Global Information Assurance Certification Paper

Defense in Depth…Including the Desktop PC

By J. Cameli

GIAC Security Essentials Certification (GSEC)

Practical Assignment

Version 1.4

I. Introduction

In the world of information systems security, defense in depth is a strategy utilizing multiple layers of security for the prevention of unauthorized access to critical systems. The purpose behind layering is to insure that a break down of any individual layer will not result in a breakdown of the entire security infrastructure. Ideally, each layer makes it increasingly more difficult for an attacker or unauthorized user to successfully access or compromise critical information systems. A successful defense in depth strategy will provide enough obstacles to either repel or discourage attempts to compromise a system or systems, and the information they may contain.

The goal of this paper is to identify vulnerabilities associated with Windows 9x and NT/2K desktop PC's, highlight the risks associated with these vulnerabilities, and propose methods for security professionals to include them in their defense in depth plans. I often refer to the desktop PC as the personal server when discussing them in terms of security. I use the term personal server, because functions once reserved for a secured network server, are now routinely performed by these devices. The desktop PC, originally used as a stand-alone word processor or simple spreadsheet/database tool, has evolved into a multi-functional networked device. Internet protocols such as http(web), smtp(mail), ftp(data transfer), telnet(terminal emulation), etc. are all regularly used by these devices to send, receive, access and store critical or sensitive data inside and outside of the company. This paper will rely on two basic principals as its foundation. First, people, policies, and practice are the three necessary ingredients to successfully create a defense in depth plan for the desktop PC. Second, there is no silver bullet for the security of desktop PC's. Ultimately, if there is enough time and effort, any desktop PC can be compromised. Does this mean we should give up….of course not! Security should not always be defined in absolute terms. Systems security within the desktop environment is about staying "one step ahead of the threats". A good defense in depth plan will

assume there will be breakdowns within its layers, account for them, and plan to minimize their impact. The key to overall success is limiting the damage created by the breakdown of any given layer. Although this paper will only be focusing on the Windows environment (9x, NT, & W2K), the general policies and practices will be applicable to all desktop environments.

II. Identifying Threats and Risks

According to the 2002 FBI/CSI Computer Crime Security Survey, 90 percent of companies surveyed detected computer security breaches within the last 12 months (1). This same survey also determined approximately 35 percent of all computer crimes are conducted by company insiders with access to corporate information (insider threats). Additionally, an article posted on www.vnunet.com, a UK based technology news site, contained the following quote, further defining the internal threat "The internal threat is essentially a people problem." he said. "People are naturally curious, and if they know confidential information is stored on the network, some of them are going to try to access it"(2). I reference this quote because I believe it highlights two key issues regarding desktop PC's, and the risks they present. First, people are naturally curious, and over time will "probe" the environment that surrounds them. Second, a desktop PC can often times provide as much incentive to exploit as a critical server. When you consider the sheer number of desktops present in a typical business organization, the opportunities for exploitation from within are tremendous.

Combine opportunity, along with the fact that most organizations will not utilize intrusion detection systems, firewalls, or even router access control lists to protect against the "probing" of desktop PC's, and you create the need for defense in depth. Although physically compromising the desktop PC may be the easiest way to exploit it, the more likely scenario in today's world of "hackers" and "attackers" is over the network. With the proper knowledge, network connectivity, and time, accessing information from desktop PC's can be relatively easy. Most individuals will choose to use this approach because there is such a minimal amount of risk when it comes to getting caught. An individual in most organizations can be routinely accessing PC's across the entire organization, completely undetected, while sitting at their desktop. The information to be obtained from the hard drives of desktop PC's can sometimes be unimaginable. How confident are you that your CFO doesn't keep copies of any sensitive financial data on his hard drive? How about your Legal department staff members and the confidential contracts or negotiations they may be working on? The scenarios can go on and on, but the point is very clear. Ultimately, can you ever completely stop this activity from occurring…perhaps not. The following sections will walk identify the various risks to be considered, while at the same time present ways of creating layers to minimize or eliminate these risks.

The first step towards developing a defense a defense in depth strategy for a desktop environment begins with understanding your general business practices, and the risks they may be creating. Below is a list of some common desktop practices, along with their associated risks.

Common Desktop Practices, and the Risks They Present

Practice => Desktop PC's are on a shared network.
Risk => Most desktop networks do not actively prohibit desktop "probing", similar to the way ACL's or Firewalls/DMZ's are designed to prevent access to or probing of critical servers/hosts. Therefore, discovery (clicking on network neighborhood, ping probing, netbios enumeration, etc.), and attempts to authenticate to the PC can all be risks associated with sharing an open network.

Practice => Desktop PC's are configured with file and print sharing enabled. Departments will create PC's with this feature, believing only their areas will access or share the information contained within the shares.
Risk => Similar to the previous example, this practice can lead to either non-password protected shares which are accessible to any desktop PC over the network, or unpatched systems which enable an individual to "crack" the password protected shares.

Practice => NT/W2K workstations are configured with administrative rights assigned to general user ID's.
Risk => Administrative rights provide the user with administrative privileges. As a result of these privileges, users could escalate their access or rights elsewhere within the organization. Additionally, the ability to obtain an administrative password on one system, will often times result in a "common" password shared across multiple systems, due to poor password practices.

Practice => Password rules minimal, rarely enforced, or non-existent.
Risk => Poor passwords can provide unauthorized access either physically or via the network to desktop PC's.

Practice => Critical or sensitive information is stored on the desktop PC, rather than a secured and monitored network server.
Risk => This critical or sensitive information can be accessed in an unauthorized manner via the desktop without anyone ever even knowing it.

III. Creating Layers of Security

Each of the risks identified as a result of common desktop PC practices can be minimized or eliminated through the creation of secured "layers". I've identified (3) separate layers, representing the foundation for a defense in depth plan for a desktop environment. Layers 1 & 2 involve people, policies, and the need for awareness and ongoing education. Layer 3 will cover specific security configurations available for the Windows 9x, NT, or W2K desktop PC. Although organizations may choose to implement these layers in different ways, the key is

to implement all three in some manner. An increase in the number of security layers between an asset and its threats will result in the direct decrease of its overall exposure.

Layer 1 => User Awareness

User awareness within a company is not only essential, but also what I consider to be the first layer of a defense in depth plan for desktop PC's. In order for this layer to be successful, the user community must be actively involved in the security program and its goals for the security of desktop PC's. It is therefore critical for any user awareness program to develop and foster a security mindset within an organization. As simple and obvious as it might seem, the best security practices are often plain old common sense. The challenge for any user awareness effort is helping people to understand that biometrics, 200 character passwords, or even DNA code checks are not the only ways of creating a secure desktop environment. Understanding the reasons for following practices such as only storing sensitive data on "secured" servers, rather than desktop PC's can also help to eliminate potential risks. It is a combination of technology and people that ultimately creates a successful defense in depth security program.

Below are some examples of how an effective user awareness program can be accomplished within an organization:

- **Maintain regular communications with the user community**

Consider multiple ways of communicating with the user community in an effort to develop and maintain user awareness. A web site regularly updated listing important security information/tips, company security policies, security group contacts, and other awareness material can be an effective tool. Sending out company wide Emails informing employees of secure practices, new policies, policy changes, etc. can also help to raise overall user awareness. Additionally, make sure the security team interacts with and "listens" to the user community. Although they may not always support what the employee raises as an issue with your security policies, providing them with an audience can often times bridge the gaps that may exist. Many employees simply want to feel as though their opinion or concerns were considered when a security policy was created. Be approachable, listen to individuals, and respond with well thought out explanations. These are all a big part of successfully creating user awareness and support.

- **Be proactive regarding security awareness.**

A key approach towards success with security awareness is the ability to do so in a timely manner. In other words, don't warn users of a new security policy 90 days after it's been implemented. Also, don't prohibit the use of tools such as instant messaging, without first explaining the risks it may be presenting to the company as a whole (citing current examples of published exploits for example). Additionally, don't discipline users for violations of security policies

created six months ago, but never "publicized" to the user community. In order to be proactive, you must always be on the "offensive". Making sure the security group has diligently notified users of new or modified security policies not only prevents Employee Relations involvement (where the claim is "I had no knowledge"), but more importantly is in the best interest of company security. Subscribing to security news sites such as CERT, SANS, BUGTRAQ, etc. not only helps you as a security professional stay on top of the big picture, but also demonstrates to the user community your groups overall knowledge of systems security. Bottom line, it's critical to be able to notify users of the risks they may be facing in a proactive fashion. Successful security plans should never utilize a "wait and see" approach.

Below is a list of some sample "topics" which might be distributed to corporate users as an overall awareness effort:

1. Password management – How to choose "strong" passwords, which are still easy to remember.
2. Data storage – What type of data/information can or cannot be stored on a desktop PC.
3. Data destruction – Guidelines for data destruction i.e. sensitive data may require more than simply deleting. It may require the use of a "wiping" utility which eliminates the ability for either hardware or software recovery. Awareness memos reminding people to "empty the recycle bin" after deleting information. (perform some random checks on your employee recycle bins…you'd be shocked at some of the information which remains in this directory, still retrievable by anyone with access)
4. Opening Email attachments – Guidelines reminding people of the danger attachments can now pose from a virus perspective. "Think before you click".
5. Virus Updates - Notify users of the latest "hoaxes" or legitimate viruses in the wild. Perception is the key to success with your users….if you can effectively and efficiently inform them of these situations, they will be much more responsive.

Layer 2 => Acceptable Use Policies

Along with user awareness, companies need to develop specific policies to reinforce and define acceptable uses of the desktop PC. The policies themselves need to identify and encourage user behavior that enhances overall security, and discourage/prohibit behavior that might reduce it. These polices should ultimately help users understand what it is they need to protect, as well as their respective role.

Some security features can be built within the operating system itself, making it possible to enforce secure behavior for the user. In the absence of such features, layers 1 (awareness) & 2 (policies) become the alternative towards securing the desktop environment through user behavior and practice.

The following steps should be considered when developing acceptable use policies for workstations within your organization:

1. Obtain senior management support for the development and deployment of acceptable use policies.
2. Designate an area within the company having responsibility for the development, maintenance, and enforcement of the policies.
3. Develop these policies by including key stakeholders in the process (i.e. make sure your not creating policies within a vacuum. Understand how policies may affect the business, as well as who they will affect.)
4. Distribute and explain the policies to all users. (formal training may be a consideration in some organizations)
5. Monitor and change these policies as your business or technologies change.

Below is a sample list of considerations for items to be included in a single policy or separate acceptable use policies for workstations.

1. User ID and Password management/use. (e.g. users shall not logon to a workstation with another users ID & Password, password configuration schemes, etc.)
2. Software(s) the user may or may not install/remove/modify (e.g. pre-installed virus protection software).
3. Network services the user may or may not use (e.g. instant messaging).
4. Information users may or may not transmit across the network, or over the Internet.
5. Acceptable methods of transmission for data transferred over the network or Internet (e.g. FTP vs. IPSEC, SSH, etc.)
6. Information users may or may not store on their hard disk.
7. Encryption requirements for information which might require storage on a desktop PC.

Layer 3 => Password Management & Windows System Configurations

The first two layers described in this paper have involved people, their practices, and policies. Layer 3 will address methods of securing a desktop through system configurations, as well as guidelines and information regarding good password practices. In order to make this section easier to follow I will break it down into two sections, Windows 9x, and NT/2K systems.

IV. Windows 9x

In general, it is commonly understood that Windows 9x systems are not very secure operating systems. As a result, proper password management, proper security patch installation, and general practices become the keys for creating layers of security for a Windows 9x operating system.

Passwords

All Windows 9x machines have various passwords which can be implemented on the desktop. Below is a discussion of the risks associated with the various types of passwords, followed by a list of possible solutions to address these risks.

Risks=>

- Login Password =>Windows 9x caches passwords using weak encryption stored in .PWL files. As a result, anyone with direct physical access to a Windows 9x workstation, or who can access the file system over the network, may be able to retrieve these files and decrypt them. Additionally, realize that the login prompt for a Windows 9x machine can always be bypassed by simply rebooting. The Windows 9x password only controls which user profile is active. Once a system is rebooted, and the Windows password button "canceled", access to the system resources is available.

- Screen Saver Password => Windows screen saver passwords are stored in the registry, also using weak encryption. Again, anyone with either physical or network access to the workstation may be able to retrieve and decrypt these passwords.

- Power On password => If someone has the opportunity to remove the cover of a PC, removing/replacing the battery, and moving the jumper on the motherboard, will "reset the cmos" resetting the password. If PC's are easily accessible in unsupervised areas, this can be a legitimate threat.

- File and Print Sharing => Another feature commonly used within the Windows 9x environment is file and printer sharing - a feature requiring utilization of NetBIOS. In general, this feature is enabled for the purpose of making desktop files available over the network to specific individuals. Unfortunately, any user who happens to be on the same subnet, or segment of the network can also potentially access these shares by simply clicking on their Network Neighborhood. There are two problems generally associated with file sharing; failure to password protect the shares, and 9x machines which have not had the latest patches applied to them, resulting in the ability to "crack" password protected shares (referred to as the "Share-Level Password" vulnerability). Either one of these problems will expose a desktop to the risk identified above concerning the Network Neighborhood concept.

Solutions=> In order to successfully create layers of security within a Windows 9x machine, a combination of "practice", and systems configuration is necessary to successfully combat many of the risks identified above.

General Practices

- Use strong passwords….sure they can potentially be obtained, but make an attacker work for it. In general, "time" can be a strong deterrent for an attacker. If they can't guess or obtain it easily, they're more likely to move on.

- Passwords should be at least 7 characters long, and contain at least (3) of the following:

1. Upper case
2. Lower case

3. Numeric
4. Special character (e.g. @, #, !, +,=, etc.)

Additionally, passwords should be changed on a regular basis (45-60 days), and should not contain "common dictionary words".
(*Note: Case sensitivity within the NT operating system is only important from the perspective of someone actually typing in the password. The issues created by the NT LM (Lan Manager) password scheme will be discussed later in the NT/2K section)

- Separate windows PC passwords from Novell or other systems passwords. A common practice for many individuals is to use the same password for all of their systems access. By understanding that a Windows PC may be compromised, it's important the user does not provide a clear path into all systems or critical information. This practice might create a layer between a desktop PC file system, a Novell file system for example.

- Separate screen saver passwords from desktop passwords. Although they both can potentially be obtained, the key here again is layers…..make an attacker work to gain complete access. (note – although this may seem trivial based upon the fact you only need one or the other(as mentioned as mentioned earlier) the real risk created by the practice of using the same password across all systems. Therefore, all the attacker may need to do is obtain one, and they may have them all.

- Don't store sensitive data on a Windows 9x PC. It's simply too easy to compromise these machines. Store sensitive/critical information on a secured server. If sensitive data must be stored on a Windows 9x machine, do some research and purchase a trusted 3rd party encryption software package.

Systems Modifications

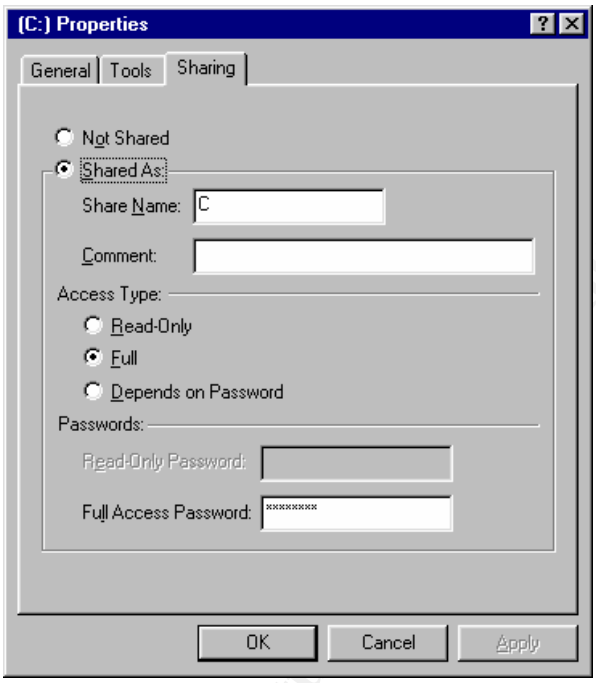
- Disable file and print sharing…make the attacker access the PC physically. This alone may deter the attacker, and make him move elsewhere. If file and print sharing is required for some business reason, apply all appropriate Windows patches to the machine, and use "strong" passwords (see above).

"Share-Level Password" Vulnerability:
Details explaining the Share-Level Password vulnerability are available at
http://www.securityfriday.com/ToolDownload/SPC/spc_002.html

There are two options available for addressing the File Sharing vulnerabilities associated with Windows 9x. If file sharing is absolutely required within your environment, you can enable a strong password for the share(s), assuming you've also applied the appropriate patches (3). By doing this, you can "allow" only those individuals who've been provided the password access to the specific shares over the network (it's critical to note the need for a "strong"

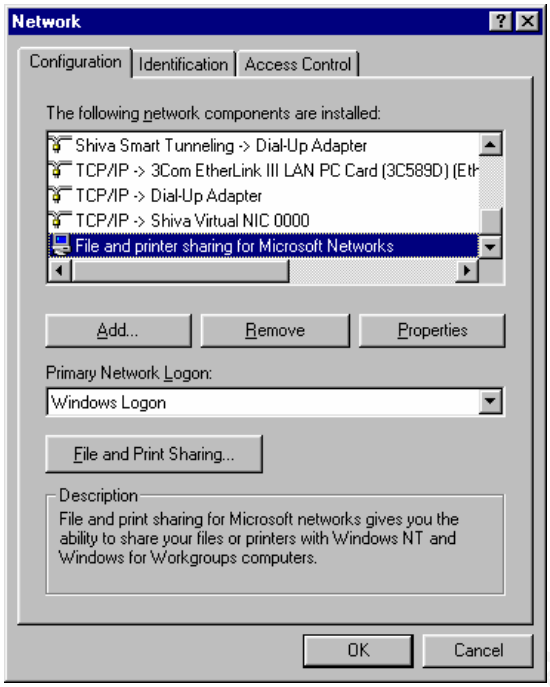
password, since shares are always be exposed to a potential “brute force” attack against the password). To do so, follow the instructions below.

Option 1 – Password Protecting the Share
Double click on “My Computer” =>Right click on the drive you are “sharing”, for example the “C” drive



You will find a tab titled “Sharing”, which enables you to dictate access type, as well as password. This, combined with the proper Microsoft patch should prevent unauthorized users from accessing the share.

Option 2 – Removing Print Sharing
Go to Start =>Control Panel =>Network



Clicking on the “Remove” button will remove File and Print Sharing entirely. Clicking on the “File and Print Sharing” button below “Primary Network Logon” results in the following screen:

This screen allows you to “disable” File and Print Sharing, without permanently removing it.

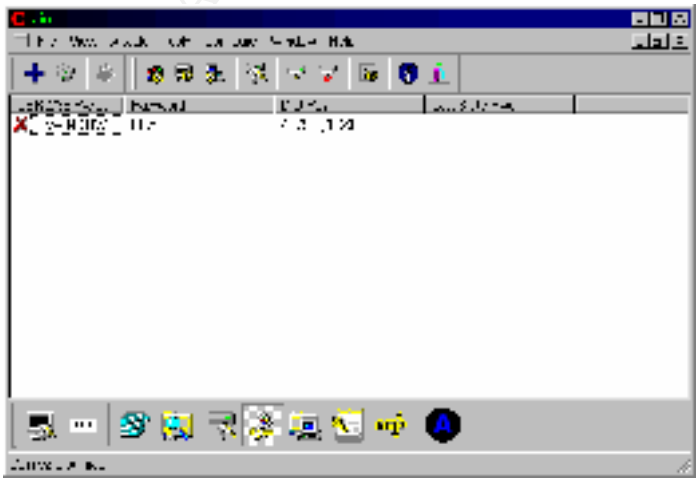
Disable password caching =>
If sensitive data is going to be routinely stored on Windows 9x PC’s, an administrator may want to consider creating/setting the following DWORD Registry Key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching = 1

Examples of exploits for a Windows 9x machine:

Several freeware tools are available on the Internet, which demonstrate how easy it is to circumvent passwords as discussed previously on the Windows 9x machines. As a result, it can be a challenge to effectively "secure" a Windows 9x machine. As a result, the security risks these machines may present, must be considered when determining how a Windows 9x desktop fits within your particular business environment as far as use, practices, etc. Below are some examples (screen shots)of several freeware tools available on the Internet, which demonstrate the various vulnerabilities identified previously with Windows 9x machines.

CAIN 2.0 => A freeware tool available on the Internet, which demonstrates how easy it is to obtain windows 9x user, screen saver, and share passwords when physical access to a desktop is available:

Results of choosing Attack=>PWL files for a Windows 9x machine (User name intentionally hidden) Password = **CHAP**



Results from choosing Attack => Screen Saver Password = **WEAK**

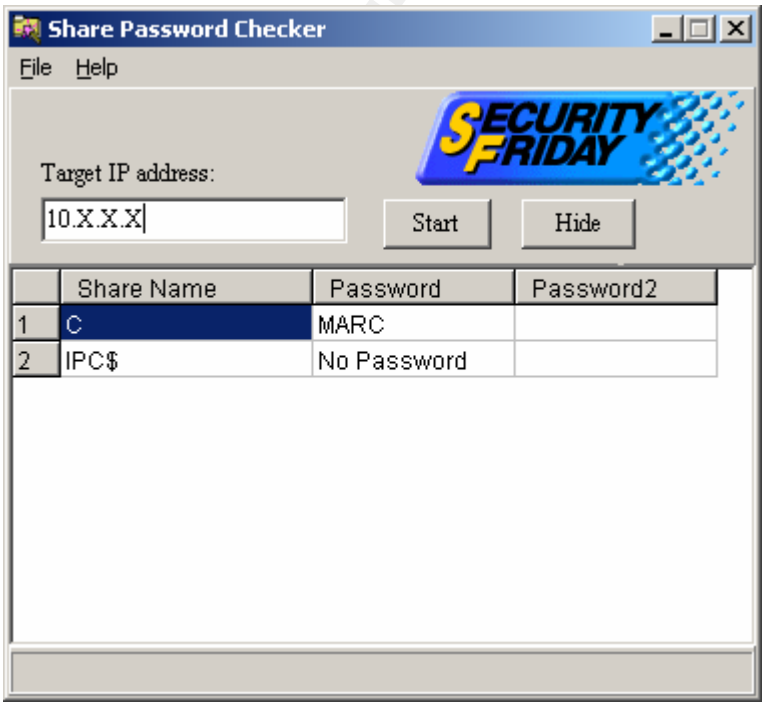
Cain 2.0 is available at:
http://online.securityfocus.com/data/tools/cain20.exe

95Sscrk => Another freeware tool which can crack the screen saver password when physical access to a desktop PC is possible

```
A:\95SSCRK>95sscrk
Win95 Screen Saver Password Cracker v1.1 - Coded by Nobody (nobody@engelska.se)
(c) Copyrite 1997 Burnt Toad/AK Enterprises - read 95SSCRK.TXT before usage!
---------------------------------------------------------------------
· No filename in command line, using default! (C:\WINDOWS\USER.DAT)
· Raw registry file detected, ripping out strings...
· Scanning strings for password key...
» Found password data! Decrypting ... Password is SIMPLE!
_ Cracking complete! Enjoy the passwords!
---------------------------------------------------------------------
```

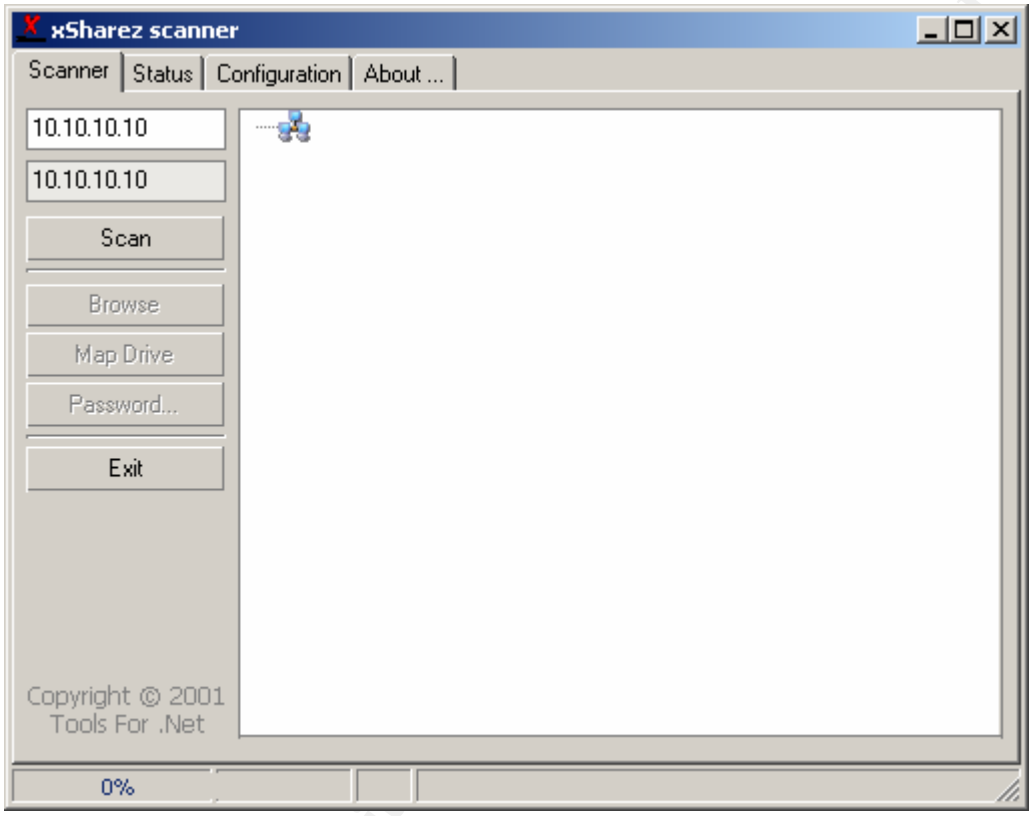
95Sscrk is available at:
http://packetstormsecurity.nl/Exploit_Code_Archive/95sscrk.zip

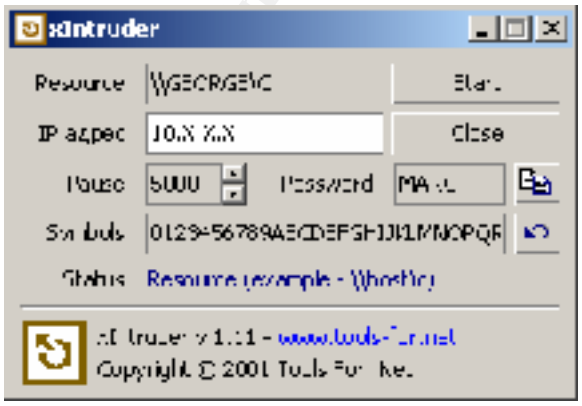
Share Password Cracker => A freeware tool which can remotely access a Windows 9x machine, and determine a) if it has been patched properly, or b) crack the password of a share if the patch has not been properly applied.



Share Password Cracker is available at:
http://www.securityfriday.com

Xsharez & Xintruder => (2) freeware tools which (Xsharez) can efficiently scan 255 addresses (or more if an upgrade is purchased), identify shares available, and (Xintruder) attempt to crack the shares if the systems are not patched properly. (These screens have been intentionally left vague)





Xsharez and Xintruder are both available at:
http://www.tools-for.net

Summary for Windows 9x desktops

- Security will be much more successful when it is implemented in layers. The Windows 9x systems are a perfect example of this. Although almost impossible to secure 100%, following the practices and systems configurations listed above, should raise the level of difficulty for anyone trying to access these systems in an unauthorized manner.
- Consider the limitations and challenges with regards to security when choosing to use a Windows 9x machine. If your organization can limit the access these types of desktops may have (i.e. critical servers, Internet, etc), as well as prevent users from storing critical information on hard drives, and rather secured servers (such as a Novell server), these may be suitable for your environment.
- Although measures can be taken to minimize the risks inherent with File and Print Sharing, and password caching for Windows 9x, administrators should recognize this OS is inherently weaker than its cousins NT & W2K.

V. Windows NT/W2K

NT has withstood years of criticism from the hacking community, even though when configured properly it can be significantly more secure than the 9x systems. Although Microsoft has patched most of the problems identified within the NT system, I believe it continues to be an area of risk because of poor configurations. In general, most security administrators will either fail to take advantage of security configuration options available with NT or W2K for the desktop PC, as well as fail to stay current with released patches and service packs. In other words, although this system can be configured in a secure manner, most organizations still fail to "lock it down". There are a large number of topics to cover when discussing security options for the NT and W2K desktop PC's. This paper will choose to focus on a few key areas, which if ignored can potentially eliminate the effectiveness of all other security options.

- **Apply Latest Service Packs and Patches**

Simple and short……..As basic as this concept may sound, it is often times simply overlooked. One of the biggest reasons Microsoft will release patches and service packs is to address identified security issues. Often times, vulnerabilities will exist at the kernel level, and there is no other recourse for addressing them other than through a patch or service pack. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp

- **File and Print Sharing**

Excluding the 'Share-Level Password" vulnerability identified for the windows 9x systems, the risks remain the same for NT or 2K desktop when utilizing this feature. Often times a gateway to critical or sensitive information

without the user even realizing it, this risk can't be ignored. Therefore, if file and print sharing is necessary, strong passwords must be utilized. In all other cases, it is highly recommended this service be disabled to remove its inherent risks. Procedures for removing file and print sharing for both systems are listed below.

NT
Click Start->Settings->Control Panel
Double-click the Network control panel
Click the Bindings tab
Highlight Server
Click Disable
Click OK

2K
Click Start->Settings->Control Panel
Double-click Network and Dial-up Connections
Right-click Local Area Connections and select Properties
Uncheck File and Print Sharing for Microsoft Networks

Registry Fixes

NetBios Null Enumeration
NT:

Even more dangerous than file and print sharing (primarily due to the lack of knowledge/awareness concerning this risk), is the risk NT & W2K systems face from network probing, enumeration, and ultimately compromise. User and Shares null session enumeration (4) is an exploit any NT system using netbios (port 139 – NT, or port 445 – W2K) can be vulnerable to. Often times overlooked, and most times misunderstood, this particular vulnerability can be the "root" cause for the majority of NT desktop exploits. Windows NT allows anonymous logon users to list user names and enumerate share names. Windows NT 4.0 Service Pack 3 and a hot fix for Windows NT 3.51 provides the ability to restrict these "NULL sessions", thus prohibiting the ability to list account names and enumerate share names. In even simpler terms, if an NT or W2K machine is not configured properly, anyone with network access can attempt to "gather" information from the desktop itself with various freeware tools. Items such as user name, user rights (e.g. Administrator, User, Guest, etc.), User passwords, and even Shares are all very important to an individual trying to exploit a desktop PC. In addition, through the use of these tools, these same machines can be accessed directly over the network without the desktop user ever even knowing.

Although the exploit itself will be demonstrated later in this section, the "fix", which prevents remote users from accessing account names and share names without authentication is identified below:

Add Value type REG_DWORD, name RestrictAnonymous, data field 1 to: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA key.

***Note – This registry change will not actually block anonymous connections, but will prevent most of the information leaks available over a null session (i.e. uset accounts and shares)**

W2K:

Same issues as NT, however WIN2K allows for even tighter controls than NT:

Add Value type REG_DWORD, name RestrictAnonymous, data field 2 to: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA key.

***Note – This registry change will restrict anonymous connections, and only connections to those ID's granted "explicit" permissions.**

Passwords

One of the most overlooked and misunderstood security feature for most systems, I believe passwords present an even bigger challenge within the NT and 2K systems **(5)**. Due to the nature in which NT & 2K passwords are stored on the Windows system, as well as the general approach towards their use from an Administrative standpoint, understanding them completely is critical. I've reference some articles discussing NT and 2K passwords, and therefore will only cover some of the key concepts in this paper.

1. Creating strong passwords in the world of NT & 2K:
   NT and 2K passwords are stored on the machine in NTLM and LM hash forms (LM maintains backward compatibility with Windows 95 & 98). The vulnerabilities associated with the LM password hashes are they are saved in all upper case, and divided into two separate seven character sections. Therefore, and 8 character password is really cracked as two separate passwords, one 7 characters, and the other 1 character. In addition, the password strength itself is diminished because 26 possible characters (entire alphabet in non-caps) are effectively eliminated from use because of the upper case issue mentioned earlier.

Recommendations:

- Use either (7) or (14) character passwords, based upon the storage method of the LM passwords. This will eliminate the risks created by the seven character "section" issue created by LM passwords. Some will argue that it is a fallacy to suggest cracking the last (3) characters of a (10) character password will lend itself to identifying the first (7). I will argue why take the chance of assisting anyone in an attempt to compromise your password.
- Avoid the common password practices of using dictionary words or phrases, phone numbers, addresses, etc. ….perhaps simple, but worth re-stating.

- Avoid taking common dictionary words, and replacing strategic letters with symbols e.g. h3ll0, s!mple, @lways, etc. Most cracking tools will still be able to break these easily.
- Consider introducing "ALT" characters for ID's of a critical nature. Passwords with at least one of these characters will considerably raise the level of difficulty for cracking (just remember they may be harder to remember).
- Consider deploying desktops with passfilt.dll (NT) or a defined security policy for passwords through Microsoft Management Console (MMC for W2K). Either one "forces" compliance with pre-defined password policies.

2. Password practices – Although failure to differentiate "Administrative" ID's from "User" ID's may be acceptable within your environment, due diligence must be applied towards the separation of Admin. ID's and passwords for these systems, vs. other critical systems.

- Problem #1 – **Administrative rights are provided to the user ID. =>** NT & 2K passwords are stored within the SAM file on the PC itself, accessible only with administrative rights to the machine itself. Therefore, the SAM file can be obtained (in a variety of ways..some to be mentioned later in this section), by any ID with administrative rights on the device. Therefore, it's important for any administrator deploying NT or 2K desktops with user ID's having administrative rights to recognize this risk. Any user with administrative rights on their desktop PC can attempt to crack the SAM file, thus obtaining the password for the Administrator ID on the same device.

- Problem #2 – **The "Administrator" ID on the NT/2K desktop, is "universal". =>**
  Based upon what was described in problem #1, imagine the risks which can be created in an environment where all desktop PC's have a universal "administrator ID present on them. Once the administrator ID's password is cracked, the individual has access to every desktop within the organization containing this same user ID and password.

- Problem # 3 – **Administrator's use the same password on their NT/2K desktop, as they do for other critical systems/servers. =>**
  Administrators will often times have access to a large number of systems, many of them considered critical or sensitive. Unfortunately, many of these same administrators will take shortcuts when it comes to due diligence regarding proper password management. As a result, many of these individuals will use the same password for their desktop PC, as they might use for a very critical server or system. Following the flow of problems #1 & #2, it should now be very apparent as to the risks created by following this practice. A poorly thought out password strategy for the use of

administrative passwords in a corporate environment could ultimately lead to the compromise of any/all systems.

- Solution #1 – If possible within the organization, limit the number of users with administrative rights on NT/2K desktops.

- Solution #2 – Create separate and unique passwords for the Administrator ID's used across departments within the organization. This practice prevents the use of any "cracked" administrator ID across all desktops (a virtual firewall effect).

- Solution #3 – Promote the non-use of "shared" passwords within the systems administration area. Bottom line….systems administrators need to understand the risks associated with using the same password for all of their system access….you get one, you've got them all!

I've only covered a few concepts in this section, but I believe each of them represents a critical layer of defense, required for the success of securing an NT/2K desktop. Other security options available such as EFS (Encrypting File System), IPSEC, and PASSPROP are examples of additional items systems administrators should study, understand, and implement if appropriate.

Below is a sample of how a poorly configured NT or W2K desktop could be compromised over the network from a common desktop. I chose this particular example, because I believe it highlights the need for the "key" layers of defense highlighted previously for the NT/W2K desktops.

Step 1 – Browsing the neighborhood…..whether it's the "network neighborhood", or using some type of scanning tool, identifying desktop PC's over the network is fairly easy for anyone to do. The key to this particular practice, is what can be discovered once a particular workstation is identified……

How easy is it to find a user ID with administrative rights and a "weak" password on an NT/W2K workstation?
Using a freeware tool such as NBTDump or NBT Enum (6) anyone can exploit an unpatched and poorly configured system through "null enumeration" over the network.

```
C:\nbtdump 10.10.10.10

Results are written to 10.10.10.10.html.
Connecting to \\10.10.10.10...Connected.
Retrieving share information...
Retrieving account list...
Checking passwords on accounts...

C:\NBTDump>
```

Results =>

NetBIOS

Share Information

Share Name :ADMIN$
Share Type :Default Disk Share
Comment:Remote Admin

Share Name :IPC$
Share Type :Default Pipe Share
Comment:Remote IPC

WARNING - Null session can be established to \\10.10.10.10\IPC$

Share Name :C$
Share Type :Default Disk Share
Comment:Default share

Share Name :D$
Share Type :Default Disk Share
Comment:Default share

Account Information
Account Name :Administrator
The Administrator account is an ADMINISTRATOR, and the password was changed 215 days ago. This account has been used 0 times to logon.

Comment :Built-in account for administering the computer/domain
User Comment :
Full name :

Account Name :JonesD
The JonesD account is an ADMINISTRATOR, and the password was changed 331 days ago. This account has been used 1 times to logon.

Comment :
User Comment :
Full name :D Jones

WARNING JonesD's password is blank

There it is, and it didn't even require me to "guess" the password. Depending on the size of your organization, the methods utilized to force the use of "strong passwords", this may or may not be a likely scenario in your environment.

Step 2 – Once you've identified a user ID with Admin. Rights and discovered the password…the rest is "history"…

Using the “net use” command available on any NT/2K system, we can remotely authenticate with administrative rights to the desktop now that we have a valid user ID and password.

```
C:\>net use \\10.10.10.10\ipc$ /user:JonesD
The password or user name is invalid for \\27.25.7.12\ipc$.

Type the password for \\10.10.10.10\ipc$:
The command completed successfully.
```

Once Authenticated, you “own” the system…..

Step 3 – Once you’ve authenticated to the desktop remotely, “grabbing” the SAM file containing all of the password hashes is easy with a tool like PWDump3 (7). PWDump3 will “dump” the password hashes to a text file remotely over the network once a user with administrator rights is authenticated to the desktop. (Note – PWDump2 is also a freeware tool which dumps the password hashes to a test file when run locally on the desktop itself, once administrative rights are obtained). PWDUMP3 will connect to any NT/2K desktop with the ADMIN$ share present, copying the service executable files there. Next, it requests the Service Control Manager to install and run the service program on the desktop. The extracted hash information resulting from the program is stored temporarily within the remote desktop’s registry, later removed along with the service program itself.

```
C:\pwdump3>pwdump3 10.10.10.10 pwdfile.txt

pwdump3 by Phil Staubs, e-business technology
Copyright 2001 e-business technology, Inc.

This program is free software based on pwpump2 by Tony Sabin under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation.  NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM.  Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Completed.
```

Why dump the passwords…..keep reading…..

Step 4 – Now that you have a file containing all of the password hashes (pwdfile.txt), using password cracking tools such as “John the Ripper (freeware) or L0phtCrack (commercial) can be used to get the Administrator ID on the same device. With a little luck (or bad luck depending on which end of the exploit you’re on), your on your way to having an Administrator password(s) which may lead towards escalating privileges and accessing information throughout the entire organization! (remember, one of the most common mistake is individuals using the same password for all their systems access..)

How could this particular exploit have been prevented…through the use of the all layers identified in this paper. Preventing remote null enumeration, differentiating between user and administrative rights, utilizing different passwords for different systems are all layers, and using "strong" passwords are all layers which could have prevented or limited the damage of this attack. Although the scenarios could vary for different types of desktop exploits, one thing remains constant. It is the combination, not the single use of these layers, which results in a secure desktop (a.k.a. defense in depth).

Summary for Windows NT/2K desktops

NT & 2K can be secure operating systems when configured and managed properly. The key to the success of securing these systems relies on the awareness and understanding of the inherent risks associated with ID's with administrative rights, poor password practices, and NetBios Null Enumeration. Just like the 9x systems, much of your security will be dependent upon the proper implementation and enforcement of policies. As demonstrated in the remote exploit example above, a breakdown in the practice of password policies, for example, can lend itself to the breakdown of the entire security infrastructure.

VI. Conclusion

The success of any defense in depth plan is directly impacted by the effectiveness of the layers implemented within the strategy itself. Although each layer may be independent of other layers, together they must all work towards achieving the goal of corporate systems security. Understanding the risk desktop PC's can create towards compromising a corporate defense in depth plan is critical. This paper identified several layers to focus on for addressing the risks associated with Windows desktop PC's; user awareness, policies, practices, and desktop configurations. The key to maintaining these layers is remembering the following… ***secure configurations are dynamic, not static***. Each of the layers presented in this paper are currently valid…how will they change six months from now, who knows? Therefore, the same time and energy dedicated to identify and implement these layers will require the same amount of energy to keep them valid. Security is an ongoing practice and approach, it's not a single act or action. In order to stay secure in any environment, systems administrators must be aware, proactive, diligent, and never satisfied with yesterday's success. The desktop PC should not be overlooked when planning for overall systems or data security. This "system" has evolved to the point where it must be considered and accounted for in any overall corporate defense in depth plan.

References

(1) "Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row" CSI Institute (April 7, 2002)
http://www.gocsi.com/press/20020407.html

(2) "Employees worse than hackers" By Nick Farrell [March 28, 2002]
http://www.vnunet.com/News/1129574

(3) Microsoft Patches available on Microsoft Web Site:
http://www.microsoft.com/technet/security/bulletin/ms00-072.asp

Win 95 – 273991USA5.EXE
Win 98 – 273991USA8.EXE

(4) "Restrict Anonymous: Enumeration and the Null User"
by Timothy M. Mullen
last updated Feb. 12, 2001
http://online.securityfocus.com/infocus/1352

"Restricting Information Available to Anonymous Logon Users"
Microsoft Knowledge Database
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q143474

"PROTOCOL STANDARD FOR A NetBIOS SERVICE RFC 1001"
http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1001.html

(5) "LANMAN Password Hash Storage"
http://geodsoft.com/howto/password/nt_password_hashes.htm

"How to Make Windows 2000 and NT 4 Passwords Uncrackable"
Review Date: January 3, 2001
Reviewer: Joel Kleppinger
http://sysopt.earthweb.com/articles/win2kpass/

"Confused yet about NT passwords? Try the 7-14 rule; those numbers work better than most" Stuart McClure & Joel Scambray (November 22, 1999)
http://www.infoworld.com/articles/op/xml/99/11/22/991122opsecwatch.xml

(6) NBTDump Tool
http://www.atstake.com/research/tools/index.html#info_gathering

NBTEnum Tool
http://ntsleuth.0catch.com/

(7) PWDump3
http://packetstormsecurity.org/Crackers/NT/pwdump3.zip

"Develop and promulgate an acceptable use policy for workstations"
http://www.cert.org/security-improvement/practices/p034.html

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event