Information Gathering

In this lab we will discuss one of essential steps must hacker perform before any other procedures it is footprinting, the fine art of gathering information. Footprinting is about scoping out your target of interest, understanding everything there is to know about that target and how it interrelates with everything around it, often without sending a single packet to your target. And because the direct target of your efforts may be tightly shut down, you will want to understand your target's related or peripheral entities as well.

#

What is Footprinting?

Footprinting is the process of creating a complete profile of the target's information technology (IT) posture, Using a combination of tools and techniques coupled with a healthy dose of patience and mind-melding, attackers can take an unknown entity and reduce it to a specific range of domain names, network blocks, subnets, routers, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its security posture. Although there are many types of footprinting techniques, they are primarily aimed at discovering information related to the following environments: Internet, intranet, remote access, and extranet. Table1 lists these environments and the critical information an attacker will try to identify.

Why Is Footprinting Necessary?

Footprinting is necessary for one basic reason: it gives you a picture of what the hacker sees. And if you know what the hacker sees, you know what potential security exposures you have in your environment. And when you know what exposures you have, you know how to prevent exploitation. Hackers are very good at one thing: getting inside your head, and you don't even know it. They are systematic and methodical in gathering all pieces of information related to the technologies used in your environment. Be forewarned, however, footprinting is often the most arduous task of trying to determine the security posture of an entity; and it tends to be the most boring for freshly minted security professionals eager to cut their teeth on some test hacking. However,footprinting is one of the most important steps and it must be performed accurately and in a controlled fashion.

DNS Reconnaissance

DNS is one of my favorite sources of information gathering. DNS offers a variety of information about public (and sometimes private!) organization servers, suchas IP addresses, server names and server functions. A DNS server will usually divulge DNS and Mail server information for the domain which it is authoritative. This is a necessity, as public requests for mailserver addresses and DNS server addresses make up our basic internetexperience. We can interact with a DNS server using various DNS clients such as host,nslookup, dig, etc.

nslookup is a computer program used in Windows and Unix to query Domain Name System (DNS) servers to find DNS details, including IP addresses of a particular computer, MX records for a domain and the NS servers of a domain. The name nslookup means "name server lookup". nslookup has the subcommands:

1. server NAME (where NAME is the name or IP address of a DNS server to query). It is not always possible to query a specific DNS server as often DNS queries are blocked to prevent denial of service attacks.
2. set type=NAME (where NAME is the type of record to look at). For example, set type mx will give the mail records.

As show in figure 1 , gathering information about iugaza.edu.ps ; also about google mail servers using `Set type =MX.`

Tracrroute:

traceroute is a computer network tool used to determine the route taken by packets across an IP network. Also it is useful to gather some information about the target server.

Other tools: Several good GUI-based traceroute tools are available. These tools draw a visual map that displays the path and destination:

- **NeoTrace**— A good GUI traceroute program that maps the path and destination.
- **VisualRoute**— Another good GUI tool that maps the path and destination.
- Also several sites can give you more information about your target like:
- **www.netcraft.com**
- **http://www.whois.net**
- Sam Spade**— www.samspade.org**
- Geektools**— www.geektools.com**
- Better-Whois.com**— www.betterwhois.com**
- DSHIELD**— www.dshield.org**