Interested in learning more about security?

SANS Institute InfoSec Reading Room

The Fundamentals Of Computer HACKING

There are three essential steps that a hacker, have to perform to get a good picture of an organization's layout. The steps are Foot printing, scanning and Enumeration. Foot printing is the ability to obtain essential information about an organization. This information includes the technologies that are being used such as, Internet, Intranet, Remote Access and the Extranet. In addition, to the technologies the security policies and procedures must be explored. By pursuing a structured procedure, attackers can systemati...

The Fundamentals Of Computer HACKING

Ida Mae Boyd

December 3, 2000

There are three essential steps that a hacker, have to perform to get a good picture of an organization's layout. The steps are Foot printing, scanning and Enumeration.

Foot printing is the ability to obtain essential information about an organization.

This information includes the technologies that are being used such as, Internet, Intranet, Remote Access and the Extranet. In addition, to the technologies the security policies and procedures must be explored.

By pursuing a structured procedure, attackers can systematically put together information from a collection of sources to compile a critical footprint of any organization. By using a combination of tools and techniques an hacker can take an unknown quality and reduce it to a specific range of domain names, network blocks and individual IP addresses of a system that is directly connected to the Internet.

The foot printing process must be performed accurately and in a controlled environment.

The following are the steps that a hacker must follow to make a foot print of an organization.

Step-1: Determine the scope of your foot printing activities – Are you going to foot print an entire organization or are you going to limit your activities to a certain location? The Internet provides a unlimited pool of resources you can use to help narrow the range of activities and provide some insight as to the type and amount of information publicly available about an organization and its employees. As a starting point, study the target organization's WEB page, many times an organization's WEB page will provide a lot of information that can assist in an attack. After studying the WEB page, you can perform an open source search for information relating to the targeted organization.

Develop any information that may make it easier to conduct "social engineering". Social engineering is a method of cracking network security by manipulating people inside the network into providing the necessary information to gain access.

Step-2: Network Enumeration – Network enumeration is a technique to identify the domain names and associated networks related to a particular organization. To enumerate these domains and begin to discover the networks attached to them, you must search the Internet. There are a lot of whois databases you can query that will provide a wealth of information about each entity an attacker is trying to foot print. There are many different tools to query the various whois databases. The following query types provide the majority of the information that the hackers use to begin their attacks:

Registrar – Displays specific registrar information and associated whois servers

Organizational – Displays all information related to a particular organization

Domain – Displays all information related to a particular domain

Network – Displays all information related to a particular network of a single IP address

Point of Contact (POC) – Displays all information related to a specific person, typically the administrative contacts

Step-3: Domain Name System (DNS) Interrogation – After identifying all the associated domains you can begin to query the DNS. DNS is a distributed database use to translate domain computer names to IP addresses and vice versa. If DNS is configured insecurely, it is possible to obtain revealing information about an organization. If a system administrator configures the DNS server incorrectly by allowing an untrusted Internet user to perform a DNS zone transfer. A zone transfer allows a second master server to update its zone database from the primary master server. Many DNS servers, however, are misconfigured and provides a copy of the zone to anyone who asks. This isn't necessarily bad if the only information provided is related to the systems that are connected to the Internet and have valid hostnames, although it makes it that much easier for attackers to find potential targets.

Step-4: Network Reconnaissance – Now that we have identified potential networks, we can attempt to determine their network topology, as well as potential access path into the network. To accomplish this, we can use the traceroute program that comes with most UNIX systems and is provided in WINDOWS NT. Traceroute is a diagnostic tool that lets you view the routes that an IP packet follows from one host to the next. Traceroute uses the Time-To-Live (TTL) option in the IP packet to obtain an ICMP TIME EXCEEDED message from each router. Each router that handles the packet is required to decrement the TTL field. The TTL field is known as a hop count. When the TTL field decrements to zero the packet is discarded.

Scanning: One of the most basic steps in mapping out a network is performing an automated ping sweep on a range of IP addresses and network blocks to determine if individual systems are alive. PING is used to send ICMP ECHO packets to a target system in an

attempt to obtain a ICMP ECHO-REPLY packets indicating the target system is a live. While ping is acceptable to determine the number of systems alive in a small to mid size network, it is inefficient for large, enterprise networks. Scanning large class A networks can take hours if not days to complete. To perform a ping sweep, you can use many of the tools that are available for both UNIX and Windows NT. One of the techniques of performing a ping sweeps in the UNIX environment is to use FPING. Unlike the traditional Ping Sweep utilities, that waits for a response from each system before moving on to the next host. FPING is a utility that will send out mass ping requests in a parallel, round robin fashion, thus, FPING will sweep many IP addresses significantly faster than ping.

Enumeration: If the initial target attempt and non-intrusive probing haven't turned up any immediate results. The attacker will turn to identifying valid user accounts, or poorly protected resource shares. There are many ways to extract valid account or exported resource names from a system by using a process called enumeration. Enumeration involves active connections to a system and directed queries. As such, they must be logged on or otherwise noticed. Much of the information collected through enumeration may appear to be harmless. Once a valid username or share is enumerated, it's usually only a matter of time before the hacker guesses the corresponding password or identifies some weakness associated with the resource sharing protocol. The type of information enumerated by hackers can be loosely grouped into the following categories:

1. Network resources and shares
2. Users and Groups
3. Applications and Banners

Tools and Procedures used to accomplish the task of foot printing

1. Conduct open source information gathering on USENET, search engines, EDGAR database, allows a hacker to query public documents, providing important insight into the breadth of an organization by identifying its associated entities.
2. Execute a whois query using the following:

    - http://www.networksolution.com/ - whois WEB interface
    - http://www.arin.net/ - whois ARIN whois (American Registry for Internet Numbers)
    - http://whois.ripe.net/ - European whois
    - http://whois.apmc.net/ - Asia Pacific IP address allocation
    - http://whois.nic.mil/ - US Military
    - http://whois.nic.gov/ - US Government
    - Or use the native UNIX whois from the command line:

        Whois <IP Address> | more

        Whois <email Address> to gather information on the SYSADMIN, etc.

Scanning & Enumeration: At this point the attacker has a good idea of the machines on the network, their operating systems, who the system administrators are an any discussion by them as to the topology, policies, management and administration of their systems. The tools that are available are:

1. NMAP
2. STROBE
3. NESSUS
4. SATAN variants SARA and SAINT if using LINUX; WINSCAN, SAMSPADE and others if using WINDOWS. There are also commercial products such as CyberCop scanner, and Internet Security scanners may be used. These are for sale on the open market.

Internet Sources:

Farmer, Dan and Venema, Wietsa "Improving the Security of your site by breaking into it" Sun Microsystems (11/29/00)
URL: http://www.geocities.com/hackernet_99/breakintoyoursite.htm

Gibbs, Mark "Any Port is a Hacker Storm" (11/29/000)
URL: http://www.antionline.com/

Fordham, Doug "Intelligence Preparation of the Battlefield" (6/19/00)
URL: http://www.securityfocus.com/focus/ih/articles/battlefield.html (12/3/00)

Kubin, Larry "Protect Your Business From Hacker Attacks" (10/15/98)
URL: http://www.suite101.com/article.cfm/1345/11549 (11/29/00)

Books

1. Peter Norton’s Network Security Fundamentals, by Peter Norton and Mike Stockman

2. Hacking Exposed Second Edition, by Joel Scambray, Stuart McClure and George Kurtz

to top of page | to Reading Room Home

Last Updated: June 29th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Cyber Defence Japan 2017	**Tokyo, JP**	**Jul 05, 2017 - Jul 15, 2017**	**Live Event**
SANS Cyber Defence Singapore 2017	**Singapore, SG**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS ICS & Energy-Houston 2017	**Houston, TXUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Los Angeles - Long Beach 2017	**Long Beach, CAUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Munich Summer 2017	**Munich, DE**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DCUS**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
Security Awareness Summit & Training 2017	**Nashville, TNUS**	**Jul 31, 2017 - Aug 09, 2017**	**Live Event**
SANS San Antonio 2017	**San Antonio, TXUS**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS Boston 2017	**Boston, MAUS**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Prague 2017	**Prague, CZ**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Hyderabad 2017	**Hyderabad, IN**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Salt Lake City 2017	**Salt Lake City, UTUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS New York City 2017	**New York City, NYUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS Adelaide 2017	**Adelaide, AU**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Chicago 2017	**Chicago, ILUS**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VAUS**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS San Francisco Fall 2017	**San Francisco, CAUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Tampa - Clearwater 2017	**Clearwater, FLUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NVUS**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS Dublin 2017	**Dublin, IE**	**Sep 11, 2017 - Sep 16, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, ILUS**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
Rocky Mountain Fall 2017	**Denver, COUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MDUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, GB**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, DK**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS SEC504 at Cyber Security Week 2017	**The Hague, NL**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London July 2017	**OnlineGB**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**