEO.

Picture is an example only!



Note: Google.com is undoubtedly the most popular search engine in the world. It offers multiple search features like the ability to search images and news groups. However, its true power lies in its powerful commands that can be used and misused.

2. We are now going to learn how to use some of the advanced Google queries. www.exploit-db.com/google-dorks/



Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Some operators can only be used to search specific areas of Google, as these columns show.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

3. Practice utilizing the following Google Queries.
    a. The "allinurl" command is used to search for a particular string present in the URL.
        i. Go to google.com and type this in the search box:
            1. allinurl:Mile2
            2. allinurl:passwd.txt
                a. The command searched for a file called passwd.txt present in the URL on the virtual.net site.
    b. You can also search particular top level domains like .net /.org /.np /.jp /.in /.gr etc.
        i. Go to google.com and type this in the search box:
            1. allinurl:config.txt site:jp
            2. allinurl:admin.txt site:edu
4. We are now going to practice searching for Index browsing enabled directories. This is a very simple but powerful way of gaining information. First of all, we need to understand that "index browsing" enabled directories are those directories on the Internet that can be browsed just like ordinary directories. We will be using Google to find such types of "interesting" directories.
        i. Go to google.com and type this in the search box:
            1. "Index of /admin"
            2. "Index of /secret"
            3. "Index of /cgi-bin" site:.edu
                a. (Try With& without the period for edu)

Note: You can begin to think outside the box and be creative and think of other interesting ways to exploit index browsing.

5. Now we are going to practice searching for particular file types. You can specify the extension of the filename you want to search for using the "filetype" command.
        i. Go to google.com and type this in the search box:
            1. filetype:pdf site:com contactlist
            2. filetype:doc site:mil classified
6. This document is only meant to give some basic ideas about exploiting google.com.
    a. This site is also very helpful.
        i. http://searchlore.org

7. Here are examples of Google advanced searches.
    a. Web Servers Default Installation for servers with default installation:
        i. Apache Queries
            1. “It Worked!"
            2. “Test Page for Apache Installation on Web Site”
        ii. Passwords Files Disclosure Queries
            1. inurl:password.txt
            2. allinurl:passwd.txt site: website name
        iii. Bulletin Board System Password File DisclosureQuery
            1. allinurl:/wwwboard/passwd.txt
        iv. HTTP Credentials Disclosure Query
            1. http://admin:*@www
        v. Sensitive Files Access Query
            1. Query: allinurl:/.bash_history
        vi. Sensitive Directories Access Queries
            1. "index of /members" + "Parent Directory"
            2. "index of /private" + "Parent Directory"
        vii. Microsoft Outlook Web Access Anonymous LogonQuery
            1. inurl:exchange/root.asp?acs=anon
        viii. Confidential Information’s Leak Queries
            1. "Do not distribute"
            2. "Internal use only" filetype:pdf
        ix. Proxy and Terminal (RDP) servers Queries
            1. inurl:8080
            2. inurl:tsweb site:edu
8. Later, we will look at further automating this with scripting.

3.3 Active Reconnaissance

This is to be done on your Kali Linux VM Image. (Linux Attack v2 is the Kali system)

1. Run NMAP from a command line and test different options.
    a. Open a bash shell and run the different commands against one of your Windows VMs.
        i. Ping sweep
            1. nmap -sP <target>
        ii. Full TCP Connect scan
            1. *nmap -sT <target>*
        iii. Half-open SYN scna
            1. *nmap -sS <target>*
        iv. Service Version
            1. *nmap -sV <target>*
        v. OS Detection
            1. *nmap -O<target>*
        vi. UDP scan
            1. *nmap -sU<target>*
        vii. Build your own scan utilizing timing options and fragmented packets.
            1. Here is an example
                a. nmap -sV -sS -P0 -f -T 2 <target>
    b. For the following scans, you will need to attack a UNIX box that has been setup by your instructor. Please record the IP address of the UNIX box here.
            1. _____
        ii. FIN scan(use against a Unix machine)
            1. nmap -sF <target>
        iii. Xmas scan(use against a Unix machine)
            1. nmap -sX <target>
        iv. Null scan(use against a Unix machine)
            1. nmap -sN <target>

            If necessary, use the following command to obtain dynamic ip address on Linux.

            sudo dhclient

Hint: In many Pen Tests, the professionals forget to add the -P0 to the command and then wonder why there are few machines up and running. Please remember, in the real world, you will need the -P0 on most occasions.

2. INTERMEDIATE LAB - With NMAP create a grepable file with the output.

So what is a grepable file? Here is a quote directly from Insecure.org
http://nmap.org/book/man-output.html
-oG <filespec> (grepable output)

This output format is covered last because it is deprecated. The XML output format is far more powerful and is nearly as convenient for experienced users. XML is a standard for which dozens of excellent parsers are available, while grepable output is my own simple hack. XML is extensible to support new Nmap features as they are released, while I often must omit those features from grepable output for lack of a place to put them.

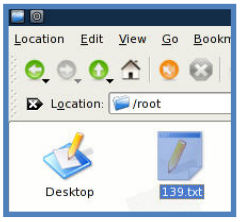
Nevertheless, grepable output is still quite popular. It is a simple format that lists each host on one line and can be trivially searched and parsed with standard Unix tools such as grep, awk, cut, sed, diff, and Perl. I usually use it for one-off tests done at the command line. Finding all the hosts with the SSH port open or that are running, Solaris takes only a simple grep to identify the hosts, piped to an awk or cut command to print the desired fields.

Grepable output consists of comments (lines starting with a pound (#)) and target lines. A target line includes a combination of 6 labeled fields, separated by tabs and followed with a colon. The fields are Host, Ports, Protocols, Ignored State, OS, Seq Index, IP ID, and Status.

The most important of these fields is generally Ports, which gives details on each interesting port. It is a comma separated list of port entries. Each port entry represents one interesting port, and takes the form of seven slash (/) separated subfields. Those subfields are: Port number, State, Protocol, Owner, Service, SunRPC info, and Version info.

As with XML output, this main page does not allow for documenting the entire format. A more detailed look at the Nmap grepable output format is available in the section called “Grepable Output (-oG)”.http://nmap.org/book/output-formats-grepable-output.html

Now, let's move on to the action!



a. Open a shell.

b. Use nmap and scan your target using the following command

   i. Type: nmap -sV -v -p 139 <target> -oG 139.txt

   ii. The target should be your VM network (192.168.1.0/24).

   iii. You are scanning your target on port 139 and outputting the results to a grepable file called 139.txt. The file will be saved in the home folder /root.

c. When that is finished:

   i. Type: cat 139.txt

   ii. This is simply going to display the file.

d. Now let's extract or cut an item out of the file.

   i. Type: grep open 139.txt | cut -d" " -f2

e. What does this show us? As seen below, it lists the IP address that nmap have TCP port 139 open. Using the cut command properly with one or more files can really make things easier for you when looking for something specific. As an example, let's say you just completed an nmap scan of 100 hosts. You can now pipe the IP addresses into another command for further processing.

3.4 Collection and Analysis with Maltego (Optional)

This is to be done on your Kali Linux VM.

1. Start Maltego using: Applications > Kali Linux > Top 10 Security Tools > Maltego

   a. This is the community edition, so you will have to register to use it. Click on the register here hyperlink if you have not already registered.

      a. You will need to provide a valid e-mail account that you can access.

      b. After registering, check you e-mail for an account activation message. Follow its instructions.

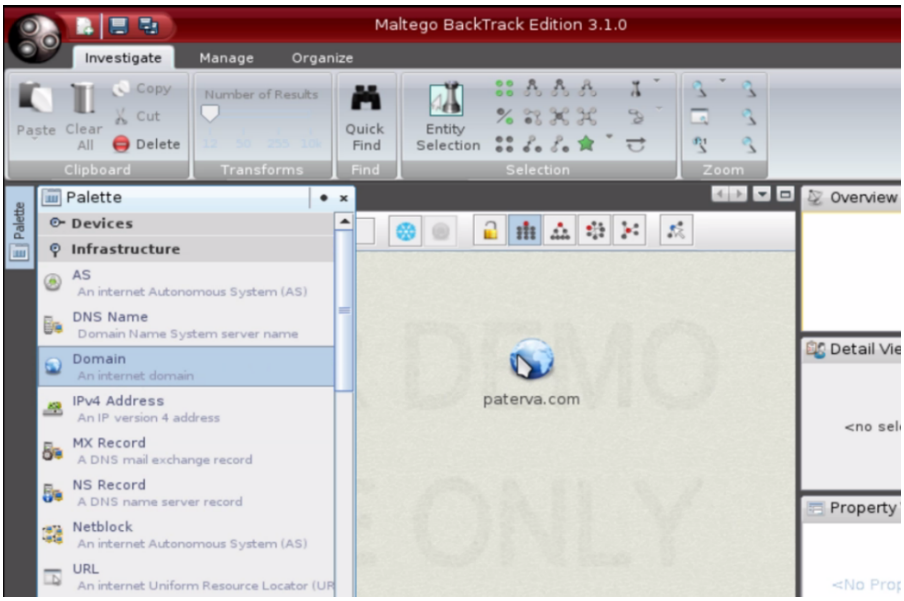
      c. Once you have a valid active Maltego account, provide those credentials to the Maltego tool.

      d. Next, select Open a blank graph and let me play around, then click Finish.

      e. NOTE: Maltego is constantly being updated, so some of its menu items may have changed since this lab was written. If you cannot determine what command to issue, ask the instructor.

If Pallette disappears, select from the menu, Manage/Windows selecting the *Green check mark(Pallette)* to enable. If this does not solve issue, look in the upper left corner of the screen and select Create New Graph.

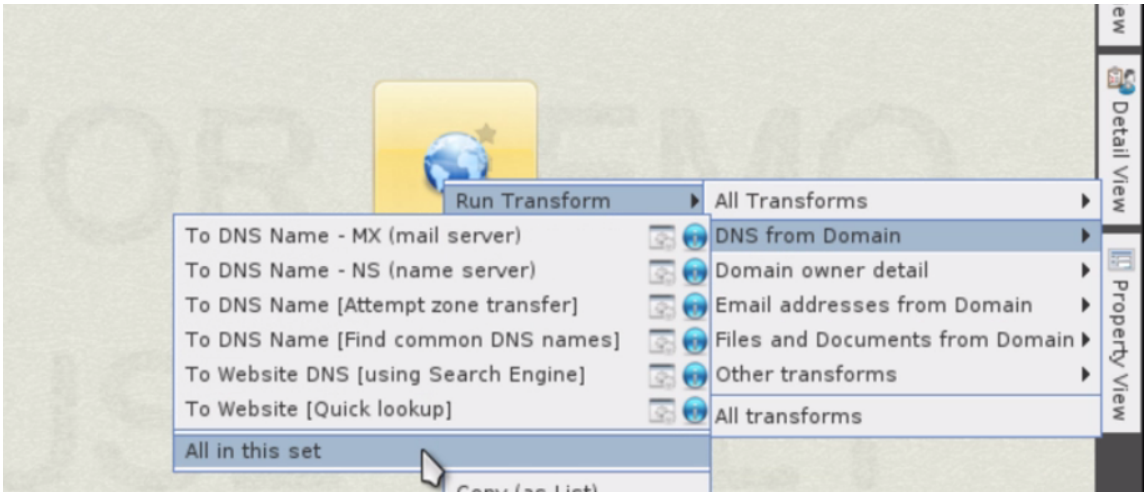
2. Left-click and hold on Domain and drag it to the work area.
   This picture is an example only!



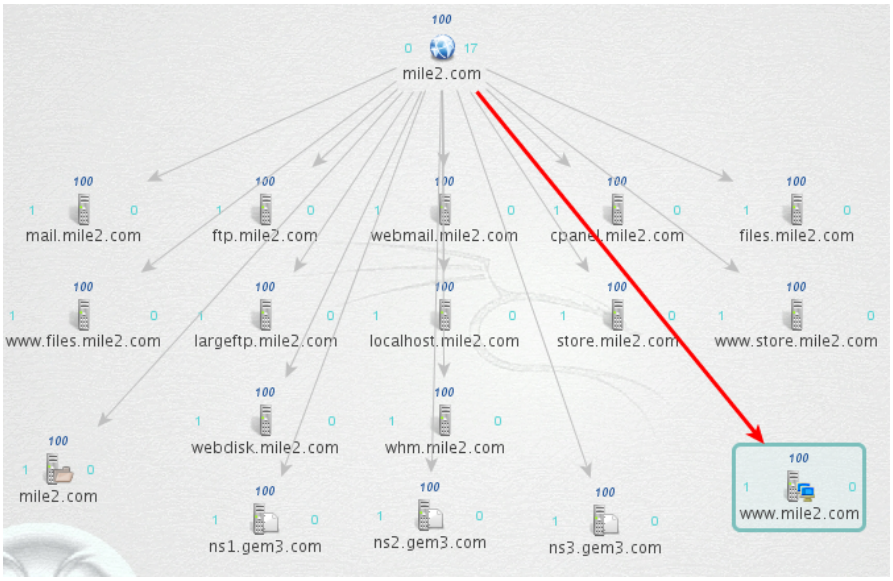
3. Double-click paterva.com and enter a domain of your choice.

4. Let's make use of a few Transforms.

   a. Right-click on the domain and choose: RunTransform → DNS from Domain→ All in this set.
      This picture is an example only!

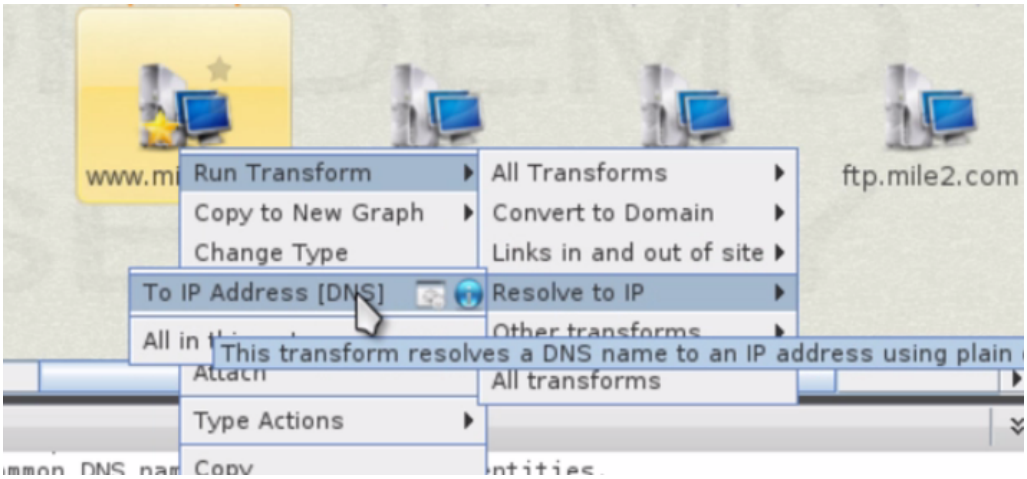


b. You will need to wait for the transform to finish.

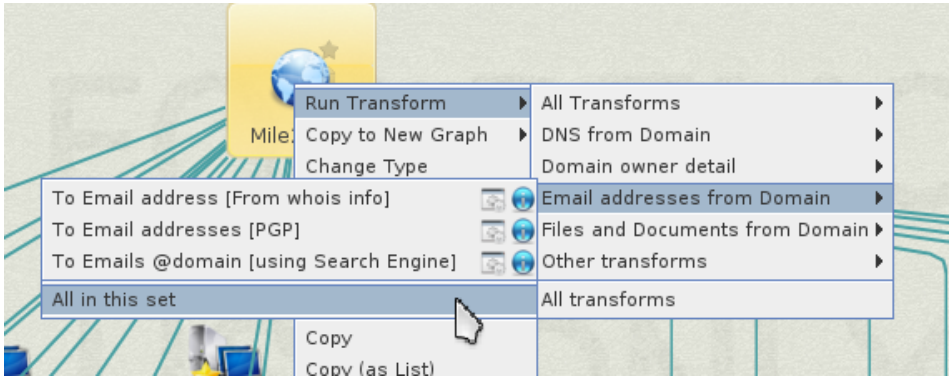


This picture is an example only!

c. Right-click on one of the DNS Names and choose: ResolveToIP → To IP Address.
This picture is an example only!



d. Now see if you can find email addresses by right-clicking on the Domain and choosing: Run Transform ->Email Addresses from Domain → All in this set



This picture is an example only!

This picture is an example only!

5. See what else you can discover with Maltego on your own.

    a. Netblocks, Links to the website from other locations and many other transforms.

3.5 Look@LAN

This is to be done on your Windows 7 Victim.

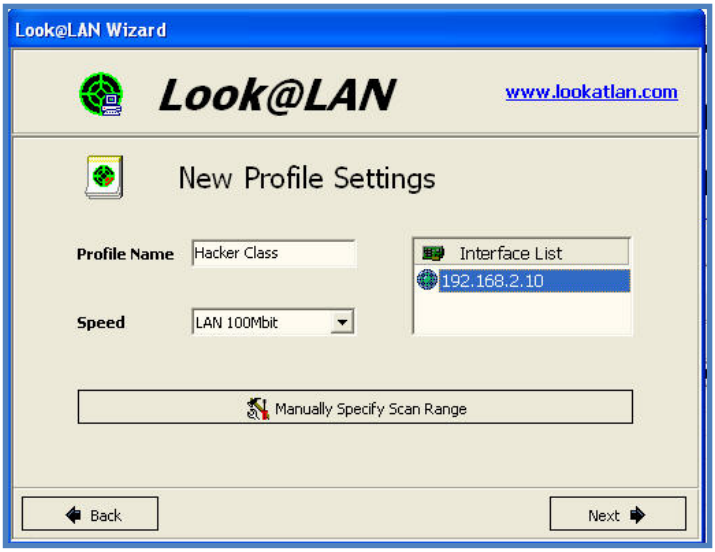
1. Run Look@LAN and record the results.

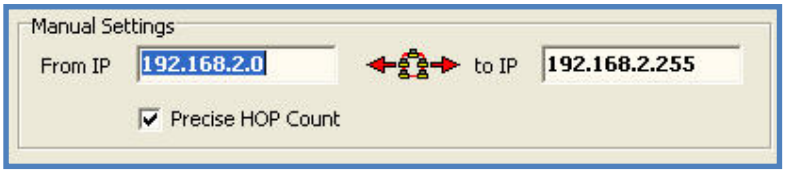
    a. Start Look@LAN

    b. Please choose *Create New Profile*

    c. Enter a profile name and then select the interface of the system you are running the program in.

d. The box labeled “Manually Specify Scan Range” allows you to set the target system if it is different than your internal subnet. In this case, we are scanning the same subnet, so you can ignore the setting.

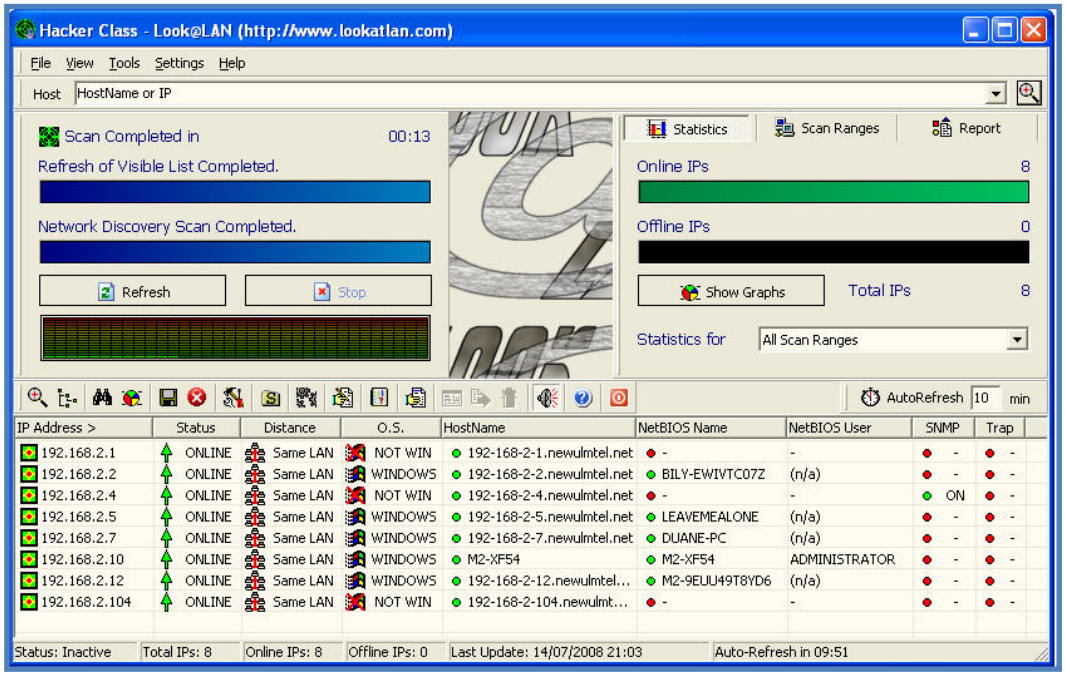


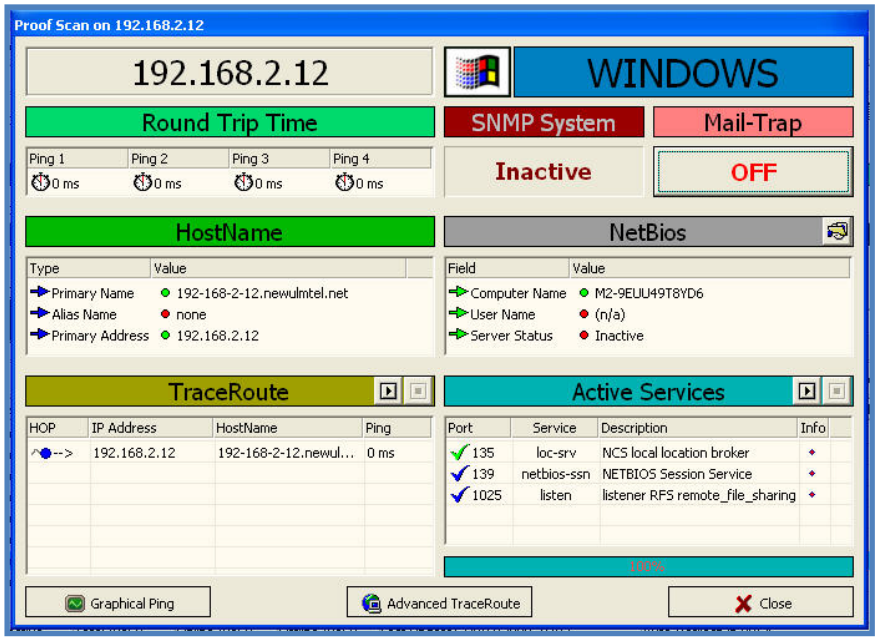


e. Choose Next

i. Look@LAN is a very noisy tool but brings results very fast. It automatically finds all the information available for the systems you are scanning. Later on, we will use this to enumerate SNMP results.

ii. If a Network Report window appears, click Hide.





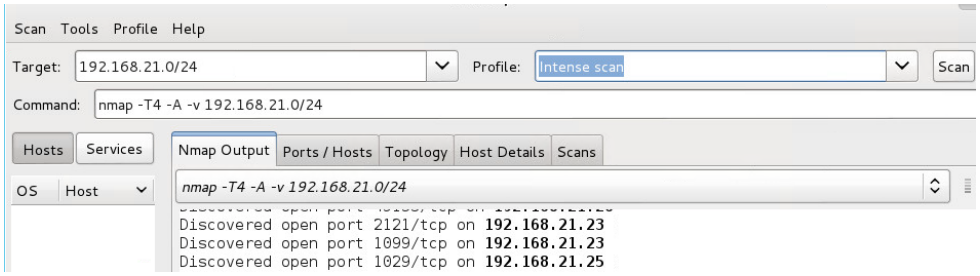
f. Double-click on one of the systems and see what type of results you can discover with this tool.

g. After exploring the results of this tool, close it and move on to the next exercise.

3.6 Zenmap

Run Zenmap in Kali Linux

1. Open a bash shell and type nmapfe



   a. Scan your lab network using the “intense scan” profile.

   b. Save the results (CTRL + s)

3.7 Hping3

This is to be done on your Kali Linux VM.

1. Utilize hping3 in Kali to verify the open ports on the computer systems you scanned in Exercise 1, 2, and 3.
2. We are going to perform this by running some basic commands with hping3.
3. Open a bash shell.
4. First let’s start by looking at the basic commands.
   a. Type: hping3 –help
      i. Take note of the following options: -c, -S, -p, -2 and -F.
      ii. These will be used extensively in the rest of Exercise 5.
      iii. Tell us what each of them mean!
         1. -c → _____
         2. -S → _____
         3. -p → _____
         4. -2 → _____
         5. -F → _____

b. Half-open SYN Scan. Type: hping3 -S <target> -p 80 -c 1

```
root@kali:~# hping3 -S 192.168.21.26 -p 80 -c 1
HPING 192.168.21.26 (eth0 192.168.21.26): S set, 40 headers + 0 data bytes
len=46 ip=192.168.21.26 ttl=128 DF id=2144 sport=80 flags=SA seq=0 win=8192 rtt=4.1 ms

--- 192.168.21.26 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.1/4.1/4.1 ms
```

c. UDP Scan (target should be a Windows computer).
Type: hping3 -2 <target> -p 139 -c 1

```
root@kali:~# hping3 -2 192.168.21.26 -p 139 -c 1
HPING 192.168.21.26 (eth0 192.168.21.26): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.21.26 name=UNKNOWN
status=0 port=2717 seq=0

--- 192.168.21.26 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 13.5/13.5/13.5 ms
```

d. FIN Scan (use against a Debian Linux machine). Type: hping3 -F <target> -p 6000 -c 1

```
root@kali:~# hping3 -F 192.168.21.21 -p 6000 -c 1
HPING 192.168.21.21 (eth0 192.168.21.21): F set, 40 headers + 0 data bytes
len=46 ip=192.168.21.21 ttl=64 DF id=33381 sport=6000 flags=RA seq=0 win=0 rtt=0.8 ms

--- 192.168.21.21 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.8/0.8 ms
```