Anti-hacker Tool Kit

Keith Jones, Mike Shema, Bradley C. Johnson

Anti-hacker Tool Kit Keith Jones, Mike Shema, Bradley C. Johnson

The "Anti-Hacker Tool Kit, Second Edition", is an invaluable resource to any network professional looking to protect his/her system, and a must-have companion to "Hacking Exposed".

Anti-hacker Tool Kit

Keith Jones, Mike Shema, Bradley C. Johnson

Anti-hacker Tool Kit Keith Jones, Mike Shema, Bradley C. Johnson

The "Anti-Hacker Tool Kit, Second Edition", is an invaluable resource to any network professional looking to protect his/her system, and a must-have companion to "Hacking Exposed".

750 pages

From the Back Cover

"This book continues the best-selling tradition of *Hacking Exposed* only by learning the tools and techniques of malicious hackers can you truly reduce security risk. Arm yourself today with the *Anti-Hacker Tool Kit*." Joel Scambray, Co-author of *Hacking Exposed*, *Hacking Exposed Windows 2000*, and *Hacking Exposed Web Applications*Stay one step ahead of even the most cunning hackers with help from this invaluable resource. Through proper use and configuration of key security tools, you'll be able to investigate and resolve existing problems within your network infrastructure with precision and a minimum of fuss. Written by experienced security professionals, this resource provides you with comprehensive coverage of the most important and up-to-date security tools in use today, explains their function, and shows you how to use each tool effectively through in-depth implementation examples and case studies. Learn to detect and prevent system misconfigurations and Web server hacks plus, discover best practices for protecting both large and small networks. Includes best practices for use and configuration of these key tools:

-Port scanners Nmap, NetScan, SuperScan, IpEye
-Enumeration tools Enum, PSTools, and User2SID
-BackDoors NetBus, Back Orifice, and SubSeven
-Password crackers Pwltool, SMBGrind, Jack the Ripper, and LSADump2
-Sniffers Snort, BUTTSniffer, WinDump, and Dsniff
-System Audit tools Nessus, STAT, ISS Internet Scanner
-Denial of Service tools Tribe Flood network, Shaft, and Mstreams
-WardialersTHC-scan and ToneLoc
-Incident response and forensic tools TCT, EnCase, FTK, and other file viewers
-Miscellaneous and multi-purpose tools Netcat, Getadmin, Fpipe, Fport, VMWare, and many more About the Author

Bradley C. Johnson (Gaithersburg, MD) is currently the manager of the Network and Security Group at an IT provider in Silver Spring, Maryland. Bradley is responsible for the security and functionality of his company's internal network as well as its customers' networks. Excerpt.

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 it’s 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.

Leer Anti-hacker Tool Kit by Keith Jones, Mike Shema, Bradley C. Johnson para ebook en líneaAnti-hacker Tool Kit by Keith Jones, Mike Shema, Bradley C. Johnson Descarga gratuita de PDF, libros de audio, libros para leer, buenos libros para leer, libros baratos, libros buenos, libros en línea, libros en línea, reseñas de libros epub, leer libros en línea, libros para leer en línea, biblioteca en línea, greatbooks para leer, PDF Mejores libros para leer, libros superiores para leer libros Anti-hacker Tool Kit by Keith Jones, Mike Shema, Bradley C. Johnson para leer en línea.Online Anti-hacker Tool Kit by Keith Jones, Mike Shema, Bradley C. Johnson ebook PDF descargarAnti-hacker Tool Kit by Keith Jones, Mike Shema, Bradley C. Johnson DocAnti-hacker Tool Kit by Keith Jones, Mike Shema, Bradley C. Johnson MobipocketAnti-hacker Tool Kit by Keith Jones, Mike Shema, Bradley C. Johnson EPub
A7ZQN1H32M8A7ZQN1H32M8A7ZQN1H32M8