

The Anti-Hacker Toolkit

Protect, Defend, and Remediate

There are several stages to the complete security model in which every organization must be fluent. The first is *prevention*, which involves examining your current security posture. A security professional will need to audit both systems and networks in order to gain a complete understanding of the risks you expose to the online world. The second stage, which always seems to occur, is *investigation*. Investigations spring up not only from hacking but also from an employee's abuse of computing resources. The forensic process, which is performed during the investigation stage will not only give you insight to prevent the incident, but also provide a solid ground for possible legal action. There are a whole suite of tools available, some commercial and some free, to accomplish each of the stages outlined above. Mastering these tools could literally take a life-time without a head start. *Anti-hacker Toolkit* is a book that meticulously describes the most common tools that computing professionals need to utilize when auditing systems and networks or while performing computer forensics.

The Prevention Stage

The most performed duty when protecting your computer resources is probably system auditing. One of the most popular tools used for system auditing is *nmap*. There are two reasons for its wide spread use: it is cost effective and very powerful. Nmap is cost effective because it is open-source, but more importantly - free. Because it is free and a number of intelligent individuals contribute to the project, its sheer power can be daunting without a clear understanding of its numerous command line switches.

Nmap can be used to locate open ports on your network. Some of the things that open ports can signify behind your organization's walls are:

- ✂ Unauthorized Web Servers
- ✂ FTP Servers Offering Music Files for Download
- ✂ Vulnerable Legitimate Services
- ✂ Rogue Backdoors Hackers Placed in Your Network

Nmap, in its simplest form, is run when you supply it with a single IP address. However, without knowing some of the more intricate details of nmap, you could be led into a false sense of security. For instance, if you have configured your firewalls to block all unnecessary incoming network traffic from the outside world, but have not restricted port outbound TCP port 80 (because everyone needs to surf the web, right?), you may leave yourself open to reconnaissance to the outside world. With nmap, you can specify the source port for a TCP scan from the hacker's machine that would literally sidestep your firewall rules. If the attacker specified a source TCP port of 80, he would effectively be masquerading his connection as an output web connection. This is accomplished trivially by supplying the "-g" command line flag to nmap and placing the desired port afterward. *Anti-Hacker Toolkit* describes this phenomenon and many more tips and tricks you can perform with nmap to audit your network and systems. The book

provides example output and case studies in each chapter to show the use of each tool pulled from the authors' experiences in the field.

The Investigation Stage

The investigative process requires a combination of policy and technology. *Anti-Hacker Toolkit* focuses on the technology so that the evidence you collect and analyze does not become invalid if you choose to prosecute or take administrative action. The book does not assume that you are performing a specific type of investigation, either. Techniques to investigate external intrusions (a.k.a. "hacking") and incidents internal to the organization are covered equally. Possibly the most useful toolkits described in *Anti-Hacker Toolkit* are the live response kits for both Unix and Windows operating systems.

Live response toolkits are becoming more frequent when investigating computer related incidents, especially if it is caused by an external intrusion. A live response toolkit will allow you to collect the volatile evidence before it is permanently lost. We have all heard at one time or another of the law enforcement agent who was taught to yank the power plug out of the wall so he can perform a forensic acquisition of the hard drive before he can begin his investigation. In doing so, that agent will lose the following:

✂ Current Network Connections - Now we cannot see who is connected to the computer. Sometimes this is the only evidence of unauthorized access.

✂ Currently Running Processes - Every attacker seems to run backdoors and other rogue programs after he has victimized your server. Without collecting information about the running process you may not be able to prove that your data obtained additional damage. Furthermore, you may not even know of a backdoor he gave himself back into your network!

With Unix, you can even run a process and delete the original file from the disk. In this case, an attacker can run a backdoor and completely rid the disk of the binary, which in turn leaves little or no evidence of its existence.

✂ Current Network Interface Card (NIC) Status - If an attacker runs a sniffer on your network, he will be able to gain access to additional credentials. If he gains additional credentials, he will be able to access your computing resources in a manner consistent with your valid users making him harder to catch.

The list above is by no means a comprehensive compilation of evidence lost if you do not collect it with a Live Response Toolkit. *Anti-Hacker Toolkit* describes some these and more in greater detail when it shows the use of full toolkits for both Unix and Windows. The suites *Anti-Hacker Toolkit* suggests you assemble for this type of investigation are summarized in the table below:

Unix	Windows	Description	Investigative Purpose
<i>bash</i>	<i>cmd.exe</i>	Executes a Trusted Shell Before You Begin Your Response.	
<i>lsof</i>	<i>fport</i>	Maps Open Network Ports To Processes. Additionally, Lsof Maps Open Files To Processes.	Detects Backdoors And Sniffers
<i>netstat</i>	<i>netstat</i>	Views Current Network Conditions (Connections, Open Ports, Etc)	Detects Backdoors And Sniffers
	<i>nbtstat</i>	Views the NBT Name Cache	Gives Insight Into Machines Connecting To You.
<i>arp</i>	<i>arp</i>	Views Cached MAC Addresses	Gives Insight Into Machines Connecting To You.
<i>ps</i>	<i>pslist</i>	Lists Running Processes	Detects Rogue Processes Such As Backdoors and Sniffers.
<i>kill</i>	<i>kill</i>	Sends A Signal To A Running Processes (i.e. to “freeze” or “remove” a process)	Removes or Halts Rogue Processes Running In Memory.
<i>ls</i>	<i>dir</i>	Collects Time/Date Stamps From The File System.	Acquires Time/Date Stamps To Provide Investigative Leads.
	<i>auditpol</i>	Lists The Current Auditing Policy.	Used To Determine Security Posture And Selection Of Logs To Acquire.
<i>w</i>	<i>loggedon</i>	Lists The Users Currently Connected To The System.	Detects Unauthorized User Access.
<i>last, lastb</i>	<i>nlast</i>	Lists The History Of Users Connected To The System.	Detects Unauthorized User Access.
	<i>dumpel</i>	Extracts The System Event Logs In A Textual Format.	Detects Unauthorized User Access.
	<i>regdmp</i>	Extracts The System Registry In A Textual Format.	Detects Many Situations Including The Use Of Backdoors (Sub7, Netbus, etc.)
	<i>sfind</i>	Detects Streamed (hidden) Files.	Detects Secret Storage Of Hacker Tools.
<i>nc/cryptcat</i>	<i>nc/cryptcat</i>	Netcat/Cryptcat Is Used To Transfer Your Evidence To Another Machine, Thereby Not Destroying Any Evidence If You Choose Later To Duplicate The Victim Machine.	

<i>md5sum</i>	<i>md5sum</i>	This Tool Calculates The MD5 Checksum In Order To Authenticate The Evidentiary Value Of The Data You Collected.	
---------------	---------------	---	--