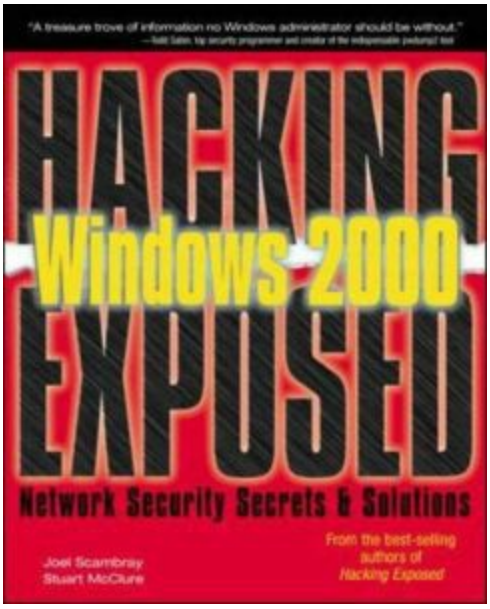

Book Hacking Exposed

Network Security Secrets and Solutions

Joel Scambray, Stuart McClure and George Kurtz
McGraw-Hill, 2001

Recommendation

You might expect a massive book about computer hacking to be tedious reading, but - surprise - this one is actually fun. You'll be impressed by the quality of the writing and the authors' clarity about complicated matters. Why have these clever writers gone public with information on how to hack into computers? They figure that hackers learn how to penetrate systems anyway. It's the network administrators and other professionals who need to understand hacking to protect their own vulnerabilities. The book, which is a bit dated now, given the programs it refers to, still conveys relevant principles about defending your work and your company from attack. *BooksInShort* recommends it as an essential reference for businesspeople who want to know why system administrators always look twitchy. It's also a good tool for any computer professional whose day - or career - might be ruined by a single moment of system weakness.

Take-Aways

- Almost nothing in the computer world is completely safe.
- Even firewalls have vulnerabilities that a hacker can decipher.
- Making your computer system's vulnerabilities public makes your system more secure.
- The more people know about a vulnerability, the better chance it has of being fixed.
- You can get constant updates on security matters on the Internet.
- Hackers have favorite software tools, like Back Office, for penetrating systems.
- Hackers first probe a targeted system - a process they call footprinting.
- Hackers then scan the information they find to penetrate to other data such as phone numbers, employee names and server information.
- Finally, hackers enumerate the data, extracting Internet addresses and identifying valid user accounts or poorly protected resources.
- System administrators must be constantly vigilant.

Summary

Why Experts Believe in Open Disclosure

If you base your computer security on knowledge about the vulnerabilities of your computer system, your security will be stronger. Publishing information about the vulnerabilities of popular computer systems has its risks, of course, but that information leads to more robust security.

> "The more people know about a vulnerability, the better chance it has of being fixed."

True, dark hat hackers will read any available information to learn more devious ways to disrupt computer users, but they would have learned about them anyway. It is more important for the computer system defense team in your company to know about network and system weaknesses than it is to throw a veil of blind secrecy over the entire matter - an approach which would only let hackers run amok. Overall, open disclosure means better security in the long run.

> "Some feel drugs are about the only thing more addicting than obtaining root access on a UNIX system."

That's the theory behind the Open Disclosure movement, which has resulted in a much more secure Internet over the years. Software designers have a much harder time denying vulnerabilities of their programs when the public is aware. Developers can't hide problems that have been announced in the media from consumers. To protect your company and your computer system, learn all you can about this issue.

The Hackers' First Step: Footprinting

Footprinting is the art of gathering target information. It is the first step in hacking, which can't begin until the hackers have identified their victim. Compare hackers, who are criminals also, to bank robbers. Smart bank robbers don't just go in shooting. They figure out the best entrances, the movements of the guards, the security protocols and so on. They case the joint. That's what the best hackers do before they break into your system, creating unwanted work delays and critical data losses.

> "If footprinting is the equivalent of casing a place for information, then scanning is equivalent to knocking on the walls to find all the doors and windows."

Hackers have to develop a storehouse of information before they can attempt to infiltrate your network. Hackers can use a combination of tools and techniques to turn a company previously unknown to them into individual IP addresses, domain names and network blocks.

Many footprinting methods exist, including using queries and downloads, and they are all designed to get information related to several specific technologies, including extranet, remote access, Internet and intranet.

> "It seems that Microsoft went out of its way in many instances to sacrifice security for ease of use when planning the architecture of Windows 95/95b/98/98SE."

The best way to defend yourself is to automate as many defensive scripts as possible, but your company's system administrator always has to be vigilant. Constant monitoring is absolutely essential.

The Hackers' Second Step: Scanning

Whereas footprinting can be described as casing the joint for information, scanning is the equivalent of checking all the doors and windows. Using the network information and IP addresses that they gathered during footprinting, hackers can penetrate to other data such as phone numbers, employee names and server information.

> "Ever since Cheswick and Bellovin wrote their epic book about building firewalls and tracking a wily hacker named

> Berferd, the thought of putting a Web server (or any computer for that matter) on the Internet without deploying a firewall has been considered suicidal. Equally as suicidal has been the frequent decision to throw firewall duties on the network adminstrator's lap."

Your company's system administrator can defend the organization from scanning by using ping sweep tools, which help pinpoint potential targets in your system.

The Hackers' Third Step: Enumeration

The next step hackers take, if they haven't been detected during the first two steps, is a process called enumeration. Assuming that initial target acquisition and probing haven't turned up any easy avenues of access, an attacker will next turn to identifying valid user accounts or poorly protected shared resources. There are many ways to extract valid account or exported resource names from systems.

> "While there are many types of footprinting techniques, they are primarily aimed at discovering information related to these technologies: Internet, intranet, remote access and extranet."

By being savvy about the weaknesses in each computer architecture system, your system administrator can figure out what hackers are up to and protect your organization from enumeration. The following rundown gives you an initial sense of where your particular system architecture might be vulnerable.

Fundamental Operating System (OS) Architectures

The underpinnings of Windows NT's SMB/CIFs/NETBIOS makes it very easy to gain user credentials and application information. You can also lock down NT by restricting access to TCP 139 and 445. It is important that the administrator remembers that Windows 2000 hasn't completely eliminated these problems and also has vulnerabilities in its Active Directory.

> "Security that is based on publishing vulnerabilities is more robust. Yes, attackers learn about the vulnerabilities, but they would have learned about them anyway. More importantly, defenders can learn about them, product vendors can fix them, and sys admins can defend against them."

Be cautious with SNMP, which was designed to give as much information as possible to managers. Unfortunately, it also provides a great entrance point for hackers because it automatically gives out data that should be private.

Applications

Finger and Rpcbind are examples of programs that give away far too much information. The software vendor involved should teach your company how to secure these applications and how to disable applications such as Finger. Be sure to check the Internet for security updates on any applications that your organization uses.

Firewalls

Your company can use firewalls effectively to screen out many leaks. Still, your defense team must patch holes as they discover them. That goes a long way toward better security.

> "NT has become a whipping boy of sorts within the hacking community."

Two types of firewalls dominate the market: application proxies and packet filtering. Both have weaknesses. Application firewalls are considered more secure, although they have performance limitations. In real life, a well-configured firewall is difficult to penetrate. However, if you use certain tools like traceroute, nmap and hping, which are available on the Internet, attackers might find a way into your system. Most current firewall vulnerabilities are due to misconfiguration of the firewall.

System Hacking: Hacking Windows 95/98 and ME

Every network administrator has to face up to the fact that Windows 95/95B/98/98SE (hereafter Win 9X) were never designed to be as secure as their cousin Windows NT/2000. In fact, it seems clear that Microsoft went out of its way to sacrifice security for ease of use when designing the architecture of Windows 9X. As time goes on, hacking Windows 95/98 will be less interesting than attacking 2000.

> "Microsoft has diligently patched most of the problems that have arisen. Thus, we think the common perception of NT as an insecure operating system is only one percent right. In knowledgeable hands, it is just as secure as any UNIX system and we would argue it is probably more so."

Keep these concerns in mind if you are using Windows 9X:

Windows 9X is inert – Hackers can't do a lot to Win 9X because it lacks built-in remote logon facilities. The only thing an intruder can do is trade files, but you can prevent that with proper password protection. Still, you should not deploy unsecured Win 9X systems on the Internet. The ease with which 9X services can be initiated, plus the lack of secondary defense protocols, means that there are potential problems for your organization.

- **Script weaknesses** – Hacker tools such as SubSeven make infiltration of a 9X machine much easier. Make sure these tools are never installed on a machine without the specific involvement and knowledge of your systems administrator.
- **Keep your patches updated** – You have to keep current. If you don't, you leave your system vulnerable.
- **Machine access** – If a hacker gets physical access to a Win 9X machine then you're pretty much dead in the water. The only solutions that could still save you are third-party security software and bios passwords.

System Hacking: Windows NT

Hackers can attack Windows NT many ways, but that doesn't mean that it is innately insecure. Very little damage can be done remotely without the "administrators' privilege," and gaining that privilege isn't easy.

> "What is clear from these experiments is that sensibly configured Win 2000 Servers are at least as difficult to break at the OS level as any other server platform, and that the most likely avenue of entry into a server is via the application layer, bypassing OS-level security measures entirely."

With that in mind, here are some steps to secure your system if you use Windows NT:

Step One: Block Access to TCP and UDP Ports 135 to 139

If you just do this one thing, you can prevent almost every remote NT problem.

Step Two: Use Strong Passwords

Perform regular audits and set some guidelines for your employees.

Step Three: Check Administrative Discipline

Make sure that rogue administrators use "Domain Admin" credentials as local administrators on local systems.

Step Four: Update Patches

Apply the most recent patches and fixes.

Step Five: Educate Your Employees

Make sure that users understand the sensitivity of passwords. Teach them to never tell their passwords to a stranger.

System Hacking: Windows 2000

While this OS has a number of vulnerabilities, on balance it isn't any easier to break into than other operating systems. However, the jury is still out on just how secure it is.

Until the verdict comes in, you can make your Windows 2000 system more secure by taking these steps:

- **Proper version** – Make sure that you're using the proper version of Win 2000. The Server and Advanced Server should always be heavily guarded from untrusted networks, users and anything else.
- **Less is more** – The less complicated your system is, the less likely it is to be attacked. Turn off all unnecessary services.
- **Best practices** – Make sure you use the best methods for security.

DoS Attacks

A Denial of Service attack basically disrupts or completely denies service to legitimate users. It doesn't actually take a lot of skill to carry out such an attack because the needed tools are widely available, under the names "Smurf, Fraggle, boink and teardrop," among others. They may sound like children's games or soft drinks, but they have been used to cause mayhem across the Internet over the past few years by creating denial of service attacks.

These attacks annually cost businesses millions of dollars and constitute a serious threat to any system or network. These costs are related to system downtime, lost revenues and the labor involved in identifying and reacting to such attacks.

The ease of conducting a DoS attack probably explains its rising popularity. And, if you add broadband capabilities to the problem, then DoS hacks can become varied and powerful and do a lot to slow down the Internet backbone. For instance, this is the kind of attack that a political enemy could conduct. All organizations, including government offices, need complete computer security.

About the Authors

Stuart McClure and **George Kurtz** are president/CTO and CEO, respectively, of Foundstone Inc. (www.foundstone.com), of which **Joel Scrambray** is a principle. The firm provides information system security consulting services to clients ranging from members of the *Fortune* 50 to newly minted startups. McClure, who has more than ten years of IT and security experience, specializes in security assessments, firewall reviews, e-commerce application testing, host reviews, PKI technologies, intrusion detection, and incident response. Kurtz, an internationally recognized security expert, has performed hundreds of firewall, network and e-commerce related security assessments.
