CHAPTER 1

NETWORK AND SYSTEM SECURITY BASICS
It's hard to talk about any system in a vacuum, especially one that is so widely deployed in so many roles as Windows 2000. This chapter is dedicated to previewing some basic information system security defensive postures so that our discussion of the specifics of Windows 2000 is better informed.

BASIC SECURITY PRACTICES

You should ensure that the following issues have been addressed within your organization before embarking on a plan to tighten down Windows 2000. These recommendations are based on our years of combined security assessment consulting against all varieties of networks, systems, and products. Some of them overlap with specific recommendations we will make in this book, but some do not. In fact, we may violate some of these principles occasionally to prove a point—do as we say, not as we do! Remember, security is not a purely technical solution, but rather a combination of technical measures and processes that are uniquely tailored to your environment.

Block or Disable Everything That Is Not Explicitly Allowed

We will repeat this mantra time and again in this book. With some very obscure exceptions, there are no known ways to remotely attack a system with no running services. Thus, if you block access to or disable services outright, you cannot be attacked.

This is small consolation for those services that are permitted, of course (for example, application services such as IIS necessary to run a Web application). If you need to allow access to a service, make sure you have secured it according to best practices (for example, read Chapter 10 of this book to understand how to lock down IIS).

Since they are most always unique, applications themselves must be secured with good ol' fashioned design and implementation best practices.

Always Set a Password, Make It Complex, and Change It Often

Passwords are the bane of the security world—they are the primary form of authentication for just about every product in existence. Windows 2000 included. Weak passwords are the primary way in which we defeat Windows 2000 networks in professional penetration testing engagements. Always set a password (never leave it blank!), and make sure it's not easily guessed (see Chapter 5 for some Windows 2000–specific tips). Use multifactor authentication if feasible (Windows 2000 is fairly easy to integrate with smart cards, for example).

Keep Up with Vendor Patches—Religiously!

Anybody who has done software development knows that accidents happen. When a bug is discovered in a Microsoft product, however, the rush to gain fame and popularity typically results in a published exploit within 48 hours. This means you have approximately two days to apply patches from Microsoft before someone comes knocking on your door. As you will see from the severity of some of these issues described in this book, the price of not keeping up with patches is complete and utter remote system compromise (check out Chapter 10 if you need further proof).
Authorize All Access Using Least Privilege  This is a concept that is the most infrequently grasped by our consulting clientele, but it’s the one that we exploit to the greatest effect on their networks. **Authorization** occurs *after* authentication to protect sensitive resources from access by underprivileged users. Guessing a weak password is bad enough, but things get a lot worse when we discover that the lowly user account we just compromised can mount a share containing sensitive corporate financial data. Yes, it requires a lot of elbow grease to inventory all of the resources in your IT environment and assign appropriate access control, but if you don’t, you will only be as strong as your weakest authentication link—back to that one user with the lame password.

Limit Trust  No system is an island, especially with Windows 2000. One of the most effective attacks we use against Windows networks is the exploitation of an unimportant domain member computer with a weak local Administrator password. Then, by using techniques discussed in Chapter 8, we extract the credentials for a valid domain user from this computer, which allows us to gain a foothold on the entire domain infrastructure and possibly domains that trust the current one. Recognize that every trust relationship you set up, whether it be a formal Windows 2000 domain trust or simply a password stored in a batch file on a remote computer, expands the security periphery and increases your risks.

A corollary of this rule is that password reuse should be explicitly banned. We can’t count the number of times we’ve knocked over a single Windows NT/2000 system, cracked passwords for a handful of accounts, and discovered that these credentials enable us to access just about every other system on the network (phone system switches, UNIX database servers, SNA gateways, you name it).

Be Particularly Paranoid with External Interfaces (Dial-up, Too!)  The total number of potential vulnerabilities on a network can seem staggering, but you must learn to focus on those that present the most risk. These are most often related to systems that face public networks such as Web servers and so on. Front-facing systems (as we’ll call them) should be held to higher standard of accountability than internal systems, because the risks that they face are greater. Remember that the public switched telephone network is a front-facing interface as well (see *Hacking Exposed, Third Edition*, Chapter 9 for recommendations on dial-up security, which we will not treat in this book).

Monitoring, Logging, Auditing, and Detection Should Be Enabled  This is not a book on the art of intrusion detection or forensic analysis, and we will not be covering monitoring, auditing, and logging in-depth. We do make our recommendations for Windows 2000 audit settings (enable audit of Success and Failure of everything except process tracking) but will otherwise assume everyone understands the importance of such record keeping and has implemented it appropriately. Don’t forget to actually review the logs you keep—there’s no point in keeping them otherwise.

Plan an Incident Response Capability, Business Continuity  We are going to talk a lot in this book about how to avoid getting hacked. But what happens if the unthinkable occurs and you *are* successfully attacked? There are many critical procedures that should be followed...
immediately following a security incident to stem the damage, and these procedures should be laid down in advance. However, this is not a book on incident response, and we are not going to delve into those topics here. We highly recommend *Incident Response* by Mandia and Prosise if you want to learn the ropes of this aspect of security.

**Technology Will Not Protect You from Social Attacks** This book is targeted mainly at technology-driven attacks—software exploits that require a computer and technical skills to implement. However, some of the most damaging attacks we have seen and heard of do not involve technology at all. So-called social engineering uses human-to-human trickery and misdirection to gain unauthorized access to data. This book can only protect you at the level of bits and bytes—it will not protect you from social attacks that circumvent those bits and bytes entirely. Educate yourself about common social engineering tactics (see *Hacking Exposed, Third Edition*, Chapter 14), and educate your organization through security policy (see next).

**Develop a Security Policy, Get Management Buy-In, and Distribute Widely** The classic security textbooks describe policy development as the first step in a comprehensive program of information system security. By the end of this book, you will have an excellent idea of what a Windows 2000 system security policy might look like, but there are many other elements to a corporate security policy. We strongly recommend that you consider your organization’s unique technology posture and develop at least a minimal policy before embarking on the point fixes detailed in this book. We have listed some references for good policy development at the end of this chapter, including RFCs 2196 and 2504, the Site Security Handbook and User Security Handbook, respectively; and *Information Security Policies Made Easy* by Charles Cresson Woods.

Also critical to the security policy development process is getting management buy-in. A policy without teeth is almost as bad as none at all.

**Perform Real-World Risk Assessment** Don’t let paranoia disrupt business goals (and vice-versa!). Many of the specific recommendations we make in this book are fairly restrictive. That’s our nature—we’ve seen the damage less restrictive policies can do. However, they are still just recommendations. We recognize the technical and political realities you will face in attempting to implement these recommendations. The goal of this book is to arm you with the right information to make a persuasive case for the more restrictive stance, knowing that you may not win all the arguments. Pick your battles, and win the ones that matter.

**Learn Your Platforms and Applications Better than the Enemy** This book is designed to convey a holistic view of Windows 2000 security, not just a “script-kiddie” checklist of configuration settings that will render you bulletproof. We hope that by the end of the book you will have a greater appreciation of the Windows 2000 security architecture, where it breaks down, and best practices to mitigate the risk when it does. We also hope these practices will prove timeless and will prepare you for whatever is coming down the pike in the next version of Windows (see Chapter 17) as well as from the hacking community.
SUMMARY
By following the best practices outlined in this chapter, you will have laid a solid foundation for information system security in your organization. For the rest of this book, we will move on to the specifics of Windows 2000 and the unique challenges it presents to those who wish to keep it secure.

REFERENCES AND FURTHER READING

<table>
<thead>
<tr>
<th>Reference</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commercial Tools</strong></td>
<td>ISBN: 1881585069</td>
</tr>
<tr>
<td><strong>General References</strong></td>
<td><strong><a href="http://www.faqs.org">http://www.faqs.org</a></strong></td>
</tr>
</tbody>
</table>