Thinking like a hacker

March 7, 2002 — By Eric Schultze, Chief Security Architect, Shavlik Technologies

Thinking like a successful hacker is not much different from thinking like a good developer. The most successful hackers follow a specific methodology that they have developed over time. They apply patience and carefully document every step of their work, much like developers.

The hacker's objective is to compromise the intended target or application. The hacker begins with little or no information about the target; however, by the end of the analysis, the attacker will have constructed a detailed roadmap that will allow them to compromise the target. This can only be achieved through careful analysis and a methodical approach to investigating the soon-to-be-victim.

The hacker's systematic method generally covers these seven steps:

1. Perform a footprint analysis
2. Enumerate information
3. Obtain access through user manipulation
4. Escalate privileges
5. Gather additional passwords and secrets
6. Install backdoors
7. Leverage the compromised system

This article shows you how hackers approach the tasks of breaking into networks and systems and compromising software applications. By knowing more about the hackers' methodology, you can beat them at their own game.

Perform a footprint analysis

The attacker first identifies the various domain names that he's interested in exploiting. He then performs a *footprint analysis* of the target to gather as much information as possible through publicly available sources. The footprint analysis gives the hacker an indication of how large the target might be, how many potential entry points exist, and what, if any, security mechanisms might exist to thwart the attack.

During a footprint analysis, the hacker attempts to discover all potentially related information that may be useful during the attack. This information includes:

- Company names

Domain names
Business subsidiaries
Internet Protocol (IP) networks
Phone numbers

Hackers pay particular attention to potential entry points that might circumvent the "front door." For example, rather than attempting to break through a major corporation's firewall, the attacker identifies a startup company (just acquired by the major corporation) and then attempts to leverage weak security in the smaller company that might provide unrestricted virtual private network (VPN) access to the larger target.

Port scanners are used to determine which hosts are alive on the Internet, which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports are listening on each system, and the operating system that is installed on each host. Traceroutes are performed to help identify the relationship of each host to every other and to identify potential security mechanisms between the attacker and the target.

After the port scanning and tracerouting is finished, attackers create a network map that represents their understanding of the target's Internet footprint. This map is used for the second phase of the attack: information enumeration.

Commonly used tools

Nslookup Command line tool in Windows NT 4.0, Windows 2000, and Windows XP that can be used to perform DNS queries and zone transfers.

Tracert Command line tool used by hackers to create network maps of the target's network presence.

SamSpade The SamSpade.org Web interface that performs Whois lookups, forward and reverse DNS searches, and traceroutes.

Nmap Unix-based port scanner.

ScanLine Windows NT-based port scanner.

Things to consider

Look at utilizing some of same methodologies that hackers use to assess an application that they're trying to penetrate. Questions to ask yourself about the applications that you develop include:

What is your application's footprint on the operating system?

What partner code does the application rely upon? If the partner application is hacked, will that enable the attacker to hack your application?

What information is the application, or system, presenting to unauthenticated users?

What listening ports does your software open on the system? Will malformed packets or flood attacks stop the service, or consume memory or CPU cycles?

Are there firewalls, or application chokepoints, that can be used to prevent unauthenticated users from walking in the front door?

Enumerate information

After the hackers have performed the footprint analysis and generated a map that approximates their knowledge of the target network, they then gather as much data as possible from the targeted system.

Web, FTP, and mail server version Hackers will try to determine what version of Web, File Transfer Protocol (FTP), or mail server is running by connecting to the listening TCP and UDP ports and sending random data to each. Many services respond to this random data with a *banner*—data that identifies the running application and potentially version information. Hackers will cross-reference this information to vulnerability databases such as SecurityFocus to look for possible exploits.

Sensitive information If the hackers are able to contact the host on certain ports (for example, TCP 139 or 445), they will attempt to anonymously enumerate sensitive information from the system including:

User names
Last logon dates
Password change dates
Group membership

The hacker can use the information obtained from this query in a brute force attack to gain access to the system as an authenticated user. For example, the hacker will enumerate members of the local administrators group, looking for user names like TEST or BACKUP that might have easily guessed passwords.

Commonly used tools

Netcat (listed under **Network Utility Tools**) The hacker's Swiss army knife. Used for banner grabbing and port scanning, among other things.

Epdump/Rpcdump Tools to gain information about remote procedure call (RPC) services on a server.

Getmac (Windows NT resource kit) Windows NT command to obtaining the media access control (MAC) Ethernet layer address and binding order for a computer running Windows NT 4.0, Windows 2000, or Windows XP.

DumpSec Security auditing program for Windows NT systems. It enumerates user and group details from a chosen system. This is the audit and enumeration tool of choice for Big Five auditors (PricewaterhouseCoopers, Ernst & Young, KPMG, Arthur Andersen, and Deloitte & Touche) and hackers alike.

SDKs Many software development kits (SDKs) provide hackers with the basic tools that they need to learn more about systems.

Things to consider

> What information can be obtained from listening ports? What level of permission is required to enumerate this information?
>
> Is there logging in place to determine that someone has enumerated this information?
>
> Does the potential exist for an authenticated user to view security-sensitive data or personally identified information (PII) that might compromise privacy concerns?
>
> What banner information does the application provide to the user? Can this be suppressed or modified by the system administrator?

Obtain access through user manipulation

After the hackers have learned enough basic information about their target, they will attempt to gain access to the target system by masquerading as authorized users. This means that they need a password for a user account that they have discovered through steps one and two above. There are two common ways to get that password: by using social engineering or by using a brute force attack.

Social engineering

It's amazing what an unsuspecting employee will do for someone who sounds authoritative. Some hackers will take the information that they acquired from the domain registration or the company's Web site and directly contact an employee by phone.

With a little conning, they can get that employee to reveal their password without raising any concerns. Their conversations might go something like this:

> This is the help desk and we're troubleshooting various network segments. I'm sniffing the network segment you're on, and I'd like to watch the network as you type in your password. Please tell me each character of your password as you type it in, and I will watch to make sure that I see them on the network.

Or,

> We've done an audit of your password and found it to be insecure. Please change it to xYzA1G24# so that it will be less likely to be cracked in the future.

Brute force attack

If the social engineering approach doesn't work or isn't an option, there's the brute force approach. These attacks can be waged against any application or service that accepts user authentication, including (but not limited to):

> Network basic input/output system (NetBIOS) over TCP (TCP 139)
> Direct Host (TCP 445)
> Lightweight Directory Access Protocol (LDAP), (TCP 389)
> FTP (TCP 21)
> Telnet (TCP 23)
> Simple Network Management Protocol (SNMP), (UDP 161)
> Point-to-Point Tunneling Protocol (PPTP), (TCP 1723)
> Terminal Services (TCP 3389)

If the hacker is able to contact one of these services, he will use the user names gathered in earlier steps to launch a brute force attack. Brute force guessing tools leverage dictionary files that might represent the user's password. Each dictionary word (or variant thereof) is considered a potential password and is paired with each user name until access is obtained.

Typical installations of Windows NT 4.0, Windows 2000, and Windows XP will not capture this attack because failed logon auditing is not enabled by default. Unless complex passwords are present for each user account, a dictionary attack can be quite successful against an unmonitored host.

In order to mask their identity, hackers will attempt to elude detection even if failed logon auditing has been enabled. By using computer names with non-printable ASCII characters, their computer names will appear as blank in the audit logs.

Commonly used tool

NetBIOS auditing tool Brute force password guessing tool.

Things to consider

> Is failed logon auditing enabled by default?
>
> Are there server-side mechanisms that you can use to slow down or lock out a brute force attack?
>
> Can you trace the source of the brute force logon attack back to a specific location? What location information can you obtain? DNS name or IP address? Computer name? Gateway address or specific host address?

Can the attackers subvert the event logs or application-specific logs after they get in?

Does this protocol need to be turned on by default?

Escalate privileges

After hackers have discovered a password for a user account and obtained user-level privileges to a host, they will attempt to escalate their permissions. They usually start by reviewing all the information on the host that they are able to view:

Batch files containing hardcoded user names and passwords are hacker's gold.

Registry keys containing application or user passwords are also worthy of a peek.

Reading e-mail or other documents that are stored on the system may also provide additional information to hackers that may enable them to gain privileges to other systems on the network.

If hackers are unable to enumerate any useful static information from the system, they may proceed to *trojan* the system. This usually involves copying malicious code to the user's system and giving it the same name as a frequently used piece of software.

For example, a hacker may replace Notepad.exe with a piece of trojan code that makes someone called "Eric" an administrator on the system before the program launches Notepad. The next time the system owner logs on as administrator and launches Notepad, the "Eric" account is added to the administrators group, unbeknownst to the person who launched Notepad.

If the hacker is not willing to wait for the user to take a specific action on the system, he may leverage system services to do the dirty work for them. For example, the attacker may locate a system service that launches with administrative or system privileges, and then replace this file with a trojan file to "make Eric admin." When this system is restarted, the service will launch, causing the trojan to execute with administrative privileges.

Things to consider

Are users able to view sensitive information?

Are passwords for the application stored in a secure manner?

Are passwords stored in clear text in batch files?

What registry keys can ordinary users write to? Do any of these keys execute with higher-level (or system) privileges?

Can user-level accounts modify the security context for services such that they can be used to launch trojans with local system privileges?

Are there any files that the user can overwrite that are called by services running under higher levels of privileges?

Gather additional passwords and secrets

The first thing that hackers do after they have logged on to a system with administrator credentials is to obtain the password file. Hackers can use tools such as Pwdump2 to obtain the password hashes from the local security accounts manager (SAM) database or Active Directory of a domain controller. Password hashes can be fed to programs like LC3 or John the Ripper and *cracked*.

As an administrator, hackers can obtain the clear-text passwords from the local security authority (LSA). Specifically, passwords that are used to start services are stored (obfuscated and reversibly encrypted) in the LSA. Using tools such as Lsadump2, the clear-text passwords for the accounts that are used to start corresponding services can be enumerated.

Although this may not be a risk if the account starting the service is an administrative member on this local system (or a lesser privileged account), a larger threat may be present if the account that is used to start the service is an administrative member of the domain (or higher-level domain). In the worst instance, the hacker (as a local administrator) may be able to obtain the clear-text password for a domain administrator account for a domain that they had yet to hack.

After local, and potentially domain level, passwords have been obtained, the hacker will cross-reference user name\password combinations that have been obtained with user names that they've enumerated from other systems during the enumeration phase. With enough time or the right amount of luck, the hacker will be able to obtain administrative access to all computers in the network, having only initially compromised one computer.

Commonly used tools

Pwdump2 Tool that can obtain password hashes from the SAM database or the Active Directory.

Lsadump2 Tool that exposes the contents of the LSA in clear text.

LC3 Password auditing tool that evaluates Windows NT, Windows 2000, and Windows XP password hashes.

John the Ripper Password cracking tool for several operating systems.

Things to consider

Are logs generated when the password files are accessed?

Are logs generated when the administrator attempts to inject rogue code into system processes in an attempt to access password data?

Are passwords being stored on the system for any accounts that may have greater levels of permission than the local administrator accounts?

Is the password for the administrator-level accounts on one system the same as the password for administrator accounts on other systems?

Are users encouraged to select complex passwords?

Install backdoors

In case hackers are detected and need to leave the computer in a hurry, they frequently create a backdoor on each system they compromise. Backdoors can take many forms, but the most common is a listening port on the system that will enable the hacker to access the system remotely (with or without special credentials).

Firewalls or router filtering may prevent the hacker from later accessing these ports; however, common router filtering may not block high numbered TCP ports (or any UDP ports), or may allow traffic to pass if it originates on a specific source port, like TCP 20, 53, or 8. If strong filtering or firewalling is in place, more complex backdoors may be necessary.

One form of a complex backdoor involves reverse trafficking. Reverse trafficking enables the attacker to bypass the existing security mechanisms. While routers and firewalls may prevent all unsolicited packets from entering the network from the outside, it is highly likely that a client within the firewall is allowed to initiate a connection on a specified port number to any host on the outside. A trojan of this type might be scheduled to contact the hacker's computer on a regular basis over TCP port 80. The client computer may "push" a system-level command shell to the hacker, so the hacker can then execute code on the "protected" computer.

An example of reverse trafficking was the Code Red worm. Code Red would instruct unpatched Web servers (over TCP port 80) to execute a Tiny File Transfer Protocol (TFTP) connection from the server to a host on the Internet, where it would then obtain a piece of rogue code. The initiating traffic to the Web server over port 80 was completely legitimate (and would even pass firewalls), and in most cases, the firewalls and routers would allow the Web server to initiate a TFTP (UDP 69) connection to the hacker's computer on the Internet.

There are few, if any, valid reasons why Web servers should ever need to initiate a TFTP or server message block (SMB) connection to any host on the Internet. Firewalls and routers should be configured to block unsolicited outbound traffic originating from Web or mail servers to untrusted computers on the Internet.

Commonly used tool

Netcat Hacker's Swiss army knife. Can be used to "shovel shells" to remote systems.

Things to consider

Does the system or application have any mechanism to identify trojan code that may be running on the system?

Can the system detect devices or services that the attacker has created?

Is there a baseline of known listening ports, services, and devices against which the system can be monitored to help determine if a rogue piece of code has been executed?

Are security devices (firewalls, routers) configured to prevent unwanted outbound traffic from originating from each host?

Leverage the compromised system

Port redirectors In order to circumvent traditional security devices, hackers may create port redirectors on the first compromised host that will automatically pass all traffic to other internal hosts. Port redirectors can help bypass port filters, routers, and firewalls, and may even be encrypted over a Secure Sockets Layer (SSL) tunnel to evade intrusion detection devices.

When a port redirector is used to traffic packets between the hacker's computer and the target system, the hacker's true identity is essentially "laundered." If the target system is enabled for failed logon auditing, or is running a third-party intrusion detection system, it will record the IP address or computer name of the host running the port redirector, not the hacker's computer. This may make it very difficult for the attacker to be identified, as all traffic going to and coming from the target system appears to be legitimate connections to the computer that is proxying the hacker's traffic by means of the port redirector.

Hacking other systems After the hacker has fully hacked the local system, installed their backdoors and port redirectors, and obtained all the information available to them, they will proceed to hack other systems on the network. Most often there are matching service, administrator, or support accounts residing on each system that make it easy for the attacker to compromise each system in a short amount of time. As each new system is hacked, the attacker performs the steps outlined above to gather additional system and password information.

Attackers continue to leverage information on each system until they identify passwords for accounts that reside on highly prized systems including payroll, root domain controllers, and Web servers. The process of scanning and exploiting systems in this

manner can often be automated, letting hackers grab a few hours of rest, or allowing them to focus their attentions on other areas of the target company.

It's difficult to identify this type of activity because the attacker is usually operating under the guise of a valid administrator account. Unless the attacker is caught before he gains administrator access, it may be nearly impossible to flush him from the network.

Commonly used tool

Fpipe A port redirector for Windows systems. Allows the source port for redirected traffic to be specified.

Things to consider

Are processes in place to monitor system logs across multiple computers and correlate attack sequences to suggest that an automated attack is in process?

Are group memberships reviewed on a regular basis to ensure that new "hacker accounts" haven't been added to administrative groups?

Resources

Microsoft Security Web site Public Web site with links to security bulletins and product security information.

Hacking Exposed: Network Security Secrets and Solutions, Third Edition Stuart McClure, Joel Scambray, and George Kurtz take a comprehensive look at hacker methodologies across multiple platforms and devices.

Hacking Exposed Windows 2000: Network Security Secrets and Solutions Scambray and McClure detail hacker techniques specific to Microsoft platforms.