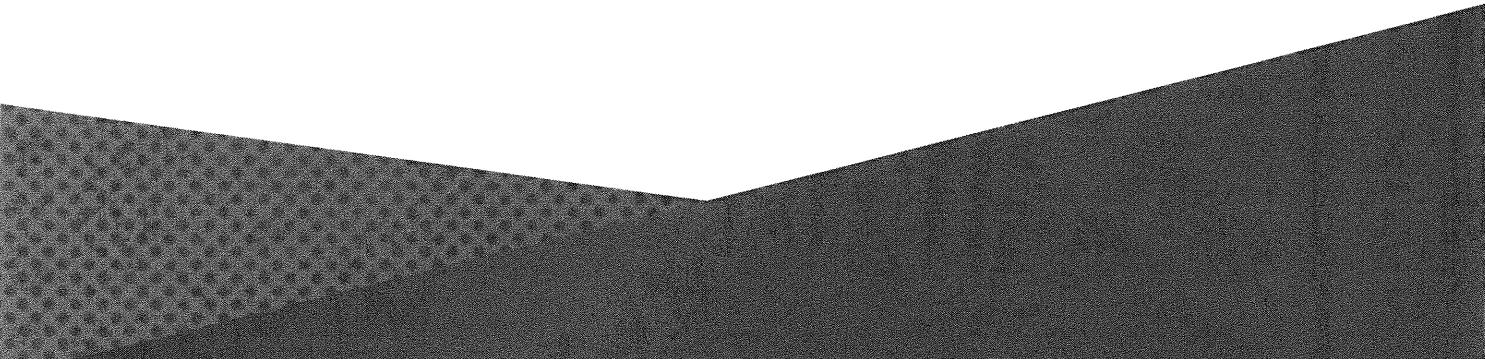


# 401.5

# Windows Security



SANS

Copyright © 2016, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND THE SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, the SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by the SANS Institute to the User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO THE SANS INSTITUTE, AND THAT THE SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND), SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to the SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of the SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of the SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

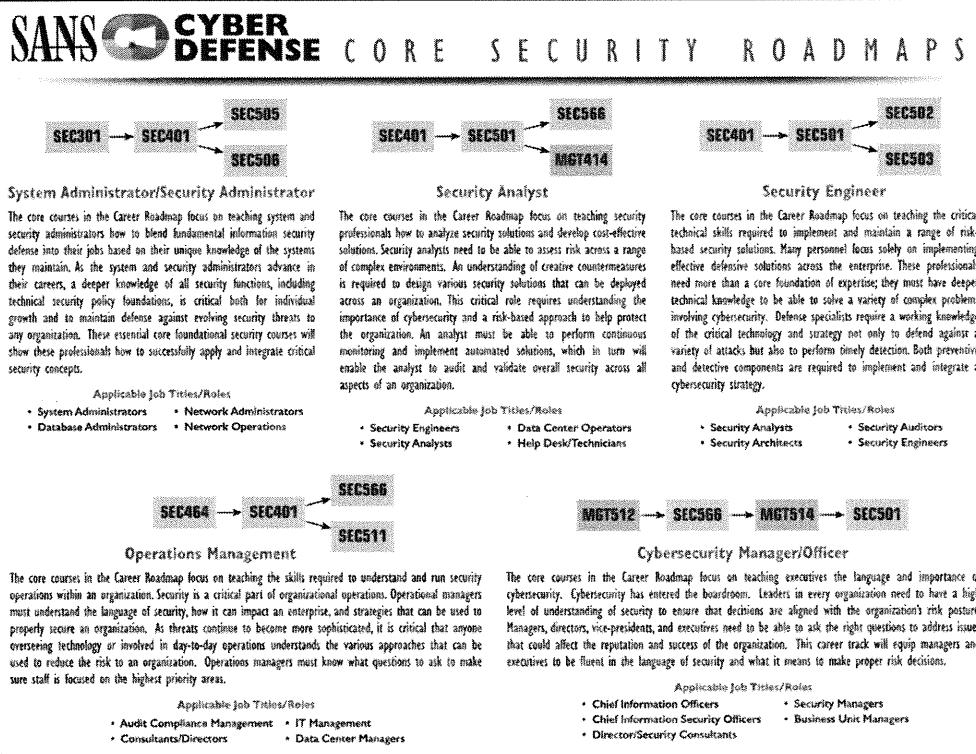
Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

# **SECURITY 401**

## **SANS Security Essentials**

SANS Security Essentials – © 2016 SANS

This page intentionally left blank.



This page intentionally left blank.

# SANS CYBER DEFENSE SPECIALIZED ROADMAPS

**SEC440 → SEC480 → SEC566**

## Security Architect

The core courses in the Career Roadmap focus on planning, designing, and implementing an effective security solution. In order for security to be effective it must be customized to the unique business, mission, and risks an organization faces. The security strategist must be able to identify core metrics and use them to design and oversee the implementation of a security system and network architecture. Having a secure robust network architecture is critical for an organization to have effective security.

### Applicable Job Titles/Roles

- Security Managers      • System Architects
- Data Center Analysts    • Design Engineers

**SEC501 → SEC511 → SEC503 → FOR572**

## Security Operations Center (SOC) Analyst

The core courses in the Career Roadmap focus on building, running, and deploying a SOC. Security has become critical for the success of an organization constantly under attack. Defense against the vast array of threats requires continuous monitoring of the network and assessment of the security infrastructure. Properly trained people who can detect and respond to attacks are critical to the overall success and security of an organization.

### Applicable Job Titles/Roles

- Security Consultants    • Security Operations Supervisors
- SOC Managers           • Security Operations Directors

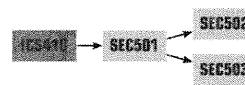
**MGT415 → SEC366 → AUD507 → SEC511**

## Security Risk Officer

The core courses in the Career Roadmap focus on assessing and analyzing risk and using that information to guide the priorities for security. In order for organizations to be successful in security, they must take a risk-based approach. Risk allows an organization to identify the vulnerabilities that have the biggest impact, based on the threats that have the highest likelihood of success, and which are most linked to the organization's critical assets. Proper metrics that map back to risk are used to assess and verify that an organization's security program is focused on the correct areas.

### Applicable Job Titles/Roles

- Risk Engineers           • System Managers
- Risk Officers            • Auditors

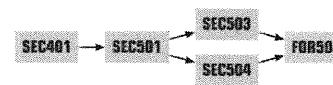


## Industrial Control Systems (ICS) Analyst

The core courses in the Career Roadmap focus on teaching how to assess, implement, and secure ICS. Anyone who works in critical infrastructure needs to understand the associated threats and methods for security and the proper ways to protect systems that support a variety of ICS environments. ICS represent unique challenges not only in terms of threats, but also in terms of the unique methods that must be used to reduce risk to these systems. The focus is on providing an appropriate level of security based on the security challenges that these organizations face.

### Applicable Job Titles/Roles

- Control System Engineers    • Control System Managers
- Operational Analysts        • System Administrators



## Intrusion Analyst

The core courses in the Career Roadmap focus on teaching the foundations of security, as well as on the prevention and detection of threats. The most masterful prevention measures may be circumvented by skilled attackers. Successful attacks must be quickly identified to minimize the damage. The focus is on implementing appropriate prevention methods, rapid detection and assessment of malicious activity, and containment of harm in the aftermath of a successful attack.

### Applicable Job Titles/Roles

- System Administrators      • IDS Specialists
- Security Analysts/Specialists    • SOC Engineers
- Intrusion Detection Analysts

This page intentionally left blank.

# Module 23: The Windows Security Infrastructure

---

SANS Security Essentials – © 2016 SANS

## **Module 23: The Windows Security Infrastructure**

This section intentionally left blank.

# The Windows Security Infrastructure

---

## SANS Security Essentials V: Windows Security

SANS Security Essentials – © 2016 SANS

### **The Windows Security Infrastructure**

Remember when Windows was simple? Windows XP desktops in a little workgroup—what could be easier? A lot has changed since then. Now, we have Windows tablets, Azure, Active Directory, PowerShell, Office 365, Hyper-V, Virtual Desktop Infrastructure (VDI), and so on. Microsoft is battling Google, Apple, Amazon.com and other cloud giants for supremacy. The trick is to do it securely, of course.

This module discusses the infrastructure that supports Windows security. This is the big picture overview of the Windows security model, and it provides the background concepts necessary to understand everything else that follows. Because it is the big picture, we can't talk about everything, but many of the details will be filled in throughout the following modules.

Specifically, this module answers the following questions:

- Which Windows operating system should I use?
- What is a workgroup?
- What are local users and groups?
- What is a Security ID (SID) number?
- What is a Security Access Token (SAT)?
- What is Active Directory?
- How do I authenticate to the domain?
- What is a forest or trust?
- What is Group Policy, and why is it so important?

# Windows Family of Products

---

The student will identify the different types of Windows operating systems and the differences between them.

SANS Security Essentials – © 2016 SANS

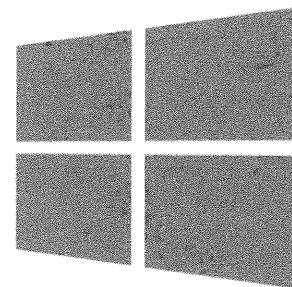
## **Windows Family of Products**

This section intentionally left blank.

# Windows Operating Systems

## Three classes of OS:

- **Client**
- **Server**
- **Embedded**



SANS Security Essentials – © 2016 SANS

### Windows Operating Systems

In general, there are three classes of operating system from Microsoft: Client, Server, and Embedded.

Client operating systems are intended for devices such as phones, tablets, laptops, and PC workstations. Users directly interact with these devices by touch, voice, gesture, keyboard, and mouse. Users often personally own these hardware devices. Client operating systems are designed for ease of use, graphical applications, and backward compatibility. Examples include Windows 7, Windows 8.1, Windows Phone, and Xbox One.

Server operating systems are intended for devices such as rack-mounted computers that often have RAID storage, a lot of memory, and multiple network interfaces. The servers can also be virtual machines (VMs). Users normally interact with these physical or virtual machines over the network, not directly by touch or sight. Server operating systems are designed for web servers, e-mail gateways, VPN gateways, file and printer sharing, VM hosting, domain controllers, DNS, DHCP, and so on. The hardware is usually owned by companies, not end users. Examples include Windows Server 2012 R2 and Windows Hyper-V Server.

Embedded operating systems are intended for devices such as Point of Sale terminals, automobile dashboards, electronic signs, industrial control equipment, robotics, sonogram machines, hand-held laser scanners, welding machines, and all the myriad "Internet of Things" devices. Although the client and server operating systems are general purpose and can be easily repurposed later, the embedded operating systems are usually customized by equipment manufacturers to suit just their hardware. Examples include Windows Embedded 8.1 and Windows Embedded Compact 2013 (for ARM).

Note that these are not completely different products under the hood. They usually share common "core" binaries for their kernels, libraries, and protocol stacks. Microsoft wants to standardize on a single, modular, base OS platform for everything going forward.

# Client Operating Systems

- Windows 2000 Workstation
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows RT
- Windows 10

- Client Editions:**
- **Starter**
  - **Home**
  - **Ultimate**
  - **Business**
  - **Professional**
  - **Enterprise**

SANS Security Essentials – © 2016 SANS

## Client Operating Systems

Microsoft has many client operating systems, extending all the way back to DOS, Windows for Workgroups, Windows 95, and so on (more than can fit in the slide, in fact). Microsoft often experiments with a new kernel or graphical interface by releasing it as a new OS version, and then fixes and polishes that experiment for the next OS release, which is usually more popular; for example, Windows Vista was a flop, but cleaned up nicely. Windows 7 and Windows 8 flopped worse than Vista, and then came Windows 10. So, where are we in that release cycle right now?

## Client Editions

Each client OS is normally released in multiple editions, and it's important for security, manageability, and licensing to install the correct one. Microsoft makes this as confusing as possible. Even the names of the editions can change from one OS version to the next, so you have to research each new release.

In general, though, editions that include words such as Starter or Home are intended for personal use, have fewer features, cannot be joined to an Active Directory domain, and cost less. Editions that include words such as Business, Professional, or Enterprise are intended for business use, have more features, can be joined to a domain, and cost more. The Ultimate editions are aimed at enthusiasts, have more features than the Home editions, can be joined to a domain, and often cost the most.

For example, if you want features such as BitLocker, AppLocker, Kerberos, Group Policy, Encrypting File System, and Active Directory domain membership, you can't use any of the Home editions. In fact, sometimes there are features you'd expect to get in the Business or Professional editions, such as AppLocker, but get only in Enterprise or Ultimate. Not a nice surprise.

## **Platforms**

Some editions of Windows come in both 32-bit (x86) and 64-bit (x64) versions for platforms with Intel/AMD CPUs. However, Microsoft wants to move away from the older 32-bit (x86) platform and support only 64-bit (x64) going forward, at least for traditional laptops and desktop PCs. For the ARM platform, there are special editions of Windows 10 and later, plus the older Windows RT and Windows Phone (which were replaced by the ARM version of Windows 10). Be careful, the Windows for ARM editions do not have the same features and cannot run all the same applications as Windows for x86/x64. Whenever purchasing a Windows tablet, always ask if it has an ARM CPU so that you'll know what you're (not) getting. And avoid Windows RT, that operating system was discontinued when Windows 10 came out.

## **Licensing**

The Starter, Home, Business, Professional, and Ultimate editions are usually purchased and licensed one at a time as either a retail license, which is not bound to a particular piece of hardware and is more expensive, or as an OEM license, which is bound to a particular computer and is less expensive. The Enterprise edition is purchased and licensed as part of an organization-wide agreement between your company and Microsoft, which is sometimes called a site license or a software assurance license, but even these names can change in the future as Microsoft moves toward subscription-based licensing for everything, including for the OS itself. Licensing is important for this course only because some security features are found only in certain editions of Windows. Windows is actually available for free on tablets and phones whose screens are 9 inches or smaller (to compete with Google Android) and also free for the Raspberry Pi.

# End of Support

- Windows XP: April 2014
- Windows Vista: April 2017
- Windows 7: January 2020
- Server 2003 R1/R2: July 2015
- Server 2008 R1/R2: January 2020

SANS Security Essentials – © 2016 SANS

## End of Support

Because of the critical importance of keeping up-to-date with security patches, it's imperative to upgrade an OS *before* it becomes obsolete. This can be expensive and painful, and it might feel totally unfair, but no product lasts forever, not even Windows XP.

Servers tend to be fewer in number and better managed, so upgrading servers is usually not a monumental task. But because of the number of client devices, the need for backward compatibility testing, user training, and other issues, upgrading clients can be more difficult and expensive. Unless your environment is small or uses Virtual Desktop Infrastructure (VDI) technologies, your project planning for a mass client upgrade should begin at least 2 years before the expected end of support.

To see Microsoft's most recent list of end-of-support dates, visit <http://support.microsoft.com/lifecycle/>.

In general, plan to be off a product before End of Mainstream Support and certainly before End of Extended Support. (The dates in the slide are for End of Extended Support.) Here are the essential terms to know:

- **End of Sales:** When the product is no longer sold to retailers or OEMs, but these resellers might stockpile licenses before End of Sales is reached.
- **End of Mainstream Support:** When warranties expire for the product, the product will no longer be improved, free incident support ends, and non-security hotfixes become unavailable unless specifically purchased during the (expensive) Extended Support phase.

- **End of Extended Support:** When security hotfixes and paid support can no longer be purchased, except in special cases with (expensive) Custom Support.
- **End of Custom Support:** When there will be no further hotfix or support options whatsoever, unless they are negotiated with Microsoft. These exceptions are negotiated on a per-product basis with each customer, are not consistently available from one country to the next, and any such exceptions will be rare (and incredibly expensive).

### **Stuck with an Expired Client OS?**

If a computer cannot be upgraded before it expires, then every month it continues to run after expiration increases the probability it will become compromised or infected with malware. In this situation, if possible, block all network connectivity to/from expired computers (or at least Internet access), switch from Internet Explorer to another browser, keep all applications up-to-date with patches, install a host-based intrusion prevention suite, back up data more frequently, and prepare for compromise as though it were inevitable. For example, use IDS to monitor the network segments of expired machines. These are merely stop-gaps, however, until an upgrade can (hopefully) be performed.

### **Underground Market Hotfixes**

Beware, there may be websites that sell unofficial hotfixes for expired operating systems, but these hotfixes 1) might not work and 2) might contain malware. Be especially wary of any hotfixes circulating for free on file-sharing sites or that are advertised through spam. Assuming they are available at all, purchase unofficial hotfixes directly from the websites of well-known and trusted vendors, and only after confirming that this will not violate any laws or regulations for your industry.

# Windows on ARM

- Intel-compatible 32-bit (x86) and 64-bit (x64) CPUs:
  - Historically dominant, faster, hotter, and power-hungry
- ARM CPUs:
  - Relatively cheaper, slower, cooler, and power-conserving.
  - Windows Phone, iPhone, and Android run on ARM.
- **Windows 10 for ARM** on phones, tablets, IoT devices:
  - Cannot run x86/x64 applications
  - Cannot be joined to an Active Directory domain (yet)
  - What happened to Windows RT? Discontinued.

SANS Security Essentials – © 2016 SANS

## Windows on ARM

Intel-compatible x86/x64 platforms have dominated the history of Windows, but there is also ARM. Windows Phone, Apple iPhone and Google Android all run on the ARM platform. Billions of CPUs that implement the ARM instruction set are sold every year for phones, tablets, GPS navigation handhelds, televisions, medical devices, and all the other "Internet of Things" (IoT). ARM devices are generally slower than x86/x64 Intel CPUs, but they also consume less battery power and produce less heat.

Breaking with more than 30 years of tradition of not directly competing with OEM resellers, Microsoft released its own tablet, the Microsoft Surface, to better control the hardware and software (just like Apple). Originally, Microsoft had an operating system named "Windows RT" for ARM devices, like one of the Surface models, but Windows RT was discontinued when Windows 10 came out. Windows 10 came in both x86/x64 and ARM flavors, so this change was partly just a rebranding exercise.

## Windows Runtime API (WinRT) and the "Metro" Graphical Interface

An operating system implements programming interfaces for developers to use. The most important low-level programming interface on Windows is the Windows API (formerly known as the Win32 API). Windows 8/RT included a new library of functions on top of the Windows API named the Windows Runtime API (WinRT). WinRT is what implements the tile-based Start Screen, touch orientation, and Metro/Modern apps in general. If you sometimes get the feeling that you are running two operating systems on Windows 8, that's because in some respects you are. Microsoft's all-in gamble is that the future is cloud-hosted services, Internet single sign-on, mobile device dominance, BYOD, touch/voice/gesture interfaces (think tablet-integrated Kinect), managed app stores, and all this is laced with social networking. The WinRT API is designed around all this. WinRT can be accessed from C++, C#, VB.NET, and even compiled JavaScript in HTML applications.

## **Application Compatibility**

Windows RT/10-ARM can run Metro apps installed only through the Windows Store and a few other applications Microsoft has chosen to port to it, such as the Microsoft Office applications and Windows Explorer. Otherwise, you cannot install your favorite x86/x64 Windows API applications on Windows RT/10 for ARM. It's Metro or no-go. (And even the word "Metro" has caused Microsoft some legal issues, so Microsoft often uses the term "Modern" or "Universal" instead.)

## **No Active Directory Integration**

For the time being at least, Windows RT/10-ARM devices cannot be joined to an Active Directory domain; though a future update might include this functionality. To manage Windows ARM devices, then, Microsoft recommends using either Windows Intune ([www.microsoft.com/intune](http://www.microsoft.com/intune)), which is Microsoft's cloud-hosted management service for a monthly fee per device, or the Microsoft System Center suite. Because Windows RT/10-ARM cannot (yet) be joined to an AD domain, you can't use Group Policy to manage it either.

# Other Microsoft Client Devices

- Windows Phone
  - A pocket-sized tablet
- Xbox One
  - It's a Hyper-V server
- HoloLens
  - Augmented reality goggles
- Surface Hub
  - TV-sized tablet with sensors



SANS Security Essentials – © 2016 SANS

## Other Microsoft Client Devices

Windows security is not just for traditional PCs, laptops and tablets. There are other device types as well.

### Windows Phone

Windows Phone is just a pocket-sized tablet, and a tablet is just a laptop without a keyboard. Windows Phone has UEFI firmware, a TPM chip, whole disk encryption, runs a full browser, supports VPNs, authenticates with Windows Azure accounts for single sign-on, etc. The point of all this is that, from a security perspective, Windows Phone is mostly just a modified version of Windows. (There are some major differences, too, of course.)

With Windows 10 and later, all of Microsoft's devices have a (mostly) common kernel, including Windows Phone, Xbox, tablets, automobile dashboards, and so on. On top of the common kernel, everything will eventually have a similar touch-oriented graphical interface with tiles.

Windows Phone 8.1 and later include the following features:

- Every Windows Phone has a TPM chip.
- BitLocker-esque encryption is used for primary storage and removable media.
- Secure Boot integrity checking is used with UEFI firmware.
- NTFS file system permissions are used, including on MicroSD storage cards.
- Digital certificate enrollment and management.
- Virtual smart card is implemented with the TPM.
- S/MIME support for encrypted e-mail.
- VPN client and EAP-TTLS Wi-Fi authentication.

- Application allow/block lists, managed through MDM.
- JTAG debug mode disabled at the factory.
- Near Field Communications (NFC) for wireless.
- Wallet app for credit card and account numbers (and NFC payments).
- Credential Locker app for storing encrypted passwords.
- Apps installed only from Windows Store or corporate "side loading."
- Apps can be installed to encrypted removable media.
- Windows Phone version of Microsoft Office apps.
- Over-the-air OS and software updates regardless of mobile carrier.
- Centralized management through Windows Intune, MDM policies, and System Center.

So, the good thing about Windows Phone is that it runs a "real" operating system, but the bad thing is that it runs a real operating system with all the potential exploits and malware this entails.

### **Windows Phone Best Practices**

Here are a few security best practices that apply to Windows Phone and most smartphones:

- Keep the phone updated with the latest OS version (at least version 8.1).
- Use centralized MDM management, such as with AirWatch, Intune, MobileIron, and so on.
- Require a PIN or password to unlock the phone, and block common PINs such as "1234."
- Train users not to store sensitive data on their mobile devices unless 1) they have encryption and 2) the data is necessary for legitimate business purposes. Don't forget about removable media, such as MicroSD cards, which should be encrypted or blocked entirely.
- Back up the data on the device on a regular basis, or keep the device in sync with another storage capability that is backed up.
- Use the app whitelisting rules to allow/block applications to enforce your policies.
- When possible, use the PIN-protected TPM virtual smart card to authenticate to LOB applications and VPN gateways. Revoke compromised certificates.
- Remotely wipe devices that have been lost or stolen.
- Configure the device so that after too many failed authentication attempts it should either wipe its own memory and storage media, or it should encrypt this data in a lock-down mode that is recoverable only by a company's IT department.
- Before enabling the Cortana personal assistant, you might want to review the fine print of what she is allowed to share with Microsoft, if you care about privacy rampancy.

### **Xbox One**

Why talk about Xbox in a security course like this? Because, believe it or not, your users' Xbox consoles will eventually become BYOD computers they will expect to use for work, just like their tablets and phones, especially for Skype and e-mail. A company might also use one in a conference room, but not for gaming.

Not the older Xbox 360, but the newer Xbox One runs a highly modified version of Hyper-V to handle the virtual machines necessary to run both games and Windows apps simultaneously in either full-screen or split-screen mode. You cannot yet run just any Metro app on the Xbox virtual machine for Windows, but that is the long-term plan. (This plan does not include mouse-oriented x86/x64 applications, though.)

The Kinect sensor includes multiple highly sensitive microphones and video cameras for motion tracking. When plugged in, the Kinect sensor is always listening. Applications such as Skype can use the Kinect for group video-teleconferencing. The Xbox dashboard can be controlled by voice commands and hand gestures. There is a free Xbox Glass application for controlling an Xbox through a laptop or tablet. For conference rooms and living rooms, there are also standalone wireless keyboards for applications such as e-mail and instant messaging. In a conference room with a large LCD screen, one part of the Xbox screen might be for a group Skype meeting, with the other part showing a spreadsheet, slide presentation, or web page.

Skype, Outlook.com, Facebook, Twitter, and other web applications support single sign-on through the Xbox because of the user's authentication with their Microsoft Account, that is, the same account used for Xbox Music, OneDrive, Office 365, and so on. The single sign-on is implemented with HTTPS protocols such as OAuth, WS-Federation and WS-Trust. The user won't be aware of any of this, though; they will only notice that they can Skype and e-mail from any of their BYOD devices the same as on their Xbox consoles. And, no doubt about it, your users will want to use their personal Skype and e-mail accounts for work from home, no matter what we in IT worry about. Indeed, the whole concept of "personal account" versus "work account" is eroding away as the trends toward cloud computing and BYOD-for-everything roll along.

Today, the Kinect sensor is an external piece of equipment, but it can also be built into TV-sized tablets and augmented-reality googles.

### **Surface Hub**

Microsoft Surface is a hand-held tablet, but Microsoft Surface Hub is a giant tablet that hangs on the wall like an 84" flat screen TV (<https://www.microsoft.com/microsoft-surface-hub/>). Surface Hub is mainly intended for team use. It includes Kinect sensors, a touch-sensitive screen with pen support ("digital ink") as a whiteboard, speakerphones for Skype, Cortana, and all the Office applications. Over time, the features of Xbox and Surface Hub will become more similar.

### **HoloLens**

Microsoft HoloLens is like Surface Hub, but worn on the head like big sunglasses with embedded speakers, microphone, motion sensors, and mini-projectors for only the user to see within the lenses (<http://www.microsoft.com/microsoft-hololens/>). A HoloLens headset is not for virtual reality, it's for augmented reality. To the wearer, the HoloLens glasses project apps and three-dimensional objects into the room of the user. HoloLens includes small speakers that change the apparent source of sounds as the user moves his or her head around. So, instead of Surface Hub on the wall running Skype and OneNote, these apps are projected into the user's room. Because of the Kinect-style sensors in the headset, the user can manipulate these apps and objects with their hands (HoloLens watches the user's hands). With Xbox integration, a HoloLens gamer could, for example, construct Minecraft objects in the room with HoloLens and then move those objects into the Xbox.

Importantly, keep in mind that all of these Microsoft devices will be designed for single sign-on with user accounts in Azure, data storage in OneDrive, Cortana assistance, Skype, Office 365, etc. These devices are just different ways to use the "ecosystem" Microsoft has built.

What about security? Will there be HoloLens zero-day exploits? Surface Hub hacks? Definitely, it's just a matter of time. Will your organization be ready?

# Server Operating Systems

- Windows NT 4.0 Server
- Windows Server 2000
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Hyper-V Server (Free)
- **What is "R2"?**

## Server Editions:

- Standard
- Enterprise
- Datacenter

SANS Security Essentials – © 2016 SANS

## Server Operating Systems

Windows Server is not intended for desktop, laptop, or tablet use, though there is nothing preventing this. Windows Server is normally installed in virtual machines running on computers that often have multiple CPUs, multiple storage devices, multiple network interface cards, a lot of memory, and possibly no monitor. These computers are often densely packed into shelving racks or "blade arrays" in special rooms or railroad-car-sized containers with their own air conditioning, dehumidifiers, and redundant power. However, a Windows Server appliance might be no bigger than a paperback novel with a System On a Chip (SOC) architecture and flash memory for storage. In either case, Windows Server is mainly intended for providing network services, such as DNS or HTTP, and not for running graphical applications with a directly attached monitor, keyboard, and mouse.

## Server Editions

There are three primary editions of Windows Server: Datacenter, Enterprise, and Standard. The different editions have different scalability and fault-tolerance capabilities, such as for clustering and Network Load-Balancing (NLB). Note that starting with Server 2012, the Enterprise edition no longer exists; there's only Standard and Datacenter, with the enhancements of Enterprise edition pushed into Standard by default.

Datacenter supports the maximum possible CPUs, memory, clustering and features. Standard supports the least. Unfortunately, you'll have to research the latest specifications included in each whenever a new OS is released.

There are also specialty editions, such as Small Business Server (SBS) and Windows Server Essentials, which are intended for small offices (less than 25 people), and Windows Storage Server, which is intended for OEM appliances, but these have the same security concerns as the major editions and can be ignored for this course. To better compete with VMware, though, note that Hyper-V Server edition is free, but it can be used only for hosting virtual machines. Despite being free, Hyper-V Server is not artificially hobbled, it supports hundreds of CPU cores, large cluster farms, live migration of VMs, terabytes of memory, and so on (at least for now).

## **What Is R2?**

Approximately every 4 years, a new major Windows Server version is released, such as Windows Server 2012, which is called the "first release" or "R1" or "RTM" version of that OS. Then, usually about 2 years after the R1 major release comes the "second release" or "R2" of that same OS, such as Windows Server 2012 R2. Microsoft originally promised that no new significant functionality would come out in any R2 release, but this has not been true. It's best to consider the R2 versions as new operating systems, which require research and testing as such. This naming strategy has made it only more confusing to manage Microsoft's server products.

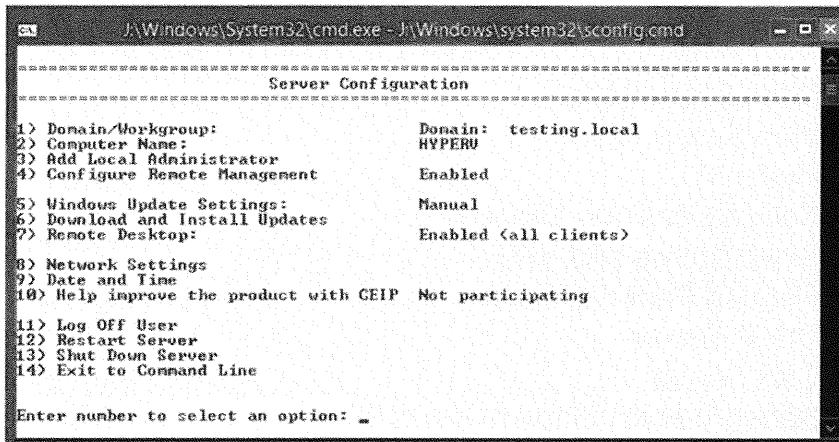
## **Platforms**

Windows Server 2008 was the last server OS to be available in a 32-bit (x86) version. Server 2008 R2 and later are only available as 64-bit (x64). Itanium CPUs are no longer supported. There is currently no Windows Server for ARM and none is publicly planned.

## **Licensing**

Window Server licensing is even more complex than the licensing of client devices. In fact, it is basically a nightmare. You have to worry about Client Access Licenses (CALs), VM instance rights, per-user or per-device access licenses for Remote Desktop Services, per-core licenses for SQL Server, OEM licensing for appliances, special deals for Azure hosting, Office 365 versions of SharePoint and Exchange, and the list goes on and on (see <http://www.microsoft.com/licensing/> and then get your legal department to dig through the fine print).

# Server Core



SANS Security Essentials – © 2016 SANS

## Server Core

Server Core is not an edition or special version of Windows Server; it's an installation option. Hence, both Windows Server Standard and Windows Server Datacenter could be installed with the Server Core option.

When installing the OS, you have the option to install it With a GUI or as Server Core. When installed with a graphical user interface, you get a taskbar, Start button, shortcuts on the desktop, Internet Explorer, Control Panel, and everything else you would expect. When you log on after using the Server Core choice, however, you do not get any of these things; you get a command shell, Notepad, and almost nothing else. Your favorite graphical management tools can still be used over the network, but, while sitting at the console of a Server Core box, most administration will be performed using PowerShell or other scripts, such as the script shown in the slide. Starting with Server 2012, the default installation option is Server Core.

The drive footprint of Server Core is only approximately 2–4 GB because unnecessary binaries are not copied over from the installation DVD. As more roles and features are enabled, this footprint size increases, of course. While running, Server Core also uses less memory. And Server Core requires fewer patches than the full GUI server, too. Hence, Server Core is especially useful for appliances and virtual machines.

With Server 2012 and later, you can install the full GUI without reinstalling the entire OS, or to remove the GUI to get back to Server Core, again without having to reinstall from scratch. This is done in PowerShell with the `Install-WindowsFeature` and `Uninstall-WindowsFeature` commands. Prior to Server 2012, a reinstall was necessary to change the Core/GUI installation option.

Server Core can run most of the same roles as the full GUI server, including IIS web server, domain controller, SQL Server, Hyper-V, DNS, DHCP, file sharing, and so on.

# Windows Server Roles

## Example Roles for Windows Server:

- Domain Controller
- Web Server (IIS)
- Hyper-V
- Remote Desktop Services
- DirectAccess and VPN
- File and Print Services
- DHCP Server
- DNS Server
- Network Policy Server (RADIUS)

SANS Security Essentials – © 2016 SANS

### Windows Server Roles

The modular components of Windows Server are grouped together into roles and features, and these can be added or removed as needed. A role is a major piece of functionality, such as being a web server or domain controller, whereas a feature is a smaller component, such as support for BitLocker disk encryption.

Roles and features can be installed or uninstalled from the command line in PowerShell or in the graphical Server Manager application. For example, to see what roles and features are currently installed on a remote server named WebServer47, run "Get-WindowsFeature -ComputerName WebServer47" in PowerShell.

So, just to keep our terminology straight, first you choose the operating system version you want (such as Server 2008 or 2012 R2), then you choose the edition (such as Standard or Datacenter), then during installation you choose the graphical interface support you prefer (Core or with a GUI), and then finally you would enable just the roles and features needed on that box.

# Windows Embedded

## Windows for the "Internet of Things":

- More modularized than Server Core
- Small footprint with the ARM platform
- Raspberry Pi, Intel NUC/Galileo, etc.
- Industry-specific hardware appliances:
  - ICS/SCADA equipment, retail point-of-sale, MRI scanners, automobile dashboards, robotics, etc.

SANS Security Essentials – © 2016 SANS

### Windows Embedded

Windows Embedded operating systems are intended for dedicated-use devices in industries such as manufacturing, utilities, retail, and healthcare. Windows Embedded products can use either client or server operating system versions, but these are usually highly modified by OEM vendors to replace the graphical interface or to support just their hardware appliances. More so than Server Core, Windows Embedded products are highly modular and can be stripped down to almost a bare kernel; for example, a Windows Embedded product doesn't need to have a protocol stack.

Example operating systems in this category include Windows Embedded Industry, Windows Embedded Compact (ARM), Windows Embedded Automotive, and, to go along with these, SQL Server for Embedded Systems, too. Strictly speaking, Xbox and Surface Hub would be examples of Windows Embedded products, except that the OEM is Microsoft itself, so they are lumped in with the clients.

Normally, only OEM vendors purchase Windows Embedded for bundling into their products, but anyone can download the bits (see <http://www.microsoft.com/windowsembedded/>).

Because Windows Embedded for ARM can be stripped down to a small footprint, Microsoft hopes to win market share in the "Internet of Things (IoT)" space, an area in which Linux dominates; for example, Windows 10 and later is free for the Raspberry Pi, like Linux, and Microsoft's marketing people may refer to the latest version of Windows Embedded as "Windows IoT" to emphasize the purpose of the product.

This manual mostly ignores Windows Embedded, but your company might use it extensively, such as in ICS/SCADA equipment or Point of Sale (POS) terminals, so keep it in mind when planning security. And as the "Internet of Things" trend grows in the next several years, these innocent-looking little devices will become more and more attractive to hackers.

# Windows Workgroups and Accounts

---

The student will understand how Windows manages workgroups and accounts locally on a Windows host.

SANS Security Essentials – © 2016 SANS

## **Windows Workgroups and Accounts**

This section intentionally left blank.

# Workgroups (1 of 3)

- **No domain controllers!**
- Standalone computers only
- Local accounts and local accounts databases only
- Permissions can be assigned to local users and groups only
- Local groups cannot have users from other machines
- **Users are typically local administrators of their own machines**
- A "workgroup admin" simply has a separate administrative account on every machine
- Workgroups tend to be small, such as less than 50 computers

SANS Security Essentials – © 2016 SANS

## Workgroups (1 of 3)

Two or more Windows computers that share information in the absence of any domain controllers is called a *workgroup*. Even if all the computers are running Windows Server 2012 Enterprise, and even if there are thousands of user accounts on each of them, they still form only a workgroup, not a domain.

Because the computer is not a member of a domain, it is called a *standalone* computer. This doesn't mean the computer refuses to be a file/print server or to share resources with others, only that it is not a member of a domain.

### Characteristics of a Workgroup

Workgroups have the following characteristics:

- There are no domain controllers.
- Each computer has a local accounts database. Users and groups in that database are called *local users* and *local groups* precisely because they exist only in that one database. This database is not shared with or replicated to any other computers.
- When privileges or permissions are assigned to a resource on a workgroup computer, they can be assigned only to local users and local groups defined on that computer. You can't assign permissions or privileges to user accounts on other machines.
- A local user account on one machine cannot be made a member of a group on another computer. Conversely, a local group can contain only local users defined on the same computer as the group itself.

- Two computers may each have a local user account with the same name, but these are two different accounts. The accounts have different Security ID (SID) numbers.
- Typically, the owner or user of a computer in a workgroup is a member of the local Administrators group on that machine, giving him full authority over it. But this authority does not extend to any other machine on the network.
- If a person is the administrator of a workgroup, that just means she has a user account on every computer in the workgroup and that that account is in the local Administrators group on each machine. Whether all these accounts are named the same or have identical passwords is another issue entirely.
- Workgroups tend to be small, usually less than 50 computers. When the number of computers is less than 10, we typically just say, "They are all standalones" instead of saying, "They are a workgroup." The term *workgroup* focuses on the people, whereas "standalones" focuses on the computers, but in both cases neither the computers nor the users are members of a domain.
- You can have standalone computers in the midst of other machines that are members of a domain. They are not anathema to each other, and each has its benefits.

# Workgroups (2 of 3)

## Benefits of workgroups:

- It is conceptually simple.
- Each computer protects itself.
- Lower initial deployment costs.
- User are typically administrators of their own machine, allowing personal creative expression and joy.

SANS Security Essentials – © 2016 SANS

### Workgroups (2 of 3)

Workgroups are not always bad. There often are important security benefits to having standalone workstations or servers.

For example, a farm of Microsoft Internet Information Server (IIS) web servers might be better protected if they are all standalone servers. Or a public-access kiosk computer might be better off as a standalone. For a small group of temporaries working on a project, a little peer-to-peer network may satisfy its needs without exposing the rest of the network to its misdeeds.

Workgroups enjoy the following benefits:

- Conceptual simplicity.
- Lower initial cost.
- Each computer protects itself from the other computers on the LAN. Putting computers into a workgroup is not putting all your eggs into one basket. (Even though it is easier to manage a basket than an armful of eggs.)
- Each infected or compromised computer, if it is a standalone, will be somewhat less able to harm other computers on the network precisely because it is a standalone. This is because a stolen account on that computer cannot be used to access any other computers.
- Users typically are members of the local Administrators groups on their machines. Users enjoy fixing their own problems and installing "free" programs from Russian websites.

# Workgroups (3 of 3)

## Drawbacks of workgroups:

- Users are insane
- Workgroup = Chaos + Anarchy
- It is difficult to manage large numbers
- No centralized policy control or auditing
- No single sign-on without great effort
- No consistent permissions across machines

SANS Security Essentials – © 2016 SANS

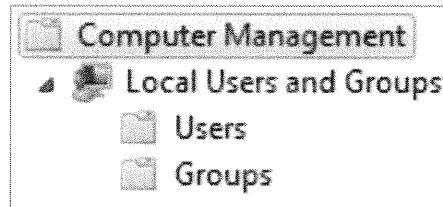
### Workgroups (3 of 3)

So why isn't every Windows network a workgroup? Why have domains at all? Unfortunately, there are some serious drawbacks to having workgroups, especially large ones.

- Users typically are members of the local Administrators or Power Users groups on their machines. Users apparently enjoy destroying their computer, blaming you for their problems and then demanding that you immediately fix them.
- Each computer in a workgroup enforces its own security. In some respects a workgroup is like a miniature replica of the Internet as a whole: Anarchy!
- Workgroups lack single sign-on. Potentially, a person might have a differently named user account on each machine, and the password for each of these accounts might be different, too. However, single sign-on could be emulated by creating an identical user account with an identical password on every machine, but this is a management and security nightmare in itself when there are more than 100 machines.
- Every computer in a workgroup is a management island. In general, workgroups don't scale to thousands of machines without gallons of elbow grease and a lot of summer interns to do the repetitive work for you.
- Because local users and groups cannot be made members of groups on other machines, it is difficult to maintain a consistent assignment of permissions and privileges across multiple machines.

# Manage Local Accounts

- Start > Administrative Tools > Computer Management
- Control Panel > User Accounts
- Command Shell:
  - `net.exe help user`



SANS Security Essentials – © 2016 SANS

## Manage Local Accounts

All Windows computers have local accounts and groups, even if the computer is a member of a domain. (Local accounts are hidden on domain controllers, but they still exist dormant.)

To manage local users and groups, try the User Accounts applet in Control Panel.

You also can use the Computer Management console found in the Administrative Tools folder, which is probably more efficient for advanced users.

A screenshot of the Windows Computer Management console window. The title bar says "Computer Management". The left pane shows the navigation tree with "Local Users and Groups" selected. The right pane displays a table of local groups with their descriptions:

Name	Description
Administrators	Administrators have complete and unrestricted access to the system.
Backup Operators	Backup Operators can override security restrictions for the system.
Guests	Guests have the same access as members of the Guests group.
Network Configuration ...	Members in this group can have some administrative privileges.
Power Users	Power Users possess most administrative powers with some restrictions.
Remote Desktop Users	Members in this group are granted the right to logon remotely.
Replicator	Supports file replication in a domain.
Users	Users are prevented from making accidental or intentional changes to system files.
HelpServicesGroup	Group for the Help and Support Center.

If you want to script user account management, there is also the NET.EXE program. Execute "net.exe help user" in CMD.EXE or PowerShell to see the available switches.

# Security ID Numbers (SIDs)

- **It's like a Windows Social Security number:**
  - Example:  
S-1-5-21-4353520176-2898672217-036752055-1000
- **Each user, computer, and group has its own unique SID number**
  - Well-known SIDs exist for certain built-in users and groups that exist on all systems (for example, Administrator and Everyone)
- **Windows cares about SIDs only when enforcing permissions and privileges**

SANS Security Essentials – © 2016 SANS

Admin account ends in 500

## Security ID Numbers (SIDs)

Every user account, computer account, and group has a unique identifying Security ID (SID) number. It's like a Social Security number. For example, here is the SID for a local user account on a Windows Vista box:

S-1-5-21-4027132841-2898672216-450591829-1000

Each computer will create SIDs for its local users and groups. (And domain controllers will do the same for domain accounts.) These SIDs are unique, except for the SIDs of some well-known users and groups, which are shorter and standardized across all boxes. For example:

- S-1-1-0 = Everyone Group
- S-1-5-11 = Authenticated Users Group
- S-1-5-32-544 = Local Administrators Group

The username of an account might be renamed, but the SID stays the same. If a user named "Eric" is deleted, and another user named "Eric" is immediately created, the new Eric will have a different SID number. If there is an account named "Obama" on Computer A, and another local account named "Obama" on Computer B, these are two different accounts.

Why? Because their SIDs are different, and that is the only thing that matters. If the two Obama accounts happen to have identical passwords, then the user could log onto one machine and appear to access the other computer over the network without being authenticated. In fact, the user's credentials are being locally cached and automatically forwarded to the other box; but at the other box the user actually is logging on with a different user account, that is, an account with a different SID. The transparency is just an illusion.

Windows actually cares only about SID numbers when it is enforcing privileges and permissions. That's because all of your SIDs go onto your "ID Card," so to speak, when you log on. And this ID Card is how the computer identifies your programs and regulates your activities. This ID Card is officially called your Security Access Token (SAT).

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered was "whoami.exe /all /fo list". The output provides detailed information about the user account and group memberships.

```
C:\>
C:\>
C:\> whoami.exe /all /fo list
USER INFORMATION
-----
User Name: testing\jason
SID: S-1-5-21-932530260-2103539867-4062103621-2103

GROUP INFORMATION
-----
Group Name: Everyone
Type: Well-known group
SID: S-1-1-0
Attributes: Mandatory group, Enabled by default, Enabled group

Group Name: BUILTIN\Performance Log Users
Type: Alias
SID: S-1-5-32-559
Attributes: Mandatory group, Enabled by default, Enabled group

Group Name: BUILTIN\Users
Type: Alias
SID: S-1-5-32-545
Attributes: Mandatory group, Enabled by default, Enabled group

Group Name: BUILTIN\Administrators
Type: Alias
SID: S-1-5-32-544
Attributes: Mandatory group, Enabled by default, Enabled group, Group owner
```

# Your Security Access Token (SAT)

**It's like your Windows driver's license card!**

- Your SAT is attached to every process you start
- Windows uses your SAT to check your permissions and privileges before allowing attempted actions
- In CMD or PowerShell, run this command:  
`whoami.exe /all /fo list`
- **Your SAT contains:**
  - **The SID number of your user account**
  - **The SIDs of all your groups**
  - **Your privileges**

SANS Security Essentials – © 2016 SANS

## Your Security Access Token (SAT)

When you log onto your desktop, your computer obtains the SID for your user account and all the SIDs for all the groups to which you belong. Your computer also finds out what your "local privilege" is on the machine, for example, the take ownership privilege.

All these SIDs and privileges are written into something like an ID Card and attached to all your processes. This ID Card is called your Security Access Token (SAT). Your SAT identifies you on your computer and is your identity on the network.

Everything the computer needs to know to enforce permissions and privilege restrictions is contained in that one little token. Just like you have to present your military ID or company ID card before you can get onto the base or into secured rooms, the operating system will ask for your SAT before it lets you access any resources. Because every program and process you launch has a copy of your SAT, the OS always can get it easily.

If you open a CMD.EXE shell or PowerShell, that process has a copy of your SAT, too. In that shell, run "whoami.exe /all /fo list" to more-or-less show the contents of your SAT. You can see your user SID number, the names and SIDs of your groups, and all your privileges.

Now, whenever a program you control tries to access a resource or to exercise a privilege, the operating system will get the SAT from your process and see if you (and your groups) are permitted to perform the requested action. If yes, the OS lets you. If no, you get an error message. This is made possible by the Access Control Lists (ACLs) on the resources and the fact that certain actions require specially-defined privileges before you can execute them. (For example, you must have the Debug Programs privilege to access raw virtual memory.)

# To Form a More Perfect Workgroup

- Standalone computers do not trust each others' Security Access Tokens, and that fundamentally is why workgroups don't scale
- What you need then:
  - A central shared database of SIDs that all stand-alone computers agree to use for single sign-on and resource authorization
  - A secure authentication protocol scheme for distributing SID information from this database to computers making SATs, such as Kerberos
  - ***In other words, you need a domain controller***

SANS Security Essentials – © 2016 SANS

## To Form a More Perfect Workgroup

Fundamentally, the problem with standalone computers in workgroups is that they don't understand, accept, or trust the SATs of the users on the other computers.

It's like a situation in which every state in the country issues driver's licenses to its members, but with no state accepting or trusting the driver's license cards other states have issued. You can't get authorization to drive across other states because those other states don't accept your driver's license as authentic. And why should they? Maybe your state just hands out driver's license cards willy-nilly with any old name to any nutcase or hacker who just asks for it!

What we need is a way to make the computers in a workgroup all use the accounts and groups defined in a single database for the entire workgroup. This would be a shared database that everyone used and trusted. The database might be hosted on one or a few special, designated servers in the workgroup, using only a secure SAT distribution protocol, such as Kerberos. Every process a user launched would get its identifying SAT from this single database, starting with the first process a user launches when they log on, namely their desktop process.

A user at one computer, when authenticated, could present his information for building a SAT to another computer over the network, like when trying to map a drive letter and that remote computer could use that SAT to calculate the user's permission and privileges. Hence, whether one is accessing resources locally or across the network, the same set of credentials (the same SAT) is always used to compute one's permissions and privileges. If all the computers in a workgroup would just "outsource" their authentication and account management tasks to one (or a few) special computers with a shared accounts database, well then we could have a *domain*.

# Windows Active Directory and Group Policy

The student will identify the features of Active Directory and Group Policy, and understand how they are used by Windows.

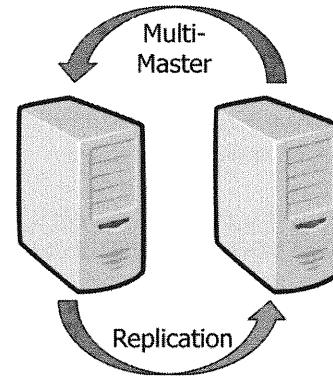
SANS Security Essentials – © 2016 SANS

## **Windows Active Directory and Group Policy**

This section intentionally left blank.

# Active Directory Domains

- **What is a domain controller?**
- **Analogy:** Active Directory is like a shared Registry for all the users and computers on the network
- Active Directory is multi-master replicated
- What does "being in the domain" mean?



SANS Security Essentials – © 2016 SANS

## Active Directory Domains

*Active Directory* is the name of the shared accounts database that gets installed on a Windows Server when it is promoted to become a domain controller. Again, what is *Active Directory*? It's just a database. A database of user accounts that otherwise would have been in the local accounts databases of standalone computers. Let's define some terms.

### Domain Controllers

A *domain controller* is just a server that helps to manage the Active Directory (AD) database on behalf of the other computers and users in the organization. The AD database contains, among other things, all the SIDs of the users, computers, and groups that have "outsourced" their authentication and account management work to the domain controller.

When a user has her SAT, it is attached to all her programs like a badge, and every request she makes for local or remote resources is checked against the permissions on that resource with the SAT-badge. How? The resource (file, database, e-mailbox, printer, whatever) will have a list of SIDs attached to it with the permissions that each SID has to the resource. This list of permissions based on user and group SIDs is called an *access control list (ACL)*.

### Multi-Master Replication and Read-Only Domain Controllers

You can make a change to the AD database on any domain controller in an AD domain, and this change will then be replicated to all other domain controllers automatically. This is called *multi-master replication*.

In a sense, every AD domain controller is a PDC because you can modify its database, and every AD domain controller is a BDC, in a sense, because it receives changes from all the others. Whenever there is a conflict, the later change overrides the earlier one. AD domain controllers use time stamps and update sequence numbers on every *property* of every object to keep the replication straight.

An important exception to multi-master replication is when a domain controller is running Windows Server 2008 or later and the administrator has decided to install that controller as a Read-Only Domain Controller (RODC). A running RODC can authenticate users and fulfill search requests, but any changes made to the AD database on the RODC will never be replicated to any other controllers. Moreover, RODC controllers cache only the credentials of the groups an administrator specifies, and the list of cached credentials is tracked so that, in case of compromise, just those users can be immediately forced to change their passwords. RODC controllers using BitLocker and a TPM cryptographic module are ideal for remote branch offices where there are no IT personnel and/or the controller is at risk of being physically compromised. Such branch office RODC controllers may also be installed using the Server Core option to give it smaller disk and memory footprint to keep costs down.

### **Being "In the Domain"**

Being *in the domain* has nothing to do with one's physical location or bandwidth. A user in Tokyo and a user in Dallas can both be in the same domain.

Strictly speaking, you are *in the domain* if you have an account in the Active Directory database. Your account has your SID and other information about you. That's it! There's not a big mystery about it. A *domain* is all the users, computers, and groups that have (or, rather, are) accounts in the AD database.

Who or what can be *in the domain*? Anything with a SID can be in a domain. Conversely, you must have a SID to exist. What can have a SID? All users, groups, and computers have SIDs. Yes, computers have their own accounts, just like human users do. They even have passwords and automatically update them periodically. When a computer that is a member of a domain boots up, it logs into the domain just like a human.

### **What Else Is in the Active Directory Database?**

Although account information is the most important thing in the AD database, there is *much* more.

---

Consider this analogy, because it is the key to understanding what the Active Directory database is intended to be: *Active Directory is like a Registry for the entire network*.

Windows computers store all their configuration settings in a tiny database called the *Registry*. It can be edited with REGEDIT.EXE. Active Directory can store many of the configuration settings for all users and computers, too.

It stores these settings in the form of *Group Policy Objects* that modify Registries and other things.

Below is a partial list of what can be stored in Active Directory:

- User account properties and passwords
- Groups and their memberships
- Computer properties and passwords
- Domain names and trust relationships
- Kerberos master keys
- Digital certificates and Certificate Trust Lists
- Organizational Units and their members

- LANs and IP subnets in the organization
- AD replication links and their settings
- Shared printer locations (UNC paths)
- Exchange Server directory information
- Group Policy Objects
- And any custom data you would like to add

Just as the Registry on a computer stores the configuration settings that affect just that one computer, Active Directory can store the configuration settings that affect the entire domain.

Active Directory is a general-purpose database and can be accessed through an industry standard protocol, LDAP. Active Directory uses the same database engine as Microsoft Exchange Server and can store millions of objects. Its maximum size is 4000 GB (4TB)!

### **Global Versus Local Users and Groups**

Local users/groups still exist in the local accounts databases of computers that have joined the domain. But now the users/groups from the AD database are available to domain member computers as well.

So now a distinction can be made. *Local* users and groups are accounts in the database of non-domain controllers; this is true whether or not that computer is a member of a domain. On the other hand, a *domain* user, computer, or group has its account in the AD database. These domain accounts are available for use by any computer that has joined the domain.

# Authentication Protocols (1 of 4)

- The SIDs of domain accounts and groups come from Active Directory and are conveyed to the computer through the authentication protocol
- A SAT is constructed on-the-fly at the computer where the user requests access to a resource
- Privileges, local account SIDs, and local group SIDs all come from the target computer

SANS Security Essentials – © 2016 SANS

## Authentication Protocols (1 of 4)

If a domain controller hands out Security Access Tokens to users and computers, does it just spew those Tokens out willy-nilly? No. Users and computers have to authenticate to a domain controller first, of course.

### Security Access Tokens Revisited

Now that you have a good feel for what Security Access Tokens (SATs) do, let's discuss exactly how they're made. In fact, SATs are never sent over the network. SATs are constructed on-the-fly inside the server, where the user is requesting access. But important *parts* of the SAT *are* sent over the network by the authentication protocol being used.

An SAT can be broken down into four parts, and each part has a source (in parentheses):

1. SID for the user's domain account (AD).
2. SIDs for the domain groups the user is a member of (AD).
3. SIDs for the local groups on the server being accessed that the user is a member of (from the server's local accounts database).
4. The list of privileges the user has on the server being accessed.

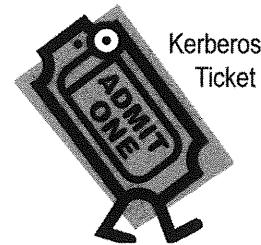
It's one of the jobs of the authentication protocol being used to convey to the target server 1) the SID for the user's domain account and 2) the SIDs for the domain groups of which the user is a member. With this information, the target server can construct a SAT to represent the user on-the-fly.

This is because the server already has the last two parts of the SAT, namely 3) the SIDs for the local groups on the server of which the user is a member and 4) the privileges the user has on that machine.

So, how can an authentication protocol convey the user's domain SIDs to the server? Two protocols concern us here: Kerberos and NTLM.

# Authentication Protocols: Kerberos (2 of 4)

- Kerberos is the default authentication protocol:
  - NTLM is used only when necessary
  - Kerberos requires Active Directory
- Kerberos uses "tickets" to convey the user's account and group SIDs to the server the user wants to access
- Ticket is encrypted based on the user's password = vulnerable to brute-force cracking!



SANS Security Essentials – © 2016 SANS

## Authentication Protocols: Kerberos (2 of 4)

The default authentication protocol in an Active Directory environment is Kerberos (RFC 4120). Kerberos is the *default* in that it will be used if it can be used; otherwise, the computers will fall back to NTLM.

The most important requirement for making Kerberos available is the presence of an Active Directory domain controller. AD domain controllers are all Kerberos *Key Distribution Centers (KDCs)* because they hold every user's and computer's Kerberos master key. Your Kerberos key is derived from your password.

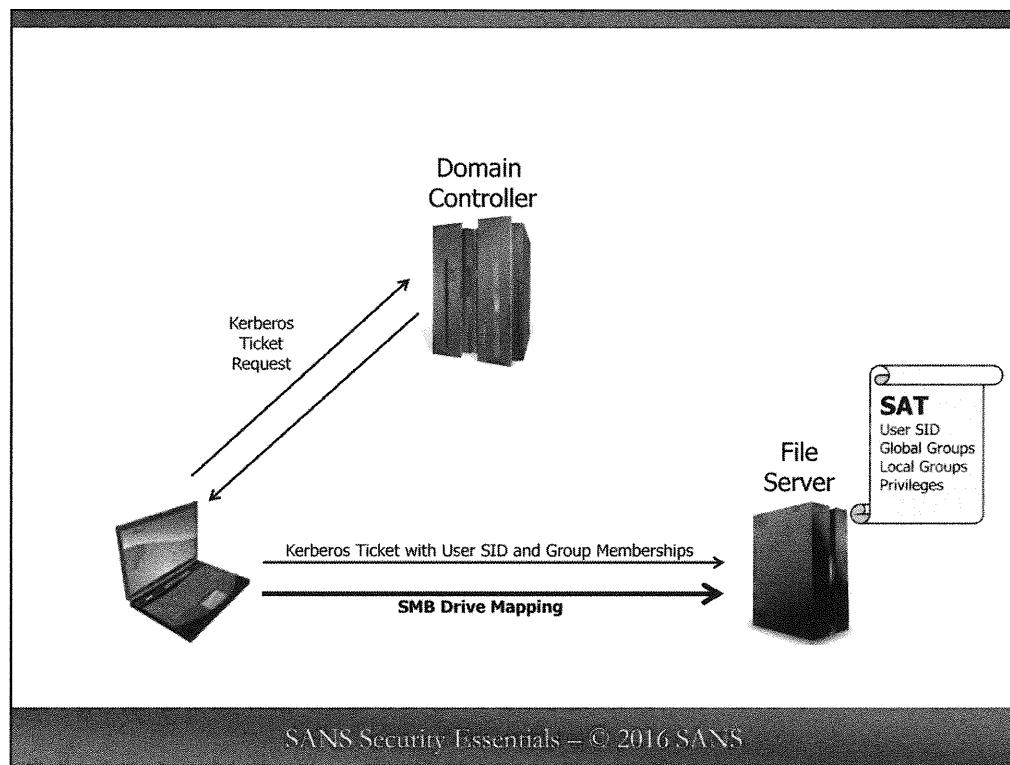
Let's examine the basic idea of Kerberos. Imagine a client named "Chris" in a domain named "SANS.ORG" and a server named "Server7." Chris wants to access Server7, so Chris has to get a ticket from the SANS.ORG ticket booth, that is, from a domain controller in the SANS.ORG domain.

Applications don't have to be "Kerberized" in Windows like they do in UNIX. Kerberos is available when any of the following protocols is used: SMB/CIFS, RPC, LDAP, HTTP, Dynamic DNS secure updates, IPsec IKE, and RSVP. But note what's not on the list: FTP and Telnet.

1. Chris authenticates to a SANS.ORG domain controller with his password used as an encryption key. Only the controller (the KDC) and the client know the client's password, so only they can decipher stuff encrypted with that password.
2. Domain controller sends Chris a *ticket* for getting access to Server7, the remote server the client wants to access.
3. Chris sends the ticket to Server7. That ticket was encrypted with the server's secret key by the domain controller, so only Server7 can decrypt it (not Chris). What's inside the ticket? All Chris's domain SIDs. Now the server knows who the client is and can construct a SAT to represent him.

Kerberos is faster than NTLM and scales better in large environments because clients can cache and reuse their tickets (just as though Chris managed to keep his ticket to Server7, so he could go on the ride over and over and over).

However, if an attacker can capture the packets of the initial Kerberos exchange (when the user first logs on), then the attacker can mount a brute-force attack to discover the user's password. This is possible because the initial ticket request is encrypted based on the user's password. The shorter and simpler the password, the more likely it will be revealed in a reasonable period of time; long and complex passphrases generally cannot be discovered in a usefully short period of time (unless your adversary is extremely well-funded). A brute-force Kerberos cracker for Windows can be found at <http://ntsecurity.nu>.



SANS Security Essentials – © 2016 SANS

### Kerberos Example (3 of 4)

As an example, imagine a user with a laptop who needs to map a drive letter using the SMB protocol to a shared folder on a file server. In the slide, the user has already authenticated to the domain controller using Kerberos (not shown), and now the user needs another Kerberos ticket for the file server. So the user sends the name of the desired file server to the domain controller as part of a request for another ticket. The domain controller responds directly to the client, not to the target file server. The Kerberos ticket given to the client is encrypted so that only the target file server can decrypt it, but the client can cache this ticket in memory and can send the ticket to the target file server when the client chooses. (Tickets do have time expiration limits, though.)

Why is the ticket encrypted? Because inside the ticket is the user's SID number, the SID numbers of the groups in Active Directory of which the user is a member, and the user's claims. A user's "claims" is the set of attributes of that user's account in Active Directory which an administrator has chosen to make available through Kerberos and other protocols, for example, an administrator might include the user's country of citizenship, military rank, or security clearance level as claims in their Kerberos tickets. The ticket needs to be encrypted so that it cannot be modified and so that the target server knows that the ticket ultimately came from the domain controller (instead of from a hacker just spinning them out of thin air). Note that the management of claims in Active Directory is not covered in this course.

When the target server has the user's Kerberos ticket, the server can construct a Security Access Token (SAT) to represent that remote user. The user's SAT includes all the information from the Kerberos ticket, plus information available locally on that file server, such as the user's local group memberships and privileges. More important, SATs are not sent over the network; they are constructed on-the-fly on each machine where they are needed. But some of the information needed to construct a SAT are sent over the network, usually with the Kerberos protocol.

# Authentication Protocols: NTLM (4 of 4)

- Predecessor to Kerberos but still supported for compatibility
- Used in workgroups because it doesn't require Active Directory
- User's password information is given to server in a hashed form, which passes it through to a domain controller, and then the domain controller sends the user's SIDs to the server (if the hash is okay)
- **NTLMv1 is vulnerable to sniff-and-crack attacks (Cain)**
- **NTLMv2 is much less vulnerable (discussed later)**
- **You can disable NTLM entirely with Windows 7 and later**

SANS Security Essentials – © 2016 SANS

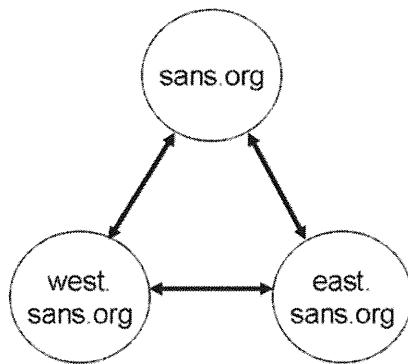
## Authentication Protocols: NTLM (4 of 4)

NTLM authentication is supported by Windows NT and later. NTLM is "I need to ask your mother" authentication. The client wants to access a server, so the client sends to the server the client's encrypted password information. The server passes this information through to a domain controller, which indirectly checks the password. If the password is good, the domain controller sends the server all the client's domain SIDs. Now the server can construct a SAT to represent the client.

NTLMv1 protection of password data is dreadful, and the password data itself (the password hashes) are not well protected either. Using a sniffing tool such as Cain, a hacker can listen in on these NTLMv1 exchanges and extract password hashes. These hashes then usually can be cracked in less than a day (often in less than 10 minutes). These are the same LanManager and NT/MD4 hashes that can be extracted from a stolen user accounts database, but they are used by NTLMv1 as keys for the sake of a challenge-and-response authentication protocol. NTLMv2, however, does not use the old LanManager hash in any form, and its handling of the NT/MD4 hash as a key for the challenge-and-response sequence is vastly improved over NTLMv1. (But you should still use a good passphrase instead of a short password.)

Nonetheless, because of NTLM's performance, scalability and security issues, we should stop using NTLM just like we should stop using LanManager. Starting with Windows 7 and Server 2008-R2, you can use Group Policy to disable support for NTLM entirely, thus permitting only Kerberos and certificate-based authentication. Eliminating NTLM is our long-term goal, but it will require several years to upgrade both our operating systems and applications. To ease the migration away from NTLM, you can use Group Policy to define exceptions for servers that still must use NTLM, and you can implement an NTLM audit-only mode to discover which servers still use it for some reason.

# Forests and Trusts



- You can have more than one domain in your organization
- Domains can be linked with trusts to permit resource sharing and single sign-on across domains
- **What is a forest?**
  - One or more domains
  - Inter-domain replication
  - Two-way transitive trusts
  - The Global Catalog
  - Global Catalog Servers

SANS Security Essentials – © 2016 SANS

## Forests and Trusts

You can have more than one Active Directory domain in your organization. These domains can be joined together by data replication links and trust links. A *forest* is one or more AD domains that replicate special portions of their domain databases with each other and that all trust each other. (Yes, a single domain by itself also counts as a forest, even though it sounds weird.)

### Inter-Domain Replication

Because AD uses multi-master replication, a modified user or group on a domain controller will be replicated to all the other controllers in that domain. But in a forest of two or more domains, such changes will also be replicated to special domain controllers in the other domain(s), too. Hence, having a multi-domain forest implies replication of AD across domain boundaries! Those special domain controllers that replicate across domain boundaries are called *Global Catalog Servers*, and that portion of the AD database that is replicated everywhere in the forest is called the *Global Catalog (GC)*. All Global Catalog Servers are domain controllers, but not all domain controllers are necessarily Global Catalog Servers. The Global Catalog itself is not a separate database from Active Directory, it is that subset of AD that is replicated everywhere.

In addition, all the domains in a forest share a single Schema and Configuration Naming Context. The Schema defines all the possible types of objects and their attributes in the directory, and the Configuration Naming Context defines all the sites, subnets, and inter-site replication links. All this Schema and Configuration data are replicated and kept in sync throughout the entire forest on all domain controllers.

For more information on Global Catalog, Schema, and Configuration Naming Context, see the white papers available at <http://www.microsoft.com/activedirectory/>. These topics can get rather complex, so they are merely outlined here as an introduction.

### **Two-Way Transitive Trusts**

All domains in a forest have two-way transitive trusts between them. This means every domain in the forest trusts every other domain in the forest. This means any user can log on at any computer and access any resources in any domain in the forest (assuming the user has the necessary permissions and privileges, of course) without regard to which domains are involved.

Let's talk about trust relationships a bit more and how they affect security. This is important because there are other types of trusts available besides just the intra-forest trusts.

# The Nature of Trust

- **Without a trust link between two domains:**
  - No single sign-on across domain boundaries
  - Can't assign permissions to users in the other domain
  - Can't log on to your desktop in the local domain with an account created in the other domain
- In a forest with multiple domains, every domain automatically trusts every other domain in the forest. This is a crucial part of what turns a bunch of domains into an *integrated forest*.

SANS Security Essentials – © 2016 SANS

## The Nature of Trust

Say your forest had only one domain (SANS.ORG) and that another forest also had only a single domain (GIAC.ORG). SANS.ORG and GIAC.ORG are two domains in two different forests, that is, two single-domain forests. By default, there would be no trust links between your domain and the other domain. Having no trust links between your domain and other one means that:

- You can't assign privileges or permissions to resources in your domain to users/groups in the other domain. For example, when setting NTFS permissions on a server in SANS.ORG, you simply won't see any users from GIAC.ORG even if you want to.
- There's no single sign-on for your users in SANS.ORG when accessing resources on servers in GIAC.ORG. For example, you log onto your desktop with your SANS.ORG domain account. When you access a server in GIAC.ORG, you are prompted for a username and password, that is, a username and password that is valid in the *other* domain, not yours. If you happen to know the username and password to an account in the other domain, you can access resources *as* that person; hence, you will have the privileges/permissions of that person. This isn't single sign-on, it's more like the other domain is just a mega-sized workgroup.
- You can't log onto your desktop with a user account from the other domain. For example, your desktop has a computer account in the SANS.ORG domain. The user account you want to use is in the GIAC.ORG domain. But because there is no trust link, your computer doesn't trust any users from the other domain to log onto it interactively. When you press Ctrl-Alt-Del to log on, you can't select the GIAC.ORG domain even if you want to.

A trust link between the two domains solves all these problems. With a two-way trust you can log on to your desktop with an account in the other domain; you can access resources in either domain as yourself (true single sign-on); and you can assign privileges/permissions on resources to any user or group you want, no matter to which domain the user or group belongs.

# Cross-Forest Trusts

## Entire forests can trust each other, too!

- **Cross-forest trusts:**
  - They can be one-way or two-way
  - When two-way, every domain trusts every other domain
  - There is no replication of any AD data between forests
- **Example of when you might use it for security:**
  - Consider exposed IIS web servers that can't be standalones
  - To which forest should they be joined?

SANS Security Essentials – © 2016 SANS

### Cross-Forest Trusts

If you have two forests and all the domain controllers run Windows Server 2003 or later, then you can create a *cross-forest trust*. With a cross-forest trust between the root domains of two forests, all the domains in both forests trust all other domains in both forests. A cross-forest trust must be created manually by you using the Active Directory Domains And Trusts console in the Administrative Tools folder off the Start menu.

### Cross-Forest Trusts Are Transitive

More important, when a cross-forest trust is created, the trust link is transitive for all domains in both of the forests. Recall that a forest can be composed of one or many domains. If the SANS.ORG forest had ten domains and the GIAC.ORG forest had five, then all the domains in both forests would trust every other domain in both forests! To say that a trust link is *transitive* means that the trust passes through in a chain, for example, if A trusts B, and B trusts C, then A also trusts C.

### Cross-Forest Trusts Can Be One-Way or Two-Way

A two-way trust is just two one-way trusts going in opposite directions. Cross-forest trusts are normally two-way, but you can make them one-way instead. For example, you could make the GIAC.ORG forest trust SANS.ORG but not vice versa.

The direction of trust determines *who* can log on *where* and whether permissions and privileges can be granted. By analogy, if I trust you, then you could borrow my motorcycle. It is my trusting you that gives you the opportunity to come back to me and ask for the bike. Hence, access to resources goes in the *opposite* direction as the direction of the trust: I trust you; therefore, you can ride my bike. The same goes for domains and forests.

Hence, if the GIAC.ORG forest trusts the SANS.ORG forest, all the users and computers in all the domains in GIAC.ORG trust all the users and computers in all the domains in SANS.ORG. This means users anywhere in SANS.ORG could be granted privileges and permissions to resources anywhere in GIAC.ORG. But it's one-way only. If you wanted to give a group in GIAC.ORG permission to log on at a workstation in SANS.ORG, you couldn't do it, not possible. Even if you wanted to grant permissions to a shared folder somewhere in SANS.ORG to a user or group in GIAC.ORG, you couldn't do that either. Because the cross-forest trust is one-way only (GIAC --> SANS) it prevents the users in GIAC.ORG from getting any access to resources in the SANS.ORG forest.

### **No Cross-Forest Replication**

Another important fact about cross-forest trusts is that they do not cause any replication of accounts (or any other data) between the two forests. Even with a two-way trust, there is no replication between the forests. This is the opposite of how it works inside a forest. Inside a forest there's a ton of inter-domain AD replication, but between domains in different forests, there is none.

### **How is This Relevant or Important? Give an Example Please!**

Imagine you have a large farm of IIS web servers exposed to the Internet. You want to use Group Policy and single sign-on to simplify their management. Or maybe your web applications require domain membership for users to authenticate with their domain credentials. For whatever reason, though, you need to join all these exposed IIS servers to an Active Directory domain, and that domain must be in some forest somewhere. But which forest? Should you join these IIS servers to a domain in the internal forest with all your other users, computers, and resources? Not if you can help it!

If possible, create a new forest just for the exposed servers that must be domain members (IIS, Exchange, RRAS VPN gateways, DNS, whatever they are). This new forest will likely have only a single domain (call it "EXPOSED.DMZ") and will exist solely for this purpose. Create a one-way cross-forest trust where your EXPOSED.DMZ forest will trust your internal forest, but not vice versa. In this situation, the lack of Active Directory replication between the two forests is a good thing! Because of the one-way trust, compromised users or computers in the EXPOSED.DMZ forest couldn't be granted privileges or permissions on computers in the internal forest even if you or your adversaries wanted to. (Other attacks are possible, though.) If the EXPOSED.DMZ forest gets trashed or rooted, hopefully the damage will stop there and not extend to the internal forest, too. And after the cross-forest trust is established, what does the firewall have to permit from the EXPOSED.DMZ forest to the internal domain controllers? Just Kerberos, not NTLM, SMB, RPC, LDAP or anything else. So, if those exposed servers must be domain members, maybe we could live with the Kerberos traffic...maybe.

# Microsoft Azure Active Directory

- User accounts in Azure AD:
  - Log on to Office 365, Outlook.com, OneDrive, Intune, and Windows
  - Use multi-factor phone authentication
  - Sync with on-premises Active Directory

SANS Security Essentials – © 2016 SANS

## Microsoft Azure Active Directory

Microsoft maintains multiple datacenters around the world with more than 1 million servers in total. These datacenters implement Microsoft's cloud-based services, such as OneDrive, Office 365, Outlook.com, and the hosting of customers' VMs. All the hardware and management software that makes these cloud services possible is called Microsoft Azure; hence, Azure is not a particular service or application, it's the platform on top of which these services and applications run (<http://azure.microsoft.com>).

As an infrastructure, Azure includes things such as the provisioning of VMs, software-defined networking for tenants, load balancing, hotsite failover, geo-redundant backups, and the other essential features that any Infrastructure as a Service (IaaS) cloud provider would have. But Azure was originally designed for Platform as a Service (PaaS) cloud computing, and this is still its primary differentiator from the others. As a platform for running web applications, Azure provides not just networking and VM hosting (like with IaaS), but also the "plumbing" many web applications require, such as load balancing, source code version control, user authentication, and access control. Microsoft's PaaS tries to hide these complexities from developers as much as possible, especially the nuts and bolts of user authentication, so developers can focus on their apps, not the underlying plumbing.

## It's A MAAD, MAAD, MAAD World!

So, what is the point of all this? Azure is not just a bunch of VMs and bandwidth people can rent. Azure is also a planetary-scale identity provider that can support multi-factor user authentication and single-sign on (SSO) to any web application hosted anywhere, on Azure or otherwise. In short, Microsoft wants to be the world's domain controller.

Microsoft Azure Active Directory (MAAD) is what implements the user accounts and groups needed for Outlook.com, OneDrive, Office 365, Intune, Xbox, and many other cloud services. When you upload files to OneDrive, check e-mail at Outlook.com, or run Skype on your Xbox, you are logging on with a user account in

Azure AD. This Azure AD user account is called your Microsoft Account, previously known as your Live ID, Passport Account or Hotmail Account. Azure AD provides single sign-on support for more than 1,400 websites, including Facebook, Twitter, Google Apps, Intuit, Dropbox, SalesForce, and Evernote. (It's not required for these sites; it's just a logon option when you go through <https://myapps.microsoft.com>.) So, you might be using a Microsoft Account right now for something and not even know it.

### **Mult-Factor Authentication**

Azure AD supports multi-factor authentication of users, which is highly recommended over just plain passwords. There are four options and they all involve the user's phone.

At logon, a random PIN number can be sent to the user's phone through SMS, which the user would type into their browser or other application. Or the user could have that PIN pushed to an app on their phone. A third option would be for Azure to dial the user's phone number and ask the user if it actually is that user attempting to log on, and, if not, to press a different button to indicate that it was unexpected and therefore may be a hack attack. Finally, instead of a phone call, a prompt could be pushed to an authenticator app on the user's phone to confirm yes/no that the authentication attempt is expected.

Configuring multi-factor authentication is relatively easy because the real work (sending the SMS text message, checking the PIN, and so on) is all done by the servers in Azure. As an Azure AD admin, you would use either the web portal or PowerShell to confirm that users have phone numbers and then simply choose the multi-factor requirement for them. The authenticator app, if used, would either be installed by the users themselves or installed for them by central IT.

### **On-Premises Directory Synchronization**

Microsoft's long-term goal is for your organization to give up managing your on-premises Active Directory entirely and to use 100 percent Azure AD. For small-sized or medium-sized organizations, this is not only possible, but also cost-effective. For larger organizations, though, this will either never happen or will take more than a decade. (The phrase "over my dead body..." might be going through your head right now.) More practical for larger companies is a hybrid solution in which user accounts, groups, and passwords from the on-premises AD are synchronized up to Azure AD, and with changes in Azure AD optionally synced back down to the on-premises AD.

When you configure the Azure AD Sync tool for this hybrid scenario, the sync can be one-way only (from on-premises AD up to Azure only) or two-way (where some changes in Azure AD are synced back down to the on-premises AD as well). All synchronization occurs over SSL/TLS channels, and when on-premises AD password hashes are synched up to Azure AD, the hashes are first rehashed multiple times with salted SHA256; nevertheless, although this extra hashing is hopefully beneficial, this is all a brave new world of hacking risks to consider. For companies that have committed to Office 365, Exchange Online, SharePoint Online, OneDrive, and so on, the single-sign on conveniences of this kind of hybrid directory synchronization might be worth it. And from Microsoft's long-term perspective, the hybrid approach is what paves the way toward your organization eventually using only Azure AD and giving up your on-premises AD entirely.

If syncing password hashes to Azure AD is totally unacceptable, another route is to use something named Active Directory Federation Services (ADFS) to implement something similar to a cross-forest trust, but ADFS is far beyond the scope of this course.

### **Azure AD Management**

Organizations that use Azure AD are called "tenants" because the visibility and management of an organization's Microsoft Accounts are kept separate from all other customers of Azure. To create or manage

your Azure AD tenancy, you can use the web interface (<https://azure.microsoft.com>) or PowerShell. Because Office 365 and Intune share the same Azure AD tenancy for an organization, the web interfaces for these products can be used too, for example, <https://portal.microsoftonline.com>. Because Azure AD is a SaaS application, it is easier to manage your tenant user accounts in Azure AD than in an on-premises AD, but at the price of loss of control and customization. For several years, then, the most popular solution for larger organizations will be a hybrid approach with some amount of synchronization between local and Azure AD, proxying with AD Federation Services, and workflows performed through Microsoft Identity Manager or similar bridge products.

# Azure Single Sign-On

- Link your user account to a Microsoft Account:
  - Windows 8 and later
  - PC Settings > Accounts
  - Local or global user
- Planetary roaming profile in OneDrive can sync some settings across all machines



SANS Security Essentials – © 2016 SANS

## Azure Single Sign-On

In Windows 8 and later, you can link your logon user account to your Microsoft Account in Azure. When you log on to your computer, you would also log into Azure AD at the same time transparently. This linking works with either a local account in your SAM database or a global account in your on-premises Active Directory. (Don't worry; if you don't want this, it can be blocked through Group Policy.)

To link your logon user account to an existing or new Microsoft Account in Azure, log on to your Windows 8 or later computer, open PC Settings > Users and Accounts > Your Account > and click the Connect to a Microsoft Account link. Now, after you log on to your desktop, you also get single sign-on to Office 365, OneDrive, and the other web services your Metro/Modern apps use, which are designed for Microsoft Account authentication.

## Microsoft Account Versus Organizational Account

Strictly speaking, there are currently two types of user accounts in Azure Active Directory, but this is only a temporary situation until Microsoft consolidates them together. A Microsoft Account is a user account in Azure AD for consumer-oriented services such as Outlook.com and OneDrive, whereas an Organizational Account is a user account in Azure AD intended for business-oriented services such as Exchange Online and Office 365 Enterprise. This distinction is confusing for users, so eventually there will just be one type, but Microsoft hasn't finished the consolidation yet. Some Microsoft/Organizational Accounts will be used only for personal computing, some only for business purposes, and some for both. Although a person might have multiple Microsoft/Organizational Accounts for their various roles and interests in life, this defeats the advantages of Azure single sign-on, so Microsoft hopes this practice will be held to a minimum. Ideally, in Microsoft's eyes, each human on the planet would have just one Microsoft Account for everything.

## Planetary Roaming User Profile

When you connect your logon user account to your Microsoft Account, you also choose which data, if any, should be synced to OneDrive. Any data synced to OneDrive can be downloaded and synced to any other

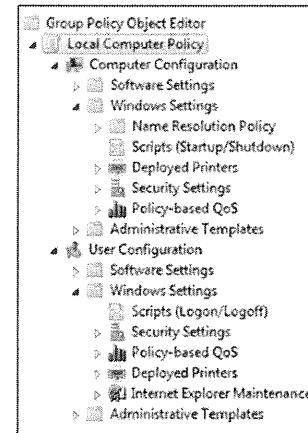
computer where you log on with the same Microsoft Account. Synced data can include saved passwords, Start screen layout, color scheme, installed Metro/Modern apps, Metro/Modern app preferences, Internet Explorer history, Internet Explorer favorites, and other Windows configuration settings. The user or network administrator chooses which data are synced or "roamed" in this way. (Don't worry; this can also be blocked through Group Policy.) Over time, more of this data will be available for syncing to Windows Phone and Xbox, also.

Another goal of Azure AD, then, is not just to provide single sign-on to cloud applications, but also to provide a planetary roaming user profile for every human as they log into their laptops, tablets, phones, game consoles, and automobiles. So, when people talk about cloud computing as just "outsourcing VM management," they're not seeing the Big Picture or where this is all headed in the next several years. Azure Active Directory is at the heart of what Microsoft is planning for the world—whether we like it or not.

# Group Policy

## Group Policy Manages:

- Password policy
- Lockout policy
- NTFS permissions
- Privileges
- Event logs
- Registry settings
- IPSec settings
- And much more



SANS Security Essentials – © 2016 SANS

## Group Policy

Group Policy Objects (GPOs) are some of the most important data replicated through Active Directory. Group Policy is a technology that you can use to configure virtually every security option on the domain-joined computers in your enterprise. Group Policy gives you centralized control that can scale to hundreds of thousands of Windows computers in your forest.

Group Policy is used to manage the following:

- Password policies
- Account lockout policies
- Kerberos policies
- Audit policies
- Custom privileges assignments
- Security options, for example, authentication protocols
- Event log sizes and wrapping options
- Custom memberships in important groups
- Startup options and permissions on services
- Registry key permissions and audit settings
- NTFS permissions and audit settings

# How Group Policy Works

- **GPOs are like configuration scripts stored in Active Directory**
- **GPOs are applied automatically:**
  - At boot-up
  - At logon
  - 90–120 minutes
- GPOs in Active Directory can be applied to domains, sites, and organizational units
- Admin Tool: Group Policy Management Console
- Every computer has a local GPO, too

SANS Security Essentials – © 2016 SANS

## How Group Policy Works

Think of Group Policy Objects (GPOs) as special logon scripts that, when run, can reconfigure almost anything on the computer, including the user's desktop.

When a computer boots up, it downloads the GPOs assigned to it and executes them automatically. Every 90 to 120 minutes thereafter, the computer checks to see that none of its GPOs have been changed, and if any have, then the computer downloads the edited GPOs and runs them automatically, too, even if the computer has not been rebooted.

Similarly, when a user logs on, her computer obtains the GPOs for that user and execute them automatically to reconfigure the user's desktop. Every 90 minutes the computer checks for any newly edited GPOs and reapplies them. Some settings do not take effect until after the user logs back on again, but many settings apply immediately.

If you want to see a Group Policy Object on Windows Vista/7, go to the Start menu > All Programs > Administrative Tools > Local Security Policy. On Windows 8 and later, go to the Start screen and just start typing **Local Security Policy** and tap the icon. This is your local GPO. It applies only to your computer, not to other machines in the domain, and it applies even if your machine is a standalone. It defines your local security policies, which may then be overwritten by domain GPO policies.

On an AD domain controller running Server 2008, you can see a domain-wide GPO by going to Start > Programs > Administrative Tools > Default Domain Policy. To edit any of your GPOs on Server 2012 or later, open the Server Manager tool, pull down the Tools menu, and select Group Policy Management. The Group Policy Management tool can also be installed on older domain controllers, too.

If you have the Group Policy Management Console installed instead, double-click your forest > double-click your domain > right-click on the Default Domain Policy icon > Edit. The GPMC is a free download from Microsoft and is built in to Windows Vista and later. The GPMC is your primary tool for managing Group Policy after you become more familiar with GPOs.

Domain GPOs are stored in the AD database and replicated to all domain controllers. Each Organizational Unit in AD can have completely different and separate GPOs linked to it. When a domain GPO is linked to an OU instead of to the domain, it applies only to the users and computers in that OU.

# Summary

- Operating Systems:
  - Client
  - Server
  - Embedded
- Workgroups
- Local versus Domain Accounts
- SIDs and SATs
- Active Directory
  - Domains
  - Forests
  - Azure AD
- Authentication:
  - Kerberos
  - NTLM
- Forests and Trusts
- Group Policy

SANS Security Essentials – © 2016 SANS

## Summary

The purpose of this section was to provide the necessary background information to understand what follows.

We started with an overview of the many different operating systems available from Microsoft. If security is your prime concern, and if your organization has the money, upgrade to at least Windows 7 if you can.

Windows 2000 and Windows XP are obsolete; let them rest in peace. Next, we talked about how Windows computers can be made to share resources with each other and be managed.

Workgroups are composed of standalone computers, each with its own separate user accounts database. A domain is a set of computers that all use a shared accounts database called Active Directory. Domain controllers are the servers that manage this database on behalf of the other computers in the domain. A user must authenticate to a domain controller before being permitted to log on to his desktop, and domain controllers authenticate users when they attempt to access other servers over the network. Microsoft Azure Active Directory is the authentication provider for Office 365, OneDrive, Xbox, and other cloud-hosted services.

The two main authentication protocols used on Windows networks are Kerberos, which is the default, and NTLM, which is retained for backward compatibility and used when Kerberos is unavailable. Both Kerberos and NTLMv1 authentication traffic can be sniffed to extract crackable information, but NTLMv1 is trivial to crack in comparison to the difficulty of brute-forcing Kerberos passwords.

A theme throughout this section has been the authorization mechanisms providing the security infrastructure. Every user, computer, and group is uniquely identified by a Security ID (SID) number. Your identity on the network is defined by your Security Access Token (SAT) which lists your SIDs and privileges on any given machine. Every program you run gets a copy of your SAT so that the operating system can know who is behind each program's requests and actions. Hence, the operating system can enforce permissions and privileges restrictions.

Active Directory domains in a forest always have two-way transitive trusts between them, forming the *complete trust* domain model, and they multi-master replicate their data.

Finally, we briefly talked about Group Policy, perhaps the most important security tool in your arsenal for locking down your network.

Websites Mentioned:

- Cain & Abel ([www.oxid.it](http://www.oxid.it))
- Windows Client ([www.microsoft.com/windows/](http://www.microsoft.com/windows/))
- Windows Server ([www.microsoft.com/windowsserver/](http://www.microsoft.com/windowsserver/))
- Windows Phone ([www.windowsphone.com](http://www.windowsphone.com))
- Windows Embedded ([www.microsoft.com/windowsembedded/](http://www.microsoft.com/windowsembedded/))
- Kerberos ([web.mit.edu/kerberos/www/](http://web.mit.edu/kerberos/www/))
- Kerberos Cracker ([ntsecurity.nu](http://ntsecurity.nu))

# Module 24: Service Packs, Hotfixes, and Backups

---

SANS Security Essentials – © 2016 SANS

## **Module 24: Service Packs, Hotfixes, and Backups**

This section intentionally left blank.

# Service Packs, Hotfixes, and Backups

---

## SANS Security Essentials V: Windows Security

SANS Security Essentials – © 2016 SANS

### Service Packs, Hotfixes, and Backups

Service Packs and hotfixes must be obtained, tested, installed, and checked. This is a painful but absolutely necessary task when securing Windows boxes. Service Packs and hotfixes also must be coordinated with one's backups so that successful restores are possible if something goes wrong. If you do anything less than a full restore of the operating system on a machine that has had a later Service Pack applied, chances are the restore will fail to make a viable OS. Backups also are critical for disaster recovery, auditing, forensics, and getting back quickly to square one in the lab when testing new changes. Not having good backups also is just the sort of thing that can get you fired, so it's important to talk about having them.

This module discusses techniques for applying Service Packs, installing hotfixes, and managing backups. In particular, this module covers:

- Slipstreamed Service Packs
- Scanning for Missing Patches
- Microsoft Update
- Windows Server Update Services (WSUS)
- Windows Backup (NTBACKUP.EXE)
- Binary Drive Images
- System Restore

# Windows Patches and Hotfixes

---

The student will understand how to manage Windows Service Packs and Hotfixes for a network of Windows hosts.

SANS Security Essentials – © 2016 SANS

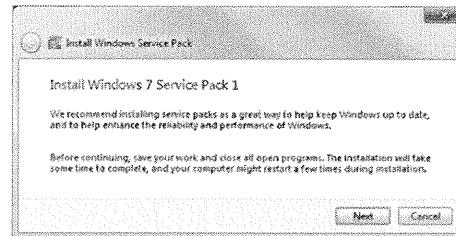
## **Windows Patches and Hotfixes**

This section intentionally left blank.

# Service Packs (1 of 2)

- **Service Pack = Large Collection of Patches**

- Test service packs in a lab on representative systems using virtual machines
- Do staged roll-outs and check for issues along the way



SANS Security Essentials – © 2016 SANS

## Service Packs (1 of 2)

A Service Pack is a collection of updates and hotfixes rolled up into one large installation package (typically 100 MB to 300 MB in size). It is critical for security that the latest Service Pack be installed on vulnerable systems.

You can get the latest Service Pack for all the Windows operating systems from Microsoft's main download website (<http://www.microsoft.com/downloads/>).

### Testing and Staging Deployments

A guaranteed recipe for disaster is to obtain a new Service Pack or patch and install it throughout the enterprise without testing it first. Though it is critical to install the latest Service Pack, doing so can break applications or cause network problems. The applications that break usually can be updated themselves, and the network problems usually can be solved, but you don't want to discover these issues the hard way.

The gentle way of discovering Service Pack problems is:

1. Test new Service Packs in a lab.
2. Deploy Service Packs in stages to limited groups of computers, starting with the least important systems and ending with the mission-critical ones, while checking for problems along the way.
3. Each mission-critical server should be assigned one or more individuals who are responsible for testing new updates, ensuring full backups are made before updates are applied, and monitoring for problems afterward.

A testing lab should have at least one representative computer for each type of system found on your network. Hardware and installed software should be as similar as possible to the varieties you actually have. If money is tight, then computer emulation products such as VMware Workstation (<http://www.vmware.com>) or Microsoft

Hyper-V (<http://www.microsoft.com>) can help, but it's best to have the actual steel and silicon. It usually takes only one bad software rollout to convince management that purchasing a few test systems can actually save the company money. (In addition, you need disposable computers when practicing your hacking skills . . . just don't tell that to the MBAs.)

Performing staged deployments is just extending the "lab" to the production network a few boxes at a time. Find the least valuable or most despised users on your network and make them your unwilling guinea pigs. If all goes well, then roll out the new software in ever-widening circles until the entire LAN is upgraded. Unless there are red-hot issues that will be fixed by the update, mission-critical servers and the desktops of management should be upgraded last. Ensure you have a full backup of the critical systems first, and consider doing the install during off-peak hours.

#### **Can't Group Policy Do It?**

Group Policy can be used to push out Service Packs to computers automatically. This is possible because Windows Service Packs come with a file named UPDATE.MSI, which can be used by the built-in Windows Installer service on each machine to handle the installation process. In fact, with an application from InstallShield (<http://www.installshield.com>) or Symantec (<http://www.symantec.com/business/package-studio>) you can create your own MSI files and push out virtually any software you want to your systems hands-free.

# Slipstreaming (2 of 2)

## Install OS and SP at the same time:

1. Copy Windows DVD to a shared folder
2. UPDATE.EXE -S C:\SharedFolder
  - This will merge the SP into the OS installation files
3. Burn a copy of the shared folder to a DVD
  - This can be bootable if you want
4. Install Windows OS from the share or the DVD, and the SP will be merged in simultaneously

SANS Security Essentials – © 2016 SANS

### Slipstreaming (2 of 2)

Wouldn't it be nice to install the operating system and the latest Service Pack in one shot? You can do it if you "slipstream" the Service Pack into the installation process!

Here's the recipe:

1. Copy the entire Windows DVD to a folder on the local server where you are sitting.
2. Get the latest Service Pack from Microsoft, and extract its files to another folder (not the folder in the prior step) by running the Service Pack executable with the "-X" switch, for example, W2KSP3.EXE -X. You will be prompted for the target extraction folder.
3. In the extraction folder, go to the \i386\Update\ subdirectory and run the following command: UPDATE.EXE -S:*PathToInstallFolder*, where *PathToInstallFolder* is the full path to the local folder where you copied the Windows DVD. The "-S" switch merges the files from the Service Pack into the \i386 folder with the OS files, overwriting the older versions of the same files there.
4. Share that installation folder on the network and burn a copy of it onto a DVD. This can be bootable if you want (<http://www.nu2.nu/bootablecd/>).
5. Install Windows from either the shared folder or the DVD, and the merged Service Pack will be installed automatically at install time!

# Hotfixes (1 of 4)

- A hotfix updates an application or OS binary file
- Hotfixes are later bundled into the next Service Pack
- **Obtaining, testing, deploying, and auditing hotfixes consumes a great deal of your time as the security administrator, but it's necessary!**
- Download hotfixes by hand from:
  - **<http://www.microsoft.com/security/>**

SANS Security Essentials – © 2016 SANS

## Hotfixes (1 of 4)

A *hotfix* is a small program from Microsoft that can replace one or a few operating system files currently on the hard drive with updated versions. A hotfix usually is intended to fix a single problem or patch a single hole, but there also are *roll-up* or *cumulative* hotfixes that fix many issues at once. Often a variety of hotfixes will be released to deal with a new spate of related problems; then Microsoft bundles these patches together into one roll-up hotfix.

Staying on top of the latest hotfixes, testing them, rolling them out to boxes, and auditing their correct distribution will consume a great deal of your time. And, again, it is essential to the security of your network that you test and apply patches soon after their release, especially on Internet-accessible servers.

You can download the latest patches and roll up hotfixes from Microsoft's security site (<http://www.microsoft.com/security/>). The best way to stay on top of new patches, though, isn't by visiting Microsoft's website four times a day. The easiest way to keep on top of new hotfixes, exploits, viruses, and so on, is by subscribing to free e-mail security bulletin services and joining security mailing lists.

## E-Mail/Newsfeed Bulletins (2 of 4)

- This is the easiest way to stay on top of new changes
- It's almost impossible to do your job well if you're not subscribing to some form of security bulletin and/or patch announcement service!
- Many excellent bulletins are free!
  - <http://www.sans.org/newsletters/>
  - <http://www.microsoft.com/security/>
  - <http://www.secunia.com/advisories/>
  - <http://www.packetstormsecurity.com>

SANS Security Essentials – © 2016 SANS

### E-mail/Newsfeed Bulletins (2 of 4)

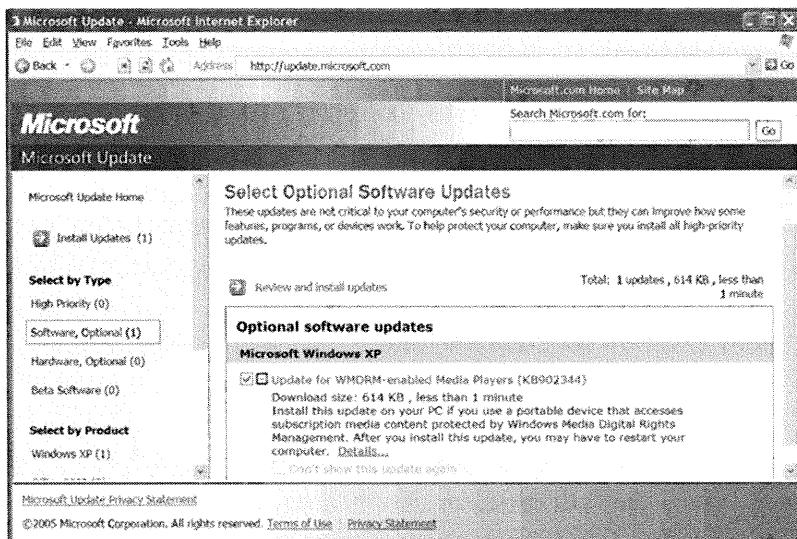
Subscribing to e-mail security bulletins and mailing lists is so important for staying up to date on risks. Perhaps if one is browsing security and hacking websites every day, then maybe it isn't necessary to subscribe to anything, but it sure makes work more difficult. Besides, many interesting people work in your field; you should get to know them!

Which bulletins to subscribe to? You can find some of the most popular services and lists at the following websites, and all are free:

- <http://www.sans.org/newsletters/>
- <http://www.microsoft.com/security/>
- <http://www.secunia.com/advisories/>
- <http://www.securityfocus.com/archive/>
- <http://www.packetstormsecurity.com>

If you'd also like to browse security sites to stay informed, then a good place to start is <http://packetstormsecurity.com>. The Packetstorm website is easy to search, contains a variety of articles from different perspectives on security, and usually has a link to any hacking/security tool you are likely to try to find.

# Microsoft Update (3 of 4)



SANS Security Essentials – © 2016 SANS

## Microsoft Update (3 of 4)

Microsoft Update is a site (<http://update.microsoft.com>) that can load an ActiveX control into Internet Explorer to scan your system for missing hotfixes and then install them. It is popular and extremely easy to use.

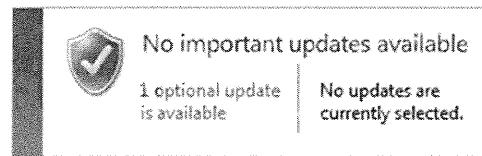
The Microsoft Update site supports Exchange Server, SQL Server, Office applications, beta software, optional software, device drivers, and more. Eventually, all Microsoft software will be supported here so that you won't have multiple hoops to jump through to patch a Windows box.

The bad thing about Microsoft Update, though, is that it isn't automatic. Wouldn't it be nice if your machine just patched itself every night without any hassles?

# Windows Update (4 of 4)

- Just like Microsoft Update but automatic:

- Hands-free
- Scheduled
- Configured in Control Panel



SANS Security Essentials – © 2016 SANS

## Windows Update (4 of 4)

Windows Update is just like Microsoft Update, but it's hands-free. Windows Update, which used to be called Automatic Updates, connects in the background on a scheduled basis and then prompts only the user to install the hotfixes after they have been downloaded.

Windows Update is built in to Windows. See the Windows Update applet in Control Panel, or, in Windows 8.1 and later, go to Change PC Settings > Update and Recovery > Windows Update. You can disable Windows Update entirely or require your interaction for the hotfixes to be downloaded and/or installed.

Also, each month Microsoft collects all their latest patches and bundles them into a single ISO file, which you can download and burn to CDs for manual deployment (<http://support.microsoft.com/kb/913086>).

Update and recovery

Windows Update

You're set to automatically install updates.

There aren't any updates to download automatically, continue to check daily for newer updates.

View details

Check now

View your update history

Choose how updates get installed

# Windows Server Update Services (WSUS)

- **Your own local Automatic Updates Server:**

- Not just hotfixes, Service Packs, too
- Not just Windows, also Exchange, SQL Server, Office, and more
- Built in to Windows Server (free) as an IIS web application

- **With your own internal WSUS Server:**

- Control exactly which hotfixes to deploy.
- Clients can download from your WSUS Server or from Microsoft.
- Create your own custom groups of computers.
- Scale up to thousands of machines when deployed in an array.

SANS Security Essentials – © 2016 SANS

## Windows Server Update Services (WSUS)

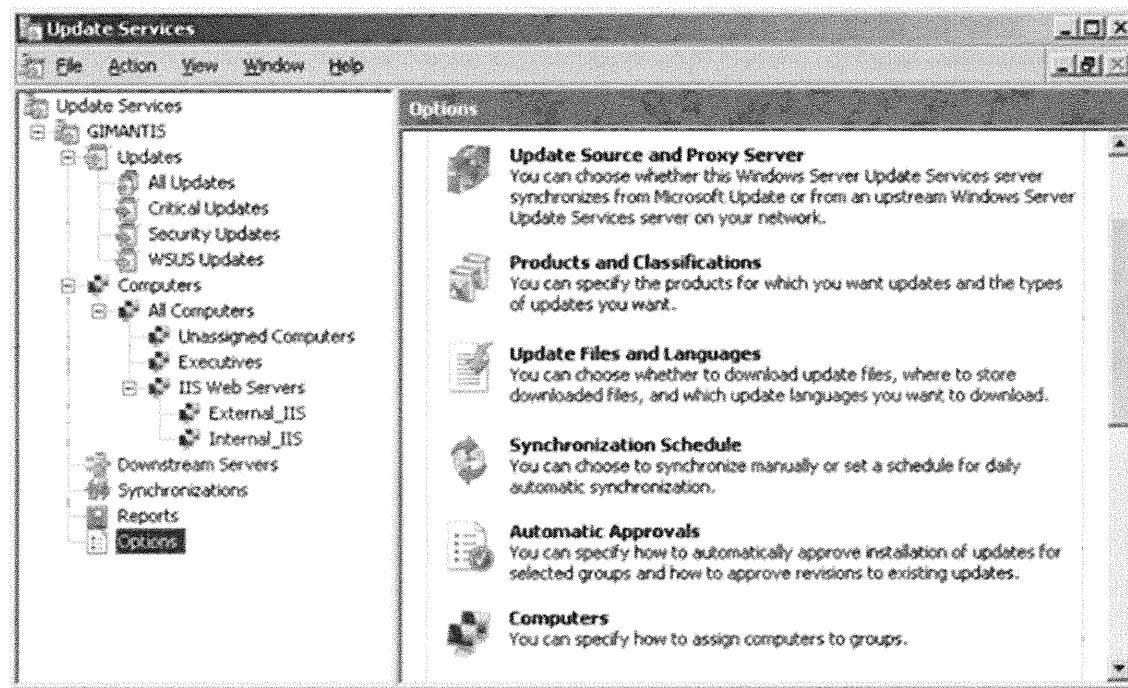
Windows Server Update Services (WSUS) is Windows Update but hosted internally on your own server(s). Client support for WSUS is installed automatically with Windows.

WSUS has several advantages for patch management:

- WSUS is free because it's built in to Windows Server as an IIS web application.
- The WSUS Server administrator chooses exactly which patches to distribute, and custom groups of computers can be created with different sets of patches approved for each group, for example, Exchange Servers, Laptops, and so on.
- WSUS clients can connect to a local WSUS Server and download their hotfixes from there instead of connecting to Microsoft, but this is configurable.
- To use WSUS, users do not have to be members of the Administrators group on their computers. In fact, WSUS clients can download and install updates even if no one is logged on at the machine.
- WSUS provides updates not just for Windows and Internet Explorer, but also for SQL Server, Exchange Server, Microsoft Office, and most other Microsoft products.
- WSUS not only distributes security hotfixes, but also Service Packs and non-security patches, such as critical device driver updates, and even some beta-version software.
- WSUS permits the grouping of computers into custom sets that can be managed and updated separately. For example, some machines might download and install updates automatically, whereas others must be updated manually. Different sets of updates can be (dis)approved for different groups of computers. These computer groups are defined by the WSUS administrator.
- A single WSUS server can handle more than 10,000 client computers, and WSUS servers can be load-balanced and chained together to form administrative arrays.

- WSUS logs to a local SQL Server database that can be queried to identify, for example, which machines have (not) successfully received a particular update, which updates are pending approval, installation failures, update histories, and other information. SQL Server does not have to be purchased separately.

Although WSUS itself is free, keep in mind that you still need to purchase hardware, Windows Server licenses, and client CAL licenses like normal. For more information about WSUS and to download it, visit <http://www.microsoft.com/wsus/>.



### How Does WSUS Work?

One or more local WSUS Servers can be installed on Windows Server 2003 or later as an IIS application. The WSUS Servers will connect to Microsoft and download the latest information about available updates on a scheduled basis (the schedule is determined by the administrator).

Administrators choose exactly which updates they want distributed inside the LAN to WSUS clients. Presumably, this is after the administrator has tested the patches in a lab. You select which hotfixes you want deployed in the WSUS console.

The patch files from Microsoft can be downloaded to the local WSUS Server and then downloaded by clients from there, or clients can be directed to download the approved updates directly from Microsoft. Caching the files locally on the WSUS Server, of course, spares Internet bandwidth consumption. If you have a large number of clients, you can make your other WSUS servers download their files from your master WSUS Server that downloads from Microsoft.

WSUS clients download updates using the Background Intelligent Transfer (BITS) service. BITS "drizzles" files down to the client in the background so that other applications are not interrupted and bandwidth is not monopolized by WSUS traffic. Clients can and should use SSL/TLS to download from WSUS.

## **WSUS Administration**

WSUS is installed with the Server Manager tool like any other role or feature. During installation, a wizard is launched that can walk you through the configuration process. Afterward, you can use the Windows Server Update Services console in the Administrative Tools folder to manage WSUS options or to run the wizard again.

WSUS clients are configured through Group Policy or simple Registry edits on standalones. WSUS clients are informed of their local WSUS Server's HTTPS path, the schedule for checking for new updates, and whether the updates should be installed automatically. Clients download the patches from the local WSUS server using HTTP or HTTPS, but HTTPS is recommended to benefit from the SSL/TLS.

Users can be permitted to have full control over the update process (requiring their approval for both download and the installation of hotfixes), or WSUS can work in the background at night to install and reboot machines, even when no one is logged on at them. (If someone is logged on when the installation process begins, the user gets a warning to save her data and log off.)

One of the benefits of WSUS is the ability to create your own custom groups of computers, and then approve or deny different sets of updates for each group of computers. For example, the patches and Service Packs approved for the Executives computer group will likely be different than the updates for the External\_IIS computer group. These groups are defined and used within WSUS alone; they do not require or use Active Directory groups.

# Third-party Patch Management

Excellent non-Microsoft products available, too:

- IBM Endpoint Manager ([www.ibm.com](http://www.ibm.com))
- Altiris ([www.symantec.com](http://www.symantec.com))
- Ecora ([www.ecora.com](http://www.ecora.com))
- Gravity Storm ([www.securitybastion.com](http://www.securitybastion.com))
- Lumension Patch ([www.lumension.com](http://www.lumension.com))
- Shavlik Technologies ([www.shavlik.com](http://www.shavlik.com))
- System Center Configuration Manager ([www.microsoft.com](http://www.microsoft.com))
- And many other companies that can't all be listed here...

SANS Security Essentials – © 2016 SANS

## Third-party Patch Management

WSUS isn't perfect, of course, and a variety of non-Microsoft tools exist to help manage hotfixes and patches, too. When comparing products, make sure to ask the vendors if their products can install the hotfix or Service Pack automatically and whether the product requires "agent" software to be installed first. Note, too, that there are vast differences in price between these products.

Many other companies provide wonderful patching solutions as well, but they all can't be listed here. If your current solution isn't on the preceding list, that doesn't mean it's bad or not as good as these.

When researching patch management solutions, consider browsing the [www.WindowsITpro.com](http://www.WindowsITpro.com) site and finding its latest article on this topic. Usually each year the magazine does an article with a comparison/contrast of the most popular update management solutions.

# Windows Backup and Restore

---

The student needs to understand best practices to manage Windows backups and to restore a Windows host from backup data.

SANS Security Essentials – © 2016 SANS

## **Windows Backup and Restore**

This section intentionally left blank.

# Importance of Backups for Security

- Eventually you *will* get hacked or infected....
- **Imagine you had to choose between having a perimeter firewall and having a good enterprise-wide backup system. Which would be better for security?**
- Having current backups is needed for:
  - Forensics analysis
  - Performing audits against a baseline
  - Disaster recovery
  - Accidental data deletion
  - Compliance with regulations

SANS Security Essentials – © 2016 SANS

## Importance of Backups for Security

Having good backups is indispensable for doing post-attack and post-infection forensics, performing an audit against a prior baseline, surviving natural or deliberate disasters, restoring accidentally lost data, and staying in legal compliance. You also need to perform a backup on critical systems before you apply a new Service Pack or patch so that you quickly can get back to square one if the update breaks something critical.

You have to assume that *eventually* your servers will be rooted, your workstations will get infected, and your databases data-diddled into garbage, so what is your plan for recovery? Every security system eventually fails, but a failure doesn't have to be a *Game-Over* catastrophe. You can live to fight another day, but only if you can recover your data. Your hardware, bandwidth, services and reputation can (usually) be replaced, but it's your data that cannot be replaced, it can be restored only from backups.

What if you had to choose between having a perimeter firewall and having an enterprise-wide reliable backup system for all servers and workstations. Assume you can't have both. Which would you choose? Which would be more important for *security*?

"The single most important thing any company or individual can do to improve security is have a good backup strategy."

—Bruce Schneier, CRYPTO-GRAM Newsletter (15.Jul.2008).

# Windows Server Backup

- Built-in backup management application:
  - WBADMIN.EXE and PowerShell scripting support
- Option to backup to Microsoft Azure:
  - Server 2012 and later
  - Monthly fee per gigabyte saved
  - Passphrase to generate key (not shared with MS)
  - Backup changes at the block level, not file level

SANS Security Essentials – © 2016 SANS

## Windows Server Backup

With Server 2008 and later, an optional feature that can be installed with the Server Manager tool is Windows Server Backup (WSB). WSB has multiple wizards to walk you through the process of manually backing up all/some volumes, scheduling automatic backups, working with System State backups, and performing "bare metal" restores. A System State backup includes the Registry and other data that is unique to a particular machine.

WSB is fully integrated into the Volume Shadow Copy system, hence, it can back up locked or open files.

When volumes are restored, you can do a full restore onto a naked drive after a total failure, restore a whole volume, or restore selected folders and files only. WSB is intended to be as easy to use as possible, even if it lacks many of the features found in commercial third-party backup solutions. WSB handles such details as full versus incremental backups in a way that is transparent to the user, including deleting the oldest versions of files in the backup to make space for new files. Backups can be saved to external hard drives, DVDs, virtual hard disks, or to shared folders on the network. On Server 2012 and later, there is also an option to save data directly to Microsoft Azure over the Internet.

WBADMIN.EXE is the command-line management tool for WSB. It has the same capabilities as the graphical WSB console and can be scripted. And on Server 2012 and later, there is PowerShell support, too, and eventually the WBADMIN.EXE tool will be deprecated.

## Azure Backup

On Windows Server 2012 and later, Windows Server Backup can back up data directly over the Internet to Microsoft's Azure cloud storage service for a fee ([azure.microsoft.com](http://azure.microsoft.com)). Files are compressed and encrypted

locally before being uploaded so that Microsoft cannot read the files. The encryption key is derived from a user-configured passphrase. The longer and more complex the passphrase, the better the encryption. All communications are SSL/TLS-encrypted on TCP/443. You can also set a retention policy such that any additional backups of a particular file older than X number days is deleted; the last version of any file backed up, though, will not be deleted even if it is older than X days.

After the initial full backup, which may consume a lot of bandwidth for many hours, only changed blocks of data are backed up. A file is composed of one or more blocks, hence, after backing up a 1 GB file, if only a few kilobytes of that file are modified, only the blocks containing the changed data are backed up, not then entire 1 GB file again. When you have consumed 80 percent of your quota limit, the management tool displays alerts.

When the customer account is created with Microsoft and the agent is installed, the rest of the configuration takes only a few minutes. It is expected that third-party vendors will offer their own cloud storage solutions, and Microsoft is encouraging them to use Windows Server Backup, hence, you should use the same tools whether you back up files to Microsoft's cloud-accessible servers or to someone else's. Currently, the Azure Backup service is only for servers, and there are no public plans to extend it to client operating systems, too; though this may change.

# Third-party Backup Solutions

---

## Many excellent non-Microsoft backup solutions available:

- ARCserve ([www.ca.com](http://www.ca.com))
- Backup Exec and NetBackup ([www.symantec.com](http://www.symantec.com))
- UltraBac ([www.ultrabac.com](http://www.ultrabac.com))
- EMC Networker ([www.emc.com](http://www.emc.com))
- Backup Express ([www.syncsort.com](http://www.syncsort.com))
- Archive ([www.commvault.com](http://www.commvault.com))
- OmniBack II and Data Protector ([www.hp.com](http://www.hp.com))
- And others that can't all be listed here...

SANS Security Essentials – © 2016 SANS

### Third-party Backup Solutions

There are many excellent third-party backup products for Windows. Good starting points in your search for better solutions are the following:

- *ARCserve* (<http://www.ca.com>)
- *Backup Exec and NetBackup* (<http://www.symantec.com>)
- *UltraBac* (<http://www.ultrabac.com>)
- *EMC Networker* (<http://www.emc.com>)
- *Backup Express* (<http://www.syncsort.com>)
- *CommVault Archive* (<http://www.commvault.com>)
- *OmniBack II and Data Protector* (<http://www.hp.com>)

Just as with third-party patch management solutions, though, these products will scale better, but they're not free.

# Binary Disk Images

## • Examples: Acronis and Symantec Ghost

- Creates an image file of an entire drive or partition
- The image file can be searched, edited, and updated
- Can be used for backup/restore of files and folders
- Can be used to create virtual machine image files
- Can be used for application and OS upgrades
- Can be used for baseline comparisons and forensics
- Does not always require a reboot (depends on product)

SANS Security Essentials – © 2016 SANS

## Binary Disk Images

A special type of backup involves creating a *binary image* of the desired disk or partition. The image contains a complete snapshot of the entire volume, including the boot sector.

A binary disk image can be reapplied to the original machine from which it was made to completely restore the machine to its state at that time. You don't have to worry about open files, transaction logs, the Registry, or other ephemeral data structures being missed because the image captures all file data. This is a problem with many regular backup programs, even if they *claim* to backup and restore all files no matter what. A binary disk image also can be applied to another drive on another machine entirely to replicate the original one, including to virtual machines.

Image files can be saved to another hard drive or partition, written to tape, burned to a DVD, or copied across the network to a server. If the image file is too large for the media chosen, many imaging products split the file into manageable chunks; during the restore process, the imaging software requests the various chunks as needed to reconstruct the original data. Also, restoring from a disk image usually is faster than restoring from more traditional formats.

Recent versions of Symantec Ghost and Acronis Recovery, for example, can be used to backup and restore folders and files without a reboot, deploy software or OS upgrades, create a virtual machine image file, and the image of a drive can be searched and edited, too.

A full disk image backup can also be used later for baseline comparisons and forensics when a host is suspected of being compromised.

# System Restore

- **Time machine for the Registry and file changes**
- **System Restore points are made:**
  - Every 24 hours
  - Just before Automatic Update installs files
  - Just before a prior snapshot is restored
  - Just before a new application or driver is installed
  - Anytime the user manually requests it
- Previous versions of user data files can be restored, too

SANS Security Essentials – © 2016 SANS

## System Restore

System Restore is available on Windows XP and later. It works invisibly in the background, saving snapshots of your computer's configuration. These snapshots are saved for weeks. The good thing is, if you have problems, you can use the System Restore Wizard to reinstall one of those saved configurations. It's like a having a time machine for the operating system.

You launch the wizard by going to Control Panel > System > System Protection. Windows Server does not have System Restore *per se*, but it does have shadow copies (see next few slides).

The System Restore snapshot, called a restore point, is created automatically at a variety of times:

- Just after installing the operating system
- Every 24 hours thereafter
- Just before Automatic Updates install new files
- Just before a user installs new software
- Just before installing a new driver
- Just before Windows Backup restores any files
- Just before a restore point is restored
- Whenever the user manually makes a restore point using the System Restore Wizard

Depending on the amount of free space on the hard drive, there might be checkpoints available for the prior one to three weeks!

### **System Restore Includes User Data Files?**

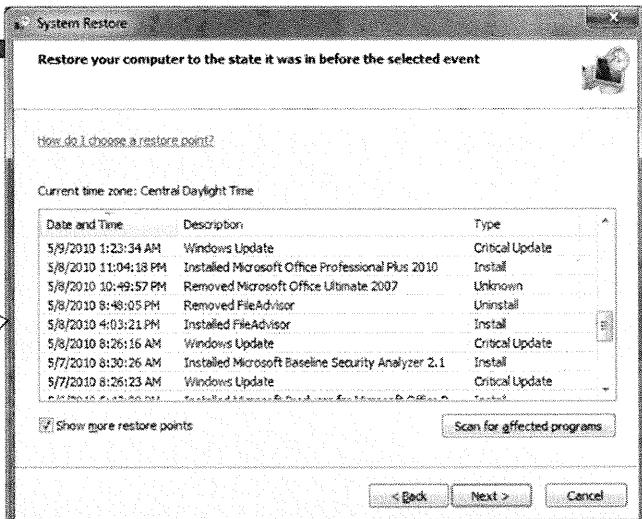
System Restore does not restore user data files in Windows XP. In Windows Vista and later, however, System Restore points do include changed data files, and older copies of folders and files can be accessed by going to the Previous Versions tab in the properties of those folders and files.

Windows XP expired in 2014, so this note shouldn't be necessary, but because of XP's popularity it is still widely believed that System Restore snapshots do not include user data files in any client OS, but this isn't true for Vista and later.

System Restore is not a replacement for full disk image backups or off-site disaster recovery backups of data files, but it is easy to enable and is handy.

# Selecting a Restore Point

To Open:  
Control Panel >  
System >  
System Protection



SANS Security Essentials – © 2016 SANS

## Selecting a Restore Point

When you launch the System Restore Wizard, you see the available restore points. You simply select the restore point you want, and your system's configuration is rolled back to that state. If you regret this action, no worries; another restore point is created automatically right before you to restore a prior one.

If you absolutely want to guarantee that a restore point is available at a certain time, then use the System Restore Wizard to request an immediate snapshot. This is a good practice whenever you are about to install a new application or device driver, or when you are about to attempt an uninstall of the same.

If nothing else, System Restore has the potential to save you hours of drudgery when fixing servers or users' desktops. If you know that the box was working fine yesterday, you can restore the system's configuration to what it was 2 days ago, and you've got a good chance it will fix the problem. You can even make and restore snapshots over the network with a script!

## Device Driver Rollback

Another feature somewhat related to System Restore is just for device drivers. After installing a new driver to replace or upgrade a prior one, the new driver may not function correctly. You can roll back the entire system using System Restore, but there is a quicker method. Go to the System applet in Control Panel > Hardware tab > Device Manager > go to the properties of the updated driver > Driver tab > click the *Roll Back Driver* button.

# PC Reset Versus PC Refresh

## • PC Reset:

- Format drive, optional sector scrub
- Reinstall Windows

## • PC Refresh:

- Keep user data
- Keep some preferences
- Keep Windows Store apps
- Delete all non-Store applications
- Reinstall Windows without reformatting

Requires  
Windows 8  
or later

SANS Security Essentials – © 2016 SANS

## PC Reset Versus PC Refresh

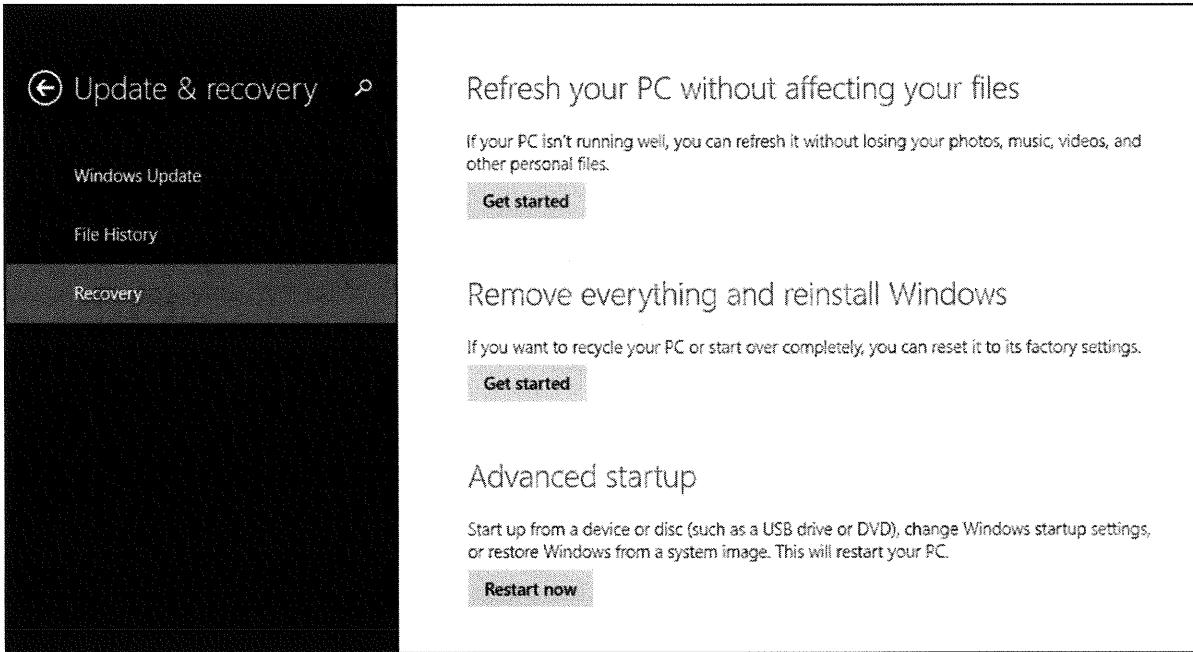
Windows 8 and later clients can easily reset their computers back to the factory defaults as an extreme form of system restore. This is called PC Reset, and on Windows 8.1 and later the reset button is located in Change PC Settings > Update & Recovery > Recovery > Remove everything and reinstall Windows > Get Started. Notice the "remove everything" part? A PC Reset deletes all data files, applications and preference settings. This is the "nuclear option" when no other technique fixes the computer or rids it of stubborn malware. However, a kiosk or dumb terminal could be reset every night.

When performing a reset, the computer reboots into the Windows Recovery Environment (Windows RE) from the hidden management partition, formats the OS drive, and reinstalls a new OS. If you choose the "thorough" option when performing a reset, every sector of the volume which originally contained the OS and data files will be overwritten with random bits in a single pass. If the drive is encrypted with BitLocker, the sector scrub isn't necessary because keying data will be deleted and overwritten with any reset.

A PC Refresh, however, is not so harsh. PC Refresh keeps your data files and personalization preferences, but other settings are restored to their factory defaults. BitLocker options and wireless connection settings are preserved, but firewall rules and non-Metro application licensing information are not preserved. Any apps installed from the Windows Store are kept, but any other applications installed from other sources are removed. When troubleshooting, the refresh method should be attempted first. The refresh button on Windows 8.1 and later is located in Change PC Settings > Update & Recovery > Recovery > Refresh your PC without affecting your files > Get Started. With a solid state drive, a refresh should require less than 10 minutes.

When performing a refresh, the computer reboots into Windows RE, searches the OS volume for data/preferences/applications, makes a backup copy, does not reformat, reinstalls the OS, restores data/preferences/applications.

If the computer suffers a few bad reboots in a row, Windows 8 and later automatically boots into Windows Recovery Environment. A PC Reset or PC Refresh can also be initiated from within Windows RE. To prepare for the worst case scenario, go to the Recovery icon in Control Panel, and create an external recovery drive with everything necessary to do a full restore from a bootable DVD or USB flash drive.



### Windows Vista/7 Backup And Restore Center

Isn't there a nice graphical tool built into Windows client operating systems for doing data file backups? Not really. On Windows Vista/7, the Backup And Restore Center applet in Control Panel allows you to backup and restore data files in a very limited and frustrating way. The applet was unpopular and rarely used, so Windows 8.1 removed this feature entirely.

It is possible that someday a built-in backup solution will be added back again by Microsoft for client operating systems, but don't hold your breath. What Microsoft really wants you to do is to create and keep all your data files in the Azure cloud on OneDrive, where Microsoft will back up your data for you. So, if a built-in backup application reappears in Windows clients, it might only support backups to Azure, just like Windows Server Backup (WSB).

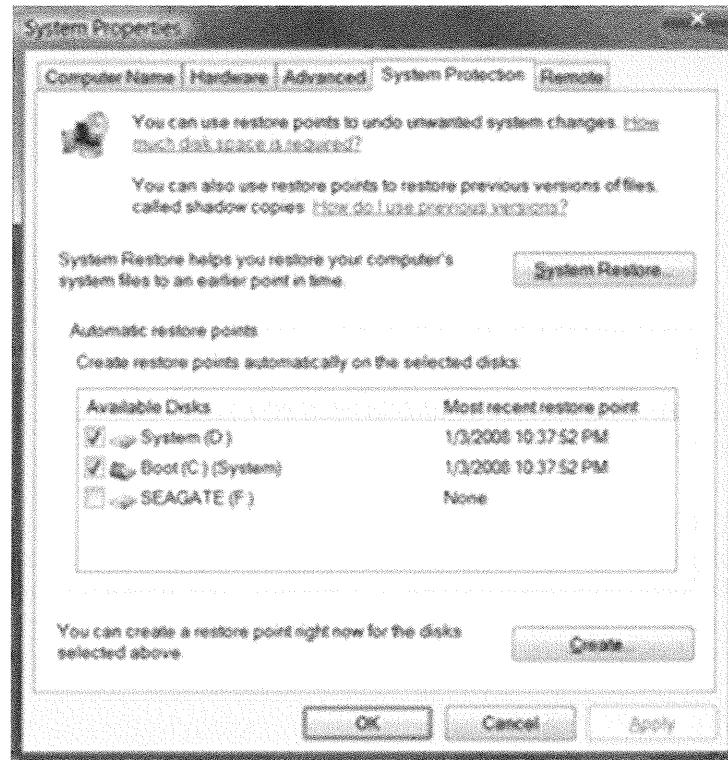
# Previous Versions & File History

- **System restore can include data files, too:**
  - In Windows 8 and later, it is now called **File History**
  - File History is not enabled by default
- **Choose which volumes are covered:**
  - Control Panel > System Applet > System Protection
- **To restore a folder or file:**
  - Right-click folder or file > Properties > Previous Versions

SANS Security Essentials – © 2016 SANS

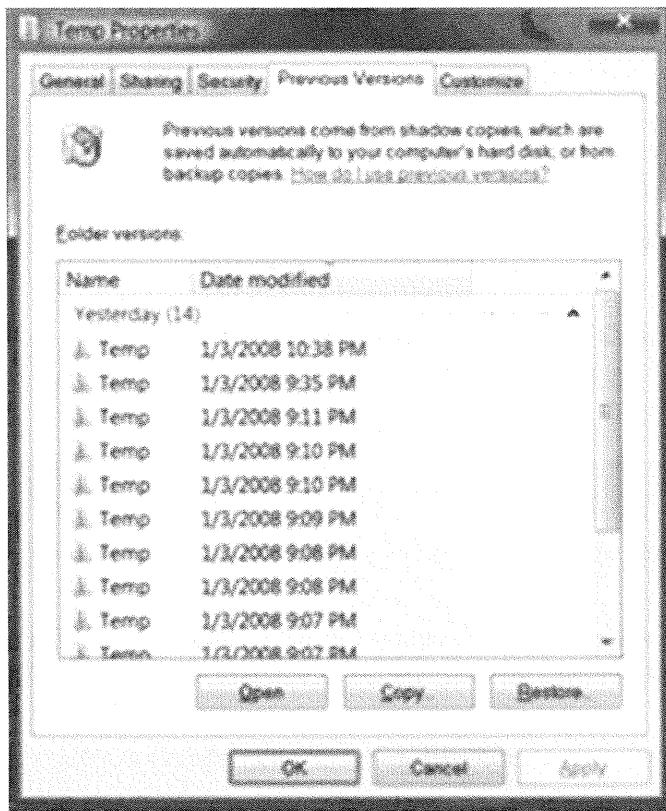
## Previous Versions

In Windows Vista and later, a System Restore snapshot can include user data files. This means users can easily restore files that have been accidentally deleted, modified or damaged since the last System Restore point was made.



To include a volume in the coverage provided by System Restore, open Control Panel > System > System Protection > System Protection tab > check the box(es) next to the drive volume(s) you want included > Apply. To immediately create a new System Restore snapshot, click the Create button.

To restore a previous version of a folder or file, right-click that folder or file > Properties > Previous Versions tab > select the desired shadow copy > select Open/Copy/Restore.



If there are no previous versions available, there is not a System Restore snapshot or backup of that object. Also, offline files and Windows operating system files cannot be restored using shadow copies.

### Windows 8.1 File History

The Previous Files feature in Windows 8 and later has been renamed to File History. It is turned off by default. To manage File History on Windows 8.1 and later, go to Change PC Settings > Update & Recovery > File History. There is also the File History applet in Control Panel. Old file versions can be saved to an external drive or to a shared folder UNC path. If the drive or shared folder is not accessible, a local cache is used instead until the normal destination is available again. Only libraries, the desktop, contacts and favorites are monitored, so if you want to monitor additional folders to keep a history of their files, you'll have to add those folders to one of the libraries (Documents, Music, Pictures or Videos).

In the Control Panel File History applet you can recover files and exclude folders that you do not want monitored. All this is the same as in Windows 7, but in Windows 8 and later you can also go to Advanced Settings in that applet and specify how quickly to save new versions (from 10 minutes to every 24 hours) and how long to keep older files in the history vault (from 1 month to forever, or whenever space is needed). Files can also be restored in File Explorer if you select a folder and then click the History button in the ribbon. A restored file can replace the current master or simply be copied elsewhere.

# ROBOCOPY.EXE

## • Command-line file copy utility

- Robust for large files such as VMs and videos
- Can "mirror" two folders or partitions
- Can copy permissions and audit settings
- Many filtering options (size, path, date, etc.)
- Extensive logging options
- Does not use the Volume Shadow Copy service, hence, cannot copy locked or open files

SANS Security Essentials – © 2016 SANS

## ROBOCOPY.EXE

Sometimes, you just want a quick, simple, reliable solution to back up data files. The command-line ROBOCOPY.EXE tool is great for copying or moving files, even when those files are large (many GBs), exist in large quantities (many thousands of files), or have long folder paths (more than 256 characters in their paths).

ROBOCOPY.EXE can "mirror" two folders such that any additions, deletions, or changes made in the primary folder will be reproduced in the target folder. For example, consider the following command:

```
robocopy.exe c:\data f:\backups\data /efsraw /mir /xo /r:3 /w:20
```

The above command mirrors the contents of c:\data and its subdirectories to f:\backups\data (/MIR switch), including EFS encrypted files (/EFSRAW), does not overwrite newer files with older files (/XO), retries a copy if the file is locked or open three times (/R:3) and waits 20 seconds between each retry attempt (/W:20).

ROBOCOPY can also resume copying where it left off instead of starting over from the beginning when the copy process is interrupted (/Z switch); can copy NTFS permissions, audit settings and owner information (/COPYALL); can monitor the source folder and trigger a copying only after a specific number of changes or minutes (/MON and /MOT); has a switch to prevent bandwidth hogging for over-the-network copying (/IPG); and includes extensive logging capabilities (/V, /LOG and /TEE).

The primary negative of ROBOCOPY is that it does not use the Volume Shadow Copy service, hence, it cannot copy files that stay continually locked. Also, the tool is not intended for "bare metal" system restores, for example, it cannot back up the Registry or System State.

# Summary

- Service Packs and Slipstreaming
- Microsoft Update Website
- Windows Update in Control Panel
- Windows Server Update Services (WSUS)
- Windows Server Backup
- System Restore
- Previous Versions & File History
- PC Reset Versus PC Restore

SANS Security Essentials – © 2016 SANS

## Summary

The main purpose of this module was to convey the importance of installing the latest Service Packs and hotfixes and to discuss techniques for simplifying the effort. Staying on top of patches is one of the most important duties a security administrator performs, but it can be a Herculean task. E-mail security bulletins and Microsoft's security website help to keep you apprised of new releases. For getting the hotfixes and Service Packs installed, there are batch files, Microsoft Update, Automatic Updates, and Windows Server Update Services (WSUS).

Maintaining good backups is essential for disaster recovery, forensics, having auditing baselines, and getting back to square one when it all goes to pieces. Windows Server Backup, System Restore, and device driver rollback all help to get a system operational again quickly. Disaster recovery often is overlooked as a security precaution, but it is how you can survive successful attacks by hackers, malware, and the forces of nature.

Now that the machine is built, patched, and regularly backed up, you can next focus on access controls. Patches and backups come before access controls and system hardening because patching and backups are more important for security!

The following is a list of the websites mentioned in this module:

- *ARCserve* ([www.ca.com](http://www.ca.com))
- *Bootable CD-ROMs* ([www.nu2.nu/bootablecd/](http://www.nu2.nu/bootablecd/))
- *BugTraq Mailing List* ([www.ntbugtraq.com](http://www.ntbugtraq.com))
- *CommVault Systems* ([www.commvault.com](http://www.commvault.com))
- *Computer Associates* ([www.ca.com](http://www.ca.com))
- *EMC NetWorking* ([software.emc.com](http://software.emc.com))

- *Hewlett Packard* ([www.hp.com](http://www.hp.com))
- *InstallShield Developer* ([www.installshield.com](http://www.installshield.com))
- *Microsoft Windows Server Update Services* ([www.microsoft.com/wsus/](http://www.microsoft.com/wsus/))
- *Microsoft Windows Update* ([windowsupdate.microsoft.com](http://windowsupdate.microsoft.com))
- *Microsoft's Download Center* ([www.microsoft.com/downloads/](http://www.microsoft.com/downloads/))
- *Microsoft's Security Homepage* ([www.microsoft.com/security/](http://www.microsoft.com/security/))
- *Packetstorm* ([packetstormsecurity.nl](http://packetstormsecurity.nl))
- *Polaris Group* ([www.polarisgroup.com](http://www.polarisgroup.com))
- *St.Bernard Software* ([www.stbernard.com](http://www.stbernard.com))
- *Symantec* ([www.symantec.com](http://www.symantec.com))
- *SyncSort* ([www.syncsort.com](http://www.syncsort.com))
- *UltraBac* ([www.ultrabac.com](http://www.ultrabac.com))
- *Hyper-V* ([www.microsoft.com](http://www.microsoft.com))
- *VMware* ([www.vmware.com](http://www.vmware.com))
- *Wise for Windows Installer* ([www.wise.com](http://www.wise.com))

# Module 25:

## Windows Access Controls

SANS Security Essentials – © 2016 SANS

### **Module 25: Windows Access Controls**

This section intentionally left blank.

# Windows Permissions and Privileges

The student will understand how permissions are applied in the Windows NT File System, Shared Folders, Encrypting File System, Printers, Registry Keys, and Active Directory, and how Privileges are applied.

SANS Security Essentials – © 2016 SANS

## Windows Permissions and Privileges

This section intentionally left blank.

# Windows Access Controls

## SANS Security Essentials V: Windows Security

SANS Security Essentials – © 2016 SANS

### Windows Access Control

Why have user accounts? Why go through all the trouble of Active Directory, Kerberos, NTLM, SIDs, SATs, mandatory user logons, and the rest of the machinery for user authentication? Well, the payoff is *selective access control*.

Permissions on files, folders, printers, Registry keys, and other items allow you to regulate access to these objects. Some users have only Read access to an object, whereas others are given Full Control. This kind of selective access control is possible only if users are authenticated first; otherwise, how would the operating system know *who* was trying to read or change the object?

Indeed, authentication and authorization are two sides of the same coin. On the one side, you can't authorize access to an object if you don't know who is requesting the access, and you can't actually know who someone is without first authenticating them. On the other side of the coin, there's no point in authenticating users if you can't regulate or audit their activities based on their unique identities. As discussed earlier, a user's identity is represented by her Security Access Token (SAT), which lists the Security ID number (SID) of the user's account and all the SIDs of the groups to which the user belongs. A SAT also lists all a user's privileges on the computer where she sits.

If you have a privilege, then you have a general capability that may apply to many different objects or to no "object" at all. For example, if you have the Take Ownership privilege, you can take ownership (discussed later) of any object on the computer, and if you have the Change System Time privilege, you can edit the BIOS clock through a variety of tools.

Auditing and logging is discussed in a later module, but the authentication-auditing connection should be clear. If you don't authenticate users, then the logs merely shows that *someone* did this or that action, but not exactly *who* performed the action. This makes logging much less useful.

By contrast with selective access control, Windows Vista introduced another way of enforcing access control that is independent of user accounts. Instead of doing only access control based on user accounts and their group memberships, Vista and later operating systems also enforce a form of *access control* for the sake of maintaining system integrity. This feature is called Mandatory Integrity Control (MIC) and is discussed later.

Another form of access control is encryption: If you can't decrypt a file, you can't read its contents. Windows Vista and later includes BitLocker Drive Encryption at the sector level. In addition to privacy, BitLocker also helps to maintain the integrity of the boot-up process if you have a Trusted Platform Module (TPM) chip in the motherboard.

Finally, Windows Vista introduced a new method of applying the principle of least privilege to the Security Access Tokens (SATs) called User Account Control (UAC), and you see MIC and UAC come together to help protect the beleaguered Internet Explorer.

Overall, then, this module explains why there is a point to authenticating users and forcing them to memorize passwords. This module discusses:

- NTFS Permissions
- Shared Folder Permissions
- Registry Key Permissions
- Active Directory Permissions
- Privileges
- Encrypting File System
- BitLocker Drive Encryption
- Mandatory Integrity Control
- User Account Control
- Internet Explorer Protected Mode

# NTFS Overview

- Windows Filesystems:
  - CDFS
  - FAT
  - FAT32
  - exFAT
  - ReFS
  - NTFS
- **NTFS Features:**
  - Permissions
  - Auditing
  - Encryption
  - Compression
  - Transactional
  - Max Size = 16 TB
- Always use NTFS

SANS Security Essentials – © 2016 SANS

## NTFS Overview

Windows supports a variety of file systems, including CDFS, FAT, FAT32, ReFS, and NTFS. CDFS is only for CD-ROMs. FAT and FAT32, though they can be used for hard drive partitions and are faster than NTFS on volumes smaller than 400 MB, but provide no auditing, access control, or fault tolerance.

Another file system, NPFS, is for use with "named pipes," a networking technology that leverages the Server Message Block (SMB) protocol for inter-process communications across a network. Even though no drives are formatted with NPFS, only buffer areas, NPFS is still a true filesystem. It's kind of like a RAM drive with a shared folder in it.

The Windows NT File System (NTFS) should be used on every hard drive. The exceptions are when you must retain the ability to boot into other operating systems or when you want the system partition to be formatted with FAT to aid in certain disaster recovery situations, for example, when your recovery software must be installed into a FAT-formatted C: drive. Beyond this rare exception, NTFS always should be used.

The NTFS filesystem has the following characteristics:

- Permissions
- Auditing
- Encryption (EFS and BitLocker)
- Compression
- Transaction-oriented processing
- Practical maximum volume size: 16,000 GB (assuming 4 KB-sized clusters)

The transaction-oriented processing of write requests helps to ensure that the filesystem stays in a consistent state even after an abrupt power failure or Blue Screen of Death (BSOD). The CHKDSK.EXE program runs automatically after a failure or BSOD, and you can use it to schedule a full volume or sector-level scan at the next reboot (see chkdsk.exe /?).

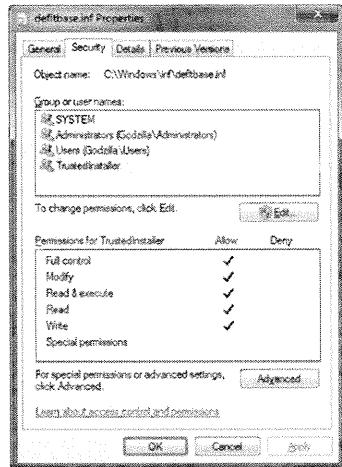
Compression is handled by the NTFS driver itself (not a separate application like 7-Zip), which makes the compression transparent to the user. To compress a folder or file, right-click it > Properties > General tab > Advanced button > check the Compress box. You can show compressed files/folder in a blue font, if wanted, by opening Windows Explorer > Tools menu > Folder Options > View tab.

There is a specialized version of NTFS called Resilient File System (ReFS) that was first introduced with Server 2012, but this file system is not (yet) suitable for general-purpose use. ReFS is optimized for large volumes that span many drives on giant file servers. Unless you have petabytes of data, NTFS is still the better choice.

Encryption, auditing, and the other features of NTFS will be discussed later in this module. For now, let's talk about the most important feature of NTFS for security: Discretionary Access Control Lists (DACLs).

# NTFS DACLs

- **NTFS DACLs are always enforced, even with:**
  - Local Users
  - IIS (HTTP and FTP)
  - Remote Desktop Protocol
  - Shared Folders
  - Telnet
- **ICACLS.EXE**
- **PowerShell Set-ACL**



SANS Security Essentials – © 2016 SANS

## NTFS DACLs

A set of NTFS permissions on a folder or file is called a *Discretionary Access Control List (DACL)*. Individual permissions in the DACL are called *Access Control Entries (ACEs)*.

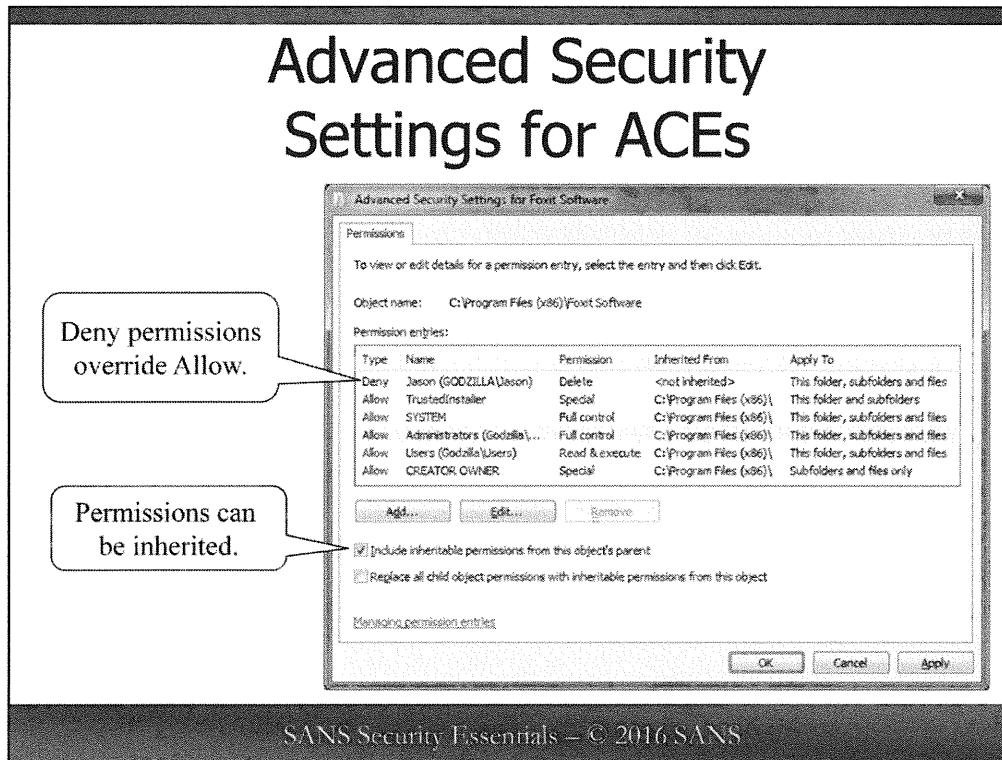
The permission ACEs are accessed through Windows Explorer > right-click the folder or file > Properties > Security tab. You can also manage NTFS permissions through the Set-ACL PowerShell cmdlet or the ICACLS.EXE command-line tool on Vista and later. (XCACLS.EXE is obsolete; it's only for Windows 2000/XP/2003 and must be download from Microsoft's website.)

Note: If you have no Security tab on the property sheet of an NTFS folder/file, then pull down the Tools menu in Windows Explorer > Folder Options > View tab > and uncheck the box at the bottom labeled Use Simple File Sharing.

The important thing to understand about NTFS permissions is that they always are enforced, no matter how the files are being accessed: via a shared folder, FTP, HTTP, Telnet, direct console access, a thin client with Terminal Services, and so on. It doesn't matter, NTFS permissions always are enforced by the operating system.

### Standard ACEs (Security Tab)

On the Security tab of an NTFS folder or file you can see the *standard* or *generic* permission ACEs. Each ACE consists of a user or group and the permissions assigned to that user/group as represented by the boxes checked below. Highlight a user/group to see which permission boxes are checked just for it. If no boxes are checked for a particular user or group, or the *Special Permissions* box is checked, there may be custom individual ACEs that don't translate into any standard ACEs.



## Advanced Security Settings for ACEs

The standard permissions are just collections of one or more *individual permission* ACEs. Individual permissions are the low-level, detailed, atomic ACEs that actually make up the DACL. If you happen to configure a set of individual permissions that do not equal the definition of a standard permission, the Security tab shows the *Special Permissions* box checked. Standard permissions are nothing but collections of individual permissions, just like water molecules are nothing but collections of hydrogen and oxygen atoms.

To manage the individual ACEs on a folder/file, right-click it > Properties > Security tab > Advanced button > Permissions tab. Highlight a permission, and click Edit to see the low-level, individual permissions available.

### Deny Overrides Allow

A user can be a member of multiple groups. These groups might have different and conflicting permissions on a single folder or file. For example, the user might be a member of two groups, one group has *Allow:Read* access to a file and the other group has *Deny:Read* access permission to the same file. What is the user's final, effective permission? The user will be denied Read access. Whenever there is a conflict between Allow and Deny permissions, the Deny permission always takes precedence.

### Explicit Versus Inherited Permissions

On the Security tab, notice that some ACEs are represented by check boxes that are somewhat gray and cannot be altered. Other ACEs have solid-colored check marks and can be altered. The gray-checked ACEs are inherited permissions, whereas the solid-checked ACEs have been assigned explicitly to that folder or file. The list of individual ACEs also includes an Inherited From column to help diagnose DACL problems.

NTFS permissions on a folder/file can be inherited from parent folders anywhere higher up in the directory structure. The root folder of a drive (for example, C:\) can have only explicit ACEs in its DACL.

You can control whether a folder/file inherits any of its ACEs. Inheritance is not mandatory. If you configure a folder/file to not inherit any permissions, only explicit ACEs exist in its DACL. To exempt a folder or file from any inherited permissions, right-click it > Properties > Security tab > Advanced button > uncheck the box labeled "Inherit from parent the permission entries that apply to child objects." When you do so, you'll be asked if you want to remove the inherited ACEs or copy them as explicit permissions.

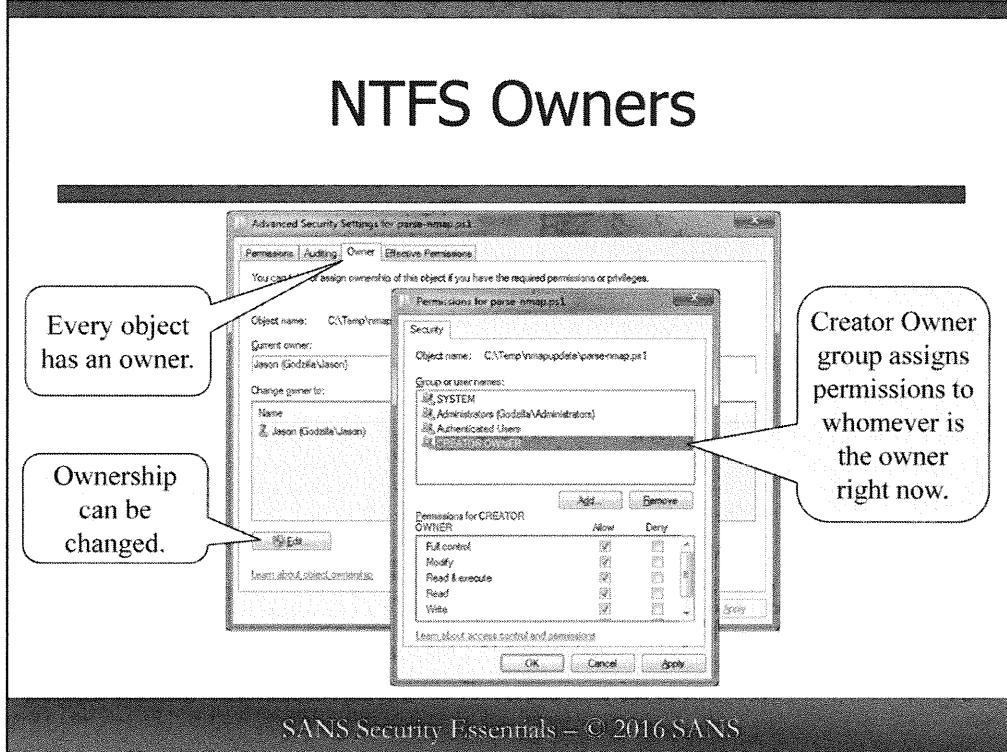
#### **Apply Onto: Scope of Inheritance**

When creating an explicit ACE, you can also configure how and where that ACE will be inherited with the Apply Onto pull-down list in the properties of an individual ACE. You can set only Apply Onto: This Object Only on a file, but the Apply Onto field on a folder can be any of the following:

- This folder only
- This folder, subfolders, and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- Files only

Be careful, you can really burn yourself with excessively complex inheritance schemes! Complexity is a security vulnerability in itself because it leads to errors and confusion. However, having this kind of control available enables you to get *exactly* the DACLs you want: If you can think it, you can probably create a *permissions scheme* to get it. The CREATOR OWNER group gives you even more flexibility.

# NTFS Owners



SANS Security Essentials – © 2016 SANS

## NTFS Owners

Every NTFS folder and file has an *owner* associated with it. You can see the current owner of a folder/file by right-clicking it > Properties > Security tab > Advanced button > Owner tab. By default, the user who creates a file or folder becomes the owner of that object. Objects created during the installation of the operating system are owned by the local Administrators group.

The owner of a folder/file can always change its permissions, even if its DACL specifies that the owner's account is denied all access. If a user is the owner of an object, that user can change that object's permissions regardless of whether you like it! The only solution is to take ownership away from the user if you are an Administrator.

## The CREATOR OWNER Group

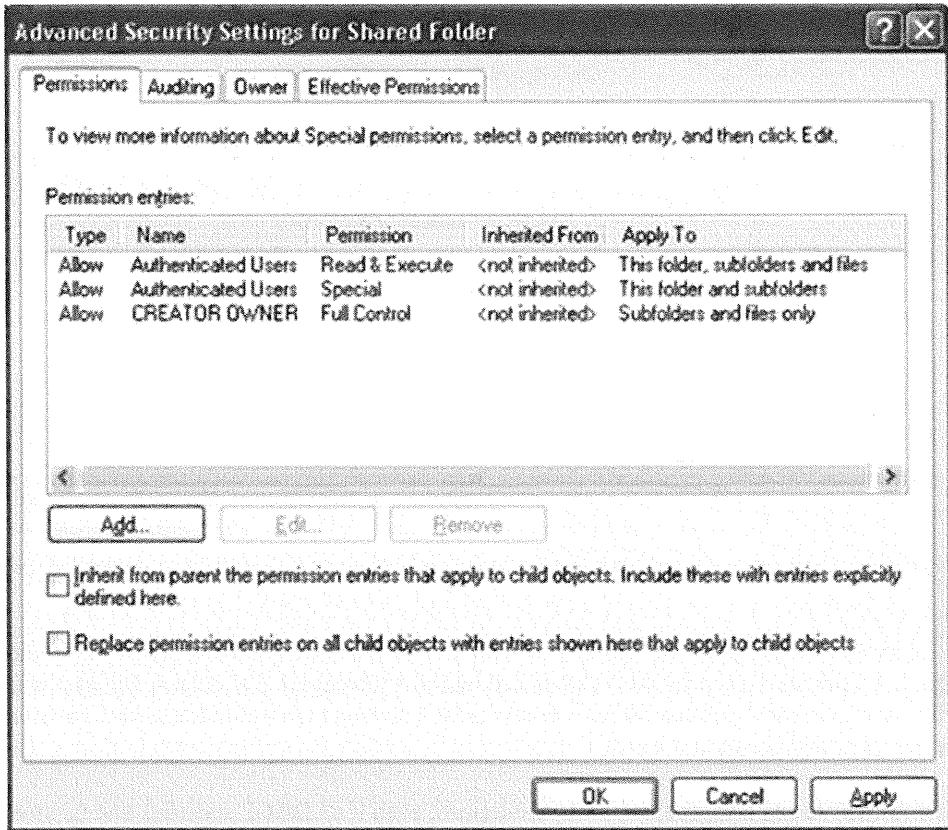
There is a special group, which acts as a stand-in for anyone as the current owner: the CREATOR OWNER group. You can grant permissions to the CREATOR GROUP once, and, even if the owner of a folder or file changes, the permissions you granted still applies to the new owner. The CREATOR OWNER group should be renamed the WHOMEVER THE OWNER HAPPENS TO BE RIGHT NOW group. You can't manage the membership of the CREATOR OWNER group; that membership is evaluated on-the-fly for each folder and file being accessed *when* it is accessed.

Here's an example of how the CREATOR OWNER group could be used to create a shared folder that acts as a public bulletin board. If a shared folder has the following DACL, then authenticated users can add files and subfolders and can read each other's files, but only the owner of each file (the one who created it) would have Full Control over it:

- Folder, Subfolders, & Files: Authenticated Users: Read
- Folder and Subfolders: Authenticated Users: Create Files

- Folder and Subfolders: Authenticated Users: Create Folders
- Subfolders and Files: CREATOR OWNER: Full Control

Anyone can add a file to share with others, but only the CREATOR OWNER of each file can delete or modify that file.



From the command line, use TAKEOWN.EXE to take ownership of many files recursively on the local or a remote computer. You'll have to have the Take Ownership privilege, of course, to do so.

# Principle of Least Privilege

- **Which NTFS permissions should I grant?**
  - Perform a "needs analysis" based on job roles
  - Grant the minimum permissions that still permit users to get their legitimate work done
- A good DACL to default to, but edit for least privilege:
  - **System:** Full Control
  - **Administrators:** Full Control
  - **CREATOR OWNER:** Full Control
  - **Authenticated Users:** Read & Execute (or Modify)

SANS Security Essentials – © 2016 SANS

## Principle of Least Privilege

What is the best NTFS DACL to assign to a folder or file? No simple answer can be given because of the conflicting demands between the operating system, applications, user-friendliness, and security, but you can always count on the Principle of Least Privilege to guide the way.

One way of stating the Principle of Least Privilege is this: Grant users the fewest permissions and privileges possible that still allow them to get their legitimate work done, but grant no more than that. Said another way: Don't give users more privileges or permissions than they need to get their legitimate work done. What's counts as "legitimate" work? That depends on their job roles and responsibilities. Before you can start customizing NTFS permissions, you must perform a *needs analysis* of the server or type of resource under consideration. What is it that you don't want certain users to do? What do you want to make sure other users *can* do? Without the answers to these questions, you can't begin to start locking down your NTFS permissions.

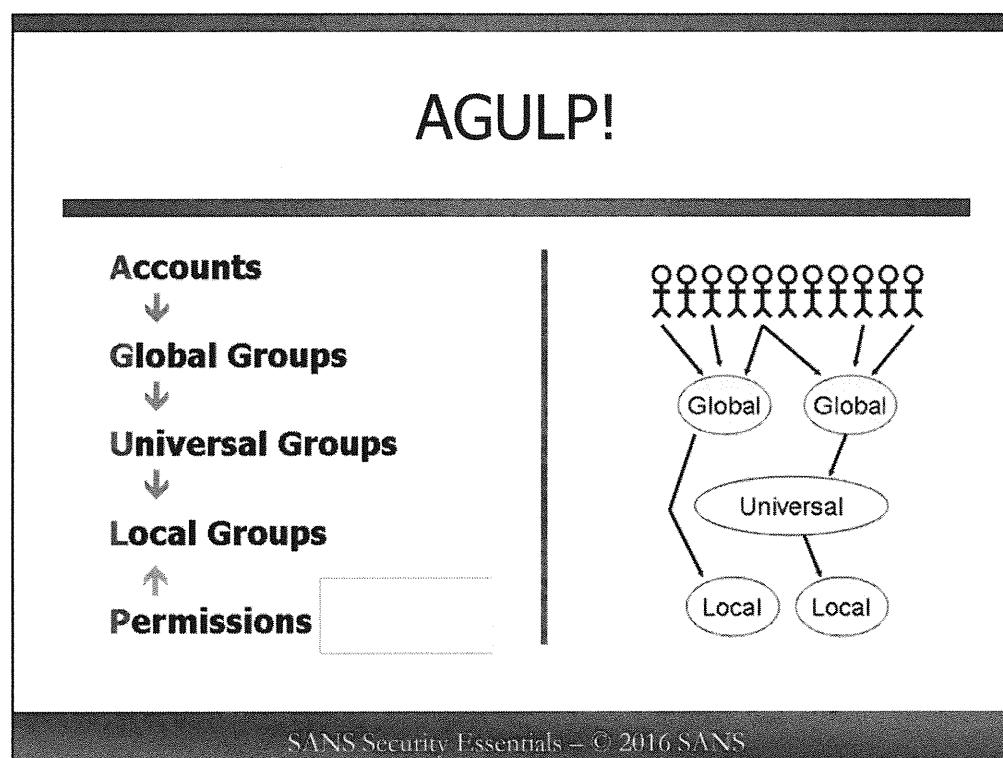
If you're not sure where to start, a reasonable default set of permissions would be Full Control for System, Administrators and CREATOR OWNER, and just Read & Execute for Authenticated Users. In a more lax environment, you might grant Modify to Authenticated Users, which would also allow editing and deleting files.

However, as a rule of thumb, the following permissions are usually a good place to start when performing your needs analysis and devising DACLs that satisfy the Principle of Least Privilege:

- System: Full Control
- Administrators: Full Control
- CREATOR OWNER: Full Control
- Authenticated Users: Read & Execute (or Modify)

Often, you'll give Authenticated Users limited permissions, such as Read & Execute, and then add another ACE for a more-limited group to have Change, too. Unless you want to give some non-administrative users the ability to change NTFS permissions, you don't need to grant Full Control; Modify almost always is enough. And even though the Power Users group still exists in Windows Vista, that group no longer has the special permissions and privileges that it used to have. In fact, the original purpose of the Power Users group (to provide elevated powers to some users without making them full Administrators) has been mostly eliminated and replaced with the User Account Control (UAC) functionality.

However, what is the most-efficient way to allocate permissions in environments with hundreds of groups and thousands of users? AGULP!



AGULP!

There is a formal model of how privileges and permissions should be applied. You can implement some or all of this model as you see fit. The model is known by its acronym, which sounds surprisingly similar to the sound most people make when they first hear the model described: *AGULP!*

Here's the AGULP model:

1. Create a unique Account for each user. Avoid permitting multiple users to log on with the same shared account.
  2. Add user accounts to Global groups according to users' geographical locations, job descriptions, and shared needs. (For example, all participants in the company 401k plan might be put into a group because they all share a need to access 401k-related resources.) A user can be a member of multiple groups simultaneously.
  3. Add Global groups to Universal security groups whenever multiple Global groups from multiple domains all need to be assigned the same privileges or permissions. A Global group can contain only members from the same domain where the Global group was created. A Universal group, however, can contain members from any domain in the entire Active Directory forest. User accounts can be added directly to Universal groups if wanted, but this causes unwanted Global Catalog replication traffic.
  4. Add Global and Universal groups to Local groups on the computers with the resources that need to be secured. These Local groups can be built in or new ones can be created, but their purpose is to organize Global and Universal groups.
  5. Assign Permissions and Privileges for these Local groups to the resources/objects that need to be secured. A Local group can be assigned privileges/permissions only to resources on the same computer where the Local group exists. And, in this model, privileges/permissions should not be granted to Global groups, Universal groups, or individual user accounts.

Note that there is a special type of Local group called a Domain Local group, hence, the AGULP acronym is sometimes written as AGUDLP instead. A standard Local group is created on a standalone or member computer in its local SAM accounts database, and this Local group can be granted permissions or privileges only on that one machine. A Domain Local group is created on a domain controller and exists in the Active Directory database, but it can be used on any member computer in the domain, not just on domain controllers. Domain Local groups cannot be created or used on standalone computers. Local groups of either type are still used to organize Global and Universal groups for the sake of granting permissions/privileges to resources, though.

If a user is a member of a Global group, and that Global group is a member of a Universal group, and the Universal group is a member of a Local group, then that user inherits all the privileges and permissions assigned to the Local group. When groups are nested inside each other, the *inner* groups inherit the privileges and permissions assigned to the *outer* groups. In the AGULP model, local groups are *outer* and Global/Universal groups are *inner*.

In sum, the purpose of a Local group is to act as the bearer of a set of privileges and permissions so that these privileges and permissions can be granted more easily to others. The purpose of a Universal group is to gather together many Global groups from multiple domains when those Global groups all happen to need the same privileges/permissions; and the purpose of a Global group is to organize users based on their shared needs, job descriptions, or geographical locations. Why organize users like this? Because if one person requires extra privileges or permissions, then it is likely that other users in the same geographical area, or with the same job description, or with the same special needs also require them. And simplifying the management of privileges/permissions is what all this crazy AGULP stuff is about!

# AD Users and Computers (1 of 2)

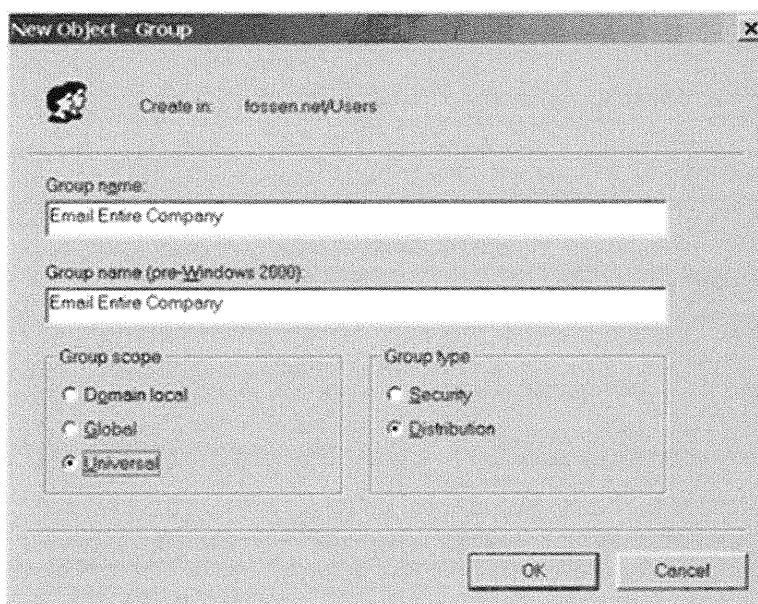
## • Active Directory Users and Computers

- Your main graphical tool for managing Active Directory
- This can be installed on workstations, too
- See the next slide for a screen shot
- Security groups can have privileges and permissions assigned to them, whereas distribution groups cannot
- Distribution groups are often for mailing lists

SANS Security Essentials – © 2016 SANS

## AD Users and Computers (1 of 2)

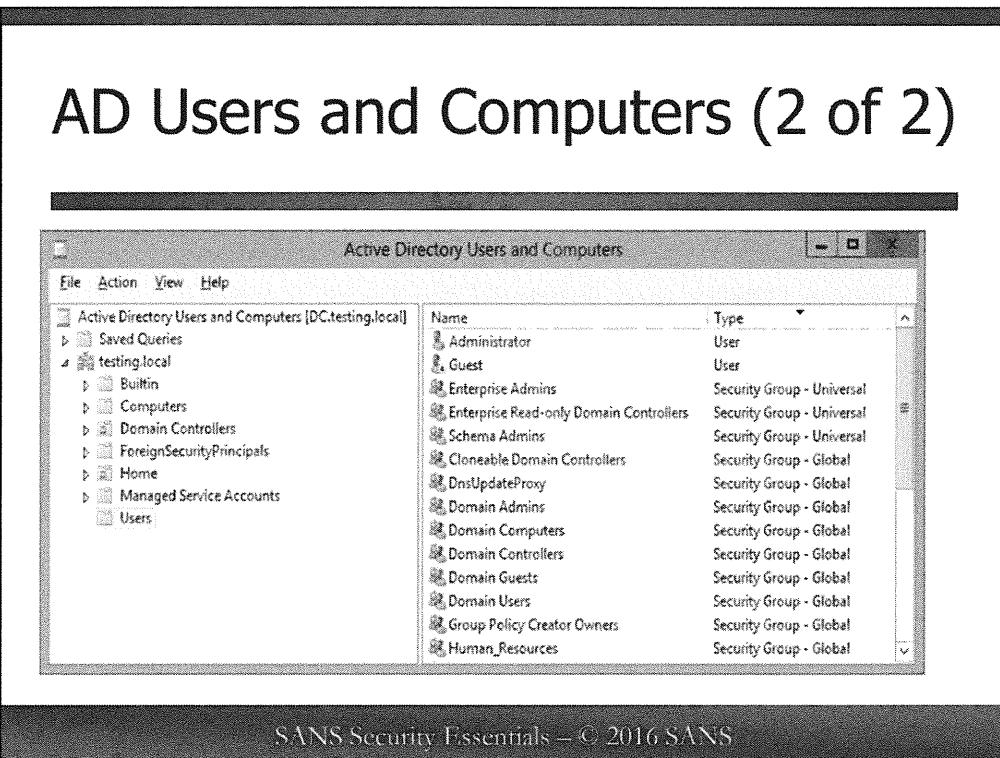
To create a Global or Universal group in Active Directory, open the Active Directory Users and Computers tool > right-click any Organizational Unit > New > Group. You can create a Domain Local, Global or Universal group this way. Each group can be marked as either a *distribution* or *security* group, for example, a *Global distribution group* is not the same thing as a *Global security group*.



A distribution group is like an e-mail list, in that you cannot assign privileges or permissions to a distribution group. Security groups, however, can have privileges and permissions granted to them. Note that Universal security groups are only available in native mode or better domains, whereas Universal distribution groups are always available. What is a native mode domain? It's an ancient distinction from the old mixed mode domains that were used to migrate from Windows NT domains.

To manage the members in a group, simply double-click the group, and go to the Members tab. There you can see the members in the group and add or remove them. By contrast, to create a Local group, open the Computer Management tool > System Tools > Local Users and Groups > and right-click Groups > New Group. You can create only Local groups using the Computer Management tool. Global and Universal groups exist in Active Directory.

To manage Local groups from scripts or the command line, execute net.exe help localgroup in a command shell.



## AD Users and Computers (2 of 2)

This slide shows a screen shot of the Active Directory Users and Computers tool.

The DNS name of the domain is testing.local. The DNS name of the domain controller to which the tool is connected is dc.testing.local.

The "Domain Controllers" yellow container is an organizational unit (OU) and it contains the computer accounts of the domain controllers for this domain.

The "Users" container is selected, so the right side of the tool shows what is inside that container. You can see the Administrator user account, which is a global account in Active Directory, not a local user account. This can be confusing, so keep in mind that every Windows computer has a local user account named Administrator, but there is also a single global account of the same name in AD, which is replicated to all domain controllers in that domain.

Inside the Users container, there is the Domain Admins global group, which is the most powerful group in the domain. In a domain, the global Administrator user account is a member of the Domain Admins group in that domain. In a forest with three domains, there would be three different global Administrator user accounts and three different Domain Admins groups (one for each domain).

Inside the Users container, there is also the Enterprise Admins group, which is a universal group, not a global group, which means that this group is replicated to every domain in a multi-domain forest. No matter how many domains there are in a forest, there will be only one Enterprise Admins group. The Enterprise Admins group is the most powerful group there is because it has full control over every domain in the forest. A Domain Admins group, by contrast, has full control over only its one associated domain.

# Shared Folder Permissions

- Server Service and the SMB/CIFS protocol
- Share DACLs are ignored for local access:
  - Full Control
  - Change
  - Read
- No inheritance of share permissions
- Multiple share names with different permissions
- PowerShell: Get-Help \*SmbShare\*

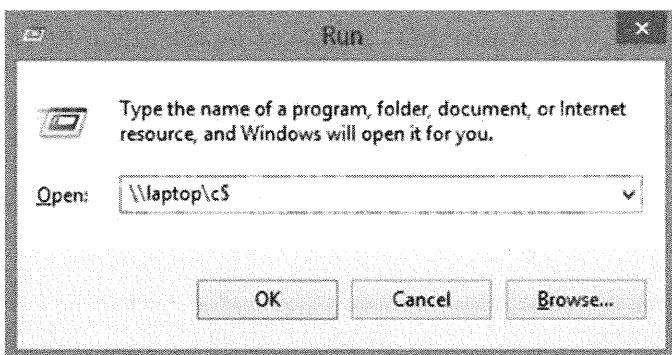
SANS Security Essentials – © 2016 SANS

## Shared Folder Permissions

A folder can be shared on the network. This is made possible by the File and Print Sharing service, otherwise known as the Server service, and the Server Message Block (SMB) protocol. You may have heard of the Common Internet File System (CIFS) protocol. But CIFS is not a new protocol; it's just SMB plus a few enhancements. For example, NetBIOS no longer is mandatory for file and print sharing with CIFS like it is with SMB. But SMB and CIFS do the same thing. Most documents just refer to SMB now, not CIFS.

Shared folders can be accessed via the following methods:

- Network Places (that is, Network Neighborhood or just Network)
- Mapped drive letters (New-PsDrive or NET.EXE command)
- Run line (enter \\ComputerName or \\IPAddress )
- Shortcuts (right-click on your desktop or in a folder > New > Shortcut > enter the \\ComputerName\\ShareName path to the shared folder)



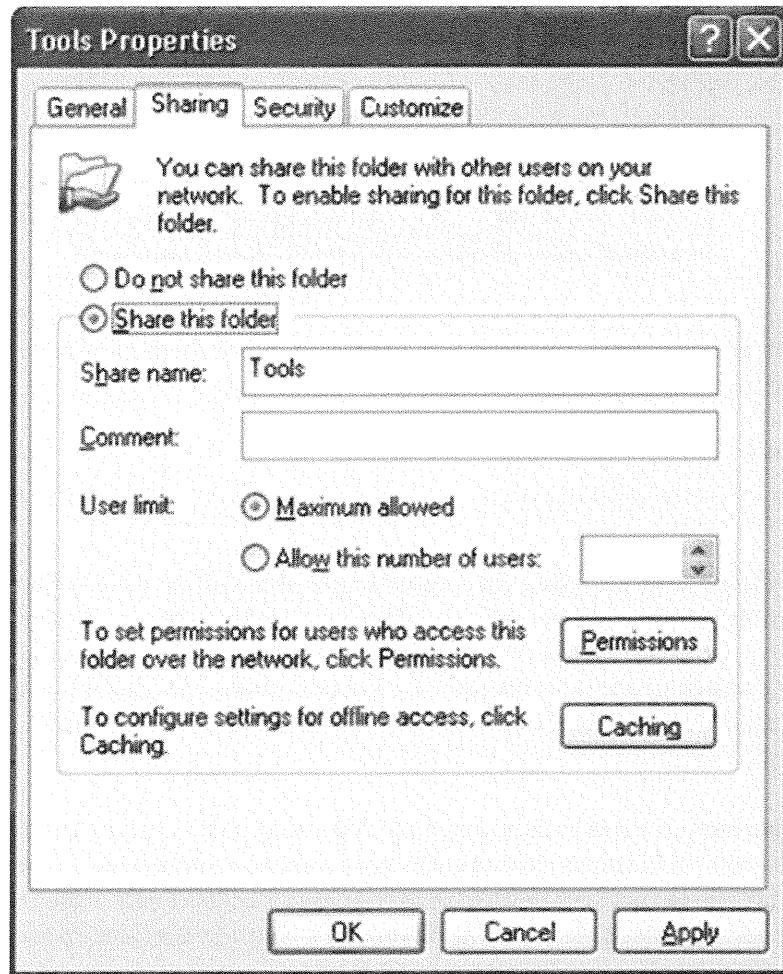
If you create a shortcut to a shared folder in the \Send To folder of your profile, then you can right-click a file and send it to that shared folder in one easy step! To get to the Send To folder in your profile, right-click the Start button and select Explore. This opens up Windows Explorer at your local copy of your profile. You can also place other programs in your Send To folder, such as NOTEPAD.EXE, and send files to those programs.

A shared folder has its own *Discretionary Access Control List* separate from any DACLs in the underlying file system. Shared folder permissions are enforced by the File and Print Sharing Service, not the NTFS filesystem driver. If a user sits locally at a computer and accesses local files with Windows Explorer or CMD.EXE, share permissions are simply ignored; share permissions are enforced only when files/folders are accessed through the SMB protocol, and SMB is not (typically) used during local access.

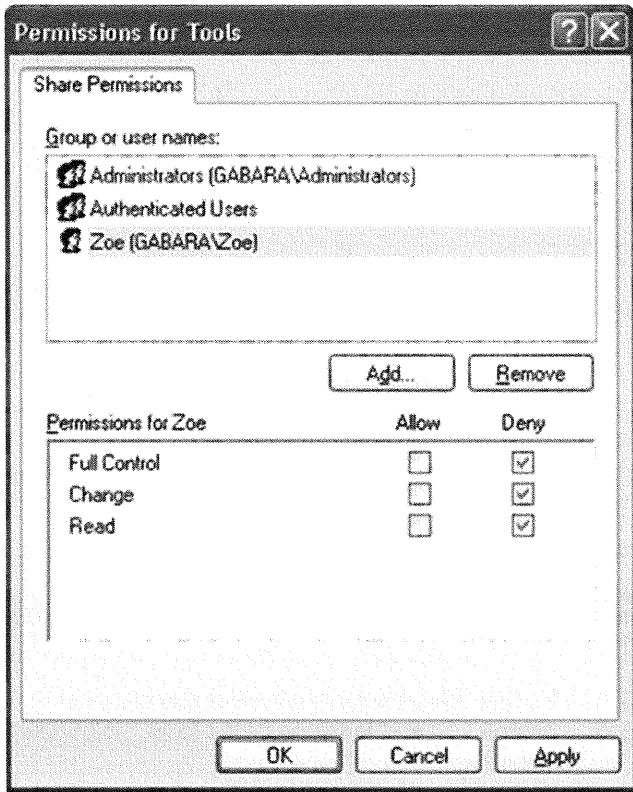
### How to Share Folders

To share a folder with Windows Explorer, right-click the folder > Properties > Sharing tab. To share a folder from the command line, use the New-SmbShare cmdlet in PowerShell or the NET.EXE SHARE command on older systems (enter **get-help smbshare** or **net help share** for more information). You can also manage shared folders on local or remote systems using the Computer Management tool.

Windows Vista tries to make folder sharing simpler by hiding configuration options on the Sharing tab in Windows Explorer. To see all the options, including the permissions options, open Windows Explorer > Tools menu > Folder Options > View tab > and scroll to the bottom and uncheck the box labeled Use Sharing Wizard.



When not using simple file sharing, you can manage the share permissions on a folder's Sharing tab by clicking the Advanced Sharing button. The default share permission in Server 2003 and later is Read for the Everyone group.



The share permissions are much simpler than the NTFS permissions, and there's no such thing as a "share owner." The possible share permissions are:

- Full Control
- Change
- Read

There is no such a thing as "share permission inheritance" across shares either. For example, if I share the C:\ folder as "C-Drive" with Everyone:Full Control, and I share the C:\Winnt folder as "SystemRoot" with Everyone:Read, when I access the \\Server\SystemRoot share, my share permission is Read, not Full Control. However, beware of overlapping shares! If I access the \\Server\C-Drive share and drill down to the C:\Winnt folder, then my share permission to that folder will be Full Control. It all depends on which sharename I use to access the machine.

A single folder on your hard drive can be shared multiple times using different share names and different permissions for each name! In Windows Explorer, after you've shared a folder once, click on the New Share button to share it again; you can now pull down a list of share names on this folder in the Sharing tab, select a share name, and manage the permissions on that share separately from the other share names.

# Hidden and Administrative Shares

- **ShareName\$** ← The \$ makes it hidden!
- IPC\$ for inter-process communications
- C\$, D\$, E\$, and such
- Find hidden shares with the Computer Management console

Share Name	Folder Path
ADMIN\$	C\Windows
C\$	C:\
Data	C\Data
I\$	I:\
IPC\$	
print\$	C\Windows\system32\spool\drivers
Temp	C\Temp
Users	C\Users

SANS Security Essentials – © 2016 SANS

## Hidden and Administrative Shares

By default, a shared folder is visible in Network Places and when browsing to the computer through its Universal Naming Convention (UNC) path, for example, ComputerName at the Run line. However, if the share name ends with a dollar sign (\$), then the share name is not visible in My Network Places. The only way you can access the share is if you enter the full UNC path to it, for example, ComputerNameHiddenShare\$. You can see a list of all the shares on your computer, both visible and hidden, in both the Computer Management tool and also from the command line using Get-SmbShare in PowerShell or NET SHARE on older systems. Looking for unwanted shares, especially hidden shares, should be a part of your regular server audits.

Name	ScopeName	Path	Description
ADMIN\$	*	C:\Windows	Remote Admin
C\$	*	C:\	Default share
I\$	*	I:\	Default share
IPC\$	*		Remote IPC
Leslie	*	C:\Data\Leslie	
Photographs	*	C:\Data\Photographs	
Users	*	C:\Users	

### **Administrative Shares**

By default, the root folder of each drive-lettered volume has a hidden share. This hidden share is named after the volume itself, for example, C\$, D\$, E\$, and so on. Its permissions are *Administrators:Full Control* and nothing else. The %SystemRoot% folder also is shared as ADMIN\$, but this share also permits read access to the Authenticated Users group. These are all called the *administrative shares*, and you can get rid of them on servers if you want by setting two Registry values named *AutoShareWks* (REG\_DWORD) and *AutoShareServer* (REG\_DWORD) to zero under the following key and then rebooting:

HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters

There is another built-in share, IPC\$, but this is used for inter-process communications and should not be modified. Setting the preceding Registry values will not remove the IPC\$ share. Watch out for hidden shares with tricky names such as IPSS\$ and IPP\$ created by malicious users, viruses, or worms that are attempting to avoid notice.

# Combining NTFS and Share DACLs

- **NTFS Permissions:**

- Users: Read
- Sales: Deny All
- Amy: Change

- **Share Permissions:**

- Everyone: Change
- Administrators: Read
- Amy: Read

- **Example: Amy is a member of multiple groups:**

- What are the permissions on those groups?
- What are Amy's final or effective permissions?

SANS Security Essentials – © 2016 SANS

## Combining NTFS and Share DACLs

NTFS permissions are always enforced, even when the user is remote. When a folder is shared on an NTFS-formatted volume, both the share permissions and the NTFS permissions must be taken into account when calculating a given user's final, effective permissions to a given share. Calculating a user's effective permissions to a file in a shared folder requires three steps:

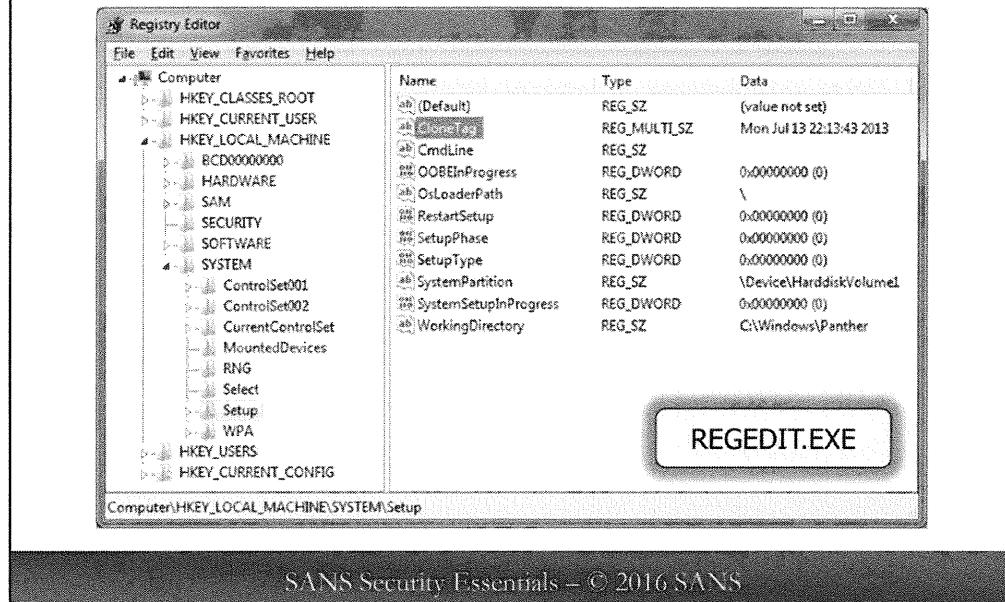
1. Assemble a list of all the share permissions the user has to the folder for that user's group memberships. Combine all these share permissions together. Whenever there is a *Deny* permission, this Deny permission overrides any other *Allow* permissions assigned. The permissions left over after this summation and exclusion-by-Deny-permissions are the *final share permissions*.
2. Assemble a list of all the NTFS permissions the user has to the file. This includes both explicit and inherited NTFS permissions. Combine all these NTFS permissions together. Whenever there is a Deny permission, this Deny permission overrides any other Allow permissions assigned. The permissions left over after this summation and exclusion-by-Deny-permissions are the *final NTFS permissions*.
3. Examine both the final share and the final NTFS permissions. For any requested action by the user (read, change, delete, and such) the more restrictive of the two final permissions is the *effective permission*. The effective permission is what determines the level of access the user enjoys.

For example, if Amy is a member of three groups, which have the Read, Change, and Full Control share permission, to a folder, then Amy's final share permission to the folder is Full Control. And if Amy also is a member of two other groups that have the *Allow:Read* and the *Deny:Read* NTFS permissions, respectively, on a file in that shared folder, then Amy's final NTFS permission to that file is Deny:Full Control. Why is Amy denied all NTFS access to the file whatsoever? Because a permission not inherited or explicitly assigned is assumed to be a Deny permission by default.

Amy was explicitly assigned Read, but this was overridden by the Deny permission; hence, Amy has no other permissions to the file, inherited or explicit. Finally, Amy's final share permission is *Allow:Full Control*, and her final NTFS permission is *Deny:Full Control*, so her effective permission is *Deny:Full Control* because it is the more restrictive.

By combining share and NTFS permissions you can achieve flexible and precise effective permissions. However, the complexity of the effective permission calculation process is a vulnerability in itself because it is prone to errors. Many administrators, therefore, choose to focus exclusively on NTFS permissions and ignore the share permissions (or view the share permissions as backups to the NTFS permissions).

# What is the Registry?



SANS Security Essentials – © 2016 SANS

## What is the Registry?

Virtually all configuration settings for the computer's hardware, operating system, applications, and its users' preferences are stored in a special miniature database called the *Registry*. The Registry can be modified directly using scripts, various command-line tools like REG.EXE, graphical tools like REGEDIT.EXE, and various cmdlets in PowerShell like Set-ItemProperty.

When using REGEDIT.EXE, the Registry appears to be structured similarly to the folders on the hard drive.

The yellow-looking folders are called *keys*, and the file-looking objects in these keys are called *values*.

If you double-click a value, a dialog box displays two things: the *type* of value it is and the *data* in the value.

There are various types of Registry values, including REG\_DWORD, REG\_BINARY, REG\_SZ, REG\_MULTI\_SZ, and REG\_EXPAND\_SZ. The type of the value determines what kind of data can be put in it and how that data must be formatted; for example, an REG\_SZ type is for strings.

You can create your own keys and values in REGEDIT using the Edit > New menu option.

# Remote Registry Service

- The Registry is remotely accessible!
- Disable the Remote Registry Service to prevent access
- Permissions on the WinReg key are interpreted as the share DACL
- The Registry key and share permissions combine to determine the final DACL

SANS Security Essentials – © 2016 SANS

## Remote Registry Service

The Registry can be accessed remotely. In REGEDIT.EXE, for example, pull down the Registry menu > Connect Network Registry > enter the name or IP address of a remote system > OK. This is made possible by the *Remote Registry Service* (REGSVC.EXE); hence, if you want to prevent all remote Registry access, stop and disable this service in the Administrative Tools > Services applet.

Be aware, though, that many management tools require the Remote Registry Service to be running on the target computers. Disable the service to enhance security, but be prepared to enable it again tomorrow. Isn't there another alternative?

## Remote Registry Share Permissions

Registry key permissions are always enforced against local or remote users, but you also can restrict who can access the Registry remotely. In effect, there are share permissions on the Registry as a whole!

How you manage these Registry share permissions, though, is somewhat strange. There's no special tool or property sheet. Instead, there is a special key in the Registry whose permissions are interpreted as your desired share permissions. Whatever permissions you set on this key regulate not only access to that single, seemingly insignificant key but also the share permissions for the Registry as a whole. You manage these permissions with REGEDIT.EXE, just like any other key.

The name of the key is winreg, and its full path is:

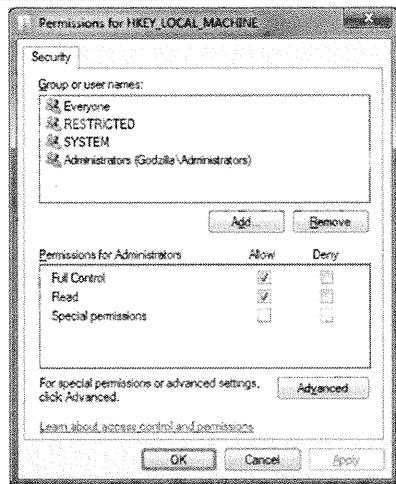
HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg\

The default permissions in Vista and later are Administrators:Full Control, Local Service:Read, and Backup Operators get a custom set of permissions which more-or-less amount to Read.

Note that the winreg key has a subkey named *AllowedPaths*. The value(s) in this subkey define the Registry paths that will still be remotely readable despite your share permissions on the winreg key! Just disable the Remote Registry Service completely if you're paranoid.

# Registry DACL

- **Registry keys have permissions, too:**
  - Inheritance from parent keys
  - Ownership
- How should these DACLs be changed?
  - Apply a template...



SANS Security Essentials – © 2016 SANS

## Registry DACL

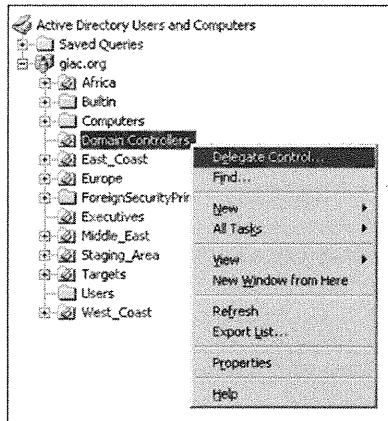
Because hundreds of security-related values are stored in the Registry, it is important to regulate access to it. Each key in the Registry has its own owner, auditing SACL, and permissions DACL. The best tool to use to manage these settings is REGEDIT.EXE.

To manage the owner, SACL, and DACL of a Registry key, open REGEDIT.EXE > highlight the key > Edit > Permissions.

### Which Permissions Should Be Changed?

Of the thousands of keys in the Registry, which should have their default permissions changed? There is no simple answer. You could spend a couple months reading Microsoft KB-articles, books on hacking and security bulletins to compile a list of keys to be secured, but this would be a Herculean effort. Fortunately, others have already done it for you! And there are tools that can be used to automate the entire process. The next module discusses how to use security templates and Group Policy to solve the problem.

# Active Directory Permissions



- **Every property of every object in AD has an ACL!**

- Parent OU Inheritance
- Ownership
- Auditing

SANS Security Essentials – © 2016 SANS

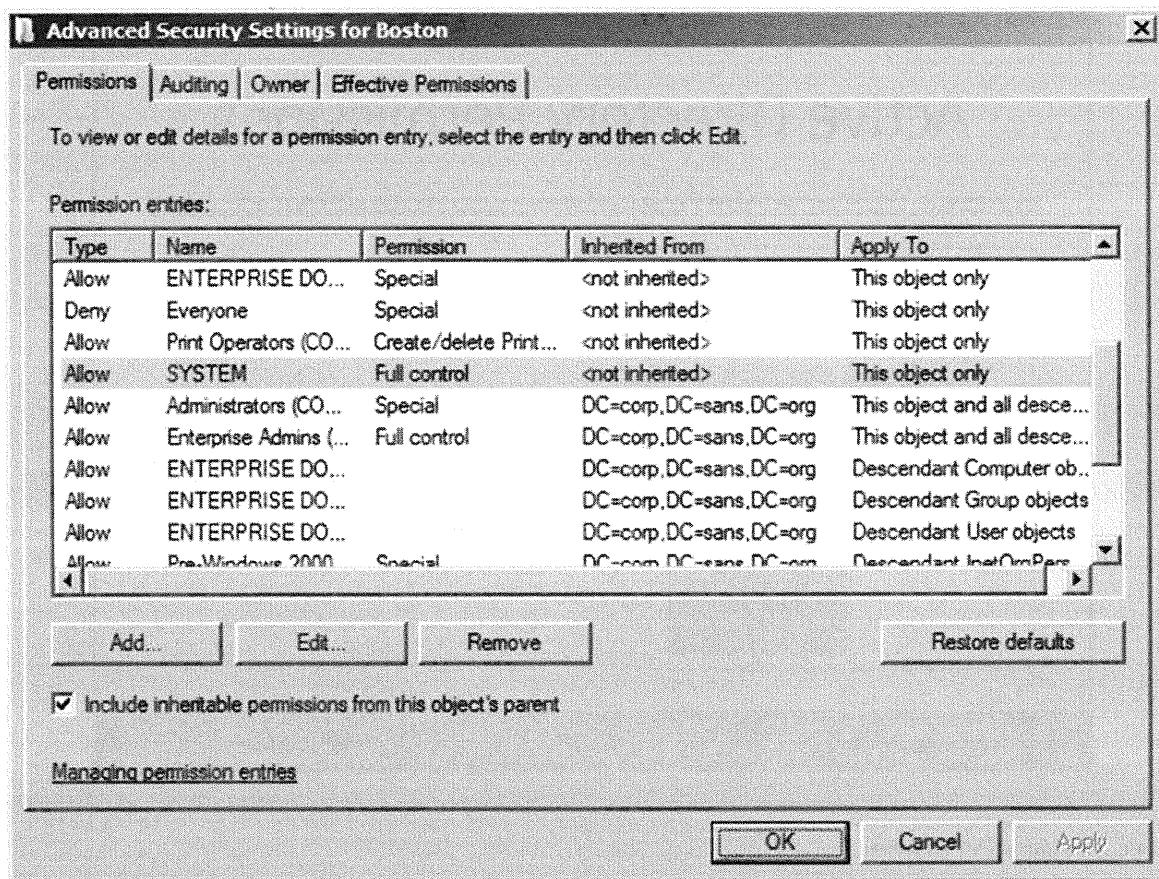
## Active Directory Permissions

As discussed before, Active Directory is the accounts-and-everything-else database that is installed on a Windows Server when it is promoted to become a domain controller. No discussion of permissions would be complete without at least mentioning Active Directory permissions.

Every property of every object in the Active Directory (AD) database has its own permissions DACL and auditing SACL. These access control lists also support the full range of inheritance options, just like in NTFS, and every object in AD has an owner for which CREATOR OWNER permissions can be assigned, too.

If you have an Active Directory domain controller available to you, you can edit AD permissions by opening the Active Directory Users and Computers snap-in > right-click any OU > View > select Advanced Features > right-click again on any object or container in AD > Properties > Security tab > Advanced button. This shows the familiar Permissions, Auditing and Owner tabs.

The screen shot in the slide shows the Active Directory Users and Computers management tool on a domain controller, plus all the organizational units in the domain (the yellow folders). By right-clicking an OU, you can launch a wizard to help you add more permissions to that OU for the sake of delegation of IT administrative powers over that OU.



This screenshot shows the ACL on an organizational unit in Active Directory. These permissions can be inherited by the thousands of users and computers underneath the OU for the sake of delegation of authority.

# Delegation of Authority in AD

- AD permissions are the basis for delegation of authority in the domain
  - Each OU could have its own OU Admins group that has Full Control over that OU but not have authority anywhere else in the domain
  - Delegation of Authority Wizard

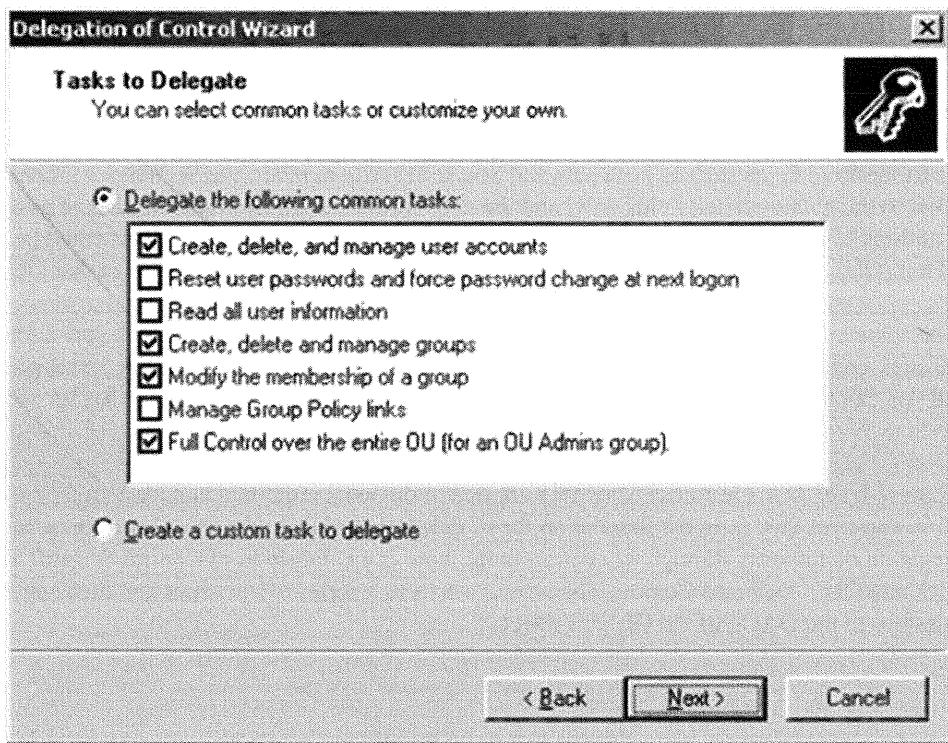
SANS Security Essentials – © 2016 SANS

## Delegation of Authority in AD

Consider an example of how property-level ACLs can be leveraged. A user account has many properties: name, phone, fax, e-mail address, password, and so on. Each one of these properties can have its own separate DACL and SACL. Domain Admins could have Full Control over all the properties; the Help Desk group could be given permissions to reset only the password and unlock the account; the Human Resources group could be given exclusive access to sensitive fields such as birth date and Social Security number; the Secretaries group could be given Write access to the phone-related fields only; and the user himself might be given the change password permission and nothing else! And because AD supports inheritance, the foregoing permissions could be set for an Organizational Unit (OU) or for the entire domain and then inherited by all the user accounts in that OU or domain.

Just as you can delegate authority over a shared folder through its permissions, so you can delegate authority over user accounts, groups, computer accounts, and everything else in AD through the permissions on the properties of AD objects. And you can track precisely who-is-doing-what because each of these properties has its own audit settings as well.

Collectively, property-level ACLs in Active Directory are one of the most important and least understood security advantages of Windows, yet they form the foundation for all delegation of authority in AD networks. In fact, to simplify the delegation of authority through AD permissions, there is a Delegation of Control Wizard! To launch the wizard, right-click any OU > Delegate Control. The wizard asks you a series of questions and then appends additional permissions to the DACL of the OU you selected.



# Mandatory Integrity Control (MIC)

- **Partial implementation of the Biba control model:**
  - Securable objects are assigned "labels" for integrity
  - Common labels: System, High, Medium (default), Low
  - WHOAMI.EXE shows label in your SAT
  - ICACLS.EXE shows and edits NTFS labels
- **The MIC Rule: *No Changes Up!***
  - Independent of NTFS permissions
  - Evaluated prior to NTFS permissions
  - Does not restrict read or execute by default, but MIC can be used for this, too

SANS Security Essentials – © 2016 SANS

## Mandatory Integrity Control (MIC)

Mandatory Integrity Control (MIC) is a partial implementation of the Biba mandatory access control model for preserving data integrity, especially the integrity of operating system files, the Registry, and the data exchanged between visible applications on the desktop. MIC is enabled by default in Windows Vista and later. MIC is also sometimes referred to as Windows Integrity Control (WIC).

MIC assigns a "label" to each securable object. Securable objects include folders, files, Registry keys, shares, processes, threads, named pipes, services, IPC objects, Active Directory objects, and just about anything else that can have permissions attached to it. The label is stored as a part of the object's System Access Control List (SACL) alongside the audit settings.

An MIC label is one of the following:

1. System
2. High
3. Medium (default)
4. Low

If an object lacks an MIC label, then that label is assumed to be Medium. Operating system files lack MIC labels, so they are handled as Medium-labeled files.

As you launch processes, your Security Access Token (SAT) is assigned to each process you launch. Your SAT includes the Security ID (SID) number of your user account, the SIDs of your groups, plus other information. In Windows Vista and later, your SAT also includes an integrity SID that identifies your MIC label. When your

SAT is inherited by a process you launch, the label will be Medium if the process were launched as a standard user (the default), High if launched with administrative privileges, or Low if that process happens to be Internet Explorer or another program designed to run as Low. Most services run with the System label.

You can see and edit these labels with Microsoft's WHOAMI.EXE and ICACLS.EXE utilities on Vista and later, the Process Explorer and ACCESSCHK.EXE tools from <http://www.microsoft.com/technet/sysinternals/>, and Mark Minasi's CHML.EXE (<http://www.minasi.com>).

### **The MIC Rule**

Here is the intended rule that MIC enforces to help maintain system integrity:

The MIC Rule: A process cannot edit or delete a securable object unless that object's MIC label is the same as or lower than the MIC label of the process.

Another way of saying this is: *No Changes Up!* A process cannot edit or delete a securable object when that object has a higher/better MIC label than the label of that process. MIC does not restrict read access, though, that's what NTFS permissions are for.

### **Evaluated Prior to DACLs**

Note that MIC is independent from and enforced prior to any Discretionary Access Control List (DACL) permissions that might otherwise have allowed the edit or deletion; for example, even if you have Full Control NTFS permissions on a file, you still might not change or delete that file because of its MIC label.

### **Does Not Restrict Read/Execute**

MIC does not restrict read or execute access by default; for example, a Low process can still read a file labeled as Medium or High, and a Low process could execute a file labeled as Medium or High. (And that new process would inherit the Low label of the parent process.) However, if a process with a High label executes a file with the Low label, that new process runs as High. Using tools like CHML.EXE, though, you can use MIC labels to restrict read and execute access by lower-labeled processes.

# Privileges (1 of 5)

- Unlike permissions, privileges are not related to particular objects
- Listed in your SAT
- Managed by Group Policy
- `whoami.exe /priv`



SANS Security Essentials – © 2016 SANS

## Privileges (1 of 5)

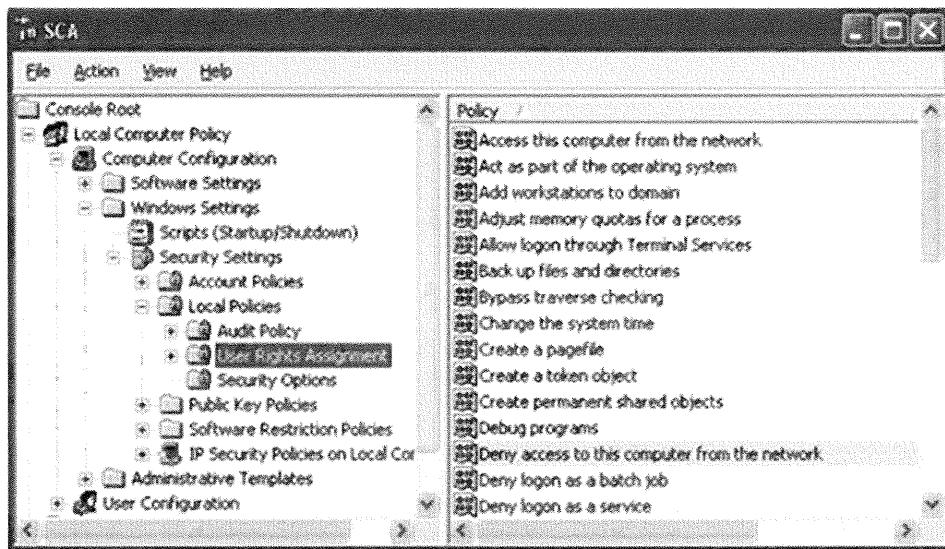
A permission always is attached to some particular object, like having Read access to a file or having Full Control over a Registry key. A *privilege*, however, references a general capability that is not tied to any particular object. (For this course, "right" and "privilege" are synonyms, but, strictly speaking, *privileges* are listed in your SAT whereas *rights* control only local or over-the-network logon attempts.)

For example, the *Take Ownership* privilege permits one to take ownership of any object, and the owner of an object can change its permissions in any way the owner wants. How is this possible? Because that capability is hard-wired into the operating system; that is, it is a *privilege* that owners enjoy over their objects because Microsoft wants it that way. Another privilege is *Force Shutdown from a Remote System*, which does not refer to any particular object but is a dangerous capability one certainly would want to restrict.

Recall that your Security Access Token (SAT) is constructed by your computer when you log on. Your SAT lists the Security ID numbers (SIDs) of all the groups to which you belong, but your SAT also contains a list of all your privileges on that particular machine. That's an important point: Privileges are machine-specific, hence, I might have the *Take Ownership* privilege on one computer but not on another.

On Windows Vista and later, you can see what privileges you have on your computer by opening a command-prompt window and running `whoami.exe /priv`.

You manage privileges through Group Policy, but even a standalone system has its own local Group Policy Object (GPO). The easiest way to manage privileges in the local GPO is by going to the Administrative Tools folder > Local Security Policy > Local Policies > User Rights Assignment. Here, you can double-click any listed privilege and add/remove groups or users from that right. You also can manage privileges with scripts or free command-line tools like *NTRIGHTS.EXE*. (Unfortunately, Microsoft's tools often refer to "privileges" as "rights" and vice versa, even though there is a technical difference, but for this course the terms can mostly be used interchangeably.)



### What Privileges Exist?

The following is a table of the privileges with a short description of each. Quickly browse the list, and then we'll discuss a few of the more important privileges for security.

Privilege (User Right)	Description
Access this computer from the network	Determines who is permitted to connect to the computer over the network using a protocol requiring user authentication. It does not apply to any packets whatsoever.
*Act as part of the operating system	Allows a process to authenticate as any user or to create a SAT with any SIDs and privileges desired. <b>This is dangerous.</b>
Add workstations to domain	Determines who can join workstations to the domain. Authenticated users have this privilege and can create up to ten computer accounts in the domain, but a modification to an Active Directory property can increase or decrease this number.
Allow log on through Remote Desktop Services	Determines, in part, who can remotely log onto the computer using Remote Desktop Protocol (RDP).
Back up files and directories	Determines who can circumvent NTFS permissions for the sake of making backups.

Bypass traverse checking	Determines whether a user can traverse directory trees even though the user may not have NTFS permissions on some of the traversed directories. This privilege does not allow the user to list the contents of a directory, only to traverse it to access subdirectories to which the user does have sufficient permissions.
Change the system time	Determines who can change the time and date on the internal clock of the computer. This privilege seems trivial, but clock modifications can cause Kerberos authentication to fail or render log data less useful.
Create a pagefile	Determines who can create pagefiles or change their size or locations.
*Create a token object	Allows a process running under the context of an account with this privilege to create a SAT for the sake of accessing local resources. <b>This is a dangerous privilege.</b>
Create permanent shared objects	Determines which accounts can be used by kernel-mode processes to create an object in the object manager's cache. This is rarely used.
*Debug programs	Determines which users can attach a debugger to any process. <b>This is a dangerous privilege.</b>
Deny access to this computer from the network	Determines who is not permitted to connect to the computer over the network using a protocol requiring user authentication. This overrides any other right that would otherwise allow the user to connect.
Deny log on as a batch job	Determines which accounts are denied logons as batch jobs.
Deny log on as a service	Determines which service accounts are prevented from registering a process as a Windows service. This policy overrides any other right that would otherwise permit this action.
Deny log on locally	Determines who is prevented from logging on interactively at the computer. This overrides any other right that would otherwise permit an interactive logon.
Deny log on through Remote Desktop Services	Determines, in part, who is prevented from logging on remotely using Remote Desktop Protocol (RDP).
Enable computer and user accounts to be trusted for delegation	Determines who can enable the "Trusted for Delegation" value in the properties of a user or computer account.
Force shutdown from a remote system	Determines who is allowed to shut down a computer from a remote location.
Generate security audits	Determines who can write events to the security Event Log.

Increase quotas	Determines which service accounts can increase the processor quota assigned to another process.
Increase scheduling priority	Determines who can change the multitasking priority of a process with Task Manager.
* Load and unload device drivers	Determines who can load and unload device drivers. <b>This is a dangerous privilege.</b>
Lock pages in memory	Determines who can keep data in RAM and out of any paging files.
Manage auditing and security log	Determines who can manage audit settings (SACLs) on NTFS files, registry keys, Active Directory objects, etc. Also determines who can clear the security Event Log.
Modify firmware environment values	Determines who can modify environmental variables that affect the system as a whole. This does not include any user's personal environmental variables.
*Modify an object label	Determines who can change an object's Integrity Control label (system, high, low, etc.) on Windows Vista and later. <b>This is a dangerous privilege.</b>
Profile single process	Determines who can use Performance Monitor and similar tools to monitor user-launched processes.
Profile system performance	Determines who can use Performance Monitor and similar tools to monitor the performance of operating system processes.
Remove computer from docking station	Determines who can gracefully disconnect a laptop computer from its docking station.
Replace a process level token	Determines who can replace the SAT of a subprocess of the current process.
*Restore files and directories	Determines who can circumvent NTFS permissions for the sake of restoring files from backups. <b>This is a dangerous privilege.</b>
Shut down the system	Determines who can gracefully shut down the computer while logged on locally.
Synchronize directory service data	Not currently used.
*Take ownership of files or other objects	Determines who can make themselves the owner of Active Directory objects, NTFS files and folders, threads, processes, printers, and registry keys. The owner of an object can change the permissions on that object in any way desired. <b>This is a dangerous privilege.</b>

## Privileges (2 of 5)

- Allow/Deny Log On Locally
  - Restrict who can log on interactively at the keyboard
- Allow/Deny Access This Computer from the Network
  - Restrict who can remotely authenticate to a computer
- Allow/Deny Log On Through Remote Desktop Services
  - Restrict who can use Remote Desktop Protocol (RDP)

SANS Security Essentials – © 2016 SANS

### Privileges (2 of 5)

Sometimes the terms "privilege" and "right" are used synonymously, but, strictly speaking, there is a difference. When a privilege controls where and how a user can log on, this privilege is called a "user right," and rights do not appear in a user's SAT after he has logged on. So, a logon privilege is called a "right."

To help isolate a server from certain users or groups, you should assign the *Deny Access to This Computer over the Network*, *Deny Log on Locally* and *Deny Log on Through Remote Desktop Services* user rights to those users or groups you do not trust or who have no need to logon.

The deny-style rights are useful for defining exceptions to a general policy that otherwise allows access. If a user is both allowed and denied a logon right, the denial wins.

However, if you want to deny everyone access to a server except for a certain group, then assign the *Access This Computer from the Network*, *Allow and Log on Locally* and/or *Allow Log on Through Remote Desktop Services* rights to just those groups. For example, the database servers in the Human Resources department might be restricted only to Administrators and members of the HR group.

If an adversary steals your password hash and attempts to perform a Pass-The-Hash logon over the network at a target server as you, if you do not have the *Access This Computer from the Network* logon right at that server, neither will the attacker, and the attacker's logon attempt will fail.

# Privileges (3 of 5)

## • Take Ownership of Files and Objects

- The "owner" of an object can change its permissions, no matter what the current permissions are
- Only Administrators have this by default
- Objects include files, folders, printers, AD containers, registry keys, processes, and threads

SANS Security Essentials – © 2016 SANS

### Privileges (3 of 5)

A powerful and dangerous privilege is *Take Ownership of Files or Other Objects*. The owner of an object can change its permissions in any way wanted. Objects that have owners include NTFS files and folders, Active Directory objects, printers, Registry keys, processes, and threads.

For example, a malicious user with this privilege could take ownership of an administrator's global user account in AD and change its permissions so that that user could reset the password. Similar steps could be taken to plant Trojans on domain controllers, copy or modify database records, hijack privileged processes, and so on. Hence, you should audit who has this privilege.

## Privileges (4 of 5)

- Backup/Restore Files and Directories
  - Think of these as the "circumvent NTFS permissions" privileges
  - Use Group Policy to delegate the Backup privilege, but reserve the Restore privilege for Domain Admins only

SANS Security Essentials – © 2016 SANS

### Privileges (4 of 5)

The seemingly innocuous backup/restore privileges actually are quite dangerous. Think of these as the *Ignore NTFS Permissions* privileges. Also, if a user has both of these privileges, she can assign ownership of a file to anyone she pleases, using well-known hacking tools.

Because privileges are configured on a per-machine basis, consider limiting the allocation of these privileges to non-administrators only on servers or workstations with low security priorities. Consider creating a custom group with only the *Back Up Files and Directories* privilege (and not the restore version) so that you can delegate the ability to make backups, but then reserve for Domain Admins the privilege to restore those files when necessary. Group Policy will simplify greatly the distribution of these custom privileges when you have hundreds of machines. Through Group Policy, each OU could have its own *Backup OU* group.

# Privileges (5 of 5)

## • Debug Programs

- Example of a debugger: OllyDbg ([www.ollydbg.de](http://www.ollydbg.de))
- Determines who can attach a debugger to any process
- Used by developers for troubleshooting software and by security experts (and hackers) for reverse engineering
- **Windows DLL Injection attacks require this:**
  - A new thread is injected into a running process that the attacker does not own, that is, that doesn't have her SAT
  - Cain ([www.oxid.it](http://www.oxid.it)) uses DLL Injection to dump password hashes and the operating system's LSA Secrets data

SANS Security Essentials – © 2016 SANS

## Privileges (5 of 5)

A *debugger* is an application that allows you to examine and control a running program or operating system to troubleshoot or reverse engineer it. OllyDbg, for example, is a popular and powerful debugger for Windows, and it's free (<http://www.ollydbg.de>).

The *Debug Programs* privilege permits a user to attach a debugger to any process, even if that user did not launch the process being debugged. This is dangerous because a process might contain sensitive information in cleartext or the integrity of the process could be undermined. For example, a DLL Injection attack requires the *Debug Programs* privilege to work because this attack modifies a running process by injecting a new thread into the address space of the target process.

The Cain tool (<http://www.oxid.it>) uses this trick to dump password hashes and the computer's LSA Secrets, but it works only if Cain is running as someone with the *Debug Programs* privilege.

By default, only the local Administrators group has the *Debug Programs* privilege.

Unfortunately, many regular users have been added to the local Administrators group on their workstations, and almost none of them (except for developers) actually need it. If a user's machine gets infected, the malware could use the *Debug Programs* privilege to extract secrets, such as encryption keys or other users' credentials, or to undermine the operating system. Hence, limit who has this privilege and audit changes to whom it has been granted.

# BitLocker Overview (1 of 4)

## • Whole Disk Encryption:

- Sectors encrypted with AES (128- or 256-bit)
- Boot-up integrity checking with a TPM (TPM is optional)
- Supports USB and Thunderbolt drives
- Emergency recovery PIN
- Supports some self-encrypting hard drives (eDrive spec)

SANS Security Essentials – © 2016 SANS

## BitLocker Overview (1 of 4)

The two main benefits of BitLocker Drive Encryption are:

- Verification of the integrity of boot-up files and other start-up data structures to help prevent rootkits and other malware from secretly taking control of the computer
- Sector-level encryption of entire hard drive volumes, including the paging and hibernation files on those volumes, to prevent exposure of confidential data on stolen or lost hard drives.

Hence, BitLocker is not just for keeping confidential files secret when a computer is lost or stolen; it also helps to thwart the undetected installation of malware that hooks into the boot-up process. However, this boot-up integrity checking requires a TPM chip. And BitLocker can be used on flash drives and external USB/firewire drives, too.

BitLocker can optionally make use of a Trusted Platform Module (TPM) chip in the mainboard of the computer, but a TPM chip is not absolutely required. For the sake of data recovery in an emergency or if the TPM fails, backup keys can be exported to external media, or when the computer is a domain member, even uploaded to Active Directory automatically. After the computer has booted and the user has logged on, BitLocker is 100 percent transparent to the user. It imposes approximately a 5 percent overhead on the performance of the system.

### Requirements

BitLocker is only available on Windows Vista or later, Ultimate and Enterprise editions, and on Windows Server 2008 or later. Note that it is not included in the Home, Business, or Professional editions.

The computer does not require two hard drives, but it must have at least two NTFS volumes: the "boot volume" contains the operating system files (with the %SystemRoot% folder, usually named "Windows"), whereas the "system volume" contains the files used during the very beginning of the boot-up process. (Yes, these names are the reverse of what is rational.) The system volume cannot be BitLocker encrypted, but the boot volume can.

## **Self-Encrypting Hard Drive Support**

Some hard drives perform encryption internally inside the drive hardware itself, not using Windows or the motherboard CPU. These drives are called "self-encrypting drives" or "hardware-based encryption drives", and there is almost no performance penalty for the encryption. But what locks and unlocks access to such drives? If the encryption is totally transparent, why can't a thief just plug a stolen drive into his or her own computer?

If the self-encrypting drive supports the TCG Opal 2.0 and IEEE-1667 standards, and if the motherboard firmware supports UEFI Secure Boot, then BitLocker can provide access control to the hard drive on Windows 8 and later. In this case, BitLocker acts as the overall manager of the drive, even if BitLocker or Windows is not responsible for the sector-level encryption anymore. Look for the eDrive logo on new self-encrypting drives to confirm compatibility. The so-called competition between BitLocker and self-encrypting drives doesn't really exist, it's an artificial distinction based on misunderstanding. The entire industry is moving toward self-encrypting drives.

### **Integrity-Checking and Encryption Details (When Not Using Self-Encrypting Drives)**

How does TPM integrity checking work? Information about the master boot record, boot sector, the boot manager (BOOTMGR), some of the firmware code, and other such boot-up data are all included in SHA-1 hashes secured by TPM. These stored hash values survive reboots. At the next reboot, when the boot manager later takes control of the computer, it reads an encrypted file off the hard drive, but does not decrypt it. This data was previously encrypted by the TPM. So the boot manager gives this data to the TPM, which decrypts it, checks its digital signature, and compares the hashes stored against the current hashes computed by the TPM. If the recorded and current hashes all match, the boot-up process continues; otherwise, emergency recovery is triggered, alerting the user to the potential violation of the system's integrity.

At this point, the boot-up environment is considered healthy, so the TPM gives a key to Windows to decrypt another key on the hard drive called the Full Volume Encryption Key (FVEK). The FVEK is the key that encrypts/decrypts all the sectors of the BitLocker-protected volume. The FVEK is 128-bit AES by default, but 256-bit AES can be used instead. With a self-encrypting drive, this process is different because it relies on UEFI Secure Boot (discussed later).

Now, if a PIN is used with the TPM, the SHA-1 hash of the PIN is included in the encrypted blob on the hard drive, and this hash is also checked by the TPM before granting access to the drive. Or if a USB token is used with the TPM, the key on the token is XOR'ed with the key that the TPM extracted, and this product is used to access the drive. Or if only a USB token is used because there is no TPM, then the key from the token decrypts the drive. (Note that no boot-up integrity checking is performed in this case, that is, when there's no TPM.)

To turn on BitLocker on your nonproduction testing computer, open Control Panel > BitLocker Drive Encryption > Turn On BitLocker. Follow the wizard's instructions.

While a volume is encrypted for the first time, the user can continue to perform work normally on that computer; in fact, the user can even pause the encryption process and then resume it at a later time, even after a reboot.

The encryption process takes approximately one minute per gigabyte. The performance overhead of using BitLocker is approximately 5 percent on a nonself-encrypting drive. Self-encrypting drives suffer only approximately 1 percent performance penalty, with or without BitLocker access control management.

# Trusted Platform Module (2 of 4)

- **TPM is a chip in the motherboard:**

- Performs encryption, hashing, random key generation, secure key storage, and other cryptographic functions
- Similar to a built-in smart card and can actually be used as a smart card on Windows 8 and later
- Not designed just for Microsoft, works with Linux, too

SANS Security Essentials – © 2016 SANS

## Trusted Platform Module (2 of 4)

A Trusted Platform Module (TPM) is a chip in the motherboard of a computer. It is either welded into the motherboard, like on a phone or tablet, or inserted into a special socket, like on standard motherboards. The TPM chip can perform random number generation, encryption, hashing, and other cryptographic operations. The TPM also secures the storage of cipher keys, passwords, hashes, and other secret data. It is similar to a smart card, and, in fact, Windows 8 and later can use a TPM as smart card for user authentication, such as on phones or tablets which are not shared with other users. The TPM is a vendor-neutral cryptographic device, and it can be used with Linux, too.

For more information about TPMs, see the document "TCG Architecture Overview" (<http://www.trustedcomputinggroup.org/specs/TPM>) and do an Internet search **Windows virtual smart card TPM**.

### Turning On and Initializing the TPM

Normally, a computer with a TPM and Windows pre-installed will already be configured so that Windows can use the TPM immediately. But if the TPM must be managed by hand, then the TPM must be:

1. Enabled in the computer's firmware
2. Turned on in Windows
3. Initialized in Windows with an owner's password

How the TPM is enabled in firmware is determined by the computer's manufacturer (usually by pressing F2 or F12 during boot-up, and such), but it might already be enabled at the factory.

The TPM is turned on and initialized with an owner's password by using an MMC console snap-in named TPM Management (TPM.MSC). Turning on the TPM simply makes it available for use, while "initializing" the TPM means setting an owner's password. This password is required whenever the TPM is significantly modified, for example, turned on/off, memory cleared, password changed, and so on. The user does not have to know this password.

The owner's password can be backed up to a file or printed out for recovery purposes.

## BitLocker TPM Options (3 of 4)

- **With a TPM in the Motherboard:**

- **TPM + USB Drive + PIN**
- **TPM + USB Drive**
- **TPM + PIN**
- **TPM Only (vulnerable to cold boot attack)**

- **BitLocker with No TPM:**

- Pre-boot passphrase (Windows 8 or later)
- USB drive inserted at boot-up with the key
- No boot-up integrity protection to detect malware!

SANS Security Essentials – © 2016 SANS

### BitLocker TPM Options (3 of 4)

BitLocker can be configured to run with or without a TPM chip, and with or without user interaction during boot-up. After the computer is running and the user has logged on, BitLocker is 100 percent transparent to the user no matter which TPM option is used.

The following summarizes the various ways BitLocker can be implemented. The options are arranged from most secure (top) to least secure (bottom):

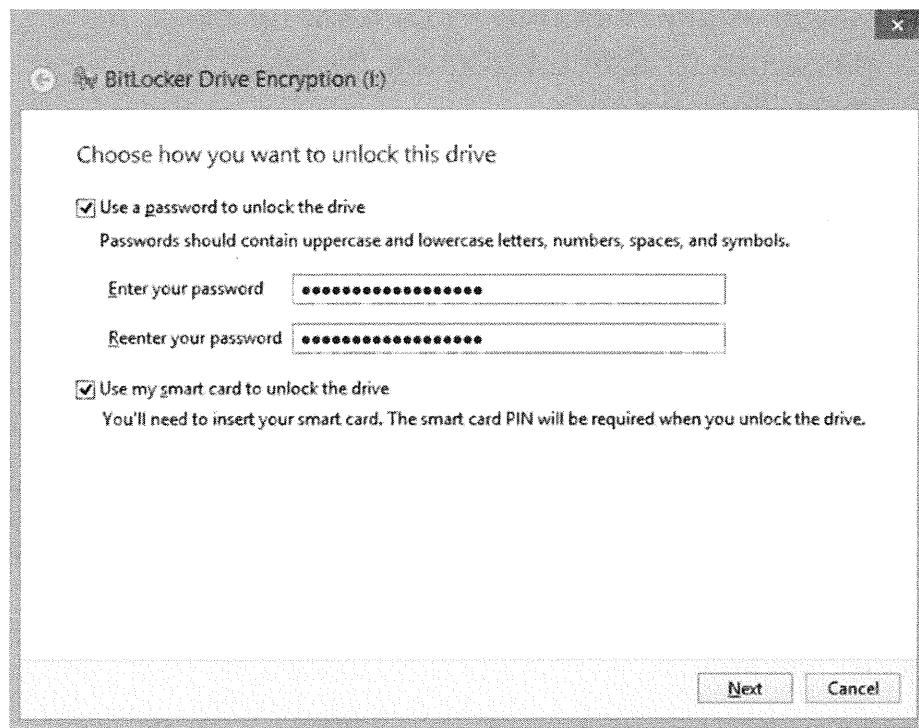
- **TPM + USB Token + PIN:** User must insert a USB token containing a key during boot-up and type in a PIN, but the token does not need to be left connected to the computer after boot-up. Boot-up integrity is checked. TPM required. Emergency recovery required if the USB token is lost or the PIN is forgotten. Requires Vista+SP1 or Server 2008 at a minimum.
- **TPM + USB Token:** User must insert a USB token containing a key during boot-up, but it does not need to be left connected to the computer after boot-up. No PIN required. Boot-up integrity is checked. TPM required. Emergency recovery required if the USB token is lost.
- **TPM + PIN:** User must enter a 4- to 20-digit PIN during the text-mode phase of boot-up. No USB token required. Boot-up integrity is checked. TPM required. Emergency recovery required if the PIN is forgotten.
- **TPM Only:** No user interaction required. No USB token or PIN necessary. BitLocker is 100 percent transparent in this case, hence, is the most convenient option, even if it is not the most secure. Boot-up integrity is checked. TPM required.
- **USB Token Only (No TPM):** User must insert a USB token containing a key during boot-up, but it does not need to be left connected to the computer after boot-up. No TPM chip or special BIOS required. No PIN can be used. Boot-up integrity is not checked, hence, no rootkit or spyware protection.

- **Passphrase (No TPM):** User must enter a passphrase after each reboot or resume from hibernation. Does not require a TPM. Boot-up integrity is not checked, hence, no rootkit or spyware protection. BitLocker key is derived from the passphrase. Requires Windows 8 or later.

Group Policy can be used to control almost every aspect of how BitLocker may be used (GPO: Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption). BitLocker can also be managed through Windows Management Instrumentation (WMI) scripting of the Win32\_EncryptableVolume class for hands-free and scalable deployment.

### **BitLocker for USB Flash Drives**

On Windows 7 and later, BitLocker can also be used on external drives, such as USB flash drives. In Windows Explorer, just right-click the drive and select Turn On BitLocker to get started. You can use either a passphrase or a smart card to secure access to the drive.



### **Cold Boot Attack**

Why have these extra PIN and USB options on top of the TPM? If someone steals your laptop and boots it into Windows, the computer is now vulnerable to a "cold boot attack" in which the BitLocker decryption key (and other sensitive data, such as passwords) can be directly extracted from RAM by pulling the batteries and power, then rebooting from another USB or DVD drive to allow a search or dump of raw memory ([http://en.wikipedia.org/wiki/cold\\_boot\\_attack](http://en.wikipedia.org/wiki/cold_boot_attack)). By requiring a pre-boot PIN or USB token, it helps to defeat cold boot attacks under the right circumstances.

# Emergency Recovery (4 of 4)

- **Back up your recovery password!**

- Password is actually a 48-digit number
- Decrypts volume even if the TPM is damaged, PIN is forgotten, or the USB token is lost
- Group Policy option to force back up of password to Active Directory for scalable mass deployments

SANS Security Essentials – © 2016 SANS

## Emergency Recovery (4 of 4)

After a volume is encrypted, you can make extra backups of the recovery password or USB startup key in case of emergency. The recovery password can be saved to another (non-encrypted) hard drive volume or USB drive, or printed out for manual re-entry. (You can also "print" to an .xps file.) Recall that the recovery password is used when one of the TPM options doesn't work, for example, the USB token is lost, PIN forgotten, and so on. When not using a TPM, the only option left over is to store the key on a USB drive that must be attached when starting the computer. A back up of the startup key is actually just another copy of the USB drive, hence, you must duplicate the startup key to another USB drive.

To make an extra backup of your BitLocker recovery password/file, open Control Panel > BitLocker Drive Encryption > Manage BitLocker Keys.

Don't be confused by the four USB-related options for BitLocker and TPMs:

- One USB drive might be for the TPM+USB option for BitLocker. This is carried around by the user and is used on a daily basis for every reboot.
- Another USB drive might be used to store a backup copy of the recovery password. This is not used except in the rare event of emergency recovery, but that same recovery password file could just as well have been burned to a CD or simply printed out. This USB drive should be left at home or locked away.
- For another computer that has no TPM, another USB drive would have to be used for BitLocker to function at all. This USB drive contains the startup key and would be used whenever the computer is rebooted. Another USB drive should be made for this computer as a backup and left at home or locked away at the office.
- The TPM owner's password can also be saved to a USB device, hard drive, CD, floppy, etc. The TPM owner's password is used only when managing the TPM, which will be rare, and the backup password file is not the same as any of the other backup files used by BitLocker.

And beware of confusing the BitLocker PIN, recovery password, and TPM password:

- The PIN, if used, is for the TPM+PIN option for BitLocker. It is entered with every reboot on computers with TPM chips that have been configured to require a PIN. This PIN is not the same as the TPM owner's password or the recovery password.
- The recovery password is used only during BitLocker emergency recovery. It is actually a number itself, so it is like a PIN, but it has a different purpose than the PIN used during TPM+PIN boot-up.
- The TPM owner's password is usually backed up as a file, but the data is just a string of ASCII characters. This password is used only when managing the TPM, which will be rare, but it is not the same as the startup PIN or recovery password.

### **Recovery Procedures**

If the TPM chip is damaged or cleared, if the boot-up environment is modified, or if the user forgets their PIN or loses their USB token, then emergency recovery is required.

When recovery is required, the computer will partially boot up and then the user will be prompted to enter the recovery password before the rest of the OS can load. The recovery password is a 48-digit PIN that looks something like this:

665703 675205 566655 025763

076677 032514 410668 550257

which is entered into the form presented to the user during emergency recovery:

All BIOS systems support the function keys at boot-up, hence, the numeric PIN is entered by pressing the function keys only, for example, F10 = 0, F1 = 1, F2 = 2, and so on. If the BIOS of a particular computer supports the entering of digits with the regular number keys, then, of course, they can be used instead. After entering the number, the computer boots up normally.

Emergency recovery on a computer without a TPM does not have to be a special process: If the primary USB drive is lost or damaged, just insert the second USB drive that was made as a backup for this purpose. Of course, this assumes a backup USB drive was made. If no secondary USB drive was made, then you have to enter the recovery password just like for the other options.

### **Force Backup to Active Directory**

If the recovery password has been lost, or if it weren't created in the first place, then the last hope is for a recovery key to have been stored in Active Directory. Using Group Policy, the plaintext BitLocker recovery password can be stored in the Active Directory database as well as an encrypted copy of the FVEK key itself. If multiple volumes on Windows Server are encrypted, recovery information will be stored for each volume in AD.

To configure this feature, open a Group Policy Object > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Turn on BitLocker backup to Active Directory Domain Services. In the GPO, if you require AD backup, BitLocker refuses to engage if the backup attempt is unsuccessful. The "key package" referenced in the GPO is the encrypted FVEK. Recovery is performed using a Microsoft-supplied script.

# UEFI Secure Boot

- Unified Extensible Firmware Interface:
  - UEFI replaces the older BIOS
  - This cannot be added later; it must be built in
- Secure Boot is mainly a UEFI feature:
  - Checks digital signatures of boot-up binaries and the firmware with a list of trusted Cas
  - Very early load of antivirus drivers
  - TPM and BitLocker are optional, recommended

SANS Security Essentials – © 2016 SANS

## UEFI Secure Boot

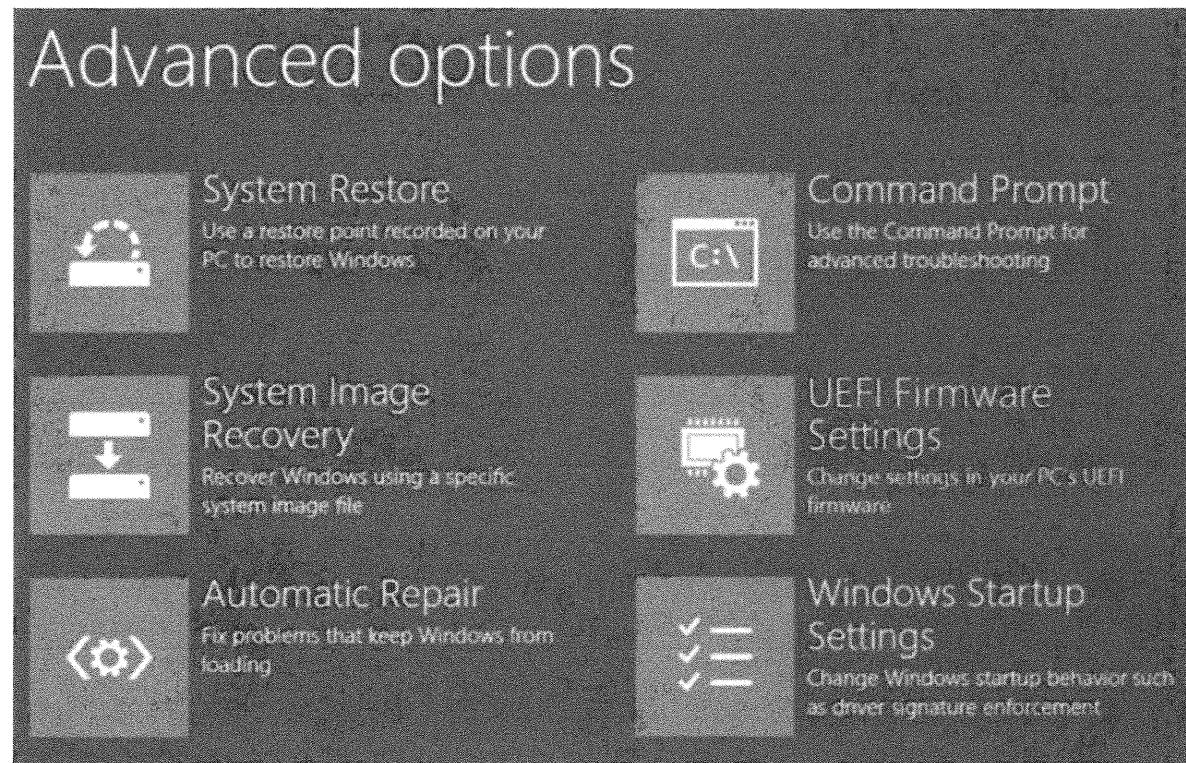
Unified Extensible Firmware Interface (UEFI) replaces the older BIOS interface to the computer's firmware. A computer must be purchased with UEFI; it cannot be added later. With UEFI, a Windows 8 and later computer can use "Secure Boot" to resist malware, which attempts to infiltrate the computer and operating system during boot-up even before the OS has loaded into memory. Secure Boot is defined in Chapter 27 of the UEFI 2.3.1 specification, so it's not a feature of the Windows operating system *per se*; though Microsoft wants OEMs to enable it on UEFI devices, and there are Windows tie-ins to it.

Secure Boot includes 1) digitally signed binaries that load the operating system, 2) digitally signed UEFI firmware, 3) early load of antivirus scanners before any other third-party software or drivers are loaded, and 4) optional Trusted Platform Module (TPM) integration to measure other aspects of the computer's boot-up components to detect changes.

Secure Boot checks the digital signatures of motherboard firmware, operating system binaries, and option ROM firmware in supported peripherals from the time of power-on until the antivirus scanner is running, at which point the AV scanner takes over the job of combating malware. The UEFI firmware ships from the factory with a list of trusted Certification Authorities (CAs) built in, and, if the motherboard manufacturer permits it, this list of CAs can be changed through Windows Update or an internal enterprise management system, such as Group Policy or Microsoft System Center. The firmware maintains two tiny encrypted databases, *Allowed CA* certificates and *Disallowed* file hashes, and these can also be made manageable by the OEM vendor.

Although Secure Boot can be disabled on a x86/x64 computer, if the OEM allows it, it is not possible to disable Secure Boot on ARM devices if that device wants to keep the Certified for Windows logo. This is controversial because it might make it difficult for other operating systems, such as Windows 7 or Linux, to be installed; time will tell what the OEM vendors will sell to the public.

Secure Boot requires UEFI, Windows 8 or later, and a GUID Partition Table (GPT) bootable hard drive partition. (Secure Boot from an older Master Boot Record partition is not supported). Secure Boot does not require a TPM or whole drive encryption, but combining all three technologies is best for resisting bootkits and other early-load malware. This triple-combo will be the default, in fact, on most Windows RT tablets using either BitLocker encryption or hardware encryption.



# Summary

- Why authenticate?
- NTFS Permissions
  - DACLs and ACEs
- Share Permissions
  - Hidden Shares
- Registry Permissions
  - Remote Access
- Active Directory
  - Permissions
  - Delegation of Authority
- Privileges
  - Group Policy
- BitLocker
  - TPM
  - UEFI Secure Boot
  - Recovery Options
- Mandatory Integrity Control
  - Process Labels
  - File Labels

SANS Security Essentials – © 2016 SANS

## Summary

So, why have user accounts? Why go through all the trouble of Active Directory, Kerberos, NTLM, SIDs, SATs, and all the rest? The purpose of this module was to discuss the two primary benefits of authenticating users: permissions and privileges. (The third benefit, auditing, will be discussed in module 30.) Indeed, selective access control is impossible without authentication, and authentication is pointless unless you intend to use that information for something, that is, privileges, permissions, or auditing.

We started out with a discussion of NTFS and shared folder permissions, including an overview of how they can be combined. NTFS, however, doesn't protect data from hackers who have physical access to computers or who have stolen backup media; for this we need encryption. The Registry is the equivalent of the entire /etc directory on a UNIX-based system, and it too has its own permissions. Though beyond the scope of this course, Active Directory permissions are critically important for the security of your network. Every property of every object in the AD database has its own ACL. AD permissions are the foundation of all delegation of authority in Windows-based networks.

Mandatory Integrity Control (MIC) works alongside the usual selective access control features of permissions and privileges. MIC helps ensure system integrity by enforcing the *No Changes Up* rule, and can be used to restrict read and execute access as well.

If you have a TPM chip in the motherboard, BitLocker also helps to ensure boot-up integrity to make spyware more difficult to install.

# Module 26: Enforcing Security Policy

SANS Security Essentials – © 2016 SANS

## **Module 26: Enforcing Security Policy**

This section intentionally left blank.

# Windows Security Templates and Group Policy

---

The student will have a high level understanding of the features of Group Policy and working with INF security templates.

SANS Security Essentials – © 2016 SANS

## **Windows Security Templates and Group Policy**

This section intentionally left blank.

# Enforcing Security Policy

---

## SANS Security Essentials V: Windows Security

SANS Security Essentials – © 2016 SANS

### **Enforcing Security Policy**

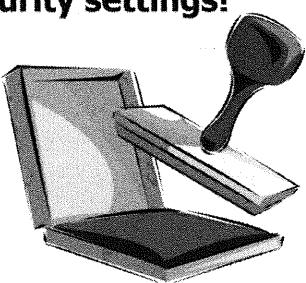
This module discusses one of the best tools for automating security configuration changes, Microsoft's Security Configuration and Analysis (SCA) snap-in, and some of the most important changes to make with it, such as password policy, lockout policy, and null user session restrictions. It also briefly discusses Group Policy Objects (GPOs) and the many security configuration changes that can be made through them throughout the domain.

In particular, this module covers:

- Applying Security Templates
- Employing the Security Configuration and Analysis Snap-in
- Understanding Local Group Policy Objects
- Understanding Domain Group Policy Objects
- Checking Recommended GPO Settings, Including:
  - Password Policy
  - Account Lockout Policy
  - Security Options
  - Internet Explorer Security
  - Miscellaneous Administrative Templates
  - Other Settings

# Security Templates (1 of 3)

- **These can be applied like What's in a Template? a rubber stamp to multiple machines for consistent security settings!**



- Password Policy
- Lockout Policy
- Kerberos Policy
- Audit Policy
- Privileges
- Event Log Settings
- NTFS Permissions
- Group Memberships
- Service Startup
- Registry Permissions

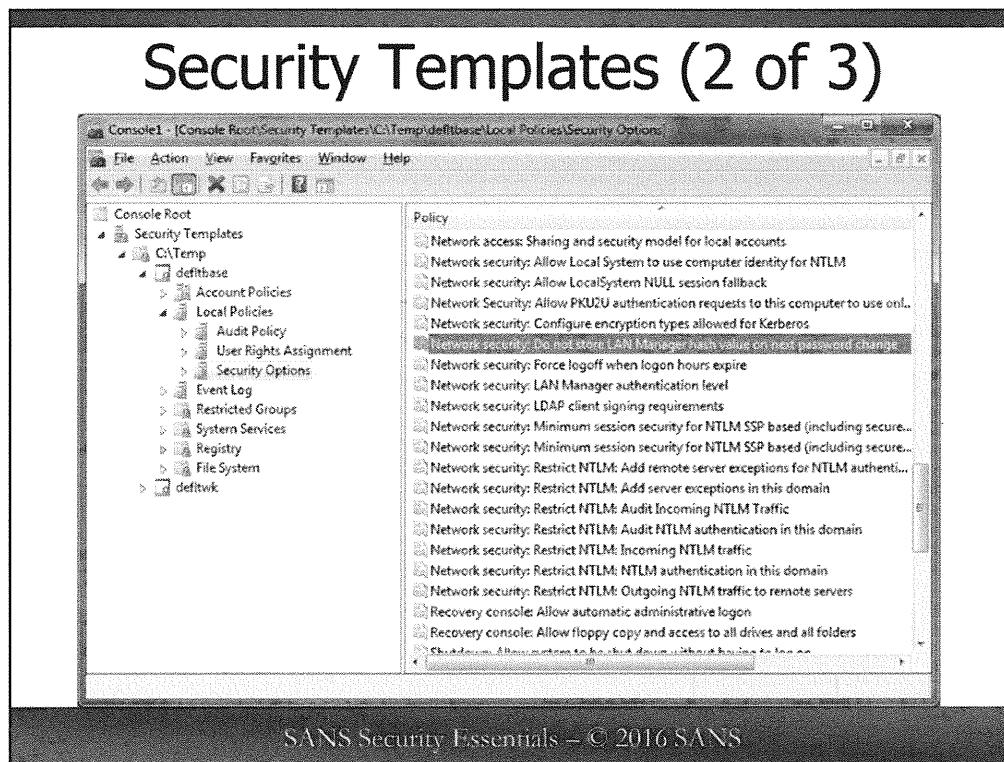
SANS Security Essentials – © 2016 SANS

## Security Templates (1 of 3)

A *security template* is a plain text configuration file that can store hundreds of security settings. A computer can be stamped with a template and reconfigured in one shot to match the settings in the template.

A template can store the following security settings:

- Password policies
- Account lockout policies
- Kerberos policies
- Audit policies
- Custom privileges assignments
- Various security options
- Event log sizes and wrapping options
- Custom memberships in important groups
- Service startup options
- Registry key permissions
- NTFS permissions and audit settings



SANS Security Essentials – © 2016 SANS

## Security Templates (2 of 3)

Security templates are kept by default in %SystemRoot%\Security\Templates\ and also %SystemRoot%\Inf, and they end with the .INF filename extension. Templates can be edited with Notepad, but a much easier method is to use a Microsoft Management Console (MMC) snap-in named *Security Templates*.

To load the snap-in and create a new template, go to the Run line and execute mmc.exe > pull down the Console menu > Add/Remove Snap-In > Add > Security Templates > Add > Close > OK. In the snap-in, double-click the templates yellow folder to open it. Right-click the yellow templates folder > New Template > enter **Generic** as the name > OK. This creates a Generic.inf file.

In the Templates snap-in, double-click a template to open it up. Browse through its containers and double-click the policy icons to configure them. When you finish, right-click the edited template and save it. If you want, browse to that template's folder using Windows Explorer and open the template in Notepad.

# Security Templates (3 of 3)

## • ***Don't start from scratch!***

- Start with a preconfigured and debugged template to save time; then test and edit to meet your needs.
- Microsoft + DISA + NIST + NSA collaboration templates:
  - Download the free **Microsoft Security Compliance Manager** kit.
  - The kit includes a variety of templates for different products.
  - The kit is regularly updated as new product versions come out.
  - Use the kit to export, compare, and otherwise manage templates.

SANS Security Essentials – © 2016 SANS

## Security Templates (3 of 3)

You don't have to create your own templates from scratch. Many players in the Windows security arena have customized templates free for the download. It is highly recommended that you begin with someone else's templates instead of starting from scratch. The reason for this is that security is bad for usability. In general, the more security options you configure, the more applications you are likely to break. Templates from Microsoft, NIST, CIS and others have been debugged and tested to improve security as much as possible while breaking as little as possible.

Remember, too, that you always can edit a template obtained from someone else in any way you want, so start with a template from someone you trust; then test and fine-tune it for your organization's needs.

### What Security Templates Are Available from Microsoft?

Microsoft has a set of security templates and best practices for various applications and versions of Windows. These templates provide an excellent starting point for your internal testing. They should not be applied without compatibility testing first. To download the templates and their associated documentation, download the free Microsoft Security Compliance Manager (SCM) tool:

**Microsoft Security Compliance Manager**  
<http://technet.microsoft.com/en-us/library/cc677002.aspx>

There is little reason to download the other operating system hardening guides if you have already obtained the Security Compliance Manager, but there are individual guides for the older products if you need to get them separately:

"Windows Server 2012 Security Baseline"  
(<http://technet.microsoft.com/en-us/library/jj898542.aspx>)

"Windows Server 2008 Security Guide"  
(<http://technet.microsoft.com/en-us/library/cc264463.aspx>)

"Windows Server 2003 Security Guide"  
(<http://go.microsoft.com/fwlink/?LinkId=14845>)

"Windows 8 Security Baseline"  
(<http://technet.microsoft.com/en-us/library/jj916413.aspx>)

"Windows Vista Security Guide"  
(<http://www.microsoft.com/technet/windowsvista/security/guide.mspx>)

"Threats and Countermeasures" (helps to explain settings in the other guides)  
(<http://go.microsoft.com/fwlink/?LinkId=15159>)

#### **What Templates Are Available From NIST And The US Government?**

**[FDCC]** The federal NIST version of Microsoft's templates were incorporated into the Federal Desktop Core Configuration (FDCC) standards:

- <http://nvd.nist.gov>
- <https://blogs.technet.com/b/fdcc/>
- <http://www.microsoft.com/industry/government/solutions/fscc/>

**[USGCB]** More recently, the U.S. Department of Defense and NIST have updated the FDCC standards and renamed the project to the "United States Government Configuration Baseline (USGCB)." The USGCB templates and GPOs now replace the earlier FDCC standards and should be preferred when there is a choice.

- <http://usgcb.nist.gov>

**[DISA STIG]** United States Department of Defense (DoD) Directive 8500.1 requires that all DoD computers be configured using security configuration guidelines developed by the Defense Information Systems Agency (DISA) and the National Security Agency (NSA). These guidelines come in the form of Security Technical Implementation Guides (STIGs) which include security templates, checklists, scripts, SCAP XML specifications, and other documents. These DISA STIGs are available to the public:

- <http://iase.disa.mil/stigs/>

**[CIS]** The Center for Internet Security (CIS) not only has security templates available, but also configuration guides to go with them. Government representatives participated in the creation of many of the CIS templates. Get the latest versions from the CIS site:

- <http://www.cisecurity.org>

# SCA Snap-in

- **Security Configuration and Analysis:**
  - MMC console snap-in
  - Applies a template to a computer (reconfigure)
  - Compares a template to a computer's actual settings (audit)
- Warning: There is no undo feature!
- Cannot apply a template to a computer across the network (That's what Group Policy is for.)

SANS Security Essentials – © 2016 SANS

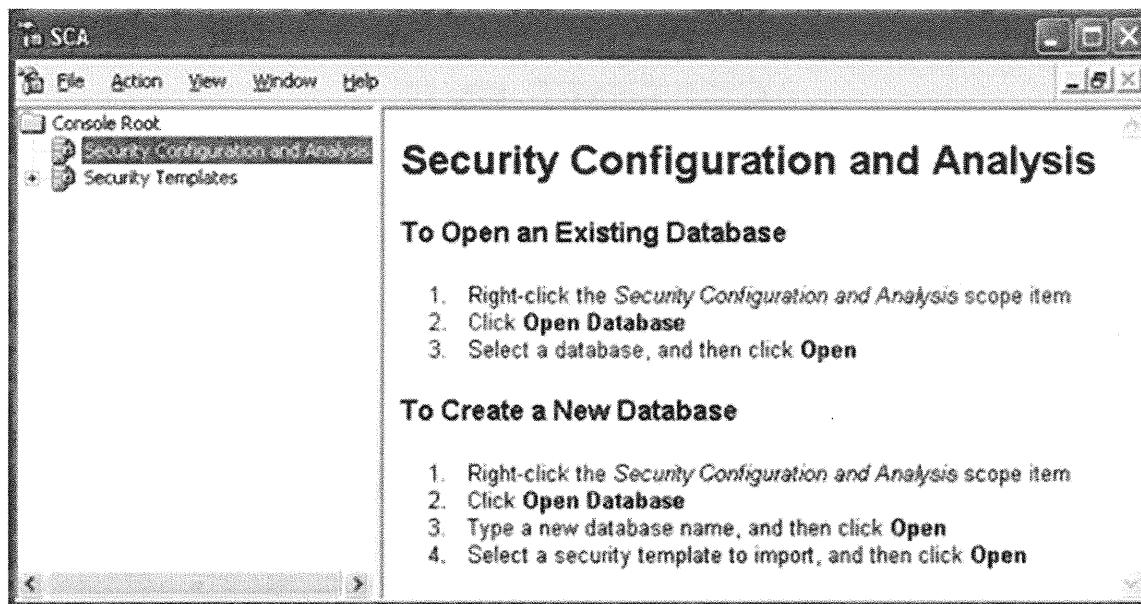
## SCA Snap-in

What good is a security template if you can't use it? The Security Configuration and Analysis (SCA) snap-in is used to reconfigure a computer to match the settings in a security template in one easy step. (The tool's other uses will be discussed later.) The SCA snap-in is the industrial press that applies templates to computers on the assembly line as you build them.

Install the SCA snap-in in the same MMC console as the Security Templates snap-in using the same procedures described previously.

When you first click the SCA snap-in, instructions for using it appear on the right side of the console. Follow the instructions to create a new database; don't worry, the *database* is just a small temp file. To create a new database, right-click the SCA snap-in > Open Database > enter any database name you want > Open. If a dialog box does not immediately appear to import a template, then right-click the SCA again > Import Template > double-click an INF template file. This imports the template's settings into the temporary database.

After a template has been imported into the database, reconfigure the computer to match the template by right-clicking the SCA > Configure Computer Now > OK.

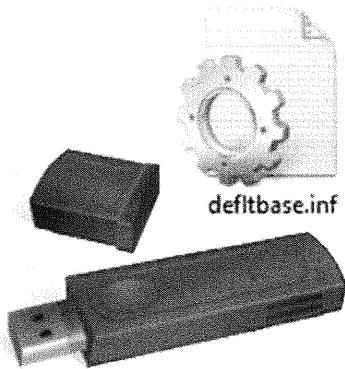


Warning! There is no *undo* feature in the SCA tool. Test new security settings on non-production systems first, and make a backup of the production server you intend to reconfigure (including the *System State*) before you apply the template.

The SCA snap-in has an important limitation, though: it can be used only on the local machine where the tool is being run. However, there is a command-line version of the tool which can be scripted!

# SECEDIT.EXE

- **Command-line version of SCA**
- Script the application of a template from:
  - Shared folder
  - Flash drive
  - DVD



SANS Security Essentials – © 2016 SANS

## SECEDIT.EXE

SECEDIT.EXE is a command-line version of the SCA snap-in. Imagine creating a floppy disk with SECEDIT.EXE and a simple batch file to run it: You could field a platoon of IT staff with these floppies to quickly reconfigure hundreds of machines! Alternatively, the necessary files could be placed in a shared folder. Other computers would need only to map a drive letter to the share and run SECEDIT.EXE from there. Or a scheduled batch file could reapply settings on a critical server every night at 3 a.m. from that shared folder.

The SECEDIT.EXE tool still cannot be used to apply a template to a machine across the network, but because it is so easily scriptable, it can make applying templates much easier. To create a floppy/CD/USB with everything you need, follow these steps:

1. Use the SCA snap-in to create a database file (let's name it **dbase.sdb**), and import the settings from your favorite template(s).
2. Copy the database file to a floppy disk.
3. Create a batch file (let's name it **apply.bat**) on the floppy disk using Notepad.
4. Add this line to the batch file: `secedit.exe /configure /db A:\dbase.sdb`.

Now, simply insert the floppy disk and run the **APPLY.BAT** file. You don't have to copy the SECEDIT.EXE program to your floppy disk because it is already in the default path on the hard drive.

But where can you see these settings after they have been applied? NTFS and Registry key permissions are easy enough to see in Windows Explorer and REGEDIT.EXE, but what about all the other settings? For this you must look at Group Policy Objects.

# Local Group Policy Object (1 of 4)

- Group Policy Object Editor MMC snap-in
  - Changes take effect immediately
- **Computer Configuration:**
  - Applies even when no one is logged on
- **User Configuration:**
  - Applies to current user's desktop

SANS Security Essentials – © 2016 SANS

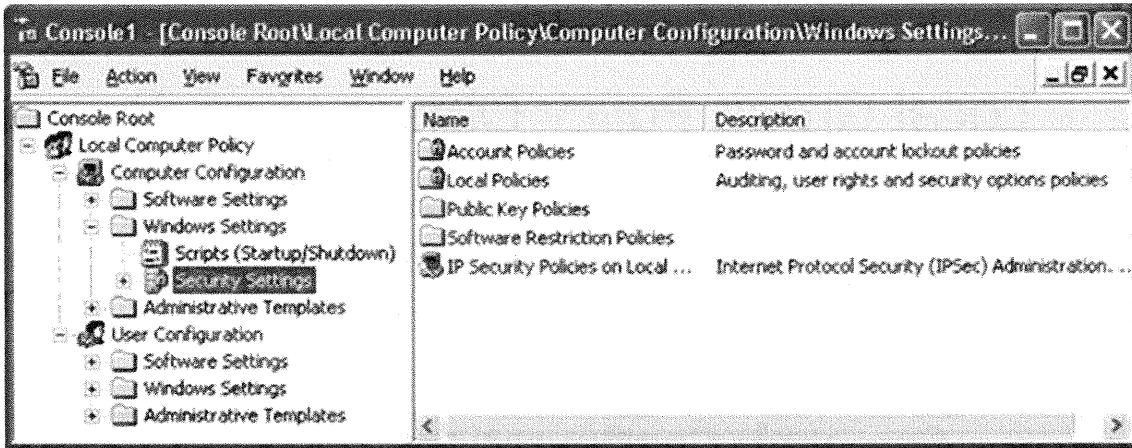
## Local Group Policy Object (1 of 4)

A security template stores settings in a form that can be applied to a computer. But applying templates is not the only way to configure security options. Permissions, of course, can be configured with a variety of tools (as discussed in the prior module), but there are other options, as well. To change these you need to examine Group Policy Objects (GPOs). We'll start with the local GPO and later discuss domain-based GPOs.

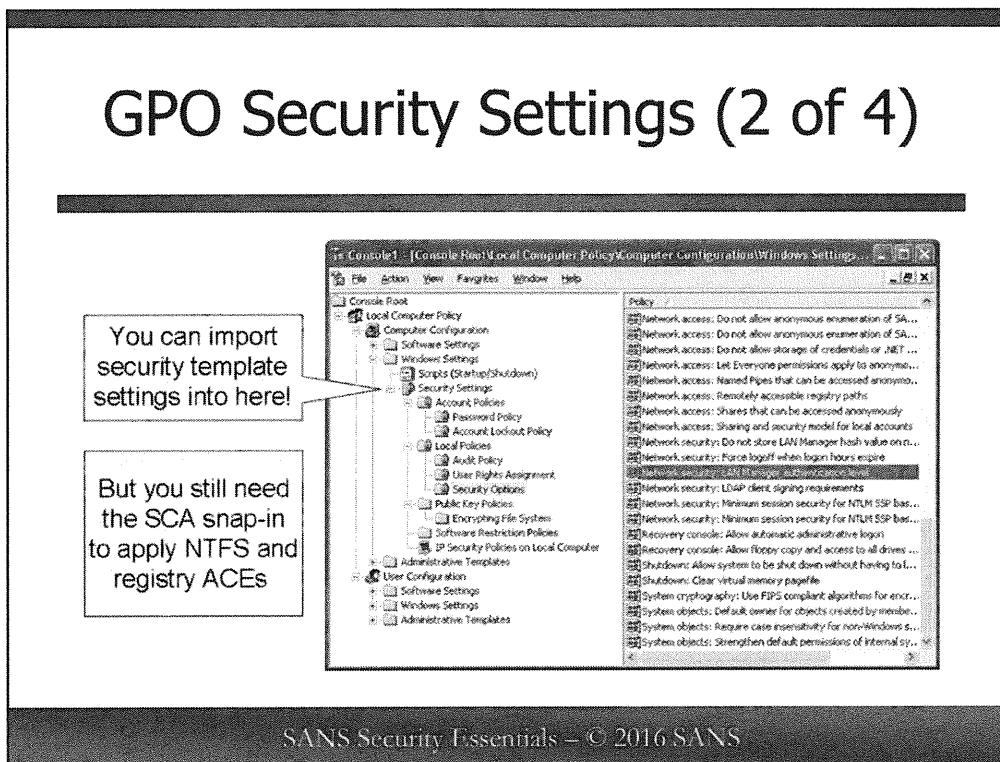
Assume you are working with a standalone system (or a system in a Windows NT domain). Your current security settings, except for NTFS and Registry key ACLs, can be viewed and edited through your local Group Policy Object. A GPO is similar to a security template, except that GPOs are applied automatically simply by editing the GPO itself; that is, you don't have to run tools like SECEDIT.EXE, GPUPDATE.EXE, or the SCA snap-in to apply these settings.

To access your local GPO, open an MMC.EXE console > Console menu > Add/Remove Snap-In > Add > Group Policy > Add > make sure that Local Computer is the selected GPO > Finish > Close > OK. Now, double-click the snap-in to expand it, and browse through the many subcontainers and their settings.

The Computer Configuration settings apply even when no one is logged on. The User Configuration settings apply to the user's desktop when a user currently is logged on. Let's browse through some of the more important settings together, but please keep in mind that there are too many to cover in a single module.



## GPO Security Settings (2 of 4)



SANS Security Essentials – © 2016 SANS

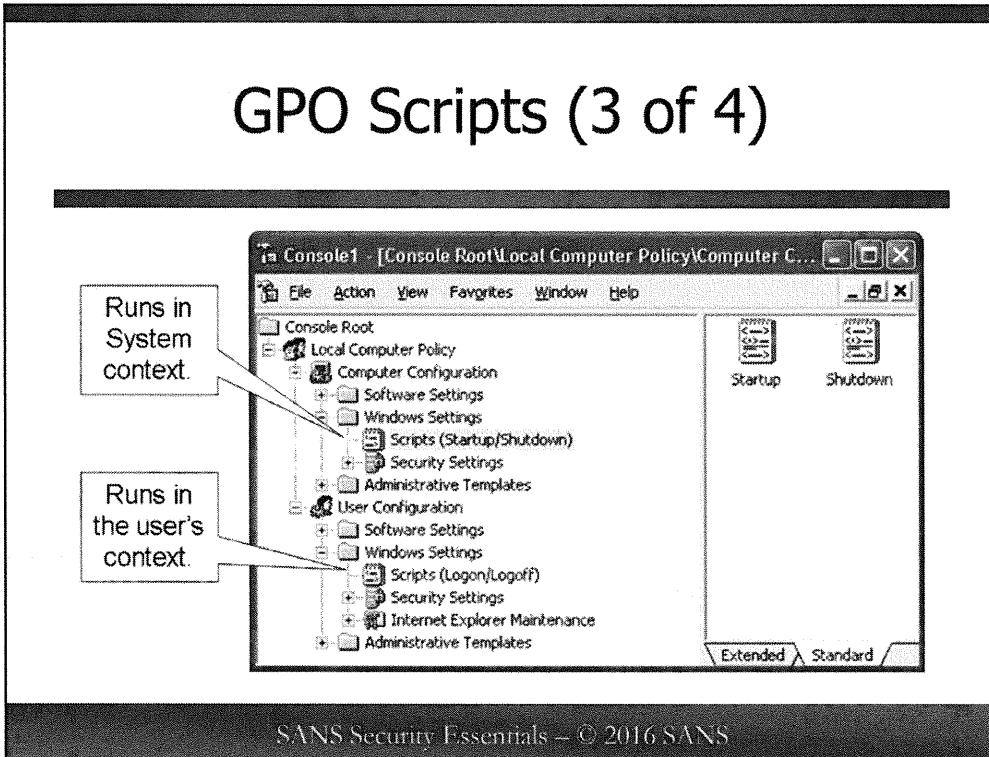
### GPO Security Settings (2 of 4)

The Computer Configuration > Windows Settings > Security Settings section bundles together the most important security settings on your system. In fact, this portion of your local GPO looks extremely similar to a security template. This is no accident. You can import a security template into your local GPO! Any settings in the template that are also in the GPO will be overridden by the template; but keep in mind that there are some settings in a template that are not available in the local GPO; that's why the SCA snap-in still is needed.

To import a template into your local GPO, right-click the Security Settings container in the GPO > Import Policy. Most changes take effect immediately, but to ensure that all settings have been reapplied, reboot the system after importing a template. Again, just as before, obtain a preconfigured template from an organization you trust; modify that template to match your preferences; and then apply it using the SCA snap-in and/or Group Policy Objects.

But if you want to edit a setting by hand, you don't have to resort to the importation of an entire template. Simply double-click a policy icon to bring up its dialog box!

## GPO Scripts (3 of 4)



### GPO Scripts (3 of 4)

You can assign scripts to be executed through a GPO, as well. These options are found under both Computer and User Configuration > Windows Settings > Scripts.

Scripts can be executed at system startup, shutdown, user logon, or user logoff. Scripts can be written in any language, as long as the necessary interpreter has been installed. By default, there is support for PowerShell, VBScript, JScript and batch files, but there are free interpreters available for Perl and Python, too (<http://www.activestate.com>, <http://www.python.org>).

Startup/shutdown scripts run in System context, whereas logon/logoff scripts run in the context of the user. You can have as many of each type of script you want, and you can mix and match your languages across your scripts as wanted.

Virtually every aspect of the operating system can be scripted, including users, groups, NTFS ACLs, shared folders, registry settings, IIS, Office application settings, and more.

# Administrative Templates (4 of 4)

- A user-friendly Registry editor!
  - And the Registry controls almost everything, of course
- Hundreds of settings are available
- You can import more ADM templates
- You can edit these templates to configure any Registry value wanted

SANS Security Essentials – © 2016 SANS

## Administrative Templates (4 of 4)

The Registry is the central configuration database for the entire computer. It can be edited with REGEDIT.EXE, of course, but this isn't user-friendly. Many security settings from the Registry are exposed, however, through the Administrative Templates containers in your GPO. Administrative Templates settings are found under both Computer and User Configuration in the GPO; if there is a conflict between the two, the setting from the Computer Configuration container wins (usually).

There are hundreds of settings under Administrative Templates. The best way to become acquainted is simply to browse through the categories. For any setting you want to configure, double-click its icon to reveal a dialog box. Notice that most items have an Explain tab with some amount of explanation for that setting (sometimes just a sentence, sometimes many paragraphs).

Most aspects of the user's interface can be configured through Administrative Templates. For example, under User Configuration > Administrative Templates > Control Panel, there is an option to restrict which Control Panel applets the user is permitted to open (and another to restrict access to the Control Panel entirely). In that same section is a subcontainer (Display) that can be used to require a password-protected screensaver.

The reason this section mentions *templates* is that you can add more yellow folders and configuration icons. If you right-click on the Administrative Templates folder, you can select Add/Remove Templates. These are not INF security templates; these are ADM/ADMX templates (ADM for all Windows versions, ADMX just for Vista and later). When you import a template, you get more configuration settings available in the GPO. Microsoft has a variety of templates that can be downloaded for free, and you can edit these templates with Notepad to add any Registry values you want. The *Microsoft Office Resource Kit*, for example, has templates to configure almost every setting in Word, Excel, Access, and Outlook.

Now, although it is nice to have these configuration options listed in one tool, it doesn't help when there are thousands of machines to be hardened. Is there a way to push these settings out automatically across the network to many machines?

# Domain Group Policy Objects

- **GPOs stored in Active Directory:**
  - Downloaded automatically at startup, shutdown, logon, and logoff
  - Refreshed on clients every 90–120 minutes
- **100% hands-free way of applying security templates to many thousands of computers around the world, but only if they are not standalones**

SANS Security Essentials – © 2016 SANS

## Domain Group Policy Objects

If your computers are members of an Active Directory domain, then all the settings in the local GPO (and more) can be pushed out to these computers automatically from your domain controllers. This is 100 percent hands-free. You are not physically touching any of the target computers or manually editing any user's local GPO. The SCA snap-in is disappointing because it doesn't work over the network, but domain-based GPOs *can* apply security templates over the network.

Domain-based GPOs are stored in the Active Directory database and replicated to all domain controllers. When a computer boots up, it downloads its domain GPO settings automatically (the Computer Configuration settings from the GPO). When a user logs on, the user's GPO settings are downloaded and applied automatically (the User Configuration settings from the GPO). Every 90–120 minutes thereafter, by default, your computer checks to see if any GPO changes have occurred, and, if so, your computer downloads and applies them on-the-fly.

# Default Domain Versus OU GPOs

- The Default Domain Policy GPO applies to everyone in the entire domain because it is assigned to the domain
- But when a GPO is assigned to an OU, that GPO applies only to the users and computers under that OU
- You can import an INF security template into a GPO to push out that template to many systems!

SANS Security Essentials – © 2016 SANS

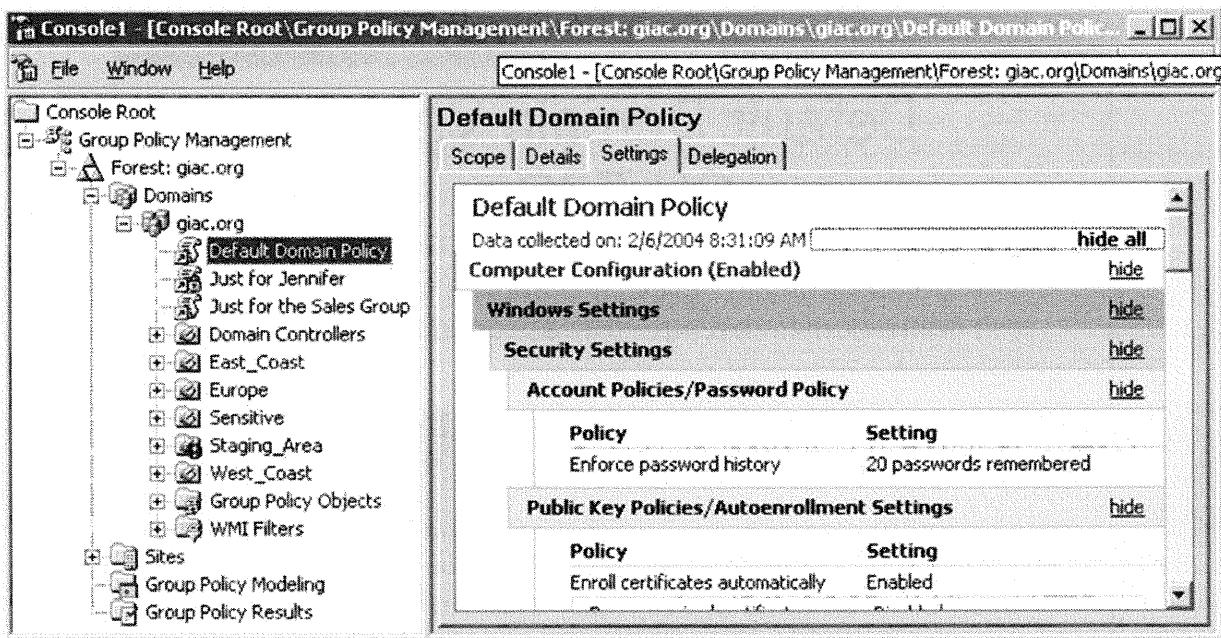
## Default Domain and OU GPOs

The Default Domain Policy GPO applies to all users and computers throughout the entire domain. If you are running Server 2008 or later, then click the Start menu > All Programs > Administrative Tools > Group Policy Management > expand your list of forests > expand your domain > right-click the Default Domain Policy GPO > Edit.

To edit the Default Domain GPO on Server 2003, log on to a domain controller as a Domain Admin > click the Start menu > Programs > Administrative Tools > Active Directory Users and Computers > right-click the name of your domain > Properties > Group Policy tab > highlight the Default Domain Policy > Edit.

The Default Domain GPO applies to everyone in the domain, whereas a local GPO applies only to the computer on which it is found. The settings in the domain-wide GPO override any conflicting settings in the local GPO on each computer, hence, administrators always have the final say.

If you want to restrict the application of a GPO just to the users and computers in a particular Organizational Unit, then create a GPO, and link it just to that OU. The Default Domain Policy GPO is linked at the top-level domain container; that's why it applies to everyone. An OU GPO, however, is linked only to a particular OU.



The Group Policy Management Console (GPMC) is built in Windows Vista/2008 and later by default. The GPMC is your primary tool for creating, editing and managing GPOs.

### Importing Templates Into GPOs

Again, just like with the local GPO, you can import a security template into a domain GPO. Once imported, all of the settings in the template (including the NTFS and registry ACLs) will be pushed out from the domain controllers automatically.

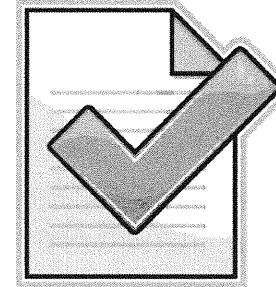
To import a security template into a domain GPO, open the GPO as described above, then open > Computer Configuration > Windows Settings > right-click on Security Settings > Import Policy > locate and select your desired template > Open.

Note that you don't have to save the GPO explicitly. Simply closing the GPO window will save it. The new GPO settings will be replicated to the other domain controllers within 15 minutes (assuming you don't have any WAN links to remote sites), and workstations and member servers will pick up those new settings within 90-120 minutes.

Now that we know how to make security configuration changes, what should those changes be? Let's discuss some of the more important security options. The old "80/20 Rule" applies here, as well: 80% of the security of your system will come from configuring just 20% of these security options, so the following are the ones on which to focus.

# Checklist of GPO Settings

- Password Policy
- Account Lockout Policy
- Security Options
- Anonymous Access Control
- Kerberos
- NTLMv2
- Guest Account
- Protecting Administrative Accounts
- Internet Explorer
- Administrative Template Settings



Next Slide →

SANS Security Essentials – © 2016 SANS

## Checklist of GPO Settings

The following pages contain a checklist to use when configuring security templates and Group Policy Objects. The checklist is intended to strike a balance between security and usability, so feel free to harden your settings as you see fit. The names of the options are slightly different between versions of Windows, but usually it is easy to figure out.

Let's consider the next few pages, then, and discuss each item separately.

# GPO > Password Policy

- **Maximum length: 127 characters:**
  - Think *passphrases*, not passwords
- **Recommended GPO settings:**
  - Enforce password history: 24 passwords
  - Maximum password age: 90 days
  - Minimum password age: 1 day
  - Minimum password length: 15 characters
  - Password must meet complexity requirements: Enabled

SANS Security Essentials – © 2016 SANS

## GPO > Password Policy

Good security always starts with a strong password policy. Even though users might complain, and management may oppose you, enforcing strong password policy is something about which you should be willing to fight because most of the other security features become moot if weak passwords are permitted. Here are the recommended minimum settings:

- Enforce password history: 24 password remembered
- Maximum password age: 90 days
- Minimum password age: 1 day
- Minimum password length: 15 characters
- Password must meet complexity requirements: Enabled

More important, remember that you can have 127-character *passphrases* in Windows, not just 14-character *passwords*. The length of the passphrase is more important than its complexity, too.

In addition, users prefer memorizing meaningful passphrases instead of random-looking passwords; for example, of the following two, which would you prefer to memorize?

1. %8Hjl@0JaF&Llc
2. My first child was born @ 10:45am on Tues

And the second one is many thousands of times stronger than the first because it contains 25 characters instead of just 14. (And they both satisfy complexity requirements.) Unfortunately, Microsoft's password policy permits only the enforcement of 14-character passwords when using Group Policy, but starting with Server 2008, you can enforce custom password policies instead.

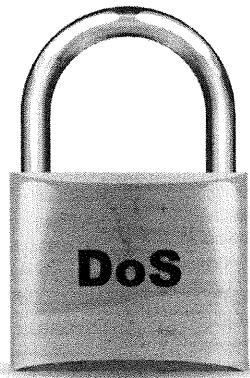
If all your domain controllers are Server 2008 or later, you can enforce different password and lockout policies for different groups. You don't have to use Group Policy to manage these. There is no built-in graphical tool for managing these custom password policies, it is all done with PowerShell cmdlets, direct Active Directory database edits, or third-party graphical tools. A free graphical tool for this is Specops Software Password Policy Basic (<http://www.specopssoft.com>). To use PowerShell, please search for the terms **powershell fine grained password policies** to see tutorials.

Password complexity requires a mixture of three out of the four categories of characters: uppercase, lowercase, numbers, and non-alphanumerics, for example, punctuation marks. The greater the variety of characters in a password, the more difficult it is to guess it. But password length is still more important than complexity.

Maximum password age prevents a compromised password from being used too long. If a password is crackable, it usually can be cracked in less than 90 days (often less than 90 minutes).

Minimum password age and password history work together. They prevent users from "recycling" their old favorite passwords over and over again. The assumption is that it's too much of a hassle to change one's password every single day for 24 days in a row just to get back to one's favorite password.

## GPO > Account Lockout Policy



- **Prevent brute force password guessing:**
  - Account lockout duration: 120 minutes
  - Account lockout threshold: 5 attempts
  - Reset account counter lockout after: 45 minutes
- But beware of DoS attacks if you authenticate Internet-exposed services with Active Directory!

SANS Security Essentials – © 2016 SANS

### GPO > Account Lockout Policy

If a hacker attempts to use a password-guessing program, then accounts should be locked out temporarily to prevent too many guesses from being checked. The minimum recommended settings are:

- Account lockout duration: 120 minutes
- Account lockout threshold: 5 attempts
- Reset account counter lockout after: 45 minutes

Windows keeps track of how many failed logon attempts have occurred for each user account. But that counter can be reset.

The idea is that a hacker will run up against the five-guess threshold almost instantaneously and trigger the longer lockout timer. If you make the lockout very long or infinite, users will be calling you constantly to reset their accounts or accounts can be permanently locked. A lockout policy can be expensive for the help desk.

There is another problem, too. If your web applications, wireless access points, VPN gateways, dial-up servers, RADIUS servers, and so on all authenticate against Active Directory, your adversaries can deliberately fail to log on as every username they know about five times in a row, thus locking out those accounts. Through social engineering, SQL injection attack or other methods, your adversaries might figure out the bulk of the usernames in Active Directory. Beware of your lockout policy becoming a Denial of Service (DoS) attack vulnerability.

# GPO > Security Options

- A variety of security settings are contained in this part of the GPO (Look in the manual; there's a long list)
- Let's discuss some of the more important ones:
  - Anonymous Access
  - Kerberos and NTLM
  - Guest Account

[Next Slide →](#)

SANS Security Essentials – © 2016 SANS

## GPO > Security Options

The Security Options container lists a variety of security switches that can be turned on. Some are critically important; others are obscure and paranoid. The following are the most important ones to configure, but feel free to enable the others, as well; however, whereas the other settings may enhance security, beware of their causing widespread interoperability problems without yielding much security advantage (which is perhaps why they are not on the list).

Here is the list of recommended minimum security options:

- **Network access:** Let Everyone permissions apply to anonymous users: Disabled
- **Microsoft network client:** Digitally sign client communication (if server agrees): Enabled
- **Microsoft network server:** Digitally sign server communication (if client agrees): Enabled
- **Interactive logon:** Disable CTRL+ALT+DEL requirement for logon: Disabled
- **Network security:** LAN Manager Authentication Level: Send LM/NTLMv1 - Use NTLMv2 session security if negotiated.
- **Accounts:** Rename administrator account: Enabled and renamed.
- **Recovery Console:** Allow automatic administrative logon: Disabled
- **Domain member:** Digitally encrypt secure channel data (when possible): Enabled
- **Microsoft network client:** Send unencrypted password to third-party SMB servers: Disabled
- **Interactive logon:** Smart card removal behavior: Lock Workstation
- **Accounts:** Guest account status: Disabled
- **Accounts:** Limit local account use of blank passwords to console logon only: Enabled

- **Interactive logon:** Message text for users attempting to log on (logon banner): "This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users also may be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials."
- **Network access:** Allow anonymous SID/Name translation: Disabled
- **Network access:** Do not allow anonymous enumeration of SAM accounts and shares: Enabled
- **Network access:** Do not allow storage of credentials or .NET Passports for network authentication: Enabled
- **Network access:** Sharing and security model for local accounts: Classic - local users authenticate as themselves
- **Network security:** Do not store LAN Manager hash value on next password change: Enabled

#### **GPO > Administrative Templates**

The following are more GPO security-related options, but these are located under the Administrative Templates folder in the GPO.

#### **System:**

- Custom user interface
- Disable the command prompt
- Disable registry editing tools
- Run only allowed Windows applications
- Don't run specified Windows applications
- Disable Autoplay [on CD-ROM or all drives]

#### **System > Logon/Logoff:**

- Disable Task Manager
- Disable Lock Computer
- Disable Change Password
- Disable Logoff
- Exclude directories in roaming profile
- Run these programs at user logon
- Disable the run once list
- Disable legacy run list

### **Windows Components > Windows Explorer:**

- Remove *Map Network Drive* and *Disconnect Network Drive*
- Hide these specified drives in My Computer
- Prevent access to drives from My Computer
- No Computers *Near Me* in My Network Places
- No *Entire Network* in My Network Places

### **Windows Components > Microsoft Management Console:**

- Restrict the user from entering author mode
- Restrict users to the explicitly permitted list of snap-ins

### **Windows Components > Task Scheduler:**

- Hide Property Pages [of tasks]
- Prevent Task Run or End
- Disable Drag-and-Drop [of .job files into the Tasks folder]
- Disable New Task Creation
- Disable Task Deletion
- Disable Advanced Menu
- Prohibit Browse [to schedule arbitrary programs or scripts]

### **Start Menu & Taskbar:**

- Remove common program groups from Start Menu
- Remove Run menu from Start Menu
- Disable and remove the Shut Down command

### **Control Panel:**

- Disable Control Panel
- Hide specified Control Panel applets
- Show only specified Control Panel applets

### **Control Panel > Add/Remove Programs:**

- Disable Add/Remove Programs
- Hide the *Add a program from CD-ROM or floppy disk* option

**Control Panel > Display:**

- Disable Display in Control Panel
- Hide Background tab
- Disable changing wallpaper
- Hide Appearance tab
- Hide Settings tab
- Hide Screen Saver tab
- Activate screen saver
- Screen saver executable name
- Password protect the screen saver
- Screen saver timeout

**Network > Network and Dial-Up Connections:**

- Prohibit deletion of RAS connections
- Prohibit access to properties of a LAN connection
- Prohibit access to current user's RAS connection properties
- Prohibit access to properties of RAS connections available to all users
- Prohibit access to the Dial-Up Preferences item on the Advanced menu
- Prohibit access to the Advanced Settings item on the Advanced menu
- Prohibit configuration of connection sharing
- Prohibit TCP/IP advanced configuration

## Anonymous Access (1 of 2)

- Null user sessions are the source of many Windows vulnerabilities in the past:
  - SMB session with blank username/password
- Open a null session manually:  
`net use \\ipaddr\IPC$ "" /user:""`
- Null sessions are rarely used anymore

SANS Security Essentials – © 2016 SANS

### Anonymous Access (1 of 2)

Null user sessions have been the cause of many Windows security vulnerabilities in the past. For example, through a null user session a remote hacker could download a complete list of all user accounts (and more) from an unfirewalled domain controller. Strictly speaking, a *null user session* is a Server Message Block (SMB) session to a Windows system where both the username and password are blank. Null user sessions were used extensively in Windows NT for legitimate management purposes, but hackers figured out how to leverage them for other purposes too. To establish a null user session to a Windows system, open a PowerShell or CMD.EXE window and execute the following command (where "target" is the IP address of the target computer):

```
net.exe use \\target\ipc$ "" /user:""
```

Other auditing tools will create the null session for you. For example, the DUMPUSERS.EXE tool (<http://www.ntsecurity.nu>) can extract a list of all user and group names with a null user session.

Null user sessions are rarely needed because computers can authenticate to each other with their own unique accounts, and trusts are two-way and transitive by default. Hence, it's a good idea to limit null user session vulnerabilities as much as possible. On networks running Server 2008, Windows 7 and later, with updated third-party applications, no one will probably even know this change had been made.

# Anonymous Access (2 of 2)

- **Security Settings > Security Options > Network Access:**
  - Let Everyone permissions apply to anonymous users:
    - Should be disabled
    - Grant access to the ANONYMOUS LOGON identity instead if you want to grant permissions to anonymous users
  - Do not allow enumeration of SAM accounts and shares:
    - Should be enabled
  - Allow anonymous SID/Name translation:
    - Should be disabled

SANS Security Essentials – © 2016 SANS

## Anonymous Access (2 of 2)

There are a few options related to restricting anonymous access which work together (KB823659).

The option named *Network access: Do not allow enumeration of SAM accounts and shares* should be set to enabled, and the *Network access: Allow anonymous SID/Name translation* option should be set to disabled. These both must be configured together this way to prevent tools like DUMPUSERS.EXE from enumerating user accounts. Tools like DUMPUSERS.EXE can still get a list of accounts if these options are incorrect because these tools can read Security ID numbers (SIDs) over the network and map these SID numbers back to the names of their owners.

Another option to control null session users is named *Network access: Let Everyone permissions apply to anonymous users*. When enabled, this causes the operating system to treat anonymous null users as members of the Everyone group for the sake of permissions on resources like shared folders. When disabled, null users are no longer included as members of the Everyone group for calculating permissions, hence, permissions granted to the Everyone group are not granted to null users. This option should be set to disabled, and, as a habit, it's best to avoid granting permissions to Everyone anyway. If you do want to grant permissions to null users, then there is a special identity for this purpose named *ANONYMOUS LOGON* to which permissions can be explicitly granted.

# Kerberos & NTLMv1 (1 of 2)

- **Kerberos:**

- Default protocol, faster, more secure
- Requires Active Directory and domain membership

- **NTLMv1:**

- Still supported for standalones and for backward compatibility
- Susceptible to password sniffing attacks, but...

SANS Security Essentials – © 2016 SANS

## Kerberos & NTLMv1 (1 of 2)

The default authentication protocol for a computer joined to an Active Directory domain is Kerberos. This means that these operating systems will try to use Kerberos whenever possible, and Kerberos support is built into the drivers for SMB, LDAP, RPC, HTTP, and other protocols for accessing resources over the network (but not Telnet or FTP, surprisingly). This is good because Kerberos is faster and more secure than NTLM. Kerberos uses UDP (mostly), and clients can cache and reuse their *Kerberos tickets*, that is, their authentication tokens, for hours. Keep in mind that Kerberos ticket exchanges can be sniffed by password hash stealing programs, so remember to use good long *passphrases*.

The bad thing about Kerberos, though, is that it requires the computer to be a member of an Active Directory domain and network access to domain controllers.

For the sake of backwards compatibility, Windows still supports NTLMv1 authentication protocol, but there's a problem: NTLMv1 authentication traffic can be sniffed with tools like Cain to reveal the user's password hashes! These password hashes then can be loaded into tools like RainbowCrack to attempt cracking. If the user has a short password, it will be easily cracked.

## Kerberos & NTLMv2 (2 of 2)

- **NTLMv2:**

- Not vulnerable to sniff-and-crack attacks if configured correctly
- A good passphrase is still necessary

- **LAN Manager Authentication Level:**

- Send NTLMv2 Response Only
- Refuse NTLMv1 and LanManager

SANS Security Essentials – © 2016 SANS

### Kerberos & NTLMv2 (2 of 2)

Fortunately, NTLMv2 is not actually vulnerable to sniff-and-crack attacks. NTLMv2 was redesigned with password sniffers in mind and can repel them if configured correctly (and you don't have a short password). Windows NT 4.0+SP4 and later systems can all support NTLMv2 (see KB147706 and Q823659 for more information) and Windows 7/2008-R2 can even turn NTLM off!

Windows has a GPO Security Option named *LAN Manager authentication level*. There are a variety of settings for this option, but actually there are only two choices worth discussing:

- Send NTLMv2 response only [Level 3]
- Send NTLMv2 response only/refuse LM & NTLMv1 [Level 5].

The first choice balances security and backwards compatibility a bit. When acting as a client and doing an outbound authentication, it causes the machine to try only Kerberos and NTLMv2, but when acting as a server processing inbound authentications too, it will still accept NTLMv1 and LanManager for inbound requests. But this can still break things.

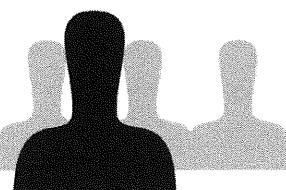
The second choice allows only Kerberos and NTLMv2 in all cases, both as a client (outbound) and as a server (inbound). This is the more secure option, but it sacrifices backward compatibility for that security. (It all depends on what you want.) Keep in mind that NTLMv2 Session Security is also required to make NTLMv2 traffic resistant to sniff-and-crack attacks, but this is used automatically with the above two levels.

Ultimately, however, NTLM will be deprecated in favor of Kerberos, and starting with Windows 7 and Server 2008-R2, NTLM can be disabled entirely via Group Policy.

# The Guest Account

---

**Automatic  
Guest  
Logon**

- Recommendations:
- Disable Guest account
- Random passphrase
- Automatic demotion to guest account with the Sharing Wizard

SANS Security Essentials – © 2016 SANS

## The Guest Account

The built-in Guest account can do some strange things. If someone attempts to authenticate to your computer, but the username provided is unknown to your computer or domain controllers (if any), then the remote user simply may be automatically and transparently logged on as guest! For this automatic Guest logon to occur, the Guest account must be enabled and have a blank password.

Therefore, assign a long complex passphrase to your Guest account and disable it! There is also a GPO option to disable the Guest account (*Accounts: Guest account status*). And don't just disable it and not assign a password.

To disable the Guest account and assign it a password, you can use the Administrative Tools > Computer Management snap-in. But a quicker and scriptable way is from the command line:

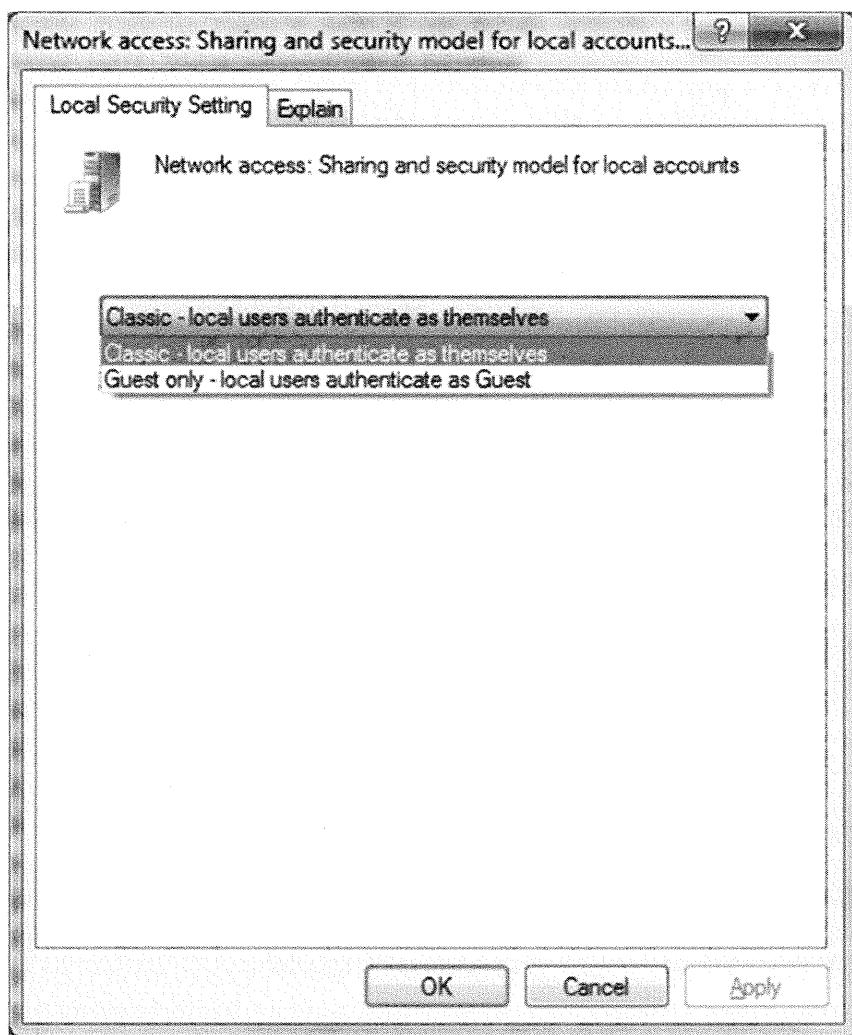
```
net.exe user guest $5mLb@?49jF&lc /active:no /times:
```

This disables the account ("active:no"), sets a complex password ("\$5mLb@?49jF&lc" or whatever you want), and prevents logon during all hours of all days ("times: " - note the blank space after the colon). A simple batch script like this could be pushed out through a domain Group Policy Object.

Some people also recommend renaming the Guest account, but the value of this is debatable. Indeed, if the account is renamed, then this may simply make it more difficult to audit the box and verify that the Guest account has been disabled! Also, another administrator might be more inclined to enable an account if it looked like a regular account. Better, perhaps, to just disable it and assign a random passphrase.

There's something else to be aware of, too. If *Simple File Sharing* is enabled, then all remote authentications to the box itself will be treated as remote access by the Guest account. This is called *automatic demotion to Guest*. To ensure that this is prevented, open Windows Explorer > Tools menu > Folder Options > View tab > uncheck the box labeled *Use Sharing Wizard*. With simple sharing disabled, users authenticate as themselves, and they specifically must be granted permissions to have access.

There also is a GPO option to control this feature (*Network access: Sharing and security model for local accounts*) which should be set to *Classic - local users authenticate as themselves*. However, it's generally best to prevent the use of local accounts at all in Active Directory environments.



# Administrative Accounts

1. Enforce strong passphrase policy
2. Require smart card authentication
3. Require Kerberos and NTLMv2; forbid LanManager and NTLMv1
4. Rename the Administrator account
5. Create a honeypot Administrator account
6. Give your administrators two user accounts each:
  - Regular account (regular activities)
  - Administrative account (only as needed)
7. Limit local account use of blank passwords to console logon only
8. Audit all access to administrative users and groups in AD

SANS Security Essentials – © 2016 SANS

## Administrative Accounts

An *administrative account* is a user who is a member of any one of these groups, especially the first three: Administrators, Domain Admins, Enterprise Admins, Schema Admins, DnsAdmins, Account Operators, Server Operators, Backup Operators, or Print Operators. Protecting these accounts is roughly equivalent to protecting the entire network! So what should be done to secure the administrative accounts?

- Enforce strong password policy, and encourage administrators to use long (20+ character) passphrases. There are third-party tools to enforce passphrase policies and this feature is built into Windows Server 2008 and later domain controllers. And no two administrative accounts should have the same passphrase, including the built-in local Administrator account.
- Consider requiring a smart card, biometric, or other multi-factor authentication device for logon with administrative accounts. You can require a smart card for interactive logons in the properties of a domain account in Active Directory (Account tab). There also is a GPO option to automatically lock the desktop of users who log on with a smart card and then remove them without first logging off.
- Require Kerberos or NTLMv2 authentication; forbid the use of LanManager or NTLMv1 (see previous).
- Rename the built-in Administrator account and change its description. There are trivial techniques to reveal the new name, but every extra hurdle helps. There also is a GPO option to do this automatically.

- Create a honeypot Administrator account after you've renamed the real one. This account will be named *Administrator* and have the same description field as the original. However, this account will not be a member of any administrative groups, will have a 50-character random passphrase, and will be disabled. It is nothing but bait.
- Administrative users should have two user accounts: their administrative account and a regular account. They should log on with their regular accounts and launch programs only with administrative privileges as necessary. The RUNAS.EXE program can be used to launch applications under different credentials than those of the logged-on user, and in the properties of shortcuts is a check box to *Run as a Different User*. In both cases, when the program is run, the user is prompted to enter the other username and password. In particular, administrators should use their regular account when browsing the Internet or checking e-mail. This feature is built into Windows Vista and later as User Account Control (UAC), though it's still slightly better to have two different user accounts.
- Ideally, each administrator should have two computers: one for regular daily use, and the other only for administrative work which is hardened and protected. This can be expensive, so consider doing administrative work only from within a virtual machine hosted on the admin's computer. The administrator will log onto the host computer with a regular unprivileged account, log onto the guest VM as that same unprivileged account, but then launch applications within the VM with an administrative account only as needed. An alternative is to host that VM on a central server and then Remote Desktop Protocol (RDP) into it using multi-factor authentication. Active Directory is only as secure as its domain controllers and administrative workstations.
- Enable the GPO option called *Accounts: Limit local account use of blank passwords to console logon only*. If any local Administrator accounts happen to have blank passwords, then at least they will not be exploitable over the network. This is a good policy to enable for everyone in any case.
- Audit all access to administrative users and groups, especially failed access, and configure one's host-based Intrusion Detection System (IDS) to raise alerts when they are modified.

# AppLocker

- **Regulate processes users can launch!**

- Helps to fight malware and unauthorized apps
- Requires Windows 7, Server 2008-R2, or later
- Software Restriction Policies:
  - The older version for Windows XP/2003/2008

- **Rules defined by:**

- SHA256 hash of program
- Local path to program
- Network path to program
- Code signing certificate
- User's group membership

- **Rules apply to:**

- Executables
- Installer packages
- Scripts
- APPX packages

SANS Security Essentials – © 2016 SANS

## AppLocker

AppLocker permits administrators to define exactly which executables can and cannot be run on Windows 7, Server 2008-R2 and later systems. AppLocker does not work on Windows XP/2003/2008, but an older version of this technology, called Software Restriction Policies, does work on these older systems. AppLocker can help to defend against viruses, worms, Trojans, hacking tools, and unwanted software in general.

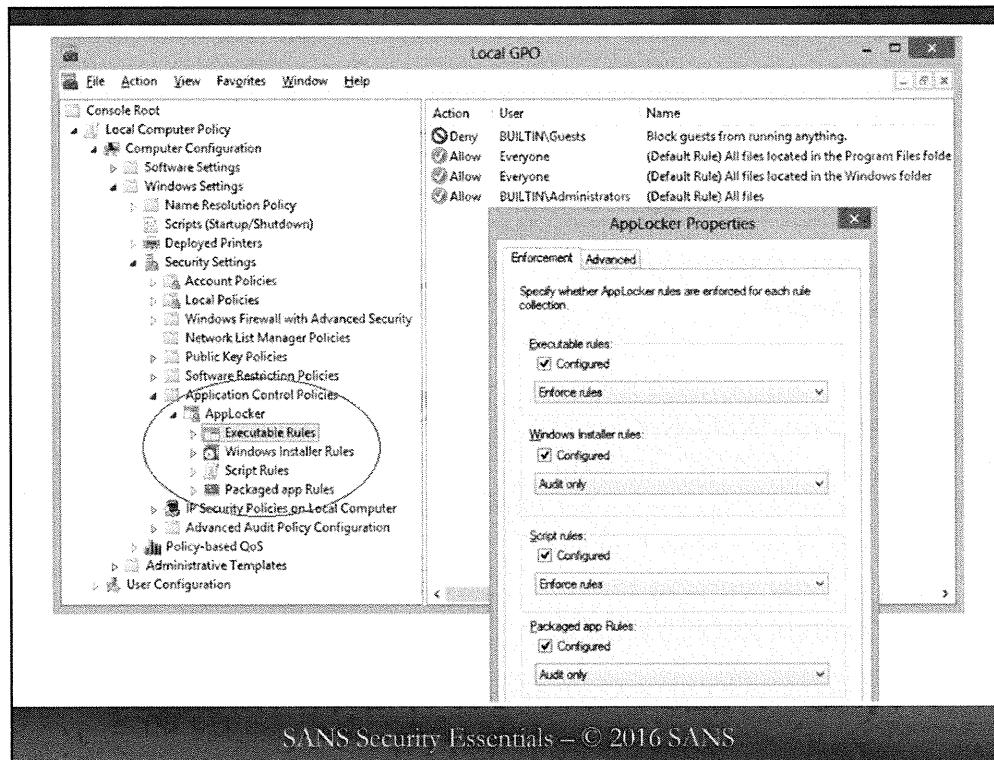
With AppLocker, you specify rules which allow or block user processes from being launched. The rules you create can use the following criteria:

1. The group(s) to which the user belongs.
2. The SHA256 hash of the program's executable file or script code.
3. Issuer of the digital certificate used to sign the executable.
4. The local or UNC path of the executable.

## Creating AppLocker Rules

To create a new AppLocker rule, open a local or domain GPO > Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker > right-click either Executable Rules, Windows Installer Rules or Script Rules > Create New Rule. The wizard walks you through the rest of the process.

Notice that you can apply different AppLocker rules to different groups. This means you can exempt certain people (such as yourself) from the restrictions AppLocker imposes.



SANS Security Essentials – © 2016 SANS

AppLocker also supports an audit-only mode which can be used to test out new rules without actually blocking any programs (and triggering user complaints). If you right-click the AppLocker container in the GPO and go to Properties, you can select Enforce Rules or Audit Only for each of the three categories of rules. When you push out AppLocker rules through Group Policy, it's best to first push them out in audit-only mode for a few weeks, and then examine the event logs on the test systems to see if anything legitimate had been accidentally blocked.

When you finish testing, you can right-click the AppLocker container again and export the rules to an XML file for importation into other GPOs. Because XML is plain text, you hand-edit these files if you want, for example, to script the addition of more hash signatures. There are also PowerShell cmdlets for AppLocker for working directly with XML rules files.

If you are not certain which rules to configure, at least start with the recommended generic rules. If you right-click the Executable Rules container, you can first select Create Default Rules; then select Automatically Generate Rules. The automatic rules are created when you select a folder, such as Program Files, and then AppLocker scans that folder's subdirectories to create rules to allow everything found there to run. You should do this, of course, only on a reference machine you presume to be clean.

When a program, script, MSI installer package, or APPX package is blocked by AppLocker, a generic error message is shown, but you can define your own error (<http://go.microsoft.com/fwlink/?LinkId=160265>). APPX packages are for Metro apps on Windows 8 and later.

### Software Restriction Policies

Software Restriction Policies (SRP) is the older technology for Windows XP/2003/2008 that is similar to AppLocker but not quite as flexible.

With SRP, you specify whether applications should be allowed or disallowed by default; then exceptions are defined for whichever default policy you choose. For example, in a high-security environment you would disallow all software execution by the user, and then specify the few exceptions necessary for the user to get his work done. Members of the local Administrators group can be totally exempted from SRP if wanted.

Exceptions to the allow-all or deny-all policy are identified by one of four methods:

1. The MD5 hash of the program's executable file.
2. Issuer of the digital certificate used to sign the executable.
3. The local or UNC path of the executable.
4. The "zone" from where the executable was downloaded (these are the same zones seen in Internet Explorer, for example, Internet, Local Intranet, Trusted Sites, and Restricted Sites), but this applies only to .MSI software packages.

### **Creating Software Restriction Policies**

Before SRP settings can be configured, you must initialize SRP in the GPO. To create a new SRP policy, go to Computer Configuration > Windows Settings > Security Settings > right-click on Software Restriction Policies > Create New Policy.

Next, decide whether you want to allow or disallow all user-launched programs by default; afterward, you define exceptions to this policy. To set a default SRP policy, in the relevant GPO go to Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies > Security Levels. Next, right-click either Disallowed, Basic User, or Unrestricted, as wanted, and select Set As Default.

If you set a rule to enforce Basic User, then programs covered by that rule are permitted to run, but they launch without any administrative privileges, even if the user who launched the program is a local administrator. This is similar to User Account Control (UAC), but it does not require Windows Vista to function (KB324036).

Next, define exceptions to your policy in the Additional Rules container. If you have default-deny policy, then you can define programs that should be allowed to run. If you have a default-allow policy, then you can define programs that are specifically forbidden. An exception is defined in one of four ways: using a hash of the executable, its digital signature issuer, its local or UNC path, or its IE zone (if it's an MSI package).

To create an exception to the default policy, right-click Additional Rules > select the type of rule you want (hash, certificate, zone or path) > configure the rule > OK.

### **Global SRP Options**

In the Software Restriction Policies container itself are three options that affect all SRP policies globally: Enforcement, Designated File Types, and Trusted Publishers.

The Enforcement options are fairly self-explanatory. Exempting local Administrators from all SRP policies is convenient and probably necessary to get their work done.

The Designated File Types option determines to which file types (based on filename extensions) SRP policies apply. If you use custom executable or script types whose extensions are not on the list, add them manually at the bottom.

The Trusted Publishers options are for 1) determining who is permitted to decide to trust certificate authorities for ActiveX controls, scripts and other signed code, when that executable content's signer is not trusted already, and 2) whether Certificate Revocation List (CRL) checking is required.

When prompted by the computer whether to trust a certain certificate when trying to run code signed with that certificate, who can decide to trust it? End users, local Administrators, or Domain/Enterprise Admins? Selecting "local computer administrators" is probably the best overall choice.

# User Account Control

- **Standard User Process (the default):**
  - Medium or low MIC label
  - SAT stripped of dangerous privileges
- **Administrative User Process:**
  - High or system MIC label
  - Standard SAT for an administrators group member
- How to launch programs with administrative powers:
  - Right-click > Run as Administrator, or modify a shortcut
- UAC can be managed or turned off via Group Policy
  - Admin Approval Modes: Prompting Options
  - Standard User Approval Modes: Fail or Prompt for Credentials

SANS Security Essentials – © 2016 SANS

## User Account Control

Users who log on and run all their programs as members of the local Administrators group endanger their computers because of malware and destructive mistakes. User Account Control (UAC) in Windows Vista and later enables users to conveniently install and run programs as low-privileged accounts and then temporarily raise privileges on an as-needed basis without logging-on-and-off or resorting to RUNAS.EXE or DROPMYRIGHTS.EXE in order to do so.

### How to Turn It Off (Everyone Asks)

UAC is enabled by default, but you can turn it off completely in Windows 7 and later by going to Control Panel > Action Center > Change User Account Control settings.

### How UAC Works

UAC does not apply to the built-in Administrator account by default. UAC does apply to all other accounts, even if those accounts have been added to the local Administrators group. Whenever a user logs on, the SAT of that user is stripped of most of its privileges and its Mandatory Integrity Control (MIC) label is set to Medium. And if that user is a member of the local Administrators group, that user acquires none of that group's privileges or permissions either for the sake of getting access to securable objects.

A process running with a SAT stripped of its higher privileges and with an MIC level of Medium or lower is said to be "running as a standard user." A process running with a SAT that includes the Administrator group's SID and other elevated privileges with an MIC level of High or better is said to be "running as administrator." This nomenclature is a bit misleading because all users log on as "standard users," but just remember that a SAT is created for a process when that process is launched and that SAT can be modified on-the-fly by the operating system for the sake of UAC and MIC.

When examining the privileges of a process with WHOAMI.EXE or Process Explorer, don't forget that a privilege labeled as "Disabled" can still be enabled by the process as needed, but if a privilege is not listed at all, then that privilege cannot be enabled for that process.

If a standard user process attempts an action that requires administrative privileges, the action usually fails. However, if that process is 32-bit, it does not specify a requestedExecutionLevel in its application manifest (PE or .NET), is not running in kernel mode, is not impersonating a different user, and is failing because of an Access Denied error from an NTFS or Registry permission on various items under %SystemRoot%, %ProgramFiles%, the SOFTWARE hive and some other locations (and not because of an MIC restriction), then the write access appears to be permitted, but it is permitted only to the "virtualized" folders and keys of the same names but not the same locations. These virtualized folders and keys were added by Microsoft for backward compatibility and are located, respectively, under %LOCALAPPDATA%\VirtualStore\ and HKCU\Software\Classes\VirtualStore\. These virtualized folders and Registry keys are per user, hence, each user will have their own separate set of virtualized folders and keys that appear to be "the real ones," but only administrative processes can actually write to the real folders and keys. (And note that 64-bit processes cannot take advantage of this folder/key virtualization.)

### **How to Launch as Admin**

If you right-click an executable or shortcut and select Run as Administrator, then that process runs as an administrative user (if permitted). If the properties of a shortcut are modified to enable Run with Different Credentials (Shortcut tab > Advanced button) then that process runs just as though you had right-clicked it and selected Run As Administrator. If the manifest in a Portable Executable (PE) binary or in a .NET assembly has the requestedExecutionLevel property set to requireAdministrator (do a strings search in the binary to see it), then that process automatically launches as an administrative user (if permitted) without the necessity of right-clicking it first.

A handy thing to do is to launch a CMD.EXE shell as administrator and then run programs from that shell to automatically launch programs as administrator without getting prompted every time.

### **UAC Group Policy Options**

Group Policy can be used to configure UAC. Inside a GPO, navigate to the following location: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. Here you will find the following UAC-related options:

- UAC: Admin Approval Mode for the Built-in Administrator Account.
- UAC: Behavior of the elevation prompt for admins in Admin Approval Mode.
- UAC: Behavior of the elevation prompt for standard users.
- UAC: Detect application installations and prompt for elevation.
- UAC: Only elevate executables that are signed and validated.
- UAC: Run all administrators in Admin Approval Mode.
- UAC: Control Switch to the secure desktop when prompting for elevation.
- UAC: Virtualize file and registry write failures to per-user locations.

The most important two options are for UAC: Behavior of the elevation prompt. This determines how UAC allows the execution of commands that require administrative privileges. For administrator-level users, the behavior options are 1) no prompt, just automatically elevate privileges, which gives the appearance that UAC is disabled, 2) prompt for consent, to simply be alerted, and 3) prompt for credentials, which requires a password or smart card. For standard users, the options are 1) no prompt, and simply fail, or 2) prompt for credentials, which requires the password or smart card of an administrative-level account.

# Internet Explorer Security (1 of 5)

- **IE has a long, sad history of exploits...**
- **Windows 10 replaced IE with the Spartan browser.**
- **Internet Explorer Protected Mode:**
  - It's UAC and integrity control for the browser!
  - IE launches with the Low MIC label
  - IE launches as a standard user process
  - If infected, the browser will not be running as administrator
  - The Low label allows only IE to write to a few drive locations

SANS Security Essentials – © 2016 SANS

## Internet Explorer Security (1 of 5)

Internet Explorer Protected Mode on Windows Vista and later is not so much a mode of IE itself, but simply the use of Mandatory Integrity Control (MIC) and User Account Control (UAC) for Internet Explorer. Windows 10 replaced IE with a new browser named Spartan that is more standards-compliant, but Spartan otherwise keeps many of the security features of IE.

When run, IE gets the Low MIC label by default. When the MIC label of IE is Low, the browser shows Protected Mode: On in its status bar in IE 8.0 (unfortunately removed in IE 9.0 and later). If IE is launched with administrative privileges, it runs with the High label and the status bar reads Protected Mode: Off. Even though IE 8.0 can be installed on Windows XP/2003, it cannot run in protected mode because those older operating systems lack MIC and UAC. Be aware that IE9 cannot be installed on XP/2003 at all. IE8 and later launches a separate process (iexplore.exe) for each tab, and each tab can have a different Protected Mode state.

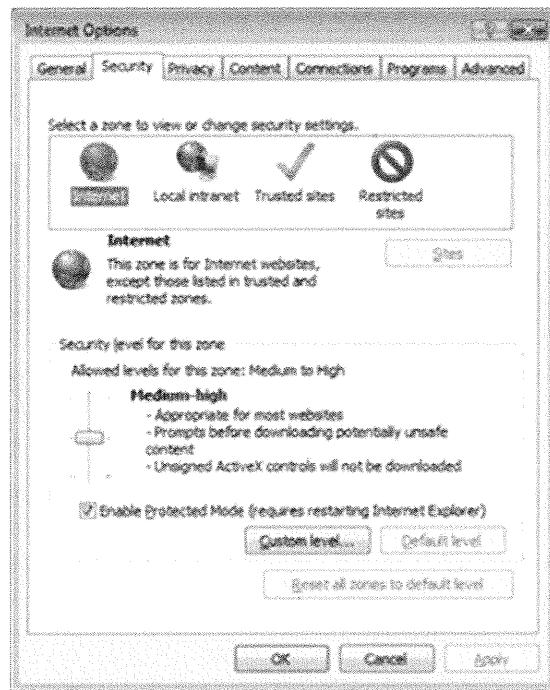


Moreover, the filesystem and Registry locations to which IE can write in Protected Mode are limited, for example, the temp, History, Favorites and cookies folders.

There are only a few folders with the Low MIC label assigned to them, and they often have the word "low" in them, such as:

- \Users\username\AppData\LocalLow
- \Users\username\AppData\Local\Microsoft\Windows\History\Low
- \Users\username\AppData\Local\Temp\Low
- \Users\username\AppData\Roaming\Microsoft\Windows\Cookies\Low
- \Windows\ServiceProfiles\NetworkService\AppData\LocalLow
- \Windows\System32\config\systemprofile\AppData\LocalLow
- \Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low

Protected Mode can be enabled/disabled on a per-zone basis. A new browser will be launched as necessary to switch to a different Mode.



When downloaded files need to be saved to arbitrary disk locations, or when an ActiveX control needs to be installed, IE will launch a "broker" process (IEUSER.EXE and IEINSTALL.EXE, respectively) with higher privileges to handle the operation after obtaining user consent. This is UAC applied to file download and ActiveX control install. When IE is run elevated, it doesn't use IEUSER.EXE as a download broker.

## Internet Explorer Security (2 of 5)

- 99% of IE settings are configurable through the Group Policy
- A few changes will block most of the exploits, even without patches, but these changes also break functionality
- Fortunately, exceptions can be defined

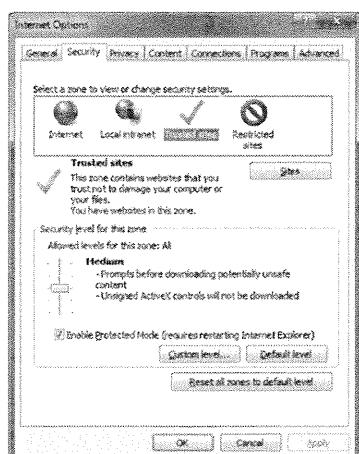
SANS Security Essentials – © 2016 SANS

### Internet Explorer Security (2 of 5)

Virtually every aspect of Internet Explorer (IE) can be managed through the Administrative Templates and Internet Explorer Maintenance containers in Group Policy Objects, which is fortunate because there's been an almost never-ending string of IE exploits since the beginning of the browser's release! It's important to stay on top of IE patches, but patching is always merely reactive. Fortunately, many of these exploits can be blocked through a few simple configuration changes, and these changes are likely to block many future exploits as well. Ninety-nine percent of the configuration options in IE can be managed through Group Policy.

The bad news is that making these changes will break much of the cool functionality in high-end websites, but exceptions can be defined. For example, you can disable client-side scripting, ActiveX controls, and Java applets in general, but still allow them when users are accessing intranet sites or when visiting sites whose fully qualified domain names (FQDNs) you have approved explicitly. In this way, business-critical sites can remain 100 percent functional while the rest of the Internet can be regarded with more skepticism.

# Internet Explorer Security (3 of 5)



- **Configure Internet Zone:**

- Active scripting: Disable
- Run ActiveX controls and plug-ins: Disable
- Download signed ActiveX controls: Disable
- Download unsigned ActiveX controls: Disable
- Initialize and script ActiveX controls not marked as safe: Disable
- Script ActiveX controls marked safe for scripting: Disable

SANS Security Essentials – © 2016 SANS

## Internet Explorer Security (3 of 5)

In your local or domain GPO, follow these steps to eliminate many IE vulnerabilities: Open the desired GPO (see above) > User Configuration > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings > at the top select Import... > Modify Settings button > click the Internet icon at the top > Custom Level button > and make sure the following options are configured:

- Download signed ActiveX controls: Disable
- Download unsigned ActiveX controls: Disable
- Initialize and script ActiveX controls not marked as safe: Disable
- Run ActiveX controls and plug-ins: Disable
- Script ActiveX controls marked safe for scripting: Disable
- Java permissions: Disable Java (or High Safety, or Custom)
- Launching programs and files in an IFRAME: Disable
- Active scripting: Disable
- Logon: Automatic Logon Only In Intranet Zone

Here are other GPO settings related to Internet Explorer that you should consider managing. All the paths in the GPO begin with *Administrative Templates* > .

Windows Components > Internet Explorer:

- Disable changing proxy settings
- Disable changing Automatic Configuration settings
- Disable changing ratings settings
- Disable changing certificate settings
- Disable AutoComplete for forms
- Do not allow AutoComplete to save passwords

Windows Components > Internet Explorer > Internet Control Panel:

- Disable the General page
- Disable the Security page
- Disable the Content page
- Disable the Connections page
- Disable the Programs page
- Disable the Advanced page

Windows Components > Internet Explorer > Browser Menus:

- **File menu:** Disable closing the browser and Explorer windows
- **Tools menu:** Disable Internet Options...menu option
- Disable Save this program to disk option

# Internet Explorer Security (4 of 5)

- **Trusted Sites Zone:**

- Define exceptions to permit dangerous features for URLs that you trust



- **Restricted Sites Zone:**

- List URLs for sites that you don't trust

SANS Security Essentials – © 2016 SANS

## Internet Explorer Security (4 of 5)

When you click OK to save your custom settings, you are returned to the Security Zones dialog box. You can now select the Trusted Sites zone and, by clicking the Sites button, add any FQDNs for sites on the Internet that you want to exempt from your new restrictive settings. For example, you may want to add <http://www.microsoft.com> to the list because Microsoft's website uses ActiveX controls and client-side scripting extensively.

The Restricted Sites zone is for the FQDNs of sites that you never want to trust, no matter what. This might be used instead of altering the Internet Sites zone if there are only a few troublesome sites that you want to exclude, but you are otherwise comfortable permitting ActiveX controls and active scripting on the rest of the Internet (perhaps because you apply patches quickly and consistently).

Remember, if you configure these settings in the domain GPO using the Active Directory Users and Computers tool at your domain controller, these settings apply to every computer in the domain.

# Internet Explorer Security (5 of 5)

## • SmartScreen Filter

- Compares URL against list of known phishing sites and malware download URLs
- Automatic and manual URL checking
- Submits phishing sites to Microsoft for inspection
- ActiveX filtering switch (IE9 and later)
- Third-party tracking protection (IE9 and later)

SANS Security Essentials – © 2016 SANS

### Internet Explorer Security (5 of 5)

The IE SmartScreen Filter (previously known as the Phishing Filter) compares each visited URL against a list of known-bad URLs maintained by Microsoft and is accessed via a web service. Bad sites include both known phishing sites and malware download URLs. SmartScreen also looks for phishy pheatures in web pages and alerts the user if these features are found (what these characteristics are exactly is not well known). Testing by NSS Labs shows that the filtering is actually quite effective in blocking more than 80 percent of the malicious URLs tested (<http://nsslabs.com/browser-security>).

Similarly, the Cross Site Scripting (XSS) Filter also examines the flow of data back-and-forth between browser and web server(s) to detect and thwart XSS attacks.

SmartScreen in IE8 and later can check each site automatically or can be invoked manually by the user by pulling down the Safety menu > SmartScreen Filter > Check This Website. Known-good or known-bad sites can be submitted to Microsoft for review and inclusion/exclusion from the list. You can suggest to Microsoft that it reviews a website for phishiness by pulling down the Safety menu > SmartScreen Filter > Report Unsafe Website. In IE9 and later, the browser's Download Manager applet also uses the SmartScreen filter while downloading files.

IE8 and later also includes the InPrivate Filter, which is for maintaining privacy against attempts to track users across multiple sites with cookies and JavaScript. To manage InPrivate options, pull down the Safety menu > InPrivate Filtering Settings. In IE9 and later, privacy is further enhanced with the Tracking Protection feature in which the browser periodically updates a user-definable list of URLs to servers that attempt to track you as you browse from site to site (Safety menu > Tracking Protection).

Finally, in IE9 and later, you can conveniently disable all ActiveX controls browser-wide, such as for Flash video, by pulling down the Safety menu > ActiveX Filtering (or using Group Policy to do the same).

# Summary

---

- Security Templates
  - SCA Snap-In
  - SECDIT.EXE
  - Local GPO
  - Domain GPO
  - Kerberos and NTLM
  - User Account Control
  - Internet Explorer
- Recommendations:
  - Password Policy
  - Account Lockout
  - Security Options
  - Administrative Accounts
  - AppLocker
  - Internet Explorer
  - Misc ADM Settings

SANS Security Essentials – © 2016 SANS

## Summary

The purpose of this module was to show how to quickly and easily make numerous security configuration changes. Our primary tools are security templates, the Security Configuration and Analysis snap-in, and Group Policy Objects.

Security templates store most of the settings about which we are concerned (for example, password and lockout policies, NTFS permissions, null user session restrictions, and so on), and there are free templates for the download from organizations that have invested a great deal of time and expertise into developing them. These preconfigured templates definitely are the way to begin, so don't start from scratch!

The Security Configuration and Analysis snap-in (SCA) is used to apply templates to a system to reconfigure that system to match the templates. The bad thing about the SCA, though, is that it works only on the local machine.

Group Policy Objects (GPOs), however, can apply templates to computers throughout the network automatically. And GPOs can be used to accomplish even more! GPOs also can push out a variety of scripts and registry settings, as well. In fact, not much can't be managed through Group Policy.

Next, we considered some recommendations for securing the Guest account, administrative users, null user session vulnerabilities, User Account Control (UAC), AppLocker, Internet Explorer, and other items.

And although the security hardening steps in this module are important, we are only half-way there. The next module discusses the bane of Windows network administrators everywhere: securing network services such as Internet Information Server.

# Module 27: Securing Windows Network Services

SANS Security Essentials – © 2016 SANS

## **Module 27: Securing Windows Network Services**

This section intentionally left blank.

# Securing Network Services

---

## SANS Security Essentials V: Windows Security

SANS Security Essentials – © 2016 SANS

### **Introduction: Securing Network Services**

It is important that you properly secure a system before you connect to a network. Even desktop Windows computers provide a variety of services on the network by default, and a Windows Server can host dozens more. Applying the latest patches isn't good enough: You want a secure host. A secure host is a machine that has been hardened specifically *in anticipation of vulnerabilities that have not been discovered yet*. You can't block all possible exploits, of course, but a few basic precautions can reduce your threat exposure greatly. Again, hotfixes are for *yesterday's* exploits; what you're trying to do here is anticipate *tomorrow's* vulnerabilities (which largely involves being paranoid).

More specifically, this module discusses:

- The Best Way to Secure a Service
- Packet Filtering
- IPSec Authentication and Encryption
- Internet Information Server (IIS)
- Terminal Services

# Windows Network Security Overview

The student will know how to take basic measures in securing Windows network services.

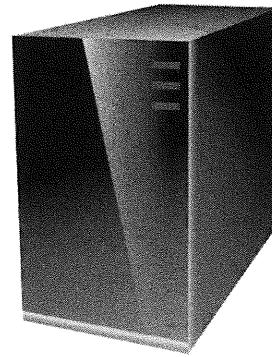
SANS Security Essentials – © 2016 SANS

## **Windows Network Security Overview**

This section intentionally left blank.

# Best Way to Secure a Service?

- **Uninstall or disable it!**
- What's unnecessary?
- Won't disabling service X break feature Y?
  - Requires lab testing; then monitors the server afterward



SANS Security Essentials – © 2016 SANS

## The Best Way to Secure a Service?

The best way to secure a service is to uninstall or disable it. Even if a zero-day exploit tool or worm is released, if the vulnerable service isn't running, you're immune to the attack. Hence, disable all unnecessary services, especially on systems exposed to the Internet.

Often, administrators new to security ask, "Is this service known to be vulnerable?" and use that as the basis for deciding whether to disable the service. This is the wrong question. If a service were known to be vulnerable, Microsoft would release a patch for it. The correct question is, "Do we need this service?" And if the answer is "No", then get rid of it. You can't anticipate what vulnerabilities and exploits will be discovered tomorrow, but today you can get rid of what you don't need. This, of course, is an application of the Principle of Least Privilege to system configuration.

Think of all your users who have figured out how to install IIS on their machines. Do they really need the most-attacked HTTP server in history on their workstations? Do they know how to patch, harden, and configure IIS correctly? Probably not.

But how do you disable unneeded services on thousands of systems?

# Server Manager (1 of 2)

- **The OS is divided into roles and features:**
  - **Roles : IIS, Domain Controller, DNS, RADIUS, and such**
  - **Features : BitLocker, Telnet Client, .NET, and such**
- Server Manager tool understands their dependencies, so when you add/remove a role or feature, all its dependencies can be added/removed at the same time.
- PowerShell examples are in the manual, too

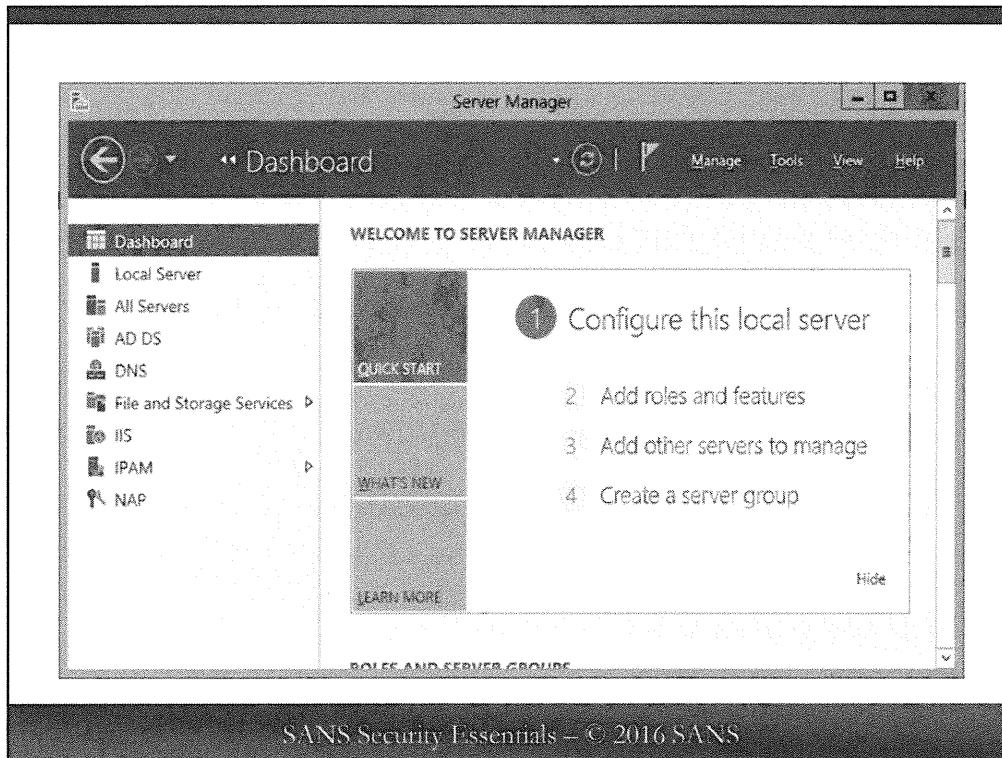
SANS Security Essentials – © 2016 SANS

## Server Manager (1 of 2)

In Windows Server 2008 and later, there is a tool named Server Manager that organizes the capabilities and services of the operating system into groups called roles and features. *Roles* are larger sets of capabilities, such as IIS and Terminal Services, and *features* are smaller, such as BitLocker and the telnet client. You can add roles and features at any time using Server Manager.

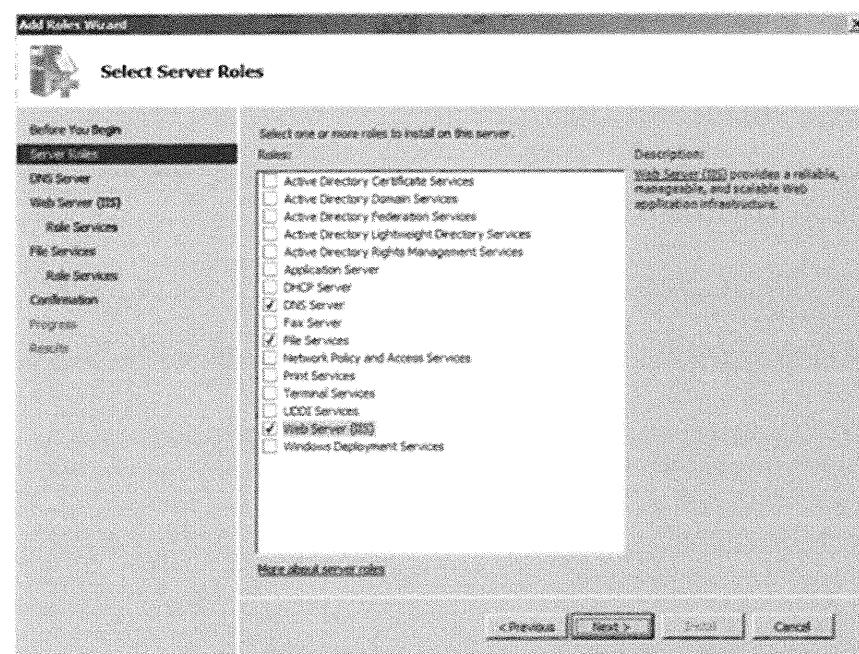
Server 2008 and later installs with a relatively minimal set of capabilities enabled by default. (And even the graphical desktop is missing with the Server Core option.) This is good from a security point of view because unneeded roles and features are not installed to begin with, and it encourages network administrators to install only what they need.

The Server Manager tool has built-in knowledge of the dependencies among these roles and features so that when you add/remove one, the tool prompts you with the list of other capabilities that will have to be added/removed too. Moreover, the majority of the system hardening tasks performed by the Security Configuration Wizard are performed automatically by Server Manager in Server 2008 and later (or they are simply the factory defaults). Hence, Server 2008 installs in a minimal configuration, it is more modular than prior server versions in that roles and features can be managed relatively independently of each other, and where there are dependencies among roles/feature the Server Manager tool has built-in knowledge of them.



## Server Manager (2 of 2)

This slide shows Server Manager running on Windows Server 2012. Adding or removing a role or feature is simple: Pull down the Manage menu, select Add or Remove. A dialog box appears showing a list of the roles/features available with check marks in the boxes next to the currently installed items. Also from the Manage menu, you can add remote servers to add/remove roles on them as well. The Tools menu contains a list of the major management tools for the roles installed, such as IIS Manager, DNS, and the Security Configuration Wizard.



So, for the sake of security then, use Server Manager to install only what you need, and if someone else has installed something you don't need, get rid of it!

### **PowerShell Examples**

In addition to the graphical console snap-in, there is also PowerShell support for managing roles and features. If you're building a large number of similar boxes, a PowerShell script could automate the (un)installation of roles and features. When running with the Server Core installation option, this is the primary way for managing roles/features because there is no standard graphical desktop interface with the Server Core option.

After you are in PowerShell on a Windows Server box, run these commands to get started:

```
import-module servermanager  
get-help -full get-windowsfeature
```

To see a list of the roles and features installed on local or remote server, run:

```
get-windowsfeature  
get-windowsfeature -computername Server47
```

To install, for example, Windows Server Backup, from within PowerShell, run:

```
install-windowsfeature -name Windows-Server-Backup
```

Note that there was an older command-line tool named SERVERMANAGERCMD.EXE, but this has been deprecated in favor of PowerShell.

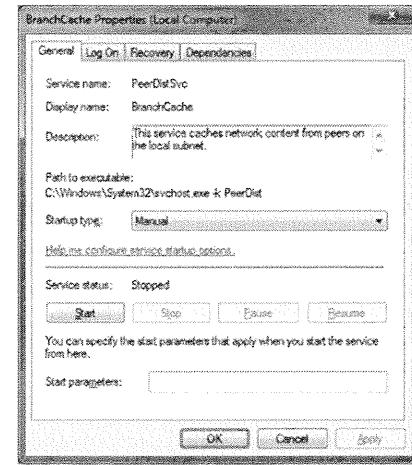
# How to Disable Services

## Many ways to disable a service:

- Services Tool
- Security Template
- Group Policy Object
- PowerShell
- SC.EXE

But how do I know which services I don't need?

What are their dependencies?

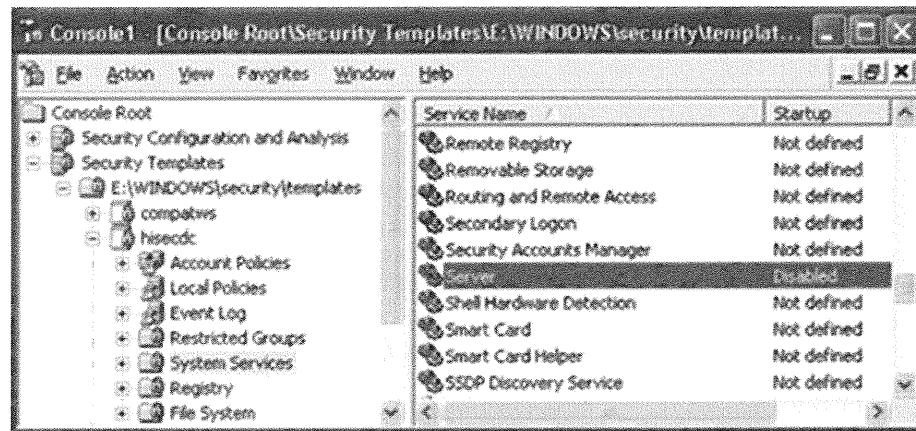


SANS Security Essentials – © 2016 SANS

## How to Disable Services

The manual way of disabling a service is by going to the Administrative Tools folder off the Start menu and launching the Services applet. For any unwanted service, double-click it in the applet, go the General tab, set its startup type to *Disabled*, and then stop the service (or reboot).

An INF security template can also define service startup settings. You can apply a template to a system with the Security Configuration and Analysis (SCA) snap-in or SECEDIT.EXE to disable all the unwanted services in one shot. This is convenient because that INF template can contain hundreds of other security-related changes as well.



But if you have thousands of computers whose services must be modified, then the answer is Group Policy. For example, to disable the World Wide Web Publishing service throughout the entire domain, open the Active Directory Users and Computers snap-in > right-click your domain > Properties > Group Policy tab > select the Default Domain Policy > Edit button > navigate to Computer Configuration > Windows Settings > Security Settings > System Services. The *System Services* section of a GPO is more-or-less the Services applet; here you can disable any service you want, and that service will be disabled on all the systems to which the GPO applies.

But what about the standalones that can't be managed through Group Policy? Using the SC.EXE command-line tool, you can query and reconfigure every aspect of every service and device driver on a local or remote computer. PowerShell can do most of this too, but SC.EXE still has tricks PowerShell cannot do yet. If you don't find SC.EXE installed on your box by default, you can download it for free from Microsoft's website. (It's a Resource Kit tool.) The old NET.EXE utility still exists, but SC.EXE and PowerShell are vastly better.

For example, to query the list of services on a remote computer named mecha with SC or PowerShell:

```
sc.exe \\mecha query  
  
get-service -computername mecha
```

To show all the details of just the Server service on a remote computer named mecha, you first have to know the Registry key name of the service (which is LanmanServer) and then you interact with the service with its unique name:

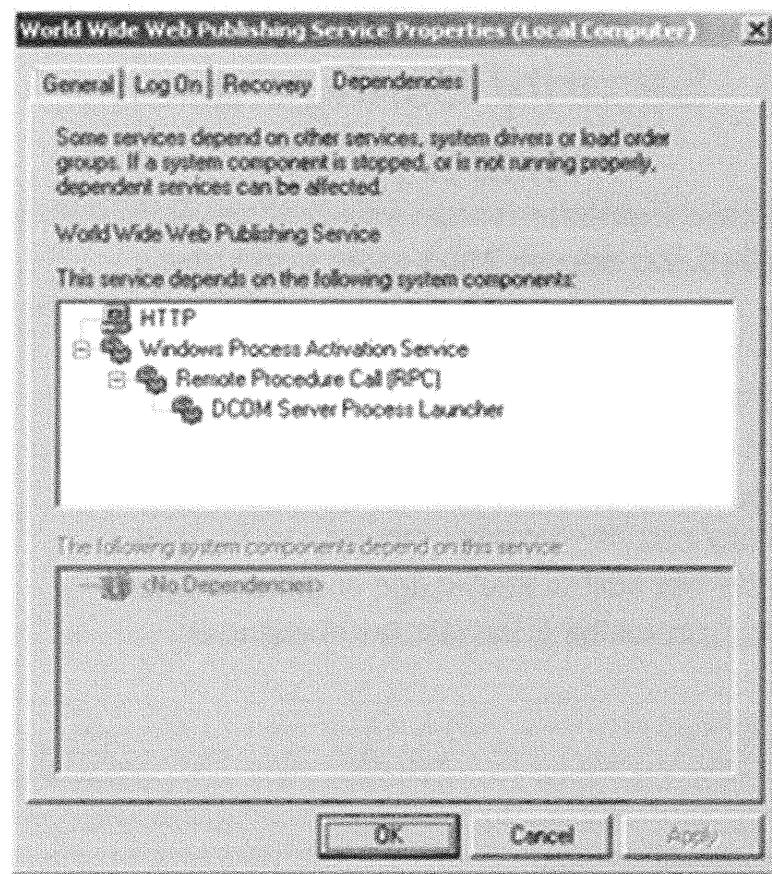
```
sc.exe getkeyname "server"  
sc.exe \\mecha queryex LanmanServer  
sc.exe \\mecha qc LanmanServer  
  
get-service -computername mecha -displayname server  
get-service -computername mecha -name LanmanServer
```

To stop and permanently disable the Server service with SC.EXE or PowerShell:

```
sc.exe LanmanServer stop  
sc.exe config LanmanServer start= disabled  
  
stop-service -name LanmanServer  
set-service -name LanmanServer -startuptype disabled
```

#### **But Which Services Are Not Needed? What Should Be Disabled?**

The hard part about disabling services, though, is knowing which ones to disable. You'll first have to decide what you want the box to do; then you can match this list against the available services. If you want the box to be a web server, then you need the World Wide Web Publishing service, and then that service might depend on other services, and so on. If you go to the Dependencies tab in the Services applet, it can help you to understand the relationships among services so that you don't disable something you need. You can also view dependency relationships from the command line with SC.EXE or PowerShell. This is one of the main advantages to using Server Manager, too, it has built-in knowledge of many of these dependencies.



Isn't there an easier way to figure out what to disable, other than doing it all by hand like this?

# Security Configuration Wizard (1 of 2)

- **Windows Server 2003+SP1 and Later**
  - Not supported on Windows client operating systems
  - Works on both local and remote servers
  - Run SCW.EXE to launch the wizard
- You select the roles you want, and SCW performs many security reconfiguration tasks for you!
- SCW has built-in knowledge of dependencies
- You can roll back the last set of changes

SANS Security Essentials – © 2016 SANS

## Security Configuration Wizard (1 of 2)

The Security Configuration Wizard (scw.exe) is a free tool that comes with Service Pack 1 for Windows Server 2003 and later. After applying SP1 or later in Server 2003, install SCW by going to the Add/Remove Programs applet in Control Panel, selecting Windows Components, and then check the box for the Security Configuration Wizard. SCW cannot be used or installed on earlier operating systems or on Windows Vista/7. To launch SCW, execute scw.exe at the Run line or in a CMD shell. It also works on Windows 2008 and later, of course.

When launched, the SCW asks you a long series of questions about what "roles" the server plays on the network, client features it requires, (un)wanted optional components and services, the versions of the operating systems that will be connecting to the server, (un)wanted IIS web service extensions, and other such issues. SCW uses this information to perform many security reconfiguration tasks for you!

The output of the SCW is an XML policy file that can be used to reconfigure a server or to analyze it for compliance with the policy. The policy file can be applied at any time with either the graphical SCW (scw.exe) or a scriptable command-line version of the SCW (scwcmd.exe configure /p:policyfile.xml). It works on local or remote machines across the network! And if you are unhappy with the effects of the reconfiguration, the SCW even supports a rollback feature to get you back to the state of your machine just prior to the application of the last XML policy file.

Depending on how you've answered the SCW's questions and what roles you've selected for your server, the SCW can make the following changes:

- Enable or disable services for the roles selected.
- Configure the Windows Firewall for the roles selected.
- Configure IPSec policies.

- Enable or disable IIS web service extensions.
- Remove unneeded IIS virtual directories.
- Configure audit policies.
- Configure LDAP and SMB message signing.
- Configure authentication protocols like LanMan and NTLMv2.

As you can see from the list above, the SCW is not a replacement for INF security templates or your own good judgment. The SCW does not work on client operating systems, it doesn't apply patches or Service Packs, it cannot manage wireless security or RDP settings, and many aspects of IIS security will still need to be changed by hand, but it's still a good tool to add to your arsenal.

## SCWCMD.EXE (2 of 2)

- **Command-line version of SCW**

- You can audit remote servers using either a list of computers or specifying an entire Organizational Unit
- **You can also export SCW policy settings to a Group Policy Object for mass distribution!**
  - But this does not include IIS security settings

SANS Security Essentials – © 2016 SANS

### SCWCMD.EXE (2 of 2)

The graphical SCW wizard is nice if you have only a couple dozen servers to configure, but if you have real heavy lifting to do, check out the command-line version of the tool: SCWCMD.EXE. This can be scripted, of course, but it has other tricks up its sleeve, too!

#### Analyze for Compliance, View Reports, and Configure

How can you know whether a remote machine is in compliance with your SCW policy? The SCW command-line tool can scan a list of computers or an entire organizational unit of computers (!) to produce XML reports of each machine's compliance with your policy. These XML reports can be viewed and printed using a graphical tool launched by running "scwcmd.exe view /x:report.xml". To see the analysis and reporting options of the tool, run scwcmd.exe analyze /?.

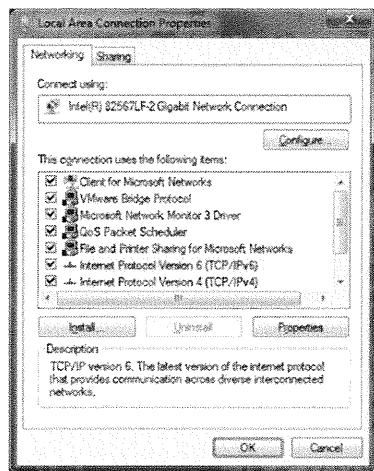
And that same computer list or OU could be used to apply an SCW policy to large numbers of computers remotely. To see these options, run "scwcmd.exe configure /?". Note that you can roll back a policy application if you regret it, but the rollback options do not include the ability to specify a computer list or OU, hence, each remote machine will have to be rolled back separately (but at least that can be scripted, too). Also, it's best if the target machines have SCW installed too or else some configuration items cannot be scanned.

#### Export to a Group Policy Object

If you need to apply different SCW policies to thousands of computers in different domains and organizational units, you'll want to do it through Group Policy.

Fortunately, SCWCMD.EXE can take an XML policy file and create a new GPO from it in Active Directory automatically! To do this, simply run "scwcmd.exe transform /p:policyfile.xml /g:GroupPolicyObjectName", and a new GPO will be created in the domain of your computer named *GroupPolicyObjectName*. When the GPO exists, it can be linked to any domain, site or OU as wanted, just like any other GPO. Unfortunately, though, the IIS security settings aren't included in the GPO.

# Network Adapter Bindings



- A "binding" is an internal communications pathway between networking components
- Each interface has its own separate set of bindings
- Example:
  - Your home computer should not leave the File and Printer Sharing binding enabled on your Internet-facing network adapter card

SANS Security Essentials – © 2016 SANS

## Network Adapter Bindings

Sometimes, a service cannot be disabled because of the sacrifices this would entail. A less drastic approach is to keep the service running and instead disable some of its bindings. A *binding* is a path of communications between a networking component (like a service or protocol) and a physical network adapter card. If you break a service's binding to one card, the service can remain accessible over a different card.

Now work through an example to make it more concrete. Do you have a 24x7 DSL or cable-modem connection to the Internet at home? If so, it is critical that you break the binding between your Server service and the interface leading out to the Internet; there is no good reason why random people on the Internet need to get to your shared folders and printers!

To do this on your system, go to the properties of the network adapter card that you use for Internet connectivity. If this is a physical interface, then the General tab will show a list of networking components with checkboxes to the left of them; if this is a dial-up or VPN interface, then the Networking tab will show the same list of components. Now, simply uncheck the box next to *File and Printer Sharing on Microsoft Networks*, and click OK.

All networking interfaces have bindings like this, including Ethernet cards, Token Ring and FDDI adapters, 802.11 wireless cards, dial-up connections, and even VPN connections. The bindings for each interface can be managed separately from the others.

# Do I Still Need NetBIOS ?

- NetBIOS is a set of connectionless and connection-oriented protocols, mainly for name resolution
  - Can be disabled 90% of the time, but it is still required for backward compatibility for older systems and applications
  - Disable manually or via DHCP
  - Remember, null user sessions do not require NetBIOS!
- NetBIOS is primarily a reconnaissance threat:  
**NBTSTAT.EXE -A 10.4.5.1**

SANS Security Essentials – © 2016 SANS

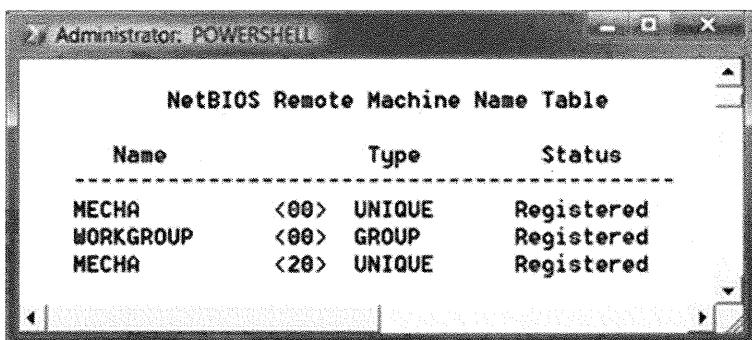
## Do I Still Need NetBIOS?

NetBIOS is a set of connectionless and connection-oriented protocols that work together to make computers accessible by their user-friendly names instead of their not-so-friendly IP or IPX addresses. NetBIOS often has been wrongly blamed for vulnerabilities that actually reside in the Server service or the Server Message Block (SMB) protocol, but it has weaknesses itself, too. Try this on your own computer, where *IPaddress* is the IP address of the local or a remote Windows system:

```
nbtstat.exe -A ipaddress
```

Hence, NetBIOS can be used to gather remote reconnaissance data. The good news is that modern Windows environments do not require NetBIOS 90% of the time. NetBIOS is required to maintain full backwards compatibility with ancient operating systems, like Windows NT, and a few legacy applications still require it, but it can be disabled safely for the most part. Disabling NetBIOS always should be done on Internet-accessible systems, too, if there isn't a compelling reason to leave it on.

To mostly disable NetBIOS on your computer, go to the properties of your network adapter card > General tab > highlight Internet Protocol (TCP/IP) > Properties button > Advanced button > WINS tab > select Disable NetBIOS Over TCP/IP. If you want to disable NetBIOS throughout your network, you can use Group Policy or your DHCP server. Windows DHCP servers support a scope option to disable NetBIOS on clients.



Name	Type	Status
MECHA	<00>	UNIQUE
WORKGROUP	<00>	GROUP
MECHA	<20>	UNIQUE

But if you want to totally eliminate NetBIOS on your box, even if this causes other problems, you can't just disable NetBIOS in the properties of TCP/IP. You have to also disable the NetBIOS device driver itself. The easiest way to do this is from the command line using the SC.EXE utility. Query the status of the driver with "sc.exe qc netbt", and set it to disabled with "sc.exe config netbt start= disabled" (to get back to defaults, set "start= system" instead). Note that this will also prevent the TCP/IP NetBIOS Helper service from starting and will thus prevent the computer from accessing SMB shared folders on other machines, including accessing the SYSVOL shared folder on domain controllers for the sake of Group Policy. Hence, disabling the NetBIOS device driver is probably overkill; just disable NetBIOS in the properties of TCP/IP instead.

### **Null User Sessions**

What about null user sessions? Don't they require NetBIOS? No! Many people believe they are immune to null user session attacks if they simply disable NetBIOS, but this is not true. Null user sessions are possible because of the Server service and the Server Message Block (SMB) protocol, and you can still use these even when NetBIOS is disabled.

Null user session issues have been discussed already, but you should consider them repeated here. Preventing null user session exploits is an important part of your regimen for securing your network services.

# Key Protocols (1 of 2)

- As discussed before, firewalls should filter out unwanted traffic
- Protocols you should memorize:
  - SMB: TCP/139/445
  - RPC: TCP/135
  - LDAP: TCP/389/636/3268/3269
  - Kerberos: TCP/UDP/88

SANS Security Essentials – © 2016 SANS

## Key Protocols (1 of 2)

After disabling unnecessary services and bindings, you should still put a firewall on the system and network as though all these dangerous services were still running. A different module discussed firewall theory at length, but there are some Windows-related specifics that should be mentioned here, too.

### Windows Network Traffic

There are certain network traffic flows that are characteristic of Windows networks. You should be familiar with their signatures and purposes so that you can recognize them in your packet traces and firewall logs. This list also will be important later when conducting audits. Hackers can use these port numbers to help "fingerprint" your boxes, too. These essential protocols and their port numbers should be memorized.

#### Server Message Block (SMB): TCP/139/445

Server Message Block (SMB) is the file and printer sharing protocol. When using NetBIOS, SMB operates on TCP/139; without NetBIOS, it uses TCP/445 and is sometimes referred to as the Common Internet File System (CIFS) protocol. All SMB/CIFS packets should be blocked going to or coming from the Internet, unless they are being tunneled through IPSec or a VPN.

#### Remote Procedure Call (RPC): TCP/135

Remote Procedure Call (RPC) networking is used extensively on Windows networks.

Trust relationships, the NetLogon secure channel, Outlook messaging, NTLM pass-through authentication, remote administration, and so on, all can use RPC-based sessions. RPC sessions typically begin with a client connection to TCP/135 on the server; then the server will redirect the client to another "ephemeral" high-numbered port for subsequent communications. Be aware, though, that RPC-over-HTTP (TCP/80/443/593) is possible, and RPC-over-SMB (TCP/139/445) is used very commonly, too.

### **Lightweight Directory Access Protocol (LDAP): TCP/389/636/3268/3269**

The Lightweight Directory Access Protocol (LDAP) is the default protocol for searching and editing the Active Directory database. Cleartext LDAP uses TCP/389, whereas SSL-encrypted LDAP goes over TCP/636. A special portion of the Active Directory database called the *global catalog* also is LDAP-accessible over TCP/3268 (cleartext) and TCP/3269 (SSL-encrypted) on domain controllers. LDAP uses Kerberos for authentication, so it is not the case that the cleartext channels send passwords in the clear, too.

### **Kerberos: UDP/TCP/88**

Kerberos is the default authentication protocol on Active Directory networks. It uses UDP/88 primarily; however, when tickets get too large, TCP/88 will be used as well. The Kerberos change password port (TCP/UDP/464) is listening on domain controllers too, but Windows clients still prefer to use an RPC session to change their passwords. Neither the Kerberos administration port (TCP/749) is used nor is the Kerberos demultiplexor (TCP/2053).

## More Key Protocols (2 of 2)

- DNS: UDP/TCP/53
- RDP: TCP/3389
- SQL Server: TCP/UDP/1433/1434
- NetBIOS: TCP/UDP/137, UDP/138, TCP/139, TCP/UDP/1512, TCP/42
- IPSec: UDP/500/4500 for IKE, Protocols 50 and 51 for ESP and AH

SANS Security Essentials – © 2016 SANS

### More Key Protocols (2 of 2)

Active Directory cannot function without DNS servers. You will see heavy traffic to your DNS servers on both UDP/53 and TCP/53. In general, everything that WINS and NetBIOS did in the past is now handled by DNS instead.

#### NetBIOS and WINS: TCP/UDP/137, UDP/138, TCP/139, TCP/UDP/1512, TCP/42

A WINS server maintains a database of NetBIOS-to-IP address mappings just as DNS servers map hostnames to IP addresses. If you have older clients, or if you still have NetBIOS enabled in your LAN, then constantly you will see heavy NetBIOS/WINS traffic. Indeed, NetBIOS is like a constant background noise that you have to exclude from your logs. (It's mind-boggling how chatty Windows machines can be.) There are many NetBIOS- and WINS-related ports:

- NetBIOS Name Service: TCP/UDP/137
- NetBIOS Datagram Service: UDP/138
- NetBIOS Session Service: TCP/139
- WINS: TCP/UDP/1512
- WINS Replication: TCP/42

#### Remote Desktop Protocol (RDP): TCP/3389

Windows Remote Desktop Services (formerly known as "Terminal Services) uses the Remote Desktop Protocol (RDP) to provide remote control of desktops and hosted applications. Windows clients use the same protocol for the Remote Assistance feature. RDP operates on TCP/3389. (Citrix ICA uses TCP/1494, which is a different protocol with a similar purpose.)

### **Internet Protocol Security (IPSec): UDP/500/4500, Protocols 50 and 51**

Internet Protocol Security (IPSec) is supported natively on Windows; it does not have to be installed. It is used for authenticating and encrypting packet data, including Layer Two Transport Protocol (L2TP) VPNs. IPSec uses UDP/500 to negotiate sessions, IP protocol number 50 for Encapsulating Security Payload (ESP), and protocol number 51 for Authentication Header (AH). UDP/4500 is used for IPSec NAT-Traversal (NAT-T). L2TP uses UDP/1701, but you should never see unencrypted UDP/1701 traffic on the wire.

### **Microsoft SQL Server: TCP/UDP/1433/1434**

SQL Server listens for queries on TCP/UDP/1433 and is monitored on TCP/UDP/1434. If you use client-server applications with SQL Server, you see a ton of this traffic.

### **Secure Sockets Layer (SSL) and Transport Layer Security (TLS): TCP/443**

SSL and TLS are widely used for web browsing, e-mail, VPNs and many other protocols intended to cross over the Internet. For good or bad, we place an immense amount of trust (or just hope) in these protocols. Strictly speaking, SSL is obsolete and only TLS should be used going forward, but SSL nonetheless is still widely deployed and the term "SSL" is entrenched in the minds of the nontechnical public, so, if only as a marketing term, SSL will be mentioned for many years to come.

### **Point-to-Point Tunneling Protocol (PPTP): TCP/1723, Protocol 47**

Point-to-Point Tunneling Protocol (PPTP) is another VPN protocol. PPTP uses both TCP/1723 and the Generic Routing Encapsulation (GRE) protocol. GRE operates on protocol ID number 47. This protocol is totally obsolete, however, and should never be used. It is mentioned here only because it refuses to die away.

# The Windows Firewall (1 of 3)

## • The Good:

- Built-in, free, and enabled by default
- Full state dynamic filtering, including RPC
- Per-application and per-service filtering rules
- IPv4 and IPv6 support
- Both ingress and egress filtering
- Deeply integrated with IPSec driver
- Manageable through Group Policy
- Command-line management with PowerShell or NETSH.EXE

## • The Bad:

- No centralized logging or alerting capabilities
- Complex

SANS Security Essentials – © 2016 SANS

## Windows Firewall (1 of 3)

The Windows XP firewall was not good. Starting with Windows Vista, the firewall was drastically enhanced and not-so-eloquently renamed to Windows Firewall *with Advanced Security* (WFAS). This section discusses only WFAS.

WFAS is built into Vista/2008 and later, is stateful, easy to configure, supported by Microsoft, can be managed through Group Policy or custom scripts (NETSH.EXE), and works with all types of interfaces (LAN cards, 802.11 wireless, dial-up connections, VPN tunnels, and so on). WFAS filters both inbound and outbound traffic with equal facility. The WFAS also is compatible with the Internet Connection Sharing service, provides good text logging in W3C Extended format, and can easily be configured to permit access to services on the host itself or to another machine behind it on the LAN, such as to an HTTP or FTP server.

Another important benefit is the deep integration of WFAS with the IPSec driver. In fact, on Vista and later, IPSec and the Windows Firewall are managed as a single product. For example, if the firewall is configured to allow inbound traffic to TCP/445 from the local LAN only, a simple check box can be set to require IPSec encryption with Kerberos authentication as well to actually get access to that port.

Because the Kerberos authentication is against Active Directory, you can further specify which groups are permitted to authenticate in the first place! This means you could restrict access to TCP/445 only to users in one or more global groups in AD, but only if the computers of those users are joined to the domain, and only if the connection is AES encrypted, and only if the source IP address is from the local LAN. IPSec is normally discussed in the context of sniffing threats, but it can also be used for access control when combined with the host-based firewall.



On the bad side, though, WFAS lacks the sophisticated intrusion detection capabilities of some other popular personal firewalls, doesn't work on Windows 2000/XP/2003, and there's no support for automatic upload of log data to a central server. There's also no integration between WFAS and other anti-malware or behavior-monitoring systems on the box, and third-party vendors who provide such features (like Kaspersky) install their own firewalls, they typically don't use WFAS. The protocol stack in Windows Vista/2008 was also redesigned from the ground up, which enables new security features (like WFAS), but it also means some of the most vulnerable and complex software in any operating system (the protocol stack) hasn't received much real-world testing.

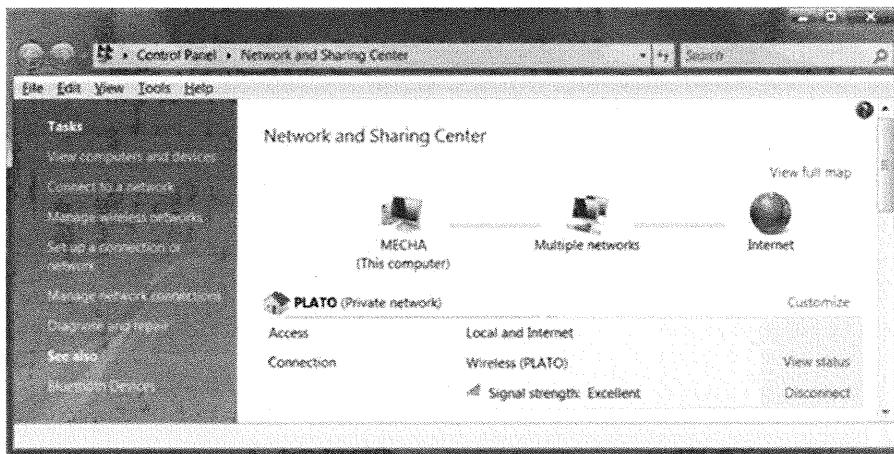
## Network Location Types (2 of 3)

- A network profile is a categorization label assigned to a network adapter card and the network to which it is attached at the moment. When first connecting, you will be prompted to choose.
- **Three network profiles available:**
  - **Domain** (selected automatically when AD is available)
  - **Public** (coffee shops, hotels, airports, and such)
  - **Private** (home and office)
- **You can have different firewall rules for each profile!**

SANS Security Essentials – © 2016 SANS

### Network Location Types (2 of 3)

When a Windows Vista or later computer is connected to a network, that network will be categorized as a public, private, or domain network. (Microsoft sometimes calls these categories "network location types" or "network profiles.") A *domain* network can be used to access domain controllers for the computer's Active Directory, and this profile is selected automatically when your domain controllers are detected. A *private* network is a trusted network that does not have domain controllers, for example, a home or small office network. A *public* network is everything else, such as airports and coffee shops with Internet access.

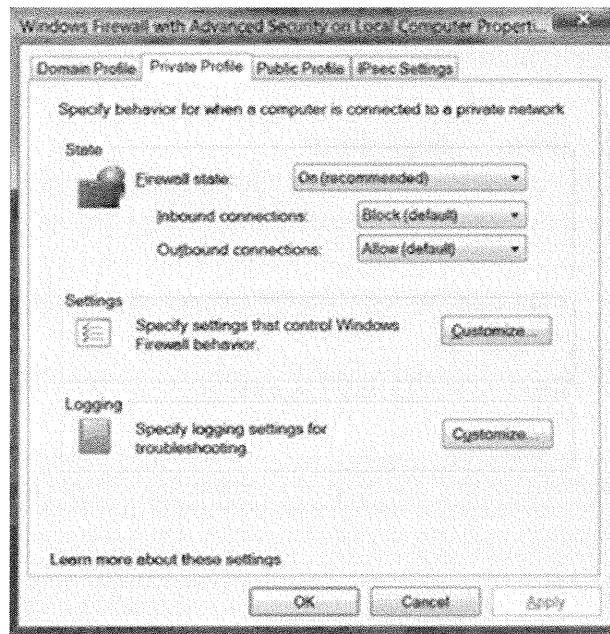


You can see and edit the category of the network to which you are currently attached by going to Control Panel > Network and Sharing Center > Customize. The computer will remember your settings the next time you connect to that network. If a domain controller is reachable, the domain category will be automatically assigned.

The Windows Firewall can have different sets of rules for each network category and switches the rulesets automatically as the computer is disconnected and reconnected to different networks. Rules for the public network are generally the most strict, whereas rules for the domain network are the least strict.

### Network Location Firewall Defaults

There are different default settings for the different network location types. To edit these per-network defaults, right-click the WFAS snap-in > Properties > choose the appropriate tab: Domain, Private or Public.



For each profile, you can enable/disable the firewall, block/allow inbound or outbound connections, configure logging options, and specify whether the user is notified when a program is prevented from receiving inbound connections (giving administrative users the opportunity to allow them in for that program). For inbound connections, if the option is set to "Block All Connections" then all inbound connections are blocked even if there is a rule which would normally allow it, while the "Block (Default)" option blocks only those inbound connections for which there isn't a rule to allow them.

Logging is written to an ASCII text file (pfirewall.log) in W3C Extended format. Note that all dropped packets are logged, if those packets are logged at all, but only the initial packet in a successful connection is recorded in order to avoid killing performance by logging all the permitted packets that follow. The maximum log size is 32MB.

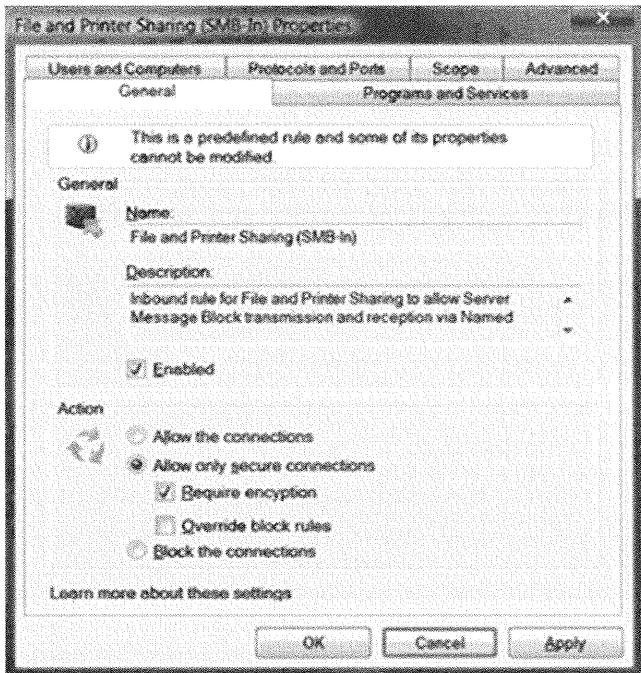
# Managing Firewall Rules (3 of 3)

- Firewall rules can be organized by the network profile(s) in which they are activated (A rule is only enforced when its associated profile is currently active)
- **Firewall-IPSec Integration:**
  - "Secure Connection" = mutual authentication and packet signing
  - "Require Encryption" = mutual authentication and encryption
- You can create exceptions for applications and service:
  - Dialog box pops up...
- Manage firewall rules through Group Policy and NETSH.EXE.

SANS Security Essentials – © 2016 SANS

## Managing Firewall Rules (3 of 3)

WFAS performs both ingress and egress filtering. Connections are regulated by the rules in the Inbound Rules and Outbound Rules containers in the WFAS snap-in. To create a new rule, right-click the Inbound/Outbound Rules container > New Rule. To edit a rule, simply double-click it.



The property sheet of each rule has the follow tabs and options:

**General:** Allow or block, or allow only if secured with IPSec, and allow with IPSec to a particular user or computer (Users and Computers tab) even if there is another rule that would otherwise block the connection.

Note that a "secure connection" is traffic signed using IPSec Authentication Header (AH) or Encapsulating Security Payload (ESP) with the encryption disabled, whereas a "secure connection with encryption required" is traffic both signed and encrypted using IPSec ESP with the encryption enabled. And if an IPSec-secured connection is only for particular users or computers (as defined on the Users and Computers tab), then the IPSec channel must be authenticated with either Kerberos or a certificate, and those users and computers must exist in Active Directory. The IPSec settings are configured using the Connection Security Rules container in the WFAS snap-in, but IPSec will be discussed later. If an appropriate IPSec Connection Security Rule is not created for a firewall rule that requires it, the firewall rule will not allow the traffic. The default IPSec settings used can be seen by right-clicking the WFAS snap-in > Properties > IPSec Settings tab.

**Programs and Services:** The exact program binary or background service(s) to which the rule applies. Hence, you can have per-application and per-service firewall rules.

**Users and Computers:** If only IPSec-secured connections are allowed (General tab) and if the IPSec authentication protocol is Kerberos or certificate, then computer and user accounts can be selected from Active Directory (not the local accounts database or the workgroup) in order to limit connections to/from just those particular users or computers.

**Protocols and Ports:** Select any protocol, including IPv6, or any port(s), including dynamically-assigned RPC and NAT ("Edge Traversal") ports, or any ICMP protocol, including custom ICMP type and code numbers, to which the rule applies.

**Scope:** Limit the source and/or destination IP address(es) to which the rule applies, including DHCP-assigned WINS, DNS, DHCP and default gateway addresses. Keep in mind that you should limit the IP addresses of the other machines which you allow to connect to you as much as possible. This is done on the Scope tab in the properties of the inbound rule. At a minimum, don't set the remote IP addresses on the Scope tab to Any IP Address.

**Advanced:** Specify the network location profile(s) and the types of network interfaces (wireless, VPN/dial-up, physical NIC) to which the rule applies, as well as whether an Internet-accessible IP address should try to be obtained (inbound rules only) for the sake of publishing a service to the Internet without the aid of a NAT-ing device in front of the computer.

### Defining Exceptions

Another way for a user with administrative privileges to add an inbound rule is to simply launch a program which attempts to listen on a new port number. This action causes a dialog box to appear which alerts the user to the attempted port binding. In the screenshot below, netcat was run to make it listen on TCP port 7890 and connect an in-coming session to a new instance of CMD.EXE ("nc.exe -L -p 7890 -e cmd.exe").

Maybe the user did this knowingly and deliberately, or maybe the system has been compromised and a back door is being opened.



The dialog box gives the user two choices:

#### **Keep Blocking:**

Don't allow the program to acquire a listening port. Train your users to choose this option when there is any doubt.

#### **Unblock:**

Create inbound rules for this program to permit it to listen on the port it is currently requesting and on any other port it may request in the future.

If you don't want this dialog box to ever appear, right-click the WFAS snap-in > select the tab for the relevant network profile > Customize button for settings > select No to display a notification (default is Yes). For non-technical users, this is perhaps the best thing to do.

#### **Order of Rule Processing**

Firewall rules are not processed from top-to-bottom in the order shown in the snap-in. The Windows Firewall does not follow the "First Match Wins" metarule, it follows the "Best Match Wins" metarule. Now, the exact criteria for making one rule better than another is not fully documented, but informal sources indicate that rules are processed roughly in this order:

1. Rules that allow/block traffic for particular services.
2. Rules that allow traffic from particular computer sets.
3. Rules that allow traffic only if it is IPSec secured (AH or ESP).
4. Rules that block traffic, inbound or outbound.
5. Rules that allow traffic, inbound or outbound, with or without IPSec.
6. Default behavior for the active network profile (allow or block).

#### **NETSH.EXE**

The Windows Firewall can be managed with NETSH.EXE from the command line. NETSH.EXE isn't just for the firewall, it's a general purpose tool for managing networking-related settings.

Here are some NETSH.EXE commands with which to experiment in a CMD shell:

To see a summary of your profile options:

```
netsh.exe advfirewall show allprofiles
```

To dump the details of every rule:

```
netsh.exe advfirewall firewall show rule name = all
```

To see how to create a rule from the command line:

```
netsh.exe advfirewall firewall set rule /?
```

#### **PowerShell (Windows 8, Server 2012 and Later)**

The older binaries like NETSH.EXE have been deprecated in favor of PowerShell. There are a large number of cmdlets for IPSec and firewall rules in Server 2012, Windows 8 and later. To see a listing of these cmdlets, run this command:

```
Get-Command -Module NetSecurity
```

#### **Group Policy**

The Windows Firewall in XP and later can also be completely managed through Group Policy. The Vista and later WFAS settings in a GPO are located under Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security.

For the Windows XP-SP2/2003 version of the Windows Firewall, its settings are found in the GPO under Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall.

If a service is important enough to let through the firewall (perimeter or personal) then it's important enough to consider using IPSec to authenticate and encrypt it!

## Windows IPsec and Other VPNs

The student will know how to configure and manage IPSEC with Group Policy, understand the strengths and weaknesses of alternative VPN protocols on a Windows host, and how to apply VPN security in a wireless environment.

SANS Security Essentials – © 2016 SANS

### **Windows IPsec and Other VPNs**

This section intentionally left blank.

# Internet Protocol Security (1 of 4)

- **The IPSec driver is built-in; no extra software is needed**
- **IPSec Benefits:**
  - Mutual authentication required (Kerberos, Certificates, NTLM)
  - Payload encryption (256-bit AES)
  - Packet digital signatures (for integrity and proof of origin)
- **IPSec Is Not Just for VPNs:**
  - Limit access to TCP/UDP ports based on group memberships in Active Directory (similar to share permissions, but for ports)
  - Encrypt RPC, SMB, DNS, LDAP or RDP without a VPN

SANS Security Essentials – © 2016 SANS

## Internet Protocol Security (1 of 4)

Internet Protocol Security (IPSec) and Virtual Private Networking (VPN) provide the next layer of security for our network services. After applying hotfixes, disabling services, breaking bindings, and firewalling hosts and the perimeter, whatever traffic is left over must be necessary and important!

IPSec is widely misunderstood. IPSec is often thought to be only for VPNs, but IPSec is actually for every single Windows computer in your organization, both inside and outside of the main perimeter firewall. The purposes or uses of IPSec are also widely misunderstood. IPSec is thought mainly (or only) to provide encryption of packet data, but the encryption feature is perhaps of only secondary importance. IPSec also requires *mutual* authentication, and a machine can be configured to require IPSec authentication before permitting any further communications with it. (By contrast, SSL usually does not require mutual authentication, hence, any random anonymous hacker can connect to your public HTTPS and SMTPS servers.) Especially when combined with a host-based firewall, IPSec mutual authentication is an effective and flexible way of regulating access to network services. If an outsider somehow attaches to one's network, they can't access network services on critical servers because they can't authenticate with IPSec! And if you want to create an enclave network, that is, a protected network within your larger LAN, you can tweak the IPSec mutual authentication requirements to implement something like an internal VLAN, but not with switches and firewalls alone, with IPSec.

Of course, IPSec also provides payload encryption, and you can use that for VPNs. VPNs using IPSec, PPTPv2, and SSL will be discussed momentarily.

## Command-Line IPSec Tools (2 of 4)

- Tools for local or remote systems, standalone or domain member:

- NETSH.EXE

- netsh.exe advfirewall consec /?

- PowerShell

- Requires Server 2012, Windows 8, or later
    - get-help \*ipsec\*

SANS Security Essentials – © 2016 SANS

### Command-Line IPSec Tools (2 of 4)

All IPSec settings can be managed from the command line using NETSH.EXE or PowerShell. Though these operating systems are obsolete, there is also support for Windows 2000 (IPSECPOL.EXE, *Resource Kit*) and Windows XP (IPSECCMD.EXE, download from Microsoft). All the tools work on either local or remote systems, if you have administrative privileges. The tools have different command-line switches, but the concepts are the same.

For example, on Vista and later, the following command shows all current IPSec rules, if any:

```
netsh.exe advfirewall consec show rule name=all
```

To see examples of how to create an IPSec connection security rule, run:

```
netsh.exe advfirewall consec add rule /?
```

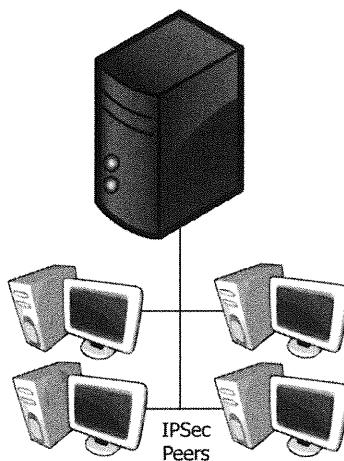
NETSH.EXE still works, but it has been deprecated in favor of PowerShell, so on Server 2012, Windows 8 and later, the following PowerShell command lists all the IPSec-related tools:

```
get-help *ipsec*
```

To see examples of how to create an IPSec rule in PowerShell, run:

```
get-help new-netipsecrerule -full
```

## IPSec & Group Policy (3 of 4)



- 100% of IPSec settings can be managed through Group Policy
- **Deployment Example:**
  1. Enable IPSec on all computers in the domain, but don't require it, only request IPSec
  2. Require IPSec only for SMB traffic for servers in one OU

SANS Security Essentials – © 2016 SANS

### IPSec & Group Policy (3 of 4)

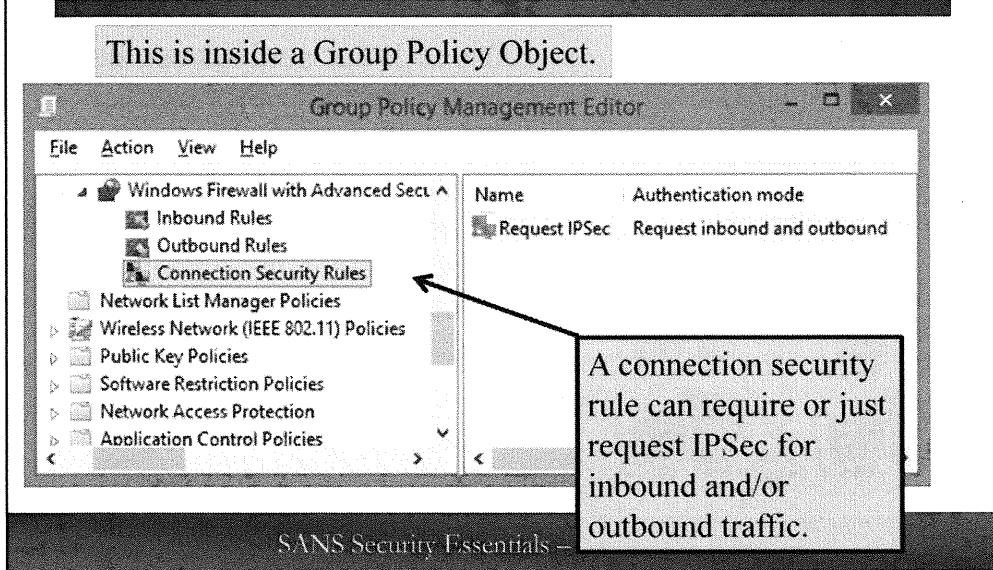
One hundred percent of IPSec settings can be managed through Group Policy. This means it is feasible to have custom IPSec configurations for thousands of computers and to change these configurations as often as needed. Each Organizational Unit (OU) could have its own separate IPSec policy; indeed, one reason for dividing computer accounts into different OUs is so that you can assign different IPSec policies to them easily.

This example enables IPSec on all computers in the domain through Group Policy. This enables IPSec, but it does not cause machines to reject non-IPSec traffic, but they request IPSec whenever possible. Next, you use Group Policy to configure all the servers in a particular OU to require IPSec, but only for SMB traffic on TCP ports 139 and 445.

This example assumes that all the computers are in an Active Directory domain inside the LAN, so they use Kerberos for the IPSec authentication. If a computer merely requests IPSec instead of requiring it, the computer first attempts IPSec negotiations with its peer, but if negotiations fail, the computer falls back down to plaintext to maintain backward compatibility. But the servers in this example OU require IPSec for their SMB traffic; hence, SMB connections to them fail when not first secured with IPSec.

Now see how it's done in Group Policy.

## Group Policy Example (4 of 4)



### Group Policy Example (4 of 4)

To request, but not require, IPSec on all computers in the domain, edit the Default Domain Policy Group Policy Object. (And because it is the Default Domain Policy GPO, it applies to all systems.) Of course, this is just a brief example; in real life this requires more careful planning and testing.

Open the Group Policy Management tool on any domain-joined computer > Forest > Domains > expand your domain > right-click the Default Domain Policy GPO > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall > right-click Connection Security Rules > New Rule > select Isolation > leave the default setting to only request authentication > Next > Next > select Computer (Kerberos V5) > Next > Next > give a name to your rule > Finish. These default settings request only IPSec authentication and do not require it.

Next, using the same Group Policy Management tool, edit the GPO assigned to an OU containing your file servers. When you create a new Connection Security Rule, though, the options instead be Custom > Next > Next > select "Require authentication for inbound connections and request authentication for outbound connections" > Next > select Computer (Kerberos V5) > Next > select the TCP protocol and enter the Endpoint 2 Ports as "139,445" > Next > Next > give a name to your rule > Finish.

In the screen shot in the slide, a "Connection Security Rule" is an IPSec rule, and this rule can be set to require IPSec or to merely request IPSec. The rule in the screen shot is requesting only IPSec, meaning that a plaintext connection would still be allowed if the IPSec negotiation failed for some reason.

An IPSec rule can apply to all traffic in/out of a computer, or the rule can be limited in scope to apply only to certain IP address ranges, certain protocols, particular ports, and so on. Hence, a rule that requests IPSec might only do so when the other computer has an IP address from the internal LAN or a particular subnet within the LAN.

# Windows IIS Security

---

The student will be apply  
best practices in securing a  
Windows IIS server.

SANS Security Essentials – © 2016 SANS

## **Windows IIS Security**

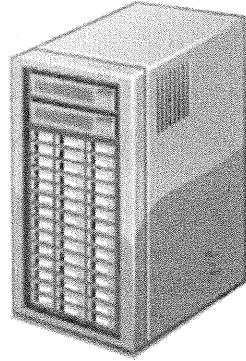
This section intentionally left blank.

Install IIS on separate drive than OS. (Directory Traversal)

# Securing Internet Information Server (IIS)

## First IIS hardening tip:

- Upgrade to the latest version of IIS you can!
  - Use IIS 7.0 on Server 2008 at a minimum



SANS Security Essentials – © 2016 SANS

## Securing Internet Information Server (IIS)

Internet Information Server (IIS) is actually a collection of services that can be installed separately or not, including HTTP and FTP, using the Server Manager tool. To make a Windows Server box a web server, IIS must be installed. This section discusses a few simple changes to your IIS server that can reduce its hackability.

### Only Use IIS 7.0 or Later

Don't use anything older than IIS 7.0 on Windows Server 2008. Older versions are too slow and too insecure.

IIS 7.0 on Windows Server 2008 has a similar architecture to IIS 6.0 from a security point of view, but its handling of ASP.NET and XML configuration files is quite different. The management graphical interface for IIS 7.0 has also changed drastically from IIS 6.0. This section discusses only IIS 7.0 on Windows Server 2008 and later, but even though the screen shots are different from IIS 6.0, many of the same hardening principles apply to IIS 6.0, too.

In general, your first IIS hardening step is to upgrade to the latest version you can, the minimum being IIS 7.0 on Server 2008. Each new version of IIS runs faster than the previous version, and, because Microsoft uses IIS in Azure for its own cloud services, Microsoft is highly motivated to make IIS as secure as it can.

# Use a Minimal Patched Install

- Start with a fresh OS installation, the latest Service Pack, and the latest patches
- Server Core installation option removes GUI and reduces OS footprint on drive (or in VM)
- Choose a standalone server if you can, or join to a separate extranet forest if you must, but avoid joining it to the main internal forest

SANS Security Essentials – © 2016 SANS

## Use a Minimal Install

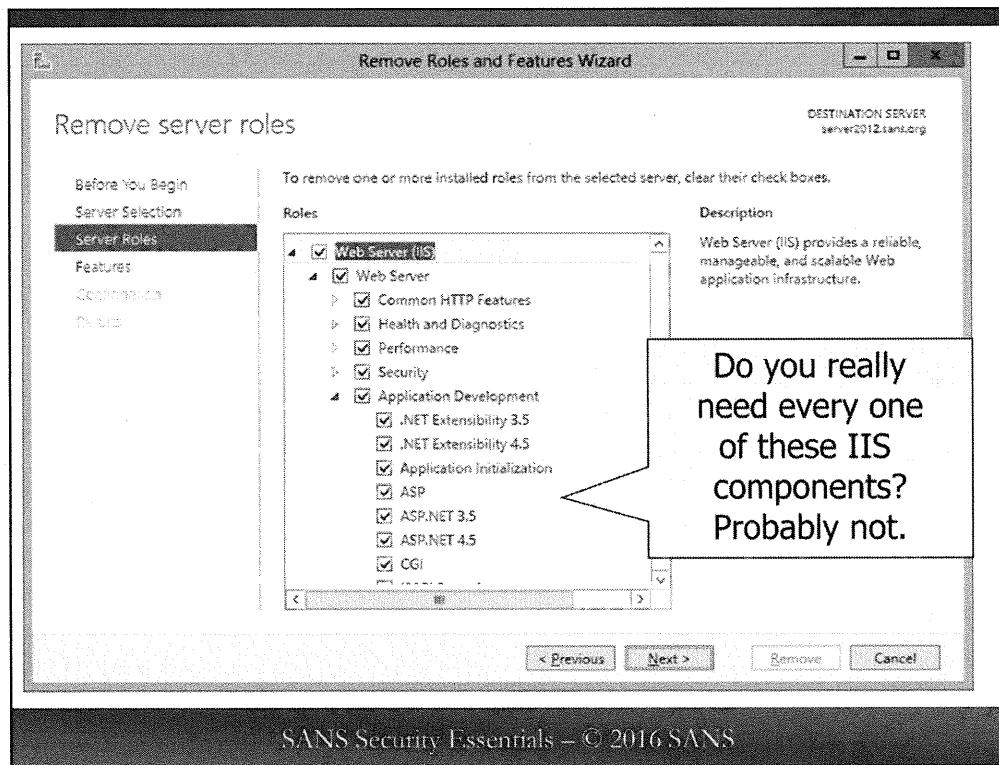
Start with a fresh install of the operating system, the latest Service Pack, and all the latest hotfixes. An installation option with Server 2008 and later is the ability to install the operating system in Server Core mode. Server Core is an installation option, not a different version or edition of Windows, hence, you could have either the Standard or Enterprise edition and then choose the Server Core installation option for either of them. If you install as Server Core, almost all operating system features that can be stripped away are stripped by default, including the graphical desktop! To support ASP.NET, however, you must have Server 2008-R2 or later, since the original Server Core in 2008 did not include the .NET Framework.

When you log on to a Server Core box, the only thing that pops up on your desktop is a command shell; there is no taskbar or Start menu. If you want to install IIS on Server Core, you certainly can, but it can make the box more difficult to manage locally because of the lack of the standard graphical tools. You can still use graphical management tools over the network, but if you RDP into the box you simply get a command shell again.

## Standalone Or Member Server

Ideally, your IIS box should be a standalone server, but it is OK for it to be a domain member if you require Group Policy, Kerberos, single sign-on, Digest authentication, or any other feature you get only with domain membership.

If IIS is a member server, it should *not* be a member of the main internal forest; it should be a member of a separate forest created just for the sake of managing your public servers. This forest should be isolated from the internal domain and all traffic scrupulously firewalled. If you must have a trust link between your extranet forest and your internal forest, try to keep it to just a one-way cross-forest trust where the extranet trusts the internal forest, but not vice versa.



SANS Security Essentials – © 2016 SANS

### Remove Unnecessary Components in Server Manager

IIS is not installed by default. When you use Server Manager to install the Web Server (IIS) role, only install the subcomponents that you actually need. IIS 7.0 and later is highly modular, so you have quite a bit of control over what gets installed. Don't worry, if you later discover that you need a component which isn't installed; just run Server Manager again and check the box(es) for what you need!

When you first install IIS with Server Manager, only the barest components are selected by default. You can serve up static HTML and graphics files, but that's it. None of the application development components (such as ASP.NET, ASP, or CGI) are selected, but you'll likely need some of these for your web applications to function.

Don't forget that if you want to script the (un)installation of roles and features, you can do so with the SERVERMANAGERCMD.EXE tool or in PowerShell. If you install with the Server Core option, this is your only choice for managing roles and features when sitting at the console.

To see which roles/features are installed right now, in an elevated CMD shell run:

```
servermanagercmd.exe -query
```

Or in PowerShell, run:

```
Get-WindowsFeature
```

# Remove Unused Handler Mappings

- A handler is a DLL or EXE that processes certain requests:
  - It can be either C++ native code or .NET managed code.
  - Static files, ASP.NET pages, and PHP scripts all have handlers.
- A handler is "mapped" to certain folders, files and extensions.
- Handlers can be easily added, removed, or replaced.
- **Many exploits against IIS handlers in the past:**
  - Code Red worm (\*.ida)
  - Internet Printing Service buffer overflow (\*.printer)
  - HTR buffer overflow attack (\*.httr)
- **Tomorrow there will be new exploits against IIS script handlers!**

SANS Security Essentials – © 2016 SANS

## Remove Unused Handler Mappings

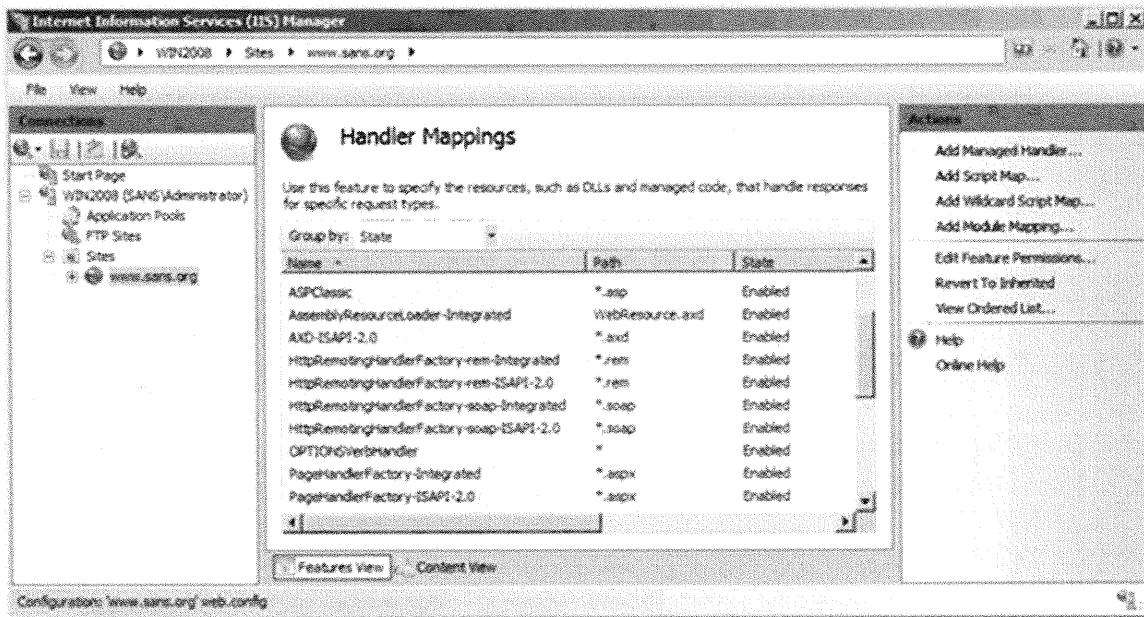
A *handler* is an IIS component that processes certain requests. The handler can be a standard DLL or EXE, usually compiled from C++ source code, which doesn't use the .NET Framework (native code) or it can be a .NET type or module (managed code) usually compiled from C# or VB.NET source. IIS comes with a large number of handlers built in, and third-party developers can easily add their own. Much of what we imagine IIS is doing under the hood is actually performed by one or more handlers. For example, if a static HTML file is requested, this is handled by the StaticFile handler, or if directory browsing is enabled, the directory list is generated by the Directory handler. Because these handlers can be added, removed, or replaced as wanted, IIS 7.0 and later is modular.

When an HTTP request arrives at your IIS server, IIS examines the path, filename, and filename extension of the requested file or folder. If any of these characteristics of the request have been *mapped* to a handler, then all the data from the browser's request (GET parameters, cookie contents, header information, form input, and so on) are given to that handler for processing. The output of this processing is then shot back to the browser as the web page. This is how Active Server Pages and PHP scripts are run.

Now, from a hacker's point of view, the situation is different. To a hacker, you foolishly have configured your server to accept arbitrary input from anonymous people on the Internet, and then you allow this input to be passed into executables (possibly running under System context) as something like command-line arguments.

These executables often are DLLs loaded into the memory address space of the web service itself (INETINFO.EXE). Consequently, all a hacker needs to do is *mangle* this input in just the right way to cause memory leaks, 100 percent CPU utilization, buffer overflows, and a variety of other nasty side effects. All this is possible because of these filename extension mappings to their script interpreters in IIS! Hence, unmap your *unused* filename extension mappings.

To view your handler mappings, open the Sites container > select right-click on your website > click Features View at the bottom > double-click the Handler Mappings icon. To edit or remove a mapping, right-click and select Delete, Edit or Add.



There are dozens of past exploits that require these mappings in order to work, and you can bet that tomorrow new ones will be discovered. The Code Red worm, for example, requires the \*.IDA mapping on Windows 2000, but if you get rid of the mapping, you are 100% immune to the Code Red worm even without the patch. The Internet Printing Service buffer overflow exploit requires the \*.PRINTER mapping on Windows 2000. The HTR scripts buffer overflow requires the \*.HTR mapping on Windows 2000. Almost all the Active Server Page exploits require the .ASP mapping, and so on. And tomorrow there will be new exploits for IIS 7.0 or later which also have handler dependencies, so it won't feel left out.

Now, when you installed IIS with Server Manager you should have only installed the minimum components you actually need. This is really the best way to remove unneeded handlers, namely, to completely uninstall its associated component. Of the handlers remaining, though, how do you know which ones you can or should remove? Time to roll up your sleeves and apply elbow grease, because only testing and Google research will reveal the minimal list. Yes, this is a huge pain, but this security hardening task of removing unneeded handlers is one of the most important in this entire section. It will someday save your bacon.

# IIS Access Controls

- **Transport Layer Security (TLS) and SSL:**
  - Provides encryption and web server authentication
- **User Authentication Options:**
  - Anonymous (shared IUSR account for everyone)
  - Non-anonymous (Basic, Digest, Kerberos, Smart Card, and such)
  - Restrict access to allow only Authenticated Users or particular global groups in Active Directory
- **Per-Folder IP Address Restrictions:**
  - Restrict access only to clients with certain IP addresses
  - Not a replacement for a firewall

SANS Security Essentials – © 2016 SANS

## IIS Access Controls

Just as the operating system enforces certain access controls through authentication requirements and permissions, so does IIS for the sake of web applications. You can configure different SSL/TLS, authentication, and IP address restrictions on each website, folder and file.

### SSL/TLS Encryption and Server Authentication

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption can strongly encrypt all data transmitted between browser and server. SSL/TLS also authenticates the web server to help prevent users from being tricked into trusting a counterfeit or bogus website.

After installing a digital certificate, you can require SSL encryption on any folder or file. To do so, select the site, folder or file > click Features View at the bottom > SSL Settings. If you don't check the *Require 128-bit Encryption* box, the browser might negotiate only a 40-bit session key. Make sure to require 128-bit encryption.

SSL/TLS should be used whenever basic authentication is required. More important, remember that your credentials are cached in your browser and sent automatically for every page that requests authentication. A common mistake is to use SSL on the initial connection to the web server (when the dialog box appears for the username and password) but then to continue requiring basic authentication on subsequent folders and files even though SSL is no longer being used.

SSL/TLS also should be used on any forms for submitting sensitive data, such as credit card numbers, passwords, account numbers, and so on. Actually, it is perfectly safe to download the form in cleartext, but the data should be posted back up to the web server using SSL when the Submit button is clicked. Examine your HTML to ensure that the form method reads:

```
action="https://...."
```

and not just:

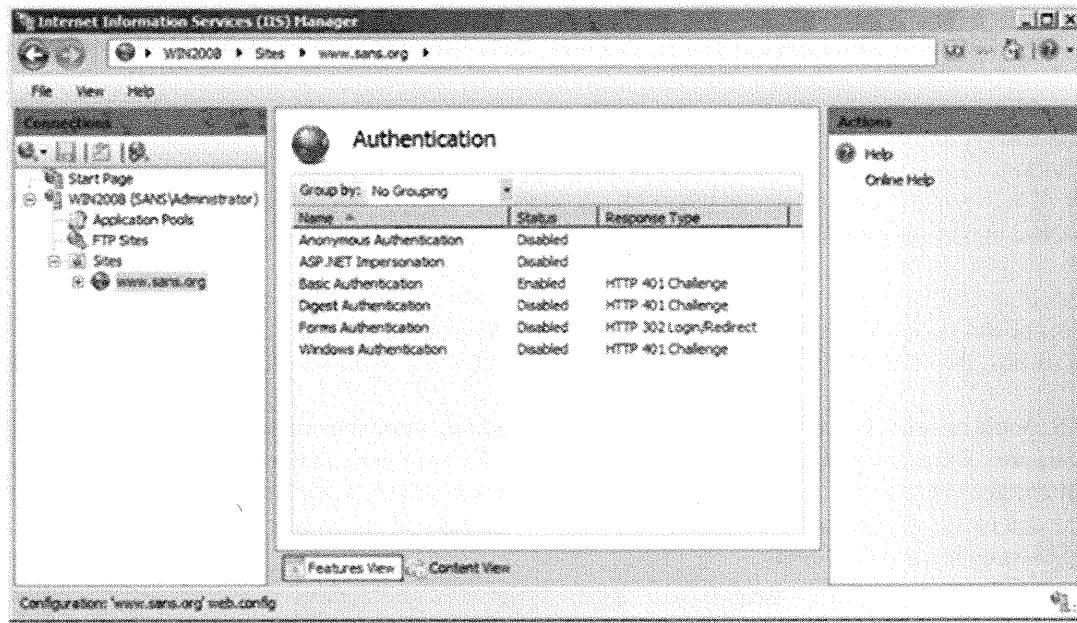
```
action="http://...."
```

### Require Authentication to Prevent Anonymous Access

IIS can use Active Directory for its accounts database if it's a domain member; otherwise, it uses only the local accounts in its own SAM database. After a user has authenticated, IIS is aware of that user's group memberships and can therefore enforce NTFS permissions. You should require authentication whenever you want to block anonymous access to sites or folders, or whenever you also want to restrict access to particular global groups.

To require user authentication on a folder or file, select it > click Features View at the bottom > Authentication icon > right-click and disable Anonymous Authentication > right-click and enable Basic authentication. Basic authentication was selected because it is compatible with all browsers; however, basic authentication also sends passwords unencrypted, so make sure to first require SSL/TLS first!

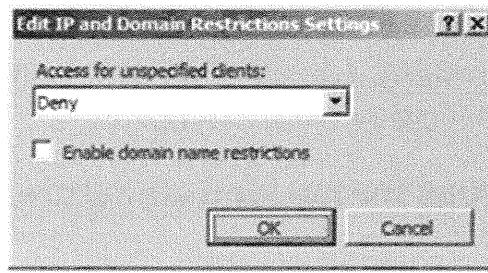
If you want to only allow members of a particular group to get access to a certain site or folder, don't forget to edit the NTFS permissions on that site or folder after requiring non-anonymous authentication. Change the NTFS permissions so that only the desired group(s) has Read access, while keeping Full Control for System and Administrators.



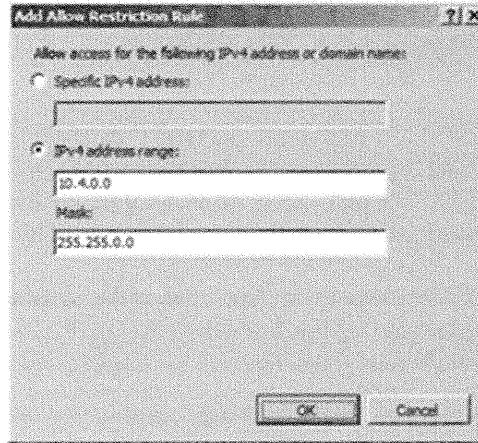
## IP Address Restrictions

Finally, you can allow or deny access to sites, folders and files based on the source IP address of the client. This is useful for sites or web applications that are intended for internal use only, such as SharePoint sites. Keep in mind that this feature is not firewalling packets, it's merely fulfilling or not fulfilling HTTP requests on the basis of source IP, hence, your IIS box could still be SYN Flooded from the Internet, for example, even though you restrict source IP addresses to the local LAN only. Nonetheless, every stone in your defensive wall adds a bit of security.

To configure IP address restrictions on a site, folder or file, select that item to highlight it > click Features View at the bottom > IPv4 Address and Domain Restrictions > right-click anywhere in the list and select Edit Feature Settings > choose Allow or Deny as the default.



Next, you'll define exceptions to your default Allow or Deny preference. To add an exception, right-click anywhere in the window > select Add Allow/Deny Entry > then enter the single IP address or the network ID plus subnet mask for a range of IP addresses.



When you're done adding exceptions, notice that you can edit the order in which the exceptions are evaluated. Similar to a firewall, the rules are processed from top to bottom, with the first matching rule winning. To change the order of processing, right-click anywhere in the window > View Ordered List > the right-click the desired rule and select Move Up or Move Down.

## What About URLSCAN?

URLSCAN.DLL is a free application-layer firewall for IIS 5.0/6.0 from Microsoft which could scan HTTP requests for user-configurable threatening patterns and then reject those requests if detected. Most of the functionality of URLSCAN is now just built into IIS 7.0 and later as part of the defaults (KB944836). IIS 7.0 and later include a module, "RequestFilteringModule", which can be further configured through XML files with more filtering options. Proper editing these XML files, though, is far beyond the scope of this course. To read more about the feature, do a Google search on "iis 7 request filtering" and there will be ample links to tutorials.

# IIS Logging

- IIS can log to text files or an ODBC database
- Change the default log folder
- Restrict with NTFS permissions
- Move log files off server ASAP:
  - Hourly logging, scheduled script to move files
  - Script the use of SMB, FTP or HTTPS
- **Review logs for hacking signatures**

SANS Security Essentials – © 2016 SANS

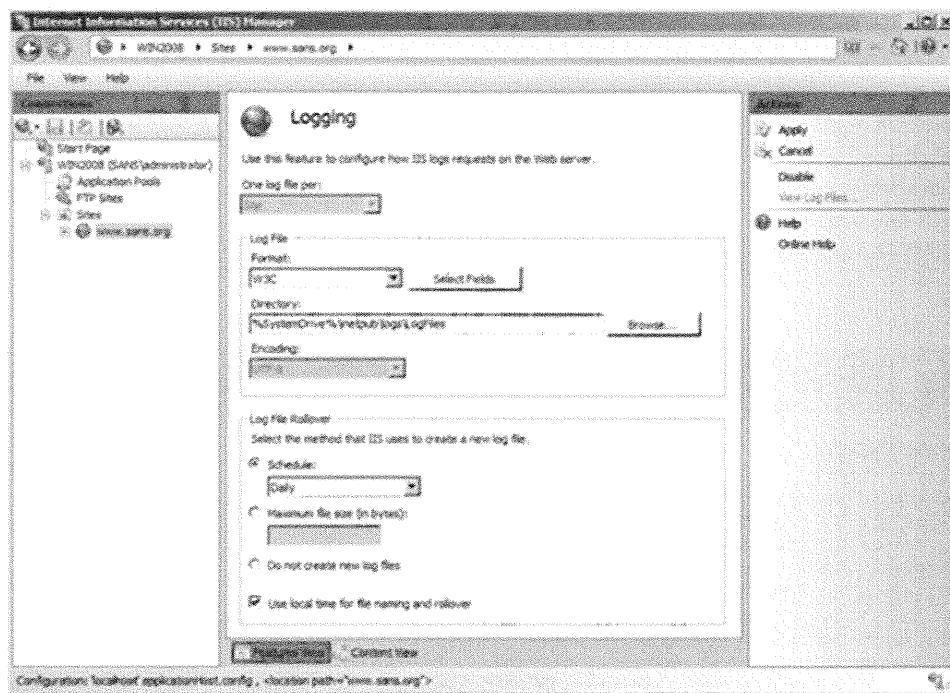
## IIS Logging

There are many other sources of audit data that could be discussed, but perhaps the most important to mention is the logging provided by Internet Information Server. Your IIS servers will be probed and attacked regularly, so it's critical that you keep good logs.

IIS log data can be written to local ASCII text files or remote ODBC database servers. Logging can be enabled/disabled on a per-site, per-folder, or per-file basis. Enabling logging is a two-step process. First, you enable the capability to log at the website. Second, you go to each folder/file that you do not want to be logged and disable the logging. This is necessary because everything will be logged by default.

To enable logging on a website in IIS 5.0/6.0, go to the Properties of the website > Website tab > check the Enable Logging box > select W3C Extended Log File Format > OK. On IIS 7.0 and later, select the website to highlight it > click Features View at the bottom > double-click the Logging icon > select Enable in the Action pane.

Next, you can enable/disable logging on a per-folder or per-file basis. On IIS 5.0/6.0 do this by right-clicking the item > Properties > Directory or File tab > (un)check the Log Visits box > OK. In IIS 7.0 and later, select the item > click Features View > Logging icon > select Enabled or Disable in the Action pane on the right.



### Securing IIS Log Files

If local logfiles are used instead of an ODBC database, the default storage folder is `\%SystemRoot%\System32\LogFiles` on IIS 5.0/6.0 and `\%SystemDrive%\intetpub\logs\LogFiles` on IIS 7.0 and later, underneath which each HTTP site will have its own subfolder. The subfolder is named after the site. You should move the default location to a different volume, however, so that an attacker won't find it so easily.

NTFS permissions on these folders should be Allow:Full Control to System and Administrators and Deny:Full Control to the IUSR account that IIS uses to represent remote anonymous users (and any other users or groups you don't trust). You also should audit all successful and failed access by the Everyone group, as well (don't worry; you won't get a new event every time IIS writes to the log, only when IIS opens and closes handles to it).

### Move Logs Off the Server ASAP

The log files should be moved off the IIS server as quickly as possible. A nice option is to configure a new log to be created every hour, and then schedule a script to run ten minutes after the hour to move the last log off the machine. Logging intervals are defined on the same property sheet above for changing the log folder location (select "Hourly," and check the box labeled "Use local time for file naming and rollover").

How you move the logs is up to you: FTP, mapped drive letter to shared folder, HTTP, SMTP, SSH secure copy, etc. HTTP is probably the easiest: configure a virtual website whose root is the logging folder; bind that site only to a non-routable private address (e.g., 10.1.1.1, and block that at the firewall too); require NTLM authentication to the site; restrict access to the site so that only the internal loghost server can access it; grant only Read access; and then use a command-line HTTP client like WGET.EXE to download a copy of the log file. If you use WebDAV instead, you can also use a convenient drive letter mapping and SSL.

### Search the Logs for Hacking Signatures

If an adversary is tickling your IIS server in a bad way, there will be traces of that scanning in the logs. Using a PowerShell script, for example, you could automatically scan the last hour's log file using regular expressions to detect those hacking signatures and to alert you when found. You can get a free example of such a script for IIS from <http://cyber-defense.sans.org/blog/downloads> named "Search-TextLog.ps1" in the SEC505 zip file. This script takes two arguments: an IIS log file, and a text file containing regular expression patterns for which to search in the IIS log. The output is a summary of the hacking signatures (matches to the regular expression patterns) found. You can update the signatures file with new patterns as new attack techniques are discovered.

```
C:\> .\Search-TextLog.ps1 IIS.log signatures.txt | format-table -AutoSize

Count Description
---- -----
74 Attempts to use a backslash in a request (folder traversal).
15 Attempts to access the /printers folder (reconnaissance).
13 Attempts to access CMD.EXE (command execution).
12 Attempts to access \Winnt or \Windows (command execution).
12 Attempts to access /scripts or /cgi-bin (reconnaissance).
10 Attempts to access the IIS Administration web site (reconnaissance).
9 Attempts to access Certificate Server web pages (reconnaissance).
6 Attempts to send many repeating characters (probable buffer overflow).
6 Attempts to use Zu Unicode encoding (IDS evasion).
5 Attempts by the Code Red Worm (buffer overflow).
3 Attempts to use ../../ to obscure the URL pattern (evade IDS).
3 Attempts to access the IIS 4.0 change password scripts (reconnaissance).
3 Attempts to access the GLOBAL.ASA file (reconnaissance).
2 Attempts to access the SHOWCODE.ASP page (vulnerable sample page).
2 Attempts to access Exchange Outlook Web Access site (reconnaissance).
2 Attempts to use the ::$DATA exploit (show source code).
2 Attempts to access Unix-related directories (reconnaissance).
2 Attempts to use the .asp. exploit (show source code)
2 Attempts to append .HTT to an ASP page (show source code).
2 Attempts to access an IIS sample page (vulnerable scripts).
2 Attempts to download the SAM backup file (bad).
1 Attempts to use a tick mark in a request (possible SQL injection).
1 Attempts to use RFP's Whisker scanner against you (you have been targeted!).
1 Attempts to access msadcs.dll (RDS exploit).
1 Attempts to execute TFTP or WGET on the web server (file transfer).
1 Attempts to access the /MSADC folder (reconnaissance).
1 Attempts to use an asterisk in a request (possible wildcard to OS command).
```

If your organization can afford it, then a host-based IDS which can analyze web server logs would be even better. The most important point, though, is that logs should not just pile up unexamined, we want continuous monitoring.

# Remote Desktop Services

---

The student will understand how Remote Desktop Services operate and how it can be secured.

SANS Security Essentials – © 2016 SANS

## Remote Desktop Services

This section intentionally left blank.

# Remote Desktop Services (1 of 3)

- **Remote control of virtual desktop with thin client.**
- Remote Desktop Services (RDS) on Windows Server:
  - Previously known as Terminal Services
  - Application Server Mode (requires user licenses)
  - Remote Administration Mode (two admins only)
- The Remote Desktop feature is similar to RDS
- Remote Assistance Invitations:
  - Invitation files are sent via e-mail or Windows Messenger
  - Invitations have a TTL and require a passphrase
- Remote Desktop Client 6.0 or later is important for security

SANS Security Essentials – © 2016 SANS

## Remote Desktop Services (1 of 3)

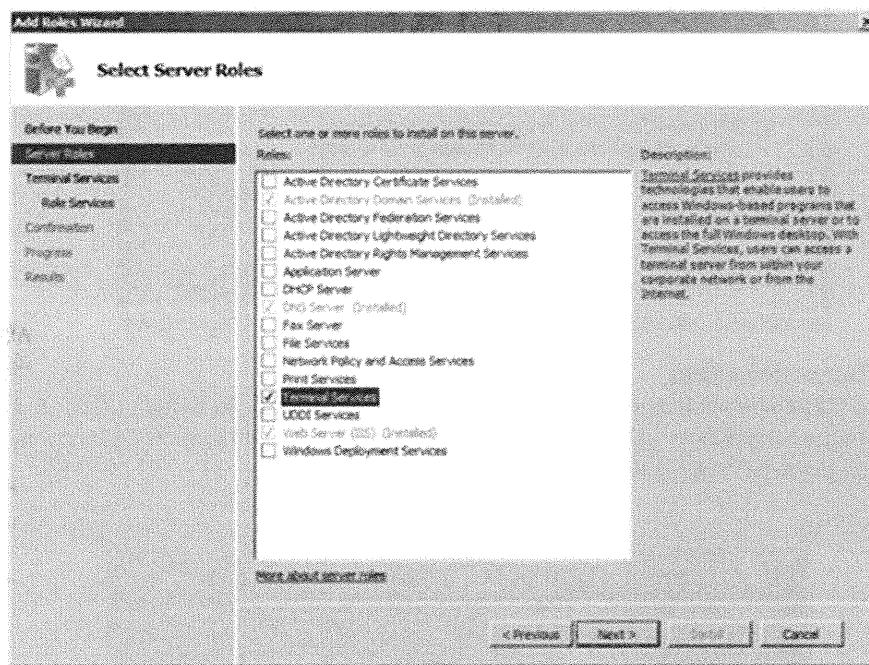
Remote Desktop Services (RDS) provides graphical remote control of virtual desktops running on Windows. It is similar to Symantec pcAnywhere or VNC in that it makes a remote desktop appear in a local application window (you can click the Start menu, see icons, etc.), except that you don't connect to *the* desktop of the remote box, you connect to a *virtual* desktop hidden in the RAM of the RDS server.



Hence, when you connect to a remote system, it is not the case that anyone sitting at that computer will see your typing and mouse clicks. In fact, a single RDS server could be running scores of virtual desktops simultaneously, each desktop separate and hidden from the others.

### Remote Desktop Services on Windows Server

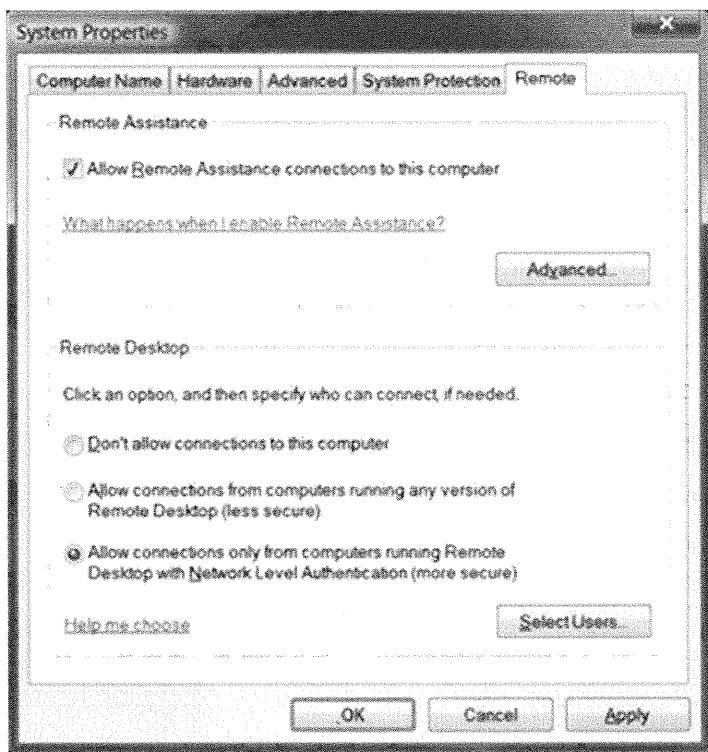
Remote Desktop Services (RDS) was previously known for years as Terminal Services. RDS is installed as a role on Windows Server 2008-R2 and later using Server Manager (or using the Add/Remove Programs applet in Control Panel on Server 2003 for Terminal Services). When installed, you have to choose its licensing mode: remote administration or application server. If you choose application server licensing, then any user can connect, but she'll require a special license from Microsoft. If you choose remote administration mode, you don't have to purchase any additional licenses, but only Administrators can connect to the box (and only two at a time).



### Terminal Services on Windows XP/Vista

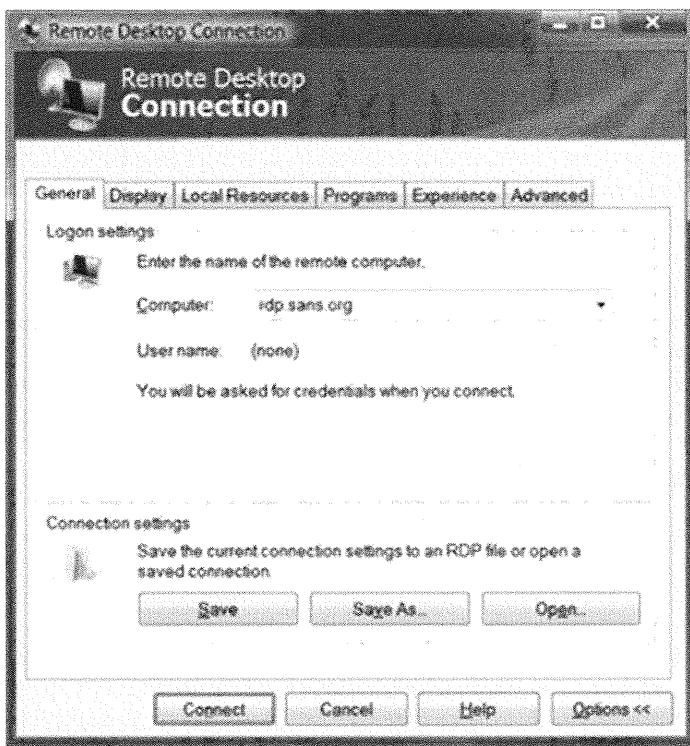
Terminal Services on Windows XP/Vista is called *Remote Desktop*. You enable/disable it using the System applet in Control Panel > Remote Settings link > Remote tab. Disable it, of course, if you don't plan to use it.

*Remote Desktop* prevents any user account with a blank password from connecting. By default, only local Administrators can connect, but in the System applet you can add other accounts, and you don't have to buy more licenses. If you are a non-administrative user, you only can connect when either no one is logged on at the remote system or when you are logged on there. If you already are logged on, the remote machine's visible desktop becomes locked. If you are a member of the local Administrators group, you can connect to any machine, but this action will forcibly log off any interactively logged-on user there.



### Remote Desktop Connection Client

Windows includes a thin-client application for connecting to remote desktops by default (MSTSC.EXE). Launch the client by going to the Start menu > All Programs > Accessories > Remote Desktop Connection, or, on Windows 8 and later, just type "remote desktop" in the Start screen.



Enter the IP address or computer name of the target, and you're ready to go! You also can click the Options button in the initial window to configure screen resolution, color depth, connection speed optimizations, and other settings. On the Local Resources tab, you can allow or disallow access to local drives, the clipboard, local printers, and other Plug-n-Play devices.

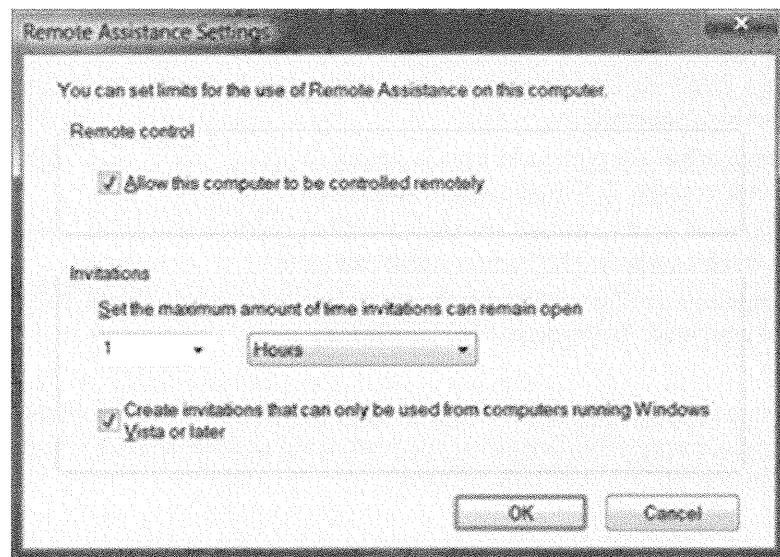
There even is an ActiveX control version of the client that can be loaded into web pages! This version is called the *Remote Desktop Services Web Access* on Server 2008-R2 and later. By default it creates a virtual directory on your website named /ts. Hence, browsers would connect to, for example, <http://www.sans.org/ts>, and the client will load into the web page displayed. Earlier versions of this product would download the ActiveX control, but RDP 6.0 and later just uses the local copy of the control because it's the same one used by the regular client.

### Remote Assistance

Remote Assistance is a feature related to Remote Desktop. The intent of Remote Assistance is to use the Remote Desktop capabilities to allow a trusted remote person to help troubleshoot problems on the local user's desktop. The local user sends an "invitation" via e-mail or Windows Messenger to the other person; the other person double-clicks the attachment in the invitation e-mail, which opens up a special Remote Desktop connection to the desktop of the person who sent the invitation. Both the local and remote users see the same active desktop, and, if granted permission, the remote user can even take control of the mouse and keyboard.

On Windows 7 you send a Remote Assistance invitation by going to the Start menu > All Programs > Maintenance > Windows Remote Assistance. This launches a wizard to walk you through the process. You can choose to send the invitation via e-mail or choose to create a separate invitation file on the hard drive. You choose for how long the invitation is good (from 1 minute to 99 days) and the passphrase the remote user must enter when connecting to the local system. This passphrase must be communicated to the remote user through some other channel, such as by phone or encrypted e-mail. The firewall will be adjusted to allow the in-coming connection automatically.

To configure the invitation policy on Windows 7, go to Control Panel > System > Remote Settings > Remote tab.



# Remote Desktop Protocol (2 of 3)

- **Windows Server 2003+SP1 and Later:**
  - Remote Desktop Protocol (RDP)
  - RDP operates on TCP/3389 by default
  - TLS encryption and server authentication
  - Digital certificate must be installed on server for TLS
  - TLS can be required or merely preferred
- **Windows Server 2008 and Later:**
  - Network Level Authentication (NLA)
  - RDP 6.x client built into Vista/2008 and later

SANS Security Essentials – © 2016 SANS

## Remote Desktop Protocol (2 of 3)

Terminal Services and Remote Desktop both use the *Remote Desktop Protocol (RDP)* on TCP port 3389. Windows uses 128-bit RC4 encryption by default, but Windows Server 2003+SP1 and later also support TLS encryption with server authentication, if a digital certificate is installed.

There are four possible encryption levels:

- **Low:** Client determines encryption strength and only data sent to the server is encrypted. Data received from the server is cleartext.
- **Client Compatible:** Encryption strength is determined by the client, but all data is now encrypted, both to and from the server. TLS is permitted if requested.
- **High:** Encryption is set to the server's highest level of encryption possible. Any clients that cannot support it will be rejected. TLS is permitted if requested.
- **FIPS Compliant:** Similar to High, but the algorithms used must be 3DES, AES, RSA and/or SHA. RC4 is not permitted. TLS is permitted if requested.

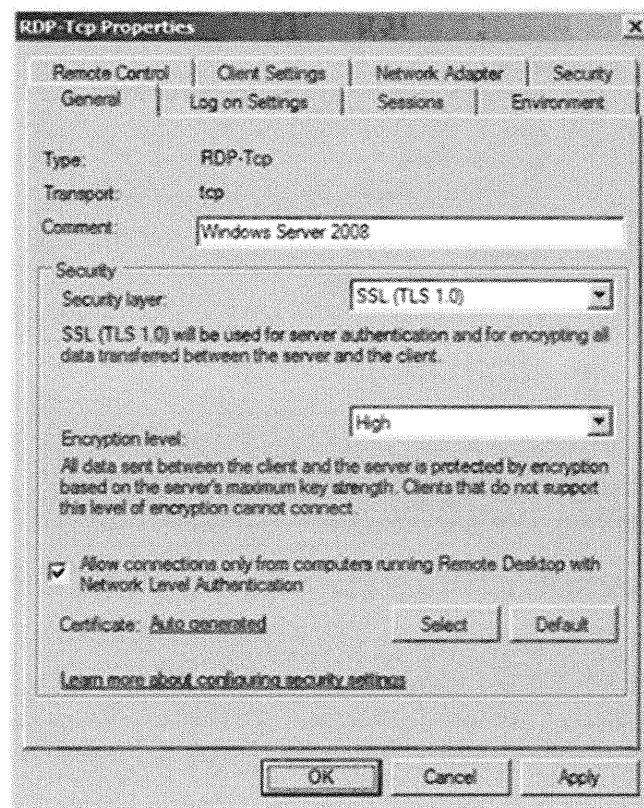
If TLS encryption is used, the packets do not use TCP port 443. The TLS-encrypted traffic still uses TCP 3389, but that channel's payload is now encrypted differently. If you want to tunnel RDP over HTTPS, install the Remote Desktop Services Gateway role on Server 2008-R2 or later.

To set your Terminal Server's encryption level to High, open the Remote Desktop Services Configuration snap-in in the Administrative Tools folder > Connections > right-click the RDP-Tcp icon > Properties > General tab > select High for the encryption level > OK.

On Windows Server 2003+SP1 and later you also have three choices for authentication:

- **RDP:** Uses native RDP encryption and authentication.
- **Negotiate:** Tries to use TLS, but falls back to native RDP if necessary.
- **SSL:** (*TLS 1.0*) is required. Native RDP encryption is not supported.

To set your Terminal Server's security layer to *SSL (TLS 1.0)*, open the Remote Desktop Services Configuration snap-in in the Administrative Tools folder > Connections > right-click the RDP-Tcp icon > Properties > General tab > select *SSL (TLS 1.0)* for the Security Layer > OK.



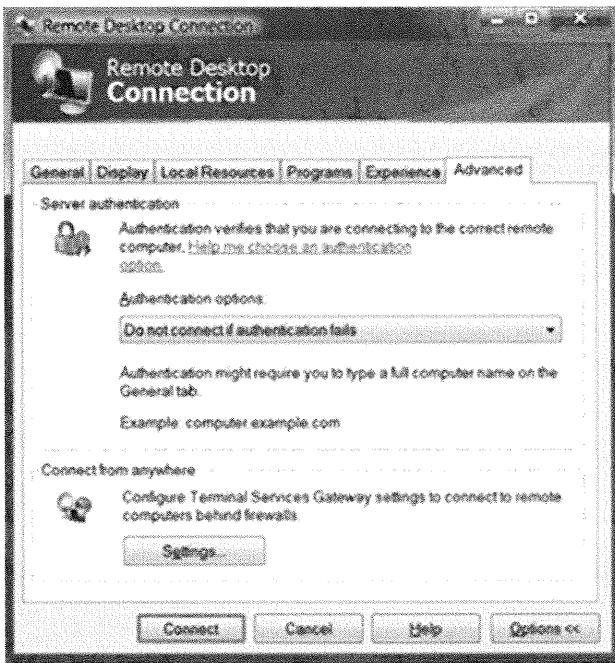
Keep in mind the TLS is only available if a digital certificate has been installed. The Windows PKI supports automatic installation of certificates through Group Policy. Clients will need to support RDP version 5.2 or later. Server 2008 and later support the ability to locally auto-generate a certificate if a PKI is not available.

Windows Vista and later come with the RDP version 6.0 at a minimum (KB925876). It's quite important to use version 6.0 or later for the sake of security. RDP 6.0 includes support for Network Level Authentication (NLA), which authenticates the client and server before a session is even created in the memory of the Terminal Server. NLA helps to prevent DoS attacks against the server and potential credentials-stealing attacks against the client.

To require NLA on Server 2008 or later, open the Terminal Services Configuration snap-in in the Administrative Tools folder > Connections > right-click the RDP-Tcp icon > Properties > General tab > check the box labeled "Allow connections only from computers running Remote Desktop with Network Level Authentication" > OK.

To require successful NLA on the client's side, open the Remote Desktop Client application > Advanced tab > set the authentication option to Do Not Connect if Authentication Fails. Remember, this requires client version 6.0 or later.

Windows 7/Server 2008-R2 and later include an RDP 7.0 client. The enhancements in RDP 7.0 are mainly for performance, not security, so for the time being an RDP 6.0 client is still considered the minimum.



In the screenshot above, note that NLA can be required for Remote Desktop access to Windows Vista too.

In Windows Server 2008 and later, RDP supports both NLA and domain account single sign-on, hence, after a user logs onto her desktop with a global user account, that user's RDP client can transparently authenticate to the Terminal Service without re-entering a password or smart card PIN number. This transparent authentication occurs after the NLA authentication of course, but the client will have to be Vista or later to make it all work seamlessly.

# RDP Best Practices (3 of 3)

- Require Network Level Authentication (in 2008 or later)
- Get latest version of thin client software from Microsoft
- Use smart card authentication for single sign-on
- Require TLS instead of RDP encryption whenever possible
- Require 128-bit (High) RDP encryption, if not using TLS
- Block access to local drives, clipboard, and PnP devices in thin client
- Disable Remote Desktop and Remote Assistance if not needed
- Require passphrase and a short TTL for assistance invitations
- Investigate Citrix as a cross-platform alternative

SANS Security Essentials – © 2016 SANS

## RDP Best Practices (3 of 3)

The following is a summary of the security best practices for both Terminal Services and Remote Desktop. Not all recommendations can be discussed in detail here.

- If possible, use Windows Server 2008 or later on the server to benefit from Network Level Authentication (NLA) and RDP single sign-on. The single sign-on works with either password or smart card authentication, so prefer smart cards too.
- Apply the latest Service Packs and hotfixes on both the RDP client and server.
- Prefer Windows Vista or later in order to obtain the single sign-on benefits.
- Make sure to block all unwanted TCP 3389 traffic at the firewall. Consider changing the default TCP port for RDP for a trivial bit of additional security through obscurity.
- Require 128-bit RC4 (High) encryption at the server at a minimum, and require TLS authentication and data encryption whenever possible.
- Consider blocking access to local hard drives, clipboard and PnP devices (except smart cards) from within the RDP client. These are potential malware vectors.
- Consider using IPSec or a VPN in addition to the RDP encryption if you are concerned about future RDP vulnerabilities.
- Use Group Policy to lock down the virtual desktops of thin-client users. Virtually every aspect of the user's desktop can be locked down this way.
- Disable Remote Desktop and Remote Assistance if you do not intend to use these features. Fortunately, this can be done through Group Policy, too.

- If you allow users to send Remote Assistance invitations, set the invitation expiration timer to a relatively short value (3 to 24 hours), and require a passphrase to connect. These options also can be configured through Group Policy.
- Do not allow clients to ignore certificate issuer warnings and to choose to connect to the RDP server anyway when there is an error during authentication of the server.
- If you will be using Remote Desktop Services for more than just remote administration, consider using Citrix to benefit from its enhanced management capabilities (<http://www.citrix.com>). Citrix also provides thin-clients for virtually all platforms desired, including Linux, Solaris, and Apple.

# Microsoft Cloud Computing

- Azure ([azure.microsoft.com](http://azure.microsoft.com))
  - IaaS, PaaS, and Azure Active Directory
- OneDrive ([onedrive.com](http://onedrive.com))
  - Personal or team file storage in Azure
- Office 365 ([office.microsoft.com](http://office.microsoft.com))
  - Office app subscriptions, e-mail, VoIP, IM, collaboration websites, e-discovery, etc.

SANS Security Essentials – © 2016 SANS

## Microsoft Office 365

You might love cloud computing or hate it, but it's in your future to some degree. As an IT professional working with Microsoft products and operating systems, you'll be expected to have at least a general familiarity with terms such as PaaS, IaaS, Office 365, and Azure. Unfortunately, Microsoft has a rather large set of cloud services with confusingly similar names. Below is a glossary of these terms for reference. This is not an endorsement of these services, or even an endorsement for cloud computing in general, but just to be familiar with the concepts.

If you're not sure where to start to see the Big Picture of what Microsoft is up to, start with <http://azure.microsoft.com> for Azure; then see <http://office.microsoft.com> for Office 365, which runs on top of Azure. You can experiment with many features for free to get a feel for what's possible.

## Categories of Microsoft Cloud Services

In general, there are three categories of Microsoft cloud services: Free, Hybrid, and Full.

- 1) There are free services to entice consumers to start them down the path toward cloud computing (OneDrive, Outlook.com, Skype, Office Online, and Office Mobile), and these services are indeed useful, but they also lack the full functionality needed by enterprises. These services are teasers, but they also train and familiarize the public on the use of Microsoft's cloud services in general.
- 2) Then there are various paid subscription versions of a few essential applications, such as e-mail and document collaboration, and these do have most of the functionality wanted, but they are sold and accessed separately (Exchange Online, SharePoint Online, Skype for Business, and OneDrive for Business). These offerings are aimed at those organizations that require a hybrid approach to cloud computing, doing a mixture of both on-premises and cloud-based services simultaneously. To Microsoft, these are also transition services, to help ease the way toward eventually doing everything in Microsoft's cloud.

- 3) Finally, there is the full cloud experience (Office 365 and Azure AD), sold for a per-user monthly subscription price, that aims to move almost all of your data and applications up to Microsoft's servers. Office 365 comes in a confusing array of bundles (Personal, Home, ProPlus, Small Business, Small Business Premium, Midsize Business, and Enterprise) and there are special programs for governments, schools, and nonprofits, too. Office 365 is also compatible with a hybrid solution, but a hybrid in which most data and applications are hosted in Azure, not on premises. Office 365 is Microsoft's ultimate goal, it's the cloud-based Rome toward which all Microsoft roads lead.

## Glossary of Terms

Here is a glossary of Microsoft cloud computing terms.

**Azure** ([azure.microsoft.com](http://azure.microsoft.com)) is Microsoft's global collection of datacenters to implement Microsoft's cloud-based services. Azure consists of more than a million servers, millions of Hyper-V virtual machines, and thousands of networking devices such as switches and routers. But the term Azure also refers to the custom software necessary to manage all this hardware for the sake of multi-tenant security, geo-redundant backups, fail-over, load balancing, VM provisioning, software-defined networking, health monitoring, patch management, customer billing, fraud detection, identity management, multi-factor authentication, and so on. Hence, Azure is the hardware and software platform that makes Microsoft's cloud services possible.

**OneDrive** ([onedrive.com](http://onedrive.com)) is for Internet-accessible file storage in Azure. OneDrive supports mobile devices, local folder syncing, Xbox game data, and Office 365 document storage. It starts free, and then the price increases with additional storage. OneDrive is mainly intended for personal use and is managed by the individual user. OneDrive (previously known as "SkyDrive") competes with Apple iCloud, Google Drive, and Dropbox.

**OneDrive for Business** is not the same thing as OneDrive, even though it is also for file storage. OneDrive for Business is purchased as part of an Office 365 subscription and is centrally managed by an organization's IT department. It has some SharePoint-like features, but it is not the same as a full SharePoint team site either.

**SharePoint Online** is for cloud file storage for multiple teams or projects, content management, live collaboration, enterprise social networking, and e-discovery for regulatory compliance. It is purchased separately or as part of an Office 365 subscription.

**Skype** ([skype.com](http://skype.com)) is for cloud chat, voice over IP, video-conferencing, and desktop sharing. It starts free, then Skype-to-phone and international calling requires the purchase of "minutes" or the purchase of an Office 365 subscription, which includes some number of "minutes" as part of the package. Skype for Business (previously known as Lync) includes extra enterprise features and integrates further with Office 365.

**Exchange Online** is for cloud e-mail, calendar, contacts and voicemail. It is intended for business or team use, and would be managed by an organization's IT department. It's not just personal messaging, it also supports enterprise features such as e-discovery, DLP, and Rights Management Services, and is deeply integrated into Azure AD. It is not free, and it is purchased separately or as part of an Office 365 subscription.

**Outlook.com** was previously known as HotMail and is not the same thing as Exchange Online. Outlook.com includes free e-mail, calendar, contacts and OneDrive-integration features. It is intended for personal use and competes with Google Gmail and Yahoo Mail.

**Intune** is for the inventory and management of BYOD hardware devices, including Android, Apple iOS, Windows, Windows RT and Windows Phone. It can enforce MDM security policies, inventory operating system versions, and inventory installed apps; remotely install apps; apply software updates; and perform remote data wipe, remote lock, and remote PIN reset. It's purchased on a per-device monthly subscription fee. Eventually, Intune and System Center Configuration Manager (SCCM) will become merged into a single product.

**Microsoft Office** "local install" or "desktop install" is the traditional bundle of Microsoft Office applications that have existed for over a decade, including Word, Excel and PowerPoint. The point of this terminology—calling it "local" or "desktop"—is that these applications are not cloud-based, they do not require Internet access to run, and their binaries are installed and run from the local hard drive. The Office binaries can be installed using traditional MSI package files or streamed over the Internet using the Click-to-Run feature in just a few minutes. The applications are also typically licensed per-device, not per-user. A local install of Microsoft Office is included in some Office 365 packages.

**Office Mobile** includes miniaturized versions of some of the Office apps for installation on Apple iPhone, Android, and Windows Phone. These apps are installed locally to the phone, and not run over the Internet. The apps are free, but are limited in functionality to entice users to purchase full Office 365 subscriptions.

**Office Online** ([office.com](http://office.com)) is for browser-based, free, cloud versions of Microsoft Word, Excel, PowerPoint, Publisher, and OneNote. Client platforms include Windows, Android, and Apple iPad (and eventually Xbox, too). But be careful; know what you're *not* getting. At the time of this writing, Office Online permits only the saving of documents to OneDrive; you cannot save document files directly to a local drive! Office Online is the free teaser version intended to increase sales of Office 365 subscriptions.

**Office 365** ([office.microsoft.com](http://office.microsoft.com)) is the paid subscription version of Office Online, but without the limitations of the free version. Office 365 is what Microsoft really wants you to use; it's the ultimate goal. All Office 365 subscriptions include OneDrive for Business with more storage space, personal DNS domain names, public website hosting, SharePoint team sites, shared calendars, and Skype integration. Some subscriptions include local desktop installs of the Office applications (both Windows and Mac), enterprise social networking (Yammer), e-discovery for regulatory compliance, Skype voicemail, and Office Mobile apps, too. Office 365 subscriptions are typically licensed per user, not per device. Office 365 uses Microsoft Azure Active Directory (MAAD) for authentication and identity management. In many ways, Office 365 is more important to Microsoft and its future plans than Windows.

**Azure Active Directory** (Azure AD) is the identity and authentication provider in Azure for Office 365, Intune, Outlook.com, OneDrive, Skype, and eventually every cloud service from Microsoft. In fact, Microsoft's aim is for Azure AD to be the identity provider for every web application in the world, providing global single sign-on (SSO) to everything. Azure AD provides optional single sign-on support for more than 1,400 websites, including Facebook, Twitter, Google Apps, Intuit, Dropbox, SalesForce, and Evernote. In Windows 8 and later, users can link their local or on-premises Active Directory account to their Microsoft Account in Azure AD, so that logging onto one's laptop also logs one into Azure AD transparently at the same time. Azure AD doesn't just run on top of Azure, it is a major part of what Azure *is*. When an organization signs up for Office 365, the organization also gets a new domain in Azure AD automatically as a part of the package. Just as you have on-premises Domain Admins, so you also have Azure AD admins managing your tenant user accounts through PowerShell or the Azure web portal.

**Infrastructure as a Service (IaaS)** is what a cloud provider offers when the provider will host the virtual machines of the customer and do little else. (The customer is called a tenant, as in a tenant of a shared apartment building.) The provider sells tenants Internet bandwidth, dynamic or static public IP addresses, VM and data storage space, CPU cycles for their VMs, back up and restore VMs after a failure, and other basic VM services, but the IaaS provider doesn't really know or care what is going on inside tenants' VMs. In fact, IaaS providers might not even offer licenses for the operating systems running in their tenants' virtual machines. Azure is an IaaS provider, even for Linux VMs.

**Platform as a Service (PaaS)** is what a cloud provider offers when the provider makes available virtual machines with licenses, plus most of the additional applications and services developers need to build and run their own applications hosted on the PaaS provider's network. Developers often need a web server (IIS), database server (SQL Server), and source code management (Visual Studio). Developers do not want to worry about patch management, load balancing, backups, capacity planning, OS upgrades, provisioning VMs, or other such details—these are the headaches of the PaaS provider. Azure is best known as a PaaS provider.

**Software as a Service (SaaS)** is what a cloud provider offers when the provider manages everything except the contents of its customers' data. In exchange for a monthly fee, the SaaS provider manages the hardware, bandwidth, storage, VMs and, most important, the source code of the applications used by the tenants. Other than reporting bugs and making feature requests, the tenants do not control the source code of the applications they run, the tenants control only their own data (and perhaps some application preference settings). Often, tenants' data resides on the VMs hosted by the SaaS provider, but this is not required. Office 365, OneDrive, Outlook.com and SharePoint Online are examples of SaaS offerings. In a way, Azure AD is itself an SaaS application, but it mainly exists for the sake of Office 365 though.

# Office 365 Security Best Practices

- Enforce good endpoint security
- Remote wipe lost or stolen devices
- Plan your Azure identity management
- Secure your Azure AD admin accounts
- Require multi-factor authentication
- Use the built-in DLP features

SANS Security Essentials – © 2016 SANS

## Office 365 Security

After you move to Office 365, you have lost control over the servers and their management. If you are unhappy about how Microsoft implements Azure and Office 365, there is almost nothing you can do about it except to move everything back on-premises or to move to another cloud provider. If you want to read Microsoft's public story about security for Azure and Office 365, feel free to do so (<http://trust.office365.com>), but, in the end, all we actually have is trust and hope.

## Endpoint Security

What we mostly have control over are the client devices. Because desktops, laptops, tablets, and phones are more easily hacked or malware-infected, client devices will also be the source of most of our security compromises. Office 365 security begins with good endpoint security. We want recent operating systems, update-to-date patches, limited administrative powers, host-based firewalls, antivirus scanners, application whitelisting, secure configurations, and everything else we have discussed. When it comes to cloud computing, most IT people worry about the networks of the cloud providers, but actually they should be more worried about the devices in the hands of their users.

## Remote Wipe

Mobile devices will inevitably be lost or stolen. Plan for this by requiring whole drive encryption, user authentication to unlock the device (PIN, picture password, virtual smart card, or similar) and automatic backup or sync of device data over the Internet or through a VPN. Train users to report lost or stolen devices as quickly as possible, and then remotely wipe these devices, change the user's passwords, reissue new user certificates and revoke the old certificates.

## Hybrid Identity Management

You will likely have a hybrid identity solution with both on-premises Active Directory and also user accounts up in Azure Active Directory. Carefully plan whether and how you will sync on-premises identity data with Azure

AD. Will you sync nothing so that users will have multiple accounts and passwords? Will you set up a gateway for Active Directory Federation Services (ADFS) to forward Azure AD authentication requests? Only sync changes in one direction, perhaps from on-premises AD up to Azure AD? Fully sync in both directions? Or will you eliminate your on-premises Active Directory entirely and go full cloud? These are complex issues that cannot be discussed here at length, but your overall mobile identity solution should be planned and managed. For guidance and AD synchronization tools, see <http://azure.microsoft.com>.

### Azure AD Admins

Just as you have Domain Admins group members in your local on-premises Active Directory, so you will also have Azure administrative accounts. These Azure admin accounts should not be used for anything other than managing your Azure and Office 365 resources. Log in with Azure admin accounts only on trusted and hardened computers, such as on VMs dedicated for this purpose. Change the passphrases of these Azure admin accounts every 30–90 days or use multi-factor authentication when appropriate.

### Multi-Factor Authentication

Azure AD support multi-factor authentication through users' phones. At logon, a random PIN number can be sent to the user's phone through SMS, which the user would type into their browser or other application. Or the user could have that PIN pushed to an app on their phone. A third option would be for Azure to dial the user's phone number and ask the user if it actually is that user attempting to log on, and, if not, to press a different button to indicate that it was unexpected and therefore may be a hack attack. Finally, instead of a phone call, a prompt could be pushed to an authenticator app on the user's phone to confirm yes/no that the authentication attempt is expected. Using multi-factor authentication is highly recommended for both users and admins. Planning for it is an important part of planning your overall identity solution. Fortunately, most of the complexities are handled on the Azure side, so setting it up in your admin center web portal is not excessively difficult.

### Data Loss Prevention

Data Loss Prevention (DLP) is a set of technologies to identify, inventory, monitor, and restrict access to sensitive information, especially information that might leak outside the organization to the Internet. Office 365 includes a number of DLP features that go beyond just assigning permissions, especially for SharePoint and Exchange. Because you are already paying for these services, investigate the DLP options for e-discovery, auditing, message encryption, document encryption, Information Rights Management (IRM), Mobile Device Management (MDM) policies, e-mail attachment transport rules, Outlook pop-up tips about PII contents, document fingerprinting by similarity, and other options.

The screenshot shows the Microsoft Office 365 Admin Center interface. The top navigation bar includes links for InPrivate, https://portal.office.com/UserManagement, Active users, Office365, Outlook, Calendar, People, Newsfeed, OneDrive, Sites, Admin, and Help. The main title is "Office 365 admin center". A search bar contains the name "Eric Cole". Below the search bar are links for active users, deleted users, security groups, and delegated admins. On the left, a sidebar menu lists dashboard, setup, users and groups (which is currently selected and highlighted in blue), domains, billing, service settings, service health, reports, and support. The main content area displays a table of active users. The table has columns for DISPLAY NAME, USER NAME, and STATUS. One row is visible, showing Cicero Plutarch, jason5@sans, and in cloud. There are also icons for adding a new user, deleting, and searching.

That being said, what are some best practices for securing the use of Office 365? What *can* we control?

### **Endpoint Security (Pre-Compromise)**

Most exploits will target the users and clients accessing Office 365, not the Azure servers themselves. Hence, focus on upgrading client operating systems, patch management, getting users out of the Administrators group, application whitelisting, anti-malware scanners, host-based firewalls, user training, and everything else discussed this week for endpoint security.

For BYOD tablets and phones, invest in a Mobile Device Management (MDM) solution which allows some amount of centralized control over these devices, e.g., VMware AirWatch, Microsoft Intune, and similar MDM products. For example, using MDM policies, require disk encryption and PIN unlock on mobile devices.

### **Remote Wipe (Post-Compromise)**

Inevitably, client devices using Office 365 will be lost, stolen, or infected with malware. Be prepared to wipe these devices, to reset user passwords, and to review possible theft or malicious changes to your data in Azure. Train users to notify the help desk promptly when their devices have gone missing or show signs of infection.

### **Azure Identity Management of Microsoft Accounts**

There are a variety of options for user identity management related to Office 365. Will users have different passwords for their Microsoft Accounts versus their on-premises Active Directory accounts? Will users be permitted to link their on-premises AD accounts to their Microsoft Accounts on Windows 8 and later? Will you automatically sync on-premises AD password changes up to Azure AD? Will password changes in Azure AD sync down into your on-premises local AD? Will you install an Active Directory Federation Services (ADFS) server in your local DMZ to proxy authentication requests from Azure AD to your internal on-premises domain controllers? These are complex problems that cannot be discussed here at length, but they do need to be carefully planned.

In general, you will have more control and potentially better security if you use local Active Directory Federation Services (ADFS) servers, but ADFS requires the most work. With ADFS, when one of your users authenticates to Office 365, a server in Azure will relay the authentication request to your own ADFS server in your DMZ, your ADFS server will authenticate the user against your internal on-premises domain controller, then relay the results of the request back up to Azure, which will then allow/block the user attempting to log into Office 365. ADFS limits the information synced to Azure AD and provides more customizable control, but is unfortunately far beyond the scope of this course.

### **Multi-Factor Authentication**

Microsoft Accounts in Azure AD can be configured to require multi-factor authentication, which is highly recommended. There are several options:

- 1) user is called on their mobile phone and prompted to press the pound key if the call from Azure was expected,
- 2) user receives a PIN by text message,
- 3) push notification to a phone app to confirm the authentication attempt, or
- 4) push notification to a phone app with a PIN.

When a PIN is sent by text message or phone app, the PIN must be entered in the Office portal web page in addition to the user's password. The password itself, of course, should be as long and complex as users will tolerate. If the user is simply called and asked to confirm the authentication attempt (option #1), the user is also told to press a different key sequence if the attempt was unexpected, which can send an alert to the Azure AD

administrator for the user's organization. Microsoft also sometimes requires multi-factor authentication when a user attempts to log on at a time or from an IP address which is very unusual for that user (Azure AD tracks and remembers prior successful authentications to learn what is "normal" for a user).

Enabling multi-factor authentication is relatively simple to do in the Office 365 admin center (log into Office 365 with your admin account, click the Admin link, go to Users and Groups).

### Azure and Office 365 Administrative Accounts

When a new tenant is created for Azure AD or Office 365, there will be at least one Microsoft Account marked as the administrator for that tenancy. More administrative accounts can be added later and it's possible to delegate some administrative responsibilities to other users, such as to consultants or third-party management companies.

Audit and protect these administrative accounts in Azure just as you would your on-premises Domain Admin accounts. For example, an administrator should have at least two Microsoft Accounts and only use their tenant admin account when necessary; administration of Azure AD or Office 365 should only be performed from a computer or VM dedicated for this purpose; admins should use long complex passphrases when multi-factor authentication is not available, and these passphrases should be changed at least monthly. Your Azure AD or Office 365 tenancy can be managed through PowerShell, so a bit of PowerShell scripting can be used to query for unexpected changes or to do bulk administration.

But if an attacker gets the passphrase to your Azure AD admin account, the attacker could also use PowerShell to inflict massive damage within seconds. If this occurs, contact Microsoft immediately, they are sometimes able to undo accidental or deliberate changes like this (there are rollback and recovery features built into Azure AD).

### Rights Management Services (RMS) and DLP

Office 365 supports built-in Data Loss Prevention (DLP) features which should be investigated, especially when the leakage of user data files to outsiders would cause serious harm. These DLP features are integrated into Azure Rights Management Services (RMS) and Office 365. RMS can encrypt data files in case the files leak outside of Office 365. There are also integration options between Azure RMS and your local on-premises SharePoint and Exchange servers, especially if you are already using RMS internally.

A nice DLP capability is being able to upload a few examples of restricted files and basically telling Azure RMS "these are the kinds of files which should not be allowed to be e-mailed to outsiders" and Azure RMS will try to extract common patterns from within the example files. False positives are a problem for any DLP solution, so Azure RMS can be configured to either block the e-mailing of restricted files or to just warn the user. You can also define your own templates for (un)restricted files and how these files are handled.

The DLP and RMS features of Office 365 cannot be discussed here, but they should be at least researched (you would be paying for them already).

### Local Encryption Key Management

Remember, no matter what Microsoft says about this issue, Microsoft *can* access your data. And anyone else who completely compromises your Azure datacenter can access your data too, even if this would be extraordinarily difficult or unlikely. Your only possible defense against these kinds of threats is to encrypt your data *before* it is uploaded to any Azure server, using encryption keys you've generated yourself, and these keys can never be exposed to Azure either.

Of course, this kind of encryption means your data could never be created or edited using any Office 365 web applications, which mostly defeats the point of using Office 365 in the first place. It also means you won't be

able to do keyword indexing, document/message searches, legal e-discovery, DLP filtering, and many other tasks in Azure with your data, such as letting Cortana help manage your calendar.

However, it should be practical to encrypt backup archives before uploading to Azure, as long as the files being backed up were never in Azure to begin with. And it should be practical to use S/MIME encryption of e-mail, which protects messages end-to-end, so that you don't have to trust Microsoft or any other ISP. Be careful, though, it can be easy to accidentally expose your users' S/MIME private keys to Azure without knowing it; for example, using Outlook Web Access (OWA) with Exchange Online, or linking the on-premises accounts of your users to their Microsoft Accounts with password roaming feature enabled, might result in accidental exposure of your users' private keys. One little checkbox or undocumented feature could undermine all your efforts if your (impossible?) goal is to use cloud services from providers you don't really trust.

Another possibility with Azure RMS is the capability to load your own private keys into a Hardware Security Module (HSM) hosted at a Microsoft datacenter, but this scenario will be rare due to the RMS dependencies and the hassles involved. Theoretically, not even Microsoft will be able to tap into the HSM to extract your RMS private keys, but there may still be flaws in how the keys are given to Microsoft in the first place. Again, it really depends on the exact details, which we just cannot dive into here.

#### **Vendor Lock-In and the Office 365 Terms of Use**

The dream of any cloud provider is to keep you paying your monthly subscription fees to the provider...forever. So, while it might be theoretically possible to move your documents, e-mails, web applications, and virtual machines from Azure to another cloud provider, or to move them all back home again, is this really practical? Could you afford the disruptions and user re-training this might require? Vendor lock-in can be a kind of self-inflicted DoS attack. And, legally, what is preventing Microsoft from changing their "Terms of Use" tomorrow and giving you a one-year deadline to either agree or hit the road? Nothing. So there are traditional IT security risks from hackers and malicious insiders, but there are also larger risks at the CEO/CIO level when getting married to a cloud provider.

# Summary

- The best way to secure a service?
- Windows Firewall
- IPSec
- SCW.EXE
- SCWCMD.EXE
- Server Manager:
  - Roles
  - Features
- IIS Web Server Security:
  - Clean install
  - Script mappings
- Remote Desktop Services:
  - TLS Encryption
  - Network Level Auth
- Azure and Office 365

SANS Security Essentials – © 2016 SANS

## Summary

The purpose of this module was to describe some general techniques for securing network services and to discuss specific hardening steps for IIS and Remote Desktop Services in particular. Especially for IIS, the goal is to create a *bastion host*, that is, a specially hardened box that, hopefully, can withstand tomorrow's new batch of exploits and attack tools. We're doomed to failure, of course, but there's a huge difference between failing occasionally and getting hacked every other day of the week.

The best way to secure a service is to uninstall it. Short of that, you also can filter all packets to/from it with a personal firewall and encrypt its packets with IPSec.

IIS probably is the most-hacked web server in the world, so it is imperative that you harden those boxes. A few simple changes can improve your threat exposure, such as unmapping unused script handlers and removing other unnecessary components.

Remote Desktop Services is very popular, but it's also dangerous because it grants complete remote control over the target system. And it's built into Windows as the Remote Assistance feature. Use only the "high" or TLS encryption for the RDP protocol; apply the latest hotfixes; disable RDP if you're not going to use it; and train users to send passphrase-protected invitations with short TTL's only to people whom they know and trust.

Finally, the Security Configuration Wizard, like SECEDIT.EXE for security templates and MBSACLI.EXE for patch scanning, is scriptable! This makes a very nice addition to your arsenal of tools that can be automated when you have many servers to secure.

# Module 28: Automation, Auditing and Forensics

SANS Security Essentials – © 2016 SANS

## **Module 28: Automation, Auditing and Forensics**

This section intentionally left blank.

# Windows Automation, Auditing and Forensics

The student will be introduced to the techniques and technologies used to audit Windows hosts.

SANS Security Essentials – © 2016 SANS

## **Windows Automation, Auditing and Forensics**

This section intentionally left blank.

# Automation, Auditing and Forensics

## SANS Security Essentials V: Windows Security

SANS Security Essentials – © 2016 SANS

### Automation, Auditing and Forensics

Auditing is the gathering and analysis of detailed information about our own networks. But why audit at all? What's the point?

*The Cuckoo's Egg* is a novel about a network administrator who, in the course of investigating a 75-cent billing error, discovered a hacker who had been sifting through classified American military networks for *months* during the Cold War. The hacker had been gathering anti-ballistic-missile secrets and selling them to the KGB. The story tells how the administrator helped trace the hacker back to his base in Germany and expose the entire espionage ring. The story is fascinating, but it's also true! It was written by the network administrator himself, Clifford Stoll. *The Cuckoo's Egg* really is a detective story, but instead of a crime scene with a dead body, there's a network and the hidden world behind it. *The Cuckoo's Egg* is actually an auditing and forensics story.

This module discusses some important auditing and forensics activities as they relate to Windows security, namely:

- Verifying Policy Compliance
- Vulnerability Scanning and Reporting
- Creating Baseline System Snapshots
- Gathering Ongoing Operational Data
- Employing Change Detection and Analysis

These topics each are vast in themselves, so we'll simply examine the essentials. First, though, examine automation, that is to say, everything you can do with Windows that does not require a mouse.

*Automation* is how to get your work done more quickly and easily. In short, it's how to accomplish things with scripts, command-line tools, and the Task Scheduler. The good news is that Windows can be managed almost entirely through command-line tools and scripts.

Automation, auditing, and forensics go together because if you can't automate your work, then the auditing and forensics work just doesn't get done, it's done only sporadically, or you can't make it scale beyond the small number of machines you can physically touch.

Besides, learning automation techniques is how you can get *paid more for working less!*

# Automation

- **95% of what can be done with graphical tools can be done from the command line and your own scripts instead!**
- **There will be many security and auditing tasks that require command-line tools or scripting skills**
- **Stand out from the crowd!**

SANS Security Essentials – © 2016 SANS

## Automation

You can manage virtually every aspect of your computer without graphical tools. Ninety-five percent of what can be done with the graphical tools, such as the applets in the Control Panel, can be done from the command line instead, especially with PowerShell. And for auditors, the quantity of information that is extractable through scripts and command-line tools is vast.

Not every security task can be accomplished by clicking a button in a graphical interface. Every environment is different. It's not possible for software vendors to anticipate every problem you will face, every report you will need to generate, or every custom change you'll need to make. To go beyond what is provided in the graphical interfaces of the tools the vendors provide, you likely need to script the solution yourself.

Indirectly, this course is also about job security, not just network security. There's an economic recession roughly every 4 years. With the trends toward cloud computing and BYOD, organizations are discovering that they need fewer IT staff today than they did in the past. So, when the next recession comes, how can you stand out from the crowd to either keep your job or to find a new job? Having scripting skills is a great differentiator. Anyone can read a help file and click Next, but if you are comfortable at the command line and can write scripts, even short basic scripts, you have a skill that is more rare and valuable.

In Linux land, the dominate scripting languages are bash, Python, and Perl, but in Windows world, everything under the sun is moving toward PowerShell.

# Microsoft PowerShell

- **PowerShell for Windows Scripting:**

- It's a free command shell to replace the old CMD.EXE
- It's installed on Windows 7, Server 2008, and later by default
- <http://www.microsoft.com/powershell/>

- **Thousands of cmdlets for almost every task:**

- Including for VMware, Amazon Web Services, and others

- **PowerShell Remoting:**

- Run commands and scripts remotely
- Supports Kerberos and SSL/TLS

SANS Security Essentials – © 2016 SANS

## Microsoft PowerShell

Microsoft PowerShell is a command shell and the scripting language for it. PowerShell replaces CMD.EXE as "the" command shell on Windows, but don't worry, the old CMD shell will still be installed for at least a decade more. PowerShell is in the process of replacing traditional command-line binaries such as NETSH.EXE, WMIC.EXE, and IPCONFIG.EXE, and every year more and more graphical tools morph into wrappers on top of PowerShell. All automation for Windows, Office 365, Hyper-V, and every other Microsoft product is being designed (or redesigned) around PowerShell. Microsoft is also encouraging third-party companies to write PowerShell tools for their own products. For example, do an Internet search for **PowerShell for VMware** or **PowerShell for Amazon Web Services** and see what pops up.

## Requirements

PowerShell is built into Windows Server 2008, Windows 7, and later, and can be installed on Windows XP-SP2, Vista, and Server 2003-SP1. To download the latest version of PowerShell, visit <http://www.microsoft.com/powershell/>.

PowerShell is a .NET Framework application. It requires .NET version 2.0 or later to be installed. When a command is run in PowerShell, the output of the command is not text, the output is one or more .NET or COM objects. These objects have properties and methods. Think of PowerShell as a simplified version of C#.

## PowerShell Remoting

PowerShell can execute commands and scripts on remote computers. In a domain environment, the remote connection is authenticated with Kerberos and encrypted with a key derived from the Kerberos exchange. With or without Active Directory, though, certificates can be installed for the sake of SSL/TLS authentication and encryption, which is recommended when remoting over the Internet. On Server 2012, Windows 8 and later, remoting is enabled by default. On earlier operating systems, the Enable-PsRemoting command must be run first. Remoting operates on TCP ports 5985 and 5986 (for SSL/TLS) by default.

# PowerShell Examples

- Run **powershell.exe** and then:

- get-process
- get-process | export-csv outputfile.csv
- get-service
- dir hklm:\system\currentcontrolset
- get-help invoke-command -full
- get-help \*net\*

SANS Security Essentials – © 2016 SANS

## PowerShell Examples

We can't discuss the PowerShell language in detail here, but here are a few sample commands. Remember that the pipe symbol (" | ") in PowerShell can pipe full .NET objects with all their properties and methods. Almost nothing is case-sensitive in PowerShell. And if one of the following examples doesn't work, it might mean you have an old version of PowerShell. (Run \$PsVersionTable to see what your version is.)

You might want to create a shortcut on your desktop for powershell.exe and then right-click it and Run as Administrator. On Windows 8 and later, just start typing **powershell** while in the Start screen to find it. There is the text-oriented console PowerShell (powershell.exe) and the graphical PowerShell ISE (powershell\_ise.exe). The graphical PowerShell ISE has a toolbar, menus, and other items to make the coding more fun.

To see a list of running processes:

```
get-process
```

Pipe the output of any command into Format-List \* to see all properties in a list:

```
get-process | format-list *
```

To save the output of a command to a comma-separated values text file:

```
get-process | export-csv -path outputfile.csv
```

To see a list of running services:

```
get-service
```

To save a service report to an HTML for display in a browser:

```
get-service | convertto-html -property status,displayname | out-file report.html
```

To list the keys underneath HKEY\_LOCAL\_MACHINE\System\CurrentControlSet in the Registry:

```
dir hklm:\system\currentcontrolset
```

To see a list of local event logs:

```
get-winevent -listlog *
```

To show the last 20 events from the System log:

```
get-winevent -logname system -maxevents 20
```

To show only error events from the last 500 events in the System log:

```
get-winevent -logname system -maxevents 500 |  
where-object {$_.leveldisplayname -match "Error"}
```

The security log can be used to identify many interesting events by their unique event ID number. To list only the last 10 user accounts created:

```
get-winevent -logname security |  
where-object {$_.id -match "^624$|^4720$"} |  
sort-object -property timecreated |  
select-object -last 10
```

PowerShell also natively supports the Windows Management Instrumentation (WMI) programming interface, just like the WMIC.EXE tool. Here is an example of extracting BIOS information from the local computer.

```
get-wmiobject -query "select * from win32_bios"
```

To see the documentation on any command, use the Get-Help cmdlet:

```
get-help invoke-command -full  
get-help *net*
```

The Get-Help cmdlet is really the only one you have to memorize. Once you remember this one, all the others can be discovered. The -Full switch for Get-Help will describe each command-line parameter and show examples of use; for example, the Invoke-Command cmdlet is for PowerShell remoting to execute commands on other machines, so seeing examples is useful to quickly get going. You can also give Get-Help keywords with zero or more wildcards (like "\*net\*") to get a list of available related cmdlets.

Again, there is too little time to discuss PowerShell syntax today. The Securing Windows course at SANS (SEC505) includes a full one-day course on PowerShell, and you can download the sample scripts for this course from <http://cyber-defense.sans.org/blog/downloads> (all the scripts are in the public domain).

# Microsoft Resource Kits (1 of 2)

- **Packed with documentation, tools, and scripts**
- There are Resource Kits for IIS, Office, SQL Server, Exchange, etc.
- In the past, you had to buy hardcopies at the bookstore

SANS Security Essentials – © 2016 SANS

## Microsoft Resource Kits (1 of 2)

Microsoft *Resource Kits* are filled with command-line tools that can be leveraged for the scripting of security. Resource Kits are available for Windows, System Center Configuration Manager, SQL Server, Exchange Server, IIS, Office, and so on. *Resource Kits* are more-or-less mandatory for managing Windows networks. You can buy hardcopies with DVDs at the bookstore if you want, but you can also find their documentation, tools, and scripts for free on Microsoft's website.

To begin your search, start at <http://technet.microsoft.com> and follow the links to the various "TechCenters" to drill down into the category of product you want to manage. You can also usually jump straight to the product you want by entering its name in the URL to Microsoft's site. For example, go to <http://www.microsoft.com/sql> if you want to find more information about SQL Server, but you could also do other product names and it usually works.

The Windows Server Resource Kit contains many tools and scripts, and the next few tables list the most useful ones.

Regdmp.exe	Dump registry key/value data to stdout.
Regfind.exe	Search and/or replace registry data.
Regini.exe	Modify registry entries with a text file.
Sc.exe	Low-level query and control of services on remote systems.
Scanreg.exe	Search registry for key or value name.
Sclist.exe	List running services on remote systems.
Instsrv.exe	Install/uninstall services on remote systems.
Showpriv.exe	Show the privileges granted to a user or group.
Showacl.exe	Show NTFS permissions on folders and files.
Showgrps.exe	List the groups to which a user belongs.
Showmbrs.exe	List the members of a group.
Snmputil.exe	Query SNMP agents from the command line.
Srvcheck.exe	List shares and their permissions on remote systems.
Srvinfo.exe	Dump a variety of information from a remote system.
Where.exe	Find folders/files on local or remote file systems.

Table: Command-Line Tools for Batch Files

Autoexnt.exe	Enable a startup batch script, with no user logon required to run script.
Clip.exe	Copy data from StdIn to the clipboard.
Forfiles.exe	Operate only on selected file types, e.g., .TXT files only.
Freedisk.exe	Allow action if a certain percentage of disk space is free.
Gettype.exe	Return operating system type and version.
Sleep.exe	Make a batch script sleep for a specified period.
Choice.exe	Prompt user to make a choice during batch file execution.
Now.exe	Echo the current date and time.
Qgrep.exe	Quick GREP, with many optional arguments to control search.
Setx.exe	Set environmental variables.
Su.exe	Execute command under the context of a different user.
Timeout.exe	Cause a batch script to wait a period of time then continue.
Waitfor.exe	Batch file utility which either waits for or sends a signal across the network to coordinate the activities of multiple remote computers running batch files calling this utility.
Whoami.exe	Return the domain and username of the current user.

## Microsoft Resource Kits (2 of 2)

- **But now you can get it all online for free:**

- <http://technet.microsoft.com>
- <http://www.microsoft.com/Windows>
- <http://www.microsoft.com/WindowsServer>
- <http://www.microsoft.com/SQLServer>
- <http://www.microsoft.com/ProductNameHere>

SANS Security Essentials – © 2016 SANS

### Microsoft Resource Kits (2 of 2)

BinDiff.exe	Compare two files at the binary level; includes option to do bulk comparison of all files in two folders and their subfolders.
DiskPart.exe	Manage partitions, disk volumes, mirrors, mount points, etc.
DriverQuery.exe	List drivers and related information with filters (more verbose).
DS*.exe	DSget.exe, DSadd.exe, DSmod.exe, DSmove.exe, DSquery.exe, and DSrm.exe manage objects in directory databases, such as Active Directory.
EventCreate.exe	Write custom events to any local/remote Event Log.
EventTriggers.exe	Automatically execute a chosen command when an event of a specifiable description/ID/source/etc. occurs in a local or remote Event Log.
FSUtil.exe	Manage file system properties, such as quotas, hard links, reparse points, 8.3 name generation, etc.

GPResult.exe	Display Resultant Set of Policy (RSoP) for a particular user and computer from the command line (new version).
IPSecCmd.exe	Command-line IPSec management tool (replaces IPSecPol.exe).
LogMan.exe	Manage Event Trace Session logs and Performance logs.
NetSh.exe	Improved networking configuration tool (try "netsh.exe diag gui").
OpenFiles.exe	List opened files on local/remote systems.
ReLog.exe	Resample existing Performance log files.
Sc.exe	Improved service controller tool (new version).
SchTasks.exe	Manage scheduled tasks on local/remote systems (replaces at.exe)
TaskKill.exe	Kill processes and process trees (more flexible than Kill.exe).
TaskList.exe	List processes and related information with filters (more verbose than 2000 version).
TypePerf.exe	Write real-time Performance data to ASCII file or console.
Wmic.exe	Command-line WMI query and configuration tool. This definitely is a tool you should know about!

# WMIC.EXE

- **Can manage tons of configuration settings!**
  - Works on local or remote systems
- Show last Service Pack number applied:
  - wmic.exe os get servicepackmajorversion
- Show shared folders on remote system named Server52:
  - wmic.exe /node:Server52 share list brief
- PowerShell replacement for this tool:
  - Get-WmiObject

SANS Security Essentials – © 2016 SANS

## WMIC.EXE

PowerShell and WMIC.EXE can be used to get or set configuration data for a wide variety of settings by talking to the Windows Management Instrumentation (WMI) service on local and remote systems. The PowerShell equivalent of WMIC.EXE is Get-WmiObject and/or Get-CimInstance.

For example, to find out the number of the last Service Pack applied, you could run this command:

```
wmic.exe os get ServicePackMajorVersion
```

Note that you can run the tool against remote systems, too, using the "/node" switch.

So, to get a list of the shared folders at a remote computer with IP address 10.4.2.2:

```
wmic.exe /node:10.4.2.2 SHARE list brief
```

To dump a list of the programs that automatically execute at boot up (Registry Run key):

```
wmic.exe /node:10.4.2.2 STARTUP list full
```

In these commands you can get one particular value from a category of information (*os get ServicePackMajorVersion*) or do a brief/full listing of all the values from that category (list brief). Entering "wmic.exe /?" can display the categories of information available (OS, SHARE, STARTUP, etc.). Just run wmic.exe <categoryname> list full for each category shown when you run wmic.exe /?.

Later in this section is a batch script (SNAPSHOT.BAT) that uses WMIC.EXE extensively to dump information. See this script for more examples of usage.

# Network Configuration Tools

Other than PowerShell,  
these are your best  
command-line tools for  
managing networking →

PowerShell:

- More than 300 cmdlets
- `get-help *net*`

- WMIC.EXE
- NETSH.EXE
- GETMAC.EXE
- IPCONFIG.EXE
- ROUTE.EXE
- NET.EXE
- NETSTAT.EXE
- NBTSTAT.EXE

SANS Security Essentials – © 2016 SANS

## Network Configuration Tools

Virtually every setting related to networking can be queried and/or reconfigured through one of the following command-line tools:

- WMIC.EXE
- NETSH.EXE
- NETDIAG.EXE
- GETMAC.EXE
- IPCONFIG.EXE
- ROUTE.EXE
- NET.EXE
- NETSTAT.EXE
- NBTSTAT.EXE

NETDIAG.EXE is mainly a troubleshooting tool that can run a variety of tests and dump the output to the command shell. Execute `netdiag.exe /?` to see the available tests. Just execute `netdiag.exe /v` to run all of them. Execute `netdiag.exe /test:testname /v` to run a particular test and show even more data.

NETSH.EXE was modeled on the Cisco command-line interface in both purpose and feel.

Execute `netsh.exe` to get to the `netsh>` prompt. Enter `?` to see the commands available in this context. Enter `int` to go into the `netsh-interface>` context, and then enter `ip` to go into the `netsh-interface-ip>` context. In this context you can get or set the IP configuration of your network adapter cards (enter `set ?` and `show ?` to see the commands).

Notice that with the `et machine IPAddress` command, you can execute all these commands on a remote box at `IPAddress` as well. In the `advfirewall` context you can manage the Windows Firewall from the command line, too.

`GETMAC.EXE` retrieves the hardware addresses of remote computers, even on the other side of routers. Output can be formatted in a variety of ways for easy searching.

If you're not familiar with `NET.EXE` already, then execute `net.exe /?`. This shows the list of subcommands `NET.EXE` supports; for each possible subcommand displayed, you can enter `net.exe subcommand /?` for more information, for example, `net.exe accounts /?`. For auditing, `NET.EXE` can be used to show shared folders, drive mappings, account and group information, and running services. However, for anything `NET.EXE` can do, there are other tools that can do it better.

The other tools have been around for some time now. `NETSTAT.EXE` can show all listening ports, `IPCONFIG.EXE` a variety of IP settings, `ROUTE.EXE` the route table, and `NBTSTAT.EXE` NetBIOS-related data. See their command-line switches for more information.

### **PowerShell Replacements**

The previous command-line tools are not fully replaced by PowerShell until you have Server 2012, Windows 8, or later. But in these operating systems, there are hundreds of cmdlets related to networking, IPSec, firewall rules, network adapter management, route tables, IPv6, DNS, the software-defined networking features of Hyper-V, and more.

If you have Windows 8 or later, run this command to see your networking-related cmdlets:

```
get-help *net*
```

For example, to see your Windows Firewall rules related to file and printer sharing:

```
get-netfirewallrule -displaygroup "File and Printer Sharing"
```

To see the details of your network adapter interfaces:

```
get-netadapter | format-list *
```

To see the IP address(es) assigned to each network adapter:

```
get-netipaddress
```

To see how to change the IP address of a network adapter:

```
get-help set-netipaddress -full
```

To see your current IPSec connection rules, if any:

```
get-netipsecrule
```

# Other Free Toolsets

- **Microsoft SysInternals tools:**
  - Process Explorer, AutoRuns, PsExec, RootkitRevealer
  - <http://www.microsoft.com/sysinternals>
- **Linux-flavored tools for Windows:**
  - All of them compiled for Windows; no emulator required
  - <http://sourceforge.net/projects/unxutils/>
- **Python and Perl for Windows:**
  - <http://www.activestate.com>
  - <http://www.python.org>

SANS Security Essentials – © 2016 SANS

live.Sysinternals.com

## Other Free Toolsets

There are many excellent free toolsets available from Microsoft and others. These toolsets are simply invaluable from a security and auditing perspective. Some of the best are the following.

### SysInternals (<http://www.microsoft.com/sysinternals/>)

SysInternals was purchased by Microsoft, which has both good and bad aspects, but the SysInternals tools are just outstandingly useful. Literally set aside an entire day and do nothing but download and get to know the SysInternals tools; they're that good. Process Explorer, for example, is a Task Manager replacement that provides deep visibility into the details of running processes. AutoRuns enables you to see and edit all commands that are automatically executed at boot-up and logon. PsExec is for remote execution of commands. RootKitRevealer can help to detect hidden rootkits. PsInfo shows a variety of computer configuration data, such as Service Pack, patches installed, software installed, and so on. And there are *a lot* more than just these.

**Note:** If you specify a username and password at the command line with PsExec.exe, the password will be transmitted in plaintext; so either use single sign-on instead of an explicit password or use IPSec to encrypt the password in transit.

### Scripting Support and Linux-Flavored Tools

Microsoft wants to compete head-on with Linux, BSD, and the other \*nix-flavored operating systems, which have wonderful scriptability. So virtually every aspect of the Windows operating system, filesystem, IIS, Active Directory, Exchange Server, SQL Server, the Office applications, and so on can be managed through custom scripts. For example, your scripts can use the same Windows Management Instrumentation (WMI) interface that the previous WMIC.EXE tool uses. And these scripts can be written in Perl, Python, JavaScript, VBScript, or PowerShell. (See <http://www.activestate.com> for free Perl and Python interpreters designed for Windows.)

If you're looking for Windows versions of UNIX/Linux tools such as grep, sed, cat, diff, dd, find, cut, sort, tail, less, wc, and so on, then visit <http://sourceforge.net/projects/unxutils/>. (Note: there's only one "i" in "unxutils" in the URL.) These GNU-licensed free tools run natively in Windows and therefore do not require an emulator.

### **How to Change Your PATH**

When you do add all these scripts and tools to your machine, you'll likely want to change your PATH environment variable to include the folder(s) where you installed them. In a CMD.EXE shell, if you run "set" you'll see your environment variables printed. One of them is the PATH variable, which determines the folders through which your computer searches when you simply execute the name of a script or binary without specifying its full directory folder path. For example, you can be in any folder in your CMD shell and still view your IP addresses by running ipconfig.exe /all even though that tool is not in the present working directory.

How? By adding more folders to the PATH variable, you can use your new scripts and tools much more easily because you won't have to enter the full folder path to them every time just like you don't have to enter the path to IPCONFIG.EXE.

On most versions of Windows you change your PATH variable by opening Control Panel > System applet > Advanced System Settings link (or Advanced tab) > Environment Variables button > select the PATH system variable at the bottom > Edit > append the full path(s) to your script or program folder(s), separating each full path with a semicolon. When you finish, close your CMD.EXE shell, relaunch it, execute "set" and you'll see the changes to your PATH.

# Push Scripts with Group Policy

- Group Policy can distribute scripts to machines and have the scripts automatically run:
  - **Startup** (runs as System)
  - **Shutdown** (runs as System)
  - **Logon** (runs as User)
  - **Logoff** (runs as User)
- Each OU could have its own set of scripts, written in different languages, customized for the needs of the computers and users in each OU

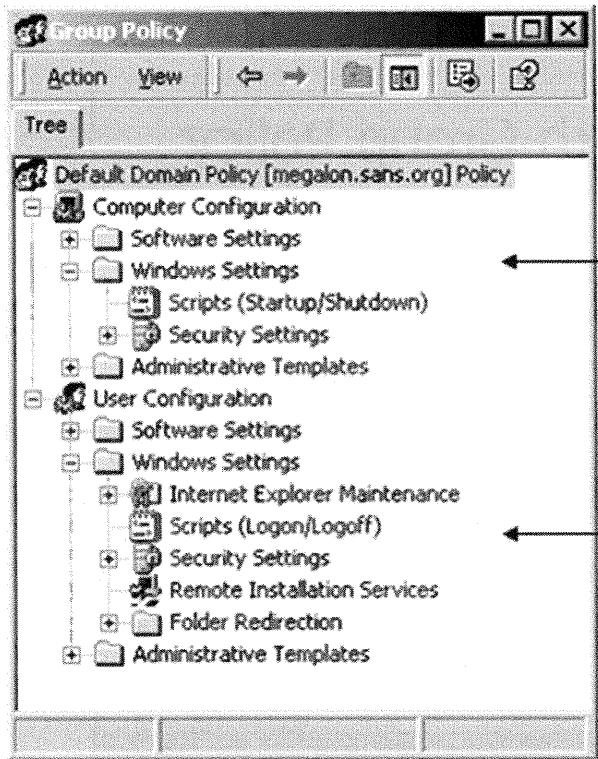
SANS Security Essentials – © 2016 SANS

## Push Scripts with Group Policy

It bears repeating in this context that Group Policy can push out scripts to machines automatically. And because Group Policy Objects can be linked to individual Organizational Units, each OU could have its own custom set of scripts.

These scripts can be executed at startup, shutdown, logon, or logoff. They can be written in any language for which the necessary interpreter is installed. Windows includes interpreters for batch files, Jscript, VBScript, and PowerShell, but interpreters for Perl and Python can be installed, as well.

You can push out as many scripts as you want, and you can mix scripts written in different languages in a single category, for example, your logoff scripts might include one batch file, two Perl scripts, and three VBScripts. Domain controllers multi-master replicate scripts to each other automatically using the File Replication Service (FRS). Logon/logoff scripts execute in the context of the user, whereas startup/shutdown scripts execute in the context of the local System account.

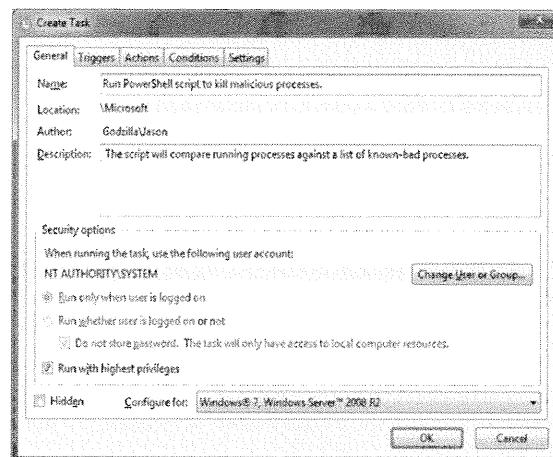


Startup/shutdown scripts are assigned to computers, independently of whoever logs on at them.

Logon/logoff scripts are assigned to users, and will follow users as they roam from computer to computer.

# Scheduling Jobs

- **Admin Tools > Task Scheduler**
- **Command Line:**
  - PowerShell
  - SCHTASKS.EXE
- **Options:**
  - Associate tasks with events
  - Run only when user is idle



SANS Security Essentials – © 2016 SANS

## Scheduling Jobs

Through command-line tools and custom scripts, you can automate your work. What you need now is a way to run these tools/scripts automatically on a recurring basis. Enter the Task Scheduler.

To access the scheduled jobs, open the Task Scheduler console in Administrative Tools, or search for **Task Scheduler** in the Start screen on Windows 8 and later. To manage remote systems, right-click the Task Scheduler snap-in at the top > Connect To Another Computer.

A single job can be scheduled to run at a hundred different times (on the Schedule tab, check Show Multiple Schedules), and each time can be scheduled on the basis of the following intervals: daily, weekly, monthly, once, at system startup, at logon, or when the computer has been idle for X number of minutes.

When a scheduled job runs under the context of the username/password of a user account, the password is encrypted and stored in the LSA Secrets portion of the Registry. (Only users who are members of the Administrators group can access the Registry's LSA Secrets. Malware, of course, can sometimes get equivalent privileges and then steal these passwords.) When a scheduled task runs as built-in identity such as System or Network Service, then there is no password.

## Command-Line Management

You also can manage jobs from the command line on local or remote systems with PowerShell or the SCHTASKS.EXE tool. The old AT.EXE utility is obsolete and should not be used.

To list the current scheduled tasks in PowerShell, run:

```
get-scheduledtask
```

To see how to create or manage scheduled tasks in PowerShell, run:

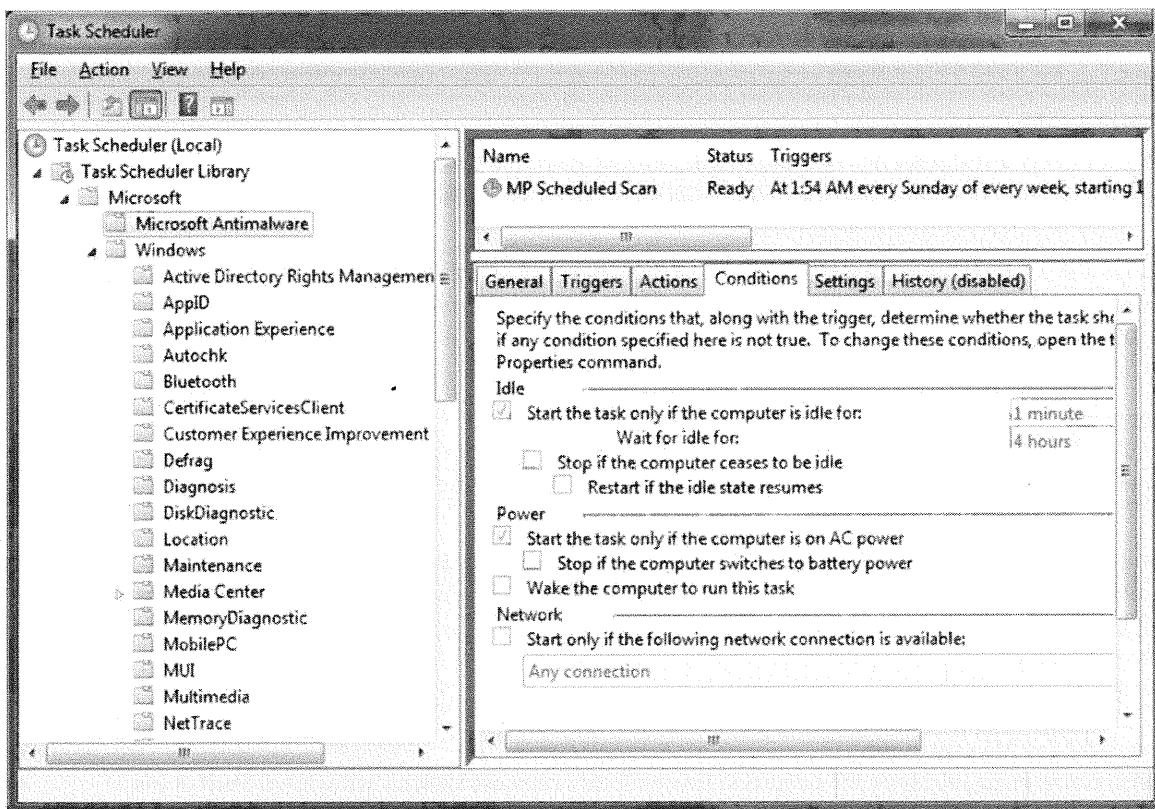
```
get-help set-scheduledtask -full
```

To see the many switches for SCHTASKS.EXE, run that tool with the "/" argument.

When a scheduled task runs a PowerShell script, note that powershell.exe can take the network (UNC) path to a remote script in a shared folder to execute it locally, for example, powershell.exe \\server\share\script.ps1. This causes the script to be downloaded from the share and executed locally, but the script never touches the local hard drive; it stays in RAM. This is handy because you can keep a master shared folder of all scripts which only you can access and then run them from there.

### Scheduled Job Accounts

Keep in mind that if you change the password for an account used to run scheduled jobs, the scheduled jobs themselves are not updated with the new password. This must be done manually in the GUI, through a script, or with a third-party tool designed for this. If you need to schedule jobs running with administrative privileges, consider creating a special account for this purpose and assigning it a long and complex passphrase (50+ characters) so that it doesn't have to be changed as often. No one is logging onto their desktop with this account, so it's not inconvenient to use a long passphrase. Make sure to audit all access to this account.



# Auditing and Forensics

- **Now that you can automate your work, the next several slides will discuss:**

1. Verifying policy compliance
2. Vulnerability scanning and reporting
3. Gathering on-going operational data
4. Creating baseline system snapshots
5. Change detection and analysis

SANS Security Essentials – © 2016 SANS

## Auditing and Forensics

Auditing and forensics are critical duties security administrators often need to perform. For the purposes of this manual, "auditing and forensics" is composed of five activities that somewhat overlap as we go from the auditing end of the spectrum toward the forensics end:

- Verifying policy compliance
- Vulnerability scanning and reporting
- Gathering on-going operational data
- Creating baseline system snapshots
- Change detection and analysis

There is overlap between these activities, but these categories are still useful for organizing our discussion. Let's discuss each of these activities in the remainder of the module.

# Verifying Policy Compliance

- Policies are written documents describing your rules and procedures for enforcing network security:
  - Change Control Board (CCB) to ensure changes are made within control parameters as a part of configuration management
- **Two ways to audit policy compliance:**
  - 1.) Maintain and check written change logs
  - 2.) Examine the machines themselves
    - Look at some tools for doing this
    - You've seen many of them already!

SANS Security Essentials – © 2016 SANS

## Verifying Policy Compliance

As the security administrator, it is your job to develop and enforce a number of written security policies. These documents describe and explain such issues as the password policy, lockout policy, antivirus policy, and acceptable use. It will be a part of your audits to verify that the measures described in these documents are actually being followed.

One way to do this is to have a log available where the relevant administrators can enter information about actions taken in compliance with various policies. For example, you might have a shared folder with an Excel spreadsheet for each server managed by IT; every time a change is made or a check is performed, the person involved should enter the date, time, his/her name, and notes describing the change/check into the spreadsheet. Script the backup of the spreadsheets to occur every night, and name each backed up file after the current date.

These spreadsheets will aid in troubleshooting and provide some accountability for those charged with policy compliance. The information in the spreadsheets can be correlated with the on-going gathering of operation data to help dissuade devious administrators from entering false records in the spreadsheets. Part of your auditing procedure will be to check that the appropriate entries have been made in the spreadsheets; because this is the primary purpose of the spreadsheets' existence, you should add columns in the spreadsheet for matching records of tasks completed with the policies that mandate those tasks. This can aid in sorting and scripting the checking of this data. If you would like to use a web-based application to make the data-gathering and analysis easier, all the better!

Another way to audit policy compliance is to examine the relevant computers themselves. Fortunately, it often is the same tool that is used to enforce a policy that can be used to verify policy compliance. Now look at some of these tools.

# The SCA Snap-in Again

- SCA can both apply a template and compare a system against a template for auditing:
  - But it's still a GUI tool, not ideal for scheduled tasks

Policy	Database Setting	Computer Setting
Enforce password history	0 passwords remembered	24 passwords remembered
Maximum password age	42 days	35 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters
Password must meet complexity requirements	Disabled	Enabled
Store passwords using reversible encryption	Disabled	Disabled

SANS Security Essentials – © 2016 SANS

## The SCA Snap-in Again

The Security Configuration and Analysis (SCA) snap-in applies security templates to systems to reconfigure NTFS permissions, password/lockout policies, Event Log settings, security options, and so on. You've seen this tool already. But not only can the SCA snap-in *apply* templates, it also can *compare* a computer's current configuration against a template and produce a report.

In the snap-in, after you create a database and import a template into it, instead of right-clicking the tool and selecting Configure Computer Now, simply select Analyze Computer Now. No changes will be made to the system whatsoever. When complete, the SCA shows all the folders in the template and all the policy icons in each folder; if the policy icon has a red X on it, that means the computer's configuration does not match the setting in the template for that policy. If the policy icon has a green check mark, then the current setting matches the template; and if the icon is just plain blue, then the template didn't specify a setting for that policy one way or the other.

The SCA snap-in produces a textual report of this analysis, as well. The full path to this text file is displayed after you select Analyze Computer Now. You also can opt to show this in the SCA snap-in, if you right-click the snap-in and choose View Log File. The drawbacks of the SCA snap-in, though, are that it's a graphical tool, and it doesn't work over the network. Fortunately, there's a command-line version of the SCA snap-in.

# SECEDIT.EXE

- **Command-line version of the SCA snap-in**
  - Compare a system against a template and produce a log
- Still cannot run against remote systems, hence:
  - Put SECEDIT.EXE and template in a shared folder
  - Batch file will map drive letter to share
  - Batch file will run SECEDIT.EXE for the audit
  - Batch file will copy its output file to share
  - Schedule batch file to run on audited servers

SANS Security Essentials – © 2016 SANS

## SECEDIT.EXE

SECEDIT.EXE is a command-line version of the SCA snap-in. It can do anything the snap-in can do (and more). Unfortunately, it still can't compare templates against remote machines, but a simple batch file can, nonetheless, greatly aid in the process. Store the tool and your templates in a shared folder along with a batch file. The batch file, when run, maps a local drive letter to that share, compares the local system against one of the templates using SECEDIT.EXE while redirecting its output to a text file, and then copies that output file to a subdirectory in the share named after the computer.

Another command-line switch, /log, could have been used to save the output log anywhere desired instead of the default shown.

The second command just uses the raw database file without specifying the template to reconfigure the machine. The database file was created, in this example, with the first command; alternatively, you could have built the database with the SCA snap-in and then used SECEDIT.EXE to apply it or audit with it.

```
E:\WINDOWS\System32\cmd.exe
E:\WINDOWS\security\templates>secedit /analyze /db dbase.sdb /cfg Generic.inf
Task is completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.

E:\WINDOWS\security\templates>secedit /configure /db dbase.sdb
Task is completed successfully.
See log %windir%\security\logs\scesrv.log for detail info.

E:\WINDOWS\security\templates>
```

# Microsoft Baseline Security Analyzer (1 of 2)

- Free Microsoft graphical and command-line tool
- Scans Windows, IIS, SQL Server, Exchange Server, IE, MS Office, and other configuration items
- **Works against local or remote systems:**
  - **This can take a range of IP addresses to scan**
- MBSA produces an easy-to-understand report that details the scans performed and describes how to correct the problems found
- Make sure to get the latest version from Microsoft

SANS Security Essentials – © 2016 SANS

## Microsoft Baseline Security Analyzer

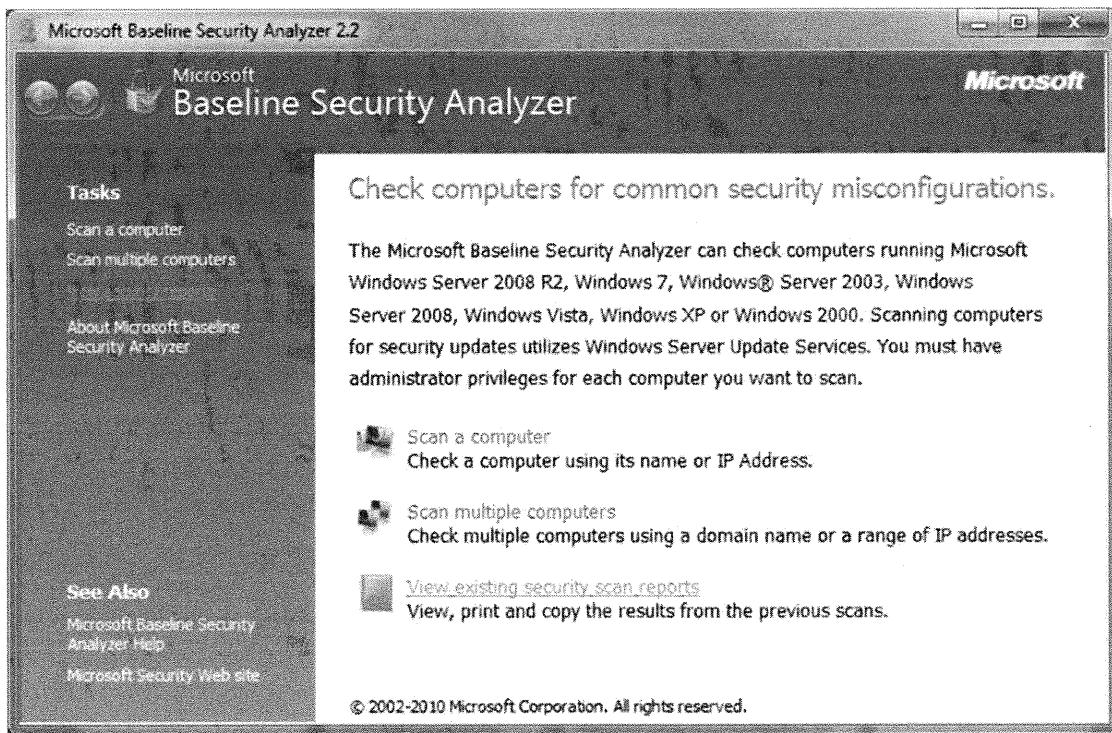
The Microsoft Baseline Security Analyzer (MBSA) is a free auditing tool from Microsoft that can scan the following products for security vulnerabilities:

- Windows OS
- Internet Explorer
- IIS
- SQL Server
- Exchange Server
- Microsoft Office (local scan only)
- Windows Media Player
- And other products as well, such as BizTalk Server, and so on.

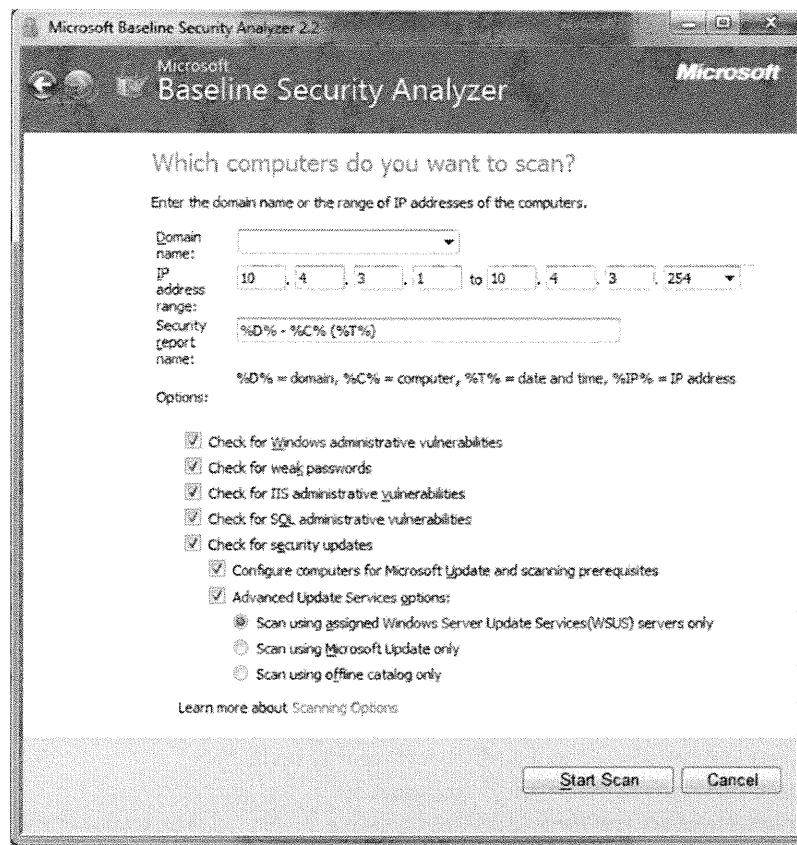
What does the MBSA do? In Overview, the MBSA Sports the following features:

- Can scan a single machine or multiple remote machines by IP address or Active Directory domain membership
- Can be run as a command-line tool (mbsacli.exe) with switches for which machine(s) to scan, which test(s) to perform, and how the output file should be saved
- Does not require special agent software on scanned hosts
- Checks the Service Pack level
- Queries for missing hotfixes
- Checks that all drive volumes are using NTFS

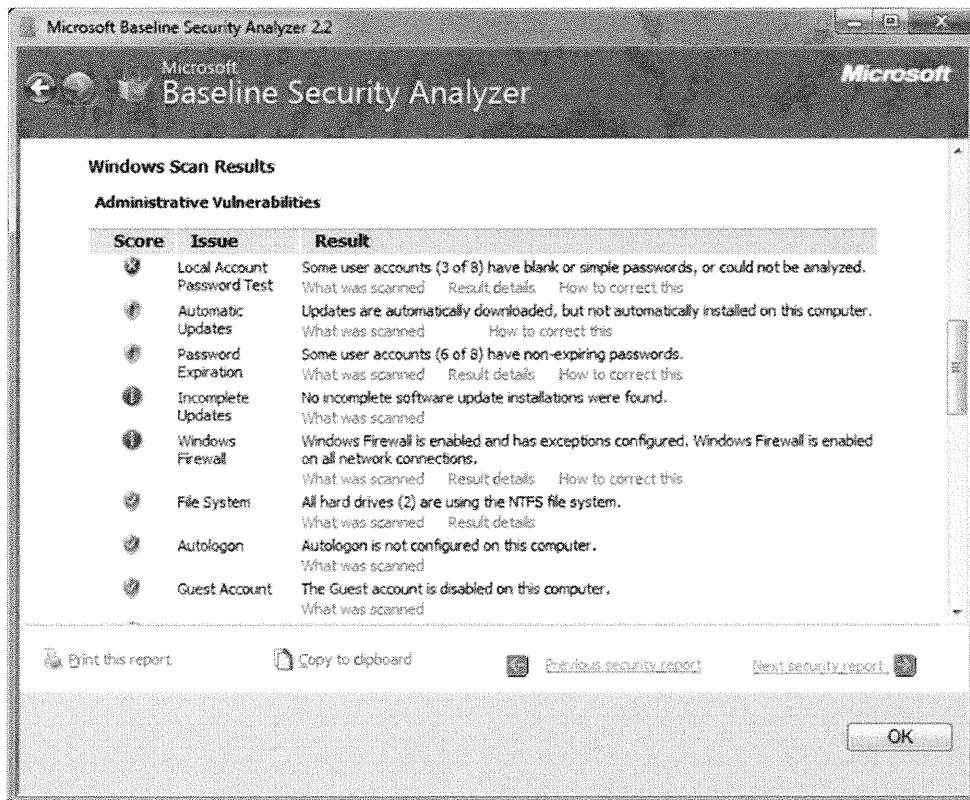
- Checks that the passwords of local accounts are not blank, identical to the user's name, identical to the machine's name, and is not password, admin, administrator, or sa
- Lists disabled and locked-out accounts
- Lists any accounts with passwords that never expire
- Verifies that the Guest account has been disabled
- Warns if null user sessions are permitted (RestrictAnonymous) and whether permissions assigned to Everyone also apply to anonymous users
- Checks that password-less automatic logon is not enabled
- Verifies that Event Log auditing is enabled
- Lists all shared folders and their permissions
- Lists the members of the local Administrators group if there are more than two
- Warns if Internet Explorer and Microsoft Outlook security "zones" are set too lax
- Alerts if Microsoft Office macro support is enabled
- Warns if either IIS or SQL Server is installed on a domain controller
- Warns if any of the following services are installed at all: IIS FTP, IIS HTTP, IIS SMTP, Telnet Server, or the Remote Access Service Manager (You can modify the list of services this option warns on.)



MBSA has been updated over the years, so make sure you have the latest version. For Windows Vista support, you must have version 2.1 or later. For 64-bit Windows 7 and Server 2008-R2 or later, it's best to have version 2.2 or later.



The MBSA also performs security checks when certain dangerous services are installed. Perhaps the most dangerous service is IIS, and the MBSA has specific checks for IIS.



Another dangerous service is SQL Server. It's dangerous because it is often exposed to the Internet (if only indirectly through IIS) and because the data it manages may be extremely valuable to the company. For SQL Server security, the MBSA will:

- Verify that the password of the system administrator (sa) account is not in any temp files, is not blank, is not "password," and is not "sa."
- Check the NTFS permissions on critical folders used for database files.
- Warn if old-style Mixed Mode authentication is being used instead of Integrated Windows authentication.
- List all accounts and groups that have the SysAdmin role in SQL Server.
- Check critical Registry key permissions that could be used to compromise the server.
- Verify that only the SysAdmin database role has the CmdExec execution right.
- Verify that the service account used by SQL Server is not the local System account or an account that is a member of any administrative groups.
- Check that the local Administrators group has the SysAdmin role in SQL Server.
- List all the databases to which the Guest account has at least read access.

### **Download the MBSA**

The MBSA can be downloaded from Microsoft's website. It's best simply to search on the full name of the tool to get the latest version, but you can also go to the Microsoft security home page (<http://www.microsoft.com/security/>) or the MBSA home page itself (last seen at <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>). It's best if your scanning system itself has IIS installed locally if you will be scanning other IIS servers over the network. Make sure to upgrade to the latest version.

### **Running the MBSA Graphical Version**

Launch the MBSA from the Start menu > All Programs > Microsoft Baseline Security Analyzer. In the page that appears, click Scan a Computer on the left side, enter the IP address in the box, and then click Start Scan. Scanning a single machine requires about 2 minutes, unless there are many local accounts on it. You also can enter a range of IP addresses and scan each machine remotely.

When finished, you see a summary report. The report has hyperlinks to describe what was scanned (click What Was Scanned) to show detailed results (click Result Details) and instructions for fixing the problems discovered (click How to Correct This). Past reports are kept, so you can come back later to review them.

Fortunately, the MBSA can be scripted because there's a command-line version, too!

## MBSACLI.EXE (2 of 2)

- Scan remote systems for missing hotfixes
- Provides a model of what you want for auditing:
  - Scheduled script
  - Analyzes or processes the data for you
  - Returns the results from remote systems in a convenient manner (e-mail, SMB, and FTP) that doesn't require constant hand-holding
- The results are in a form that's easy to use

SANS Security Essentials – © 2016 SANS

### MBSACLI.EXE

An audit to verify that all the latest patches have been applied on Internet-accessible systems should be performed at least every week. The audit could be performed with the same tool used to know which patches needed to be applied in the first place: MBSACLI.EXE. (This is a good example of how auditing and hardening are two sides of the same coin.) How could you put your new automation skills to work here?

Write a script that uses MBSACLI.EXE to scan your servers over the network and have its output redirected to a text file. Your script examines this file, extracts the names of the computers missing patches, and automatically e-mails you the list. All this sounds complicated, but the scripting is relatively easy. Schedule this script to run every night, and you'll be doing a wonderful job staying on top of patches, all with only a few hours of upfront work!

This script is a good example of what you're aiming for: a scheduled script that gathers important security information, analyzes or processes that information in some way (so you don't have to do it manually), and returns the results back to you in a manner that is easy to work with or permanently store. The easiest data to work with is plain ASCII text, which is easy to store because it is highly compressible, and text files can be returned to you conveniently through internal e-mail, SMB, or FTP. The next step, not covered in this course, would be to import that ASCII data into SQL Server or Microsoft Access. And that could be scripted, too!

### Running the MBSA Command-Line Version

The command-line version of MBSA has straightforward switches (see MBSACLI.EXE /?). For example, the following scans every computer in a range of IP addresses and saves the output to a text file:

```
mbsacli.exe /r "10.1.1.1-10.1.1.200" /f "c:\file.txt"
```

You can view the details of the report either with the graphical MBSA or by first listing the available reports (/l) and then redirecting one (/ld) from the command line to a reports file:

```
mbsacli.exe /l  
mbsacli.exe /ld "WebServer1(11-12-2012)" > reports.txt
```

In some respects, the MBSA is both an auditing tool and a basic vulnerability scanner.

# Configure Windows Logging

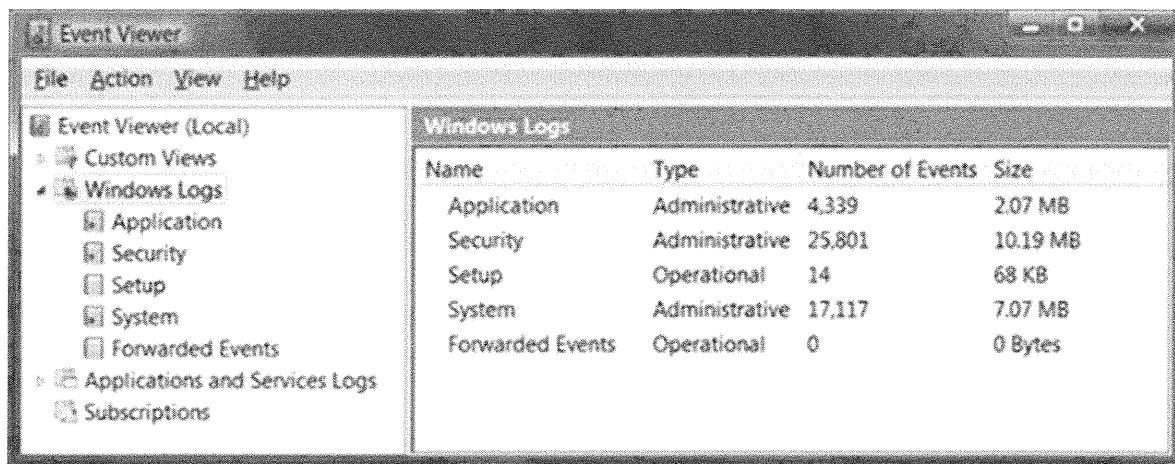
- **Windows Event Viewer logs:**
  - Application
  - Security
  - System
  - Directory Service (domain controllers)
  - DNS Server (DNS servers only)
  - File Replication Service (domain controllers)
- Research Event ID numbers in Google/Bing

SANS Security Essentials – © 2016 SANS

## Configure Windows Logging

All Windows systems have at least three Event Logs named Application, Security, and System. You can view the contents of these logs with the Event Viewer snap-in: Administrative Tools > Event Viewer. If you are a domain controller, then you also will have logs named Directory Service and File Replication Service. If you have DNS installed, you'll also have a DNS Server log.

Double-click an event icon in one of the logs to bring up its property sheet. Here you can see the event's date, time, source, user, computer, category, and event ID number. The description field in the middle may also include a few lines or paragraphs of text, including a hyperlink on which you may click to obtain more information from Microsoft about that type of event.



Often the best way to research an entry, though, is to do a search in Google/Bing on the words *Windows Event ID XXXX*, where XXXX is the event ID number in question. Also try <http://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>.

The System log mainly is for OS troubleshooting. Here you'll find entries related to service start/stop/failures, device driver issues, status reports of background maintenance operations, and so on. The Application log is where applications and third-party developers can write anything they want. You have little control over what goes here; it is entirely up to the original programmers of the software in question.



If you'd like to write your own entries to the Event Logs with a command-line tool, see LOGEVENT.EXE from the *Resource Kit*. It can write to local or remote systems.

But what about the Security log? By default, that log will be empty *unless* you specifically choose to enable security auditing.

# Security Event Log and Audit Policies

Manage with Group Policy and AUDITPOL.EXE

SANS Security Essentials – © 2016 SANS

## Security Event Log and Audit Policies

To enable logging to the Security log, go to Administrative Tools > Local Security Settings > Advanced Audit Policy Configuration. Here you can choose to log successful and/or failed events of certain types. The types of events are listed below, with recommendations in parentheses for which events to log:

- **Audit Account Logon Events** (Success, Failure): This tracks authentication requests processed by the domain controllers, even when the access is not to the domain controller itself. Think of DCs as providing a service for the sake of other machines on the network (checking usernames and passwords). This category logs whenever that service is provided. When this policy is enabled on non-domain controllers, then it applies only to the local accounts on those machines; hence, it only applies to authenticated access to those machines with local accounts.
- **Audit Account Management** (Success, Failure): This monitors user and group tasks, such as account creation, deletion, modification, and group membership changes.
- **Audit Directory Service Access** (Success, Failure): This is required to begin logging access to Active Directory objects as defined on those objects' individual System Access Control Lists (SACLs).
- **Audit Logon Events** (Success, Failure): This tracks interactive and over-the-network logons to the computer itself.
- **Audit Object Access** (Failure): This is required to begin logging access to NTFS folders and files, registry keys, and shared printers. It is not the case that enabling this category will cause all filesystem, registry, and printer access to be logged. Rather, enabling the category makes it possible to have the SACLs on those objects become live, i.e., object SACLs do nothing unless this audit policy is also enabled.

- **Audit Policy Change** (Success, Failure): Tracks changes to the audit policies themselves and changes to privileges assignments.
- **Audit Privilege Use** (Failure): Monitors the exercise of certain privileges on the machine, for example, take ownership, change system time, and so on.
- **Audit Process Tracking** (Not Defined): This is rarely enabled and usually only by programmers who are debugging their own code. This category tracks program execution, process loading and unloading, filesystem handle creation and release, indirect object access, and other low-level OS behaviors. Enabling this category causes a vast amount of extra log data and slows down the system considerably.
- **Audit System Events** (Success, Failure): Tracks system startup, shutdown, and other systemwide events. This also records clearing of the System and Security logs.

### Group Policy

Almost all audit policy settings on both servers and workstations can be remotely configured through Group Policy. Audit policy is set under Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy. Hence, when you need to configure audit settings throughout your domain, Group Policy is the way to do it.

### AUDITPOL.EXE

If you'd rather manage audit policies from the command line, use the AUDITPOL.EXE tool from the Windows Server Resource Kit. It's also built into Windows Vista/2008/7 and later by default. Starting with Vista, by the way, you can enable or disable special subcategories of audit policies using AUDITPOL.EXE, too. To see your currently activated subcategories of audit policies on Vista/2008/7 or later, run auditpol.exe /get /category:\*

Category/Subcategory	Setting
System	No Auditing
Security System Extension	Success and Failure
System Integrity	No Auditing
IPsec Driver	No Auditing
Other System Events	Success
Logon/Logoff	Success and Failure
Logon	Success and Failure
Logoff	Success and Failure
Account Lockout	Success and Failure
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	Success and Failure
Other Logon/Logoff Events	Success and Failure
Object Access	No Auditing
File System	No Auditing
Registry	No Auditing

# NTFS, Registry, and Printer SACLs

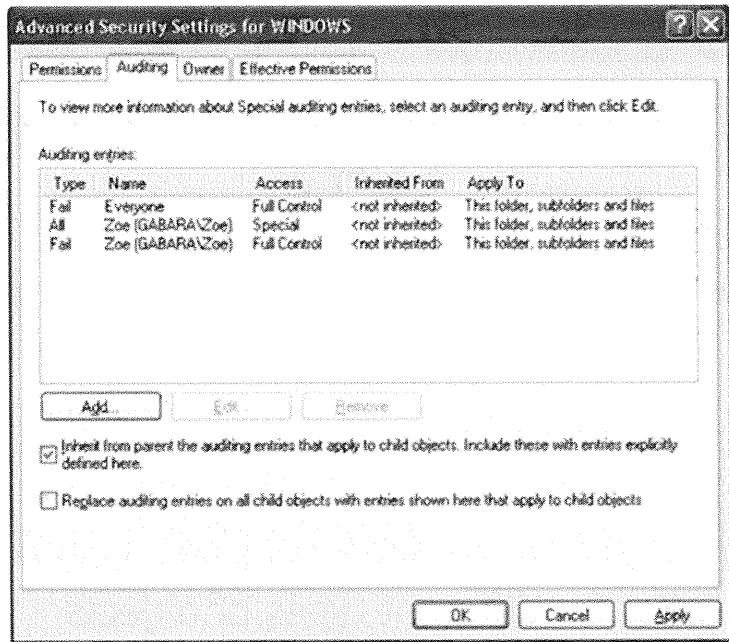
- **Two steps to enable object auditing:**
  1. Enable the Audit Object Access policy
  2. Configure the object SACLs wanted
- **System Access Control Lists (SACLs):**
  - Differ for different types of objects
  - Can be inherited, just like permissions

SANS Security Essentials – © 2016 SANS

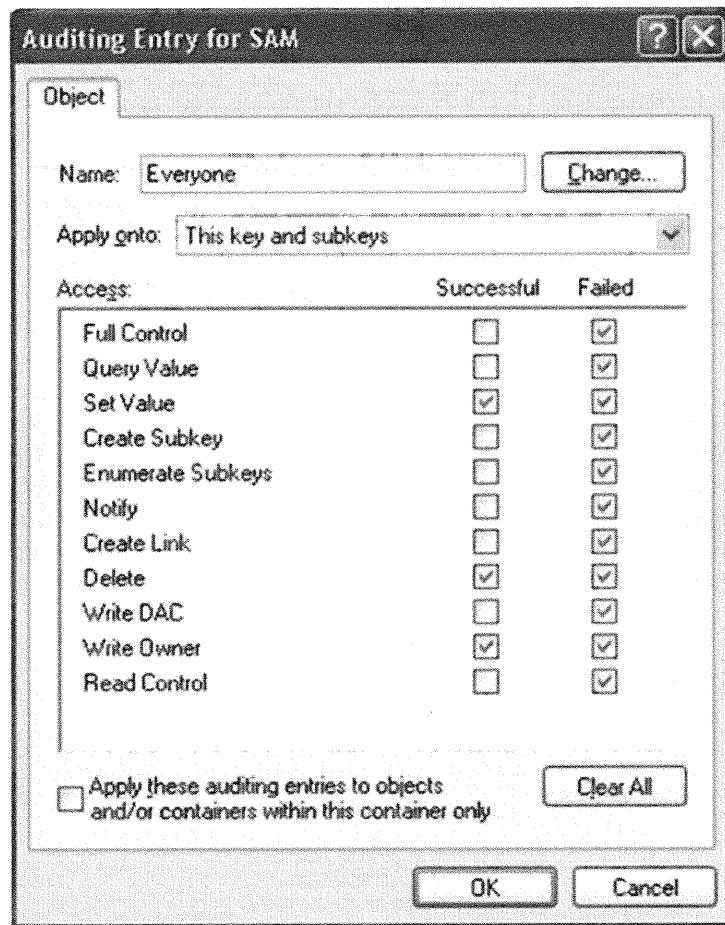
## NTFS, Registry, and Printer SACLs

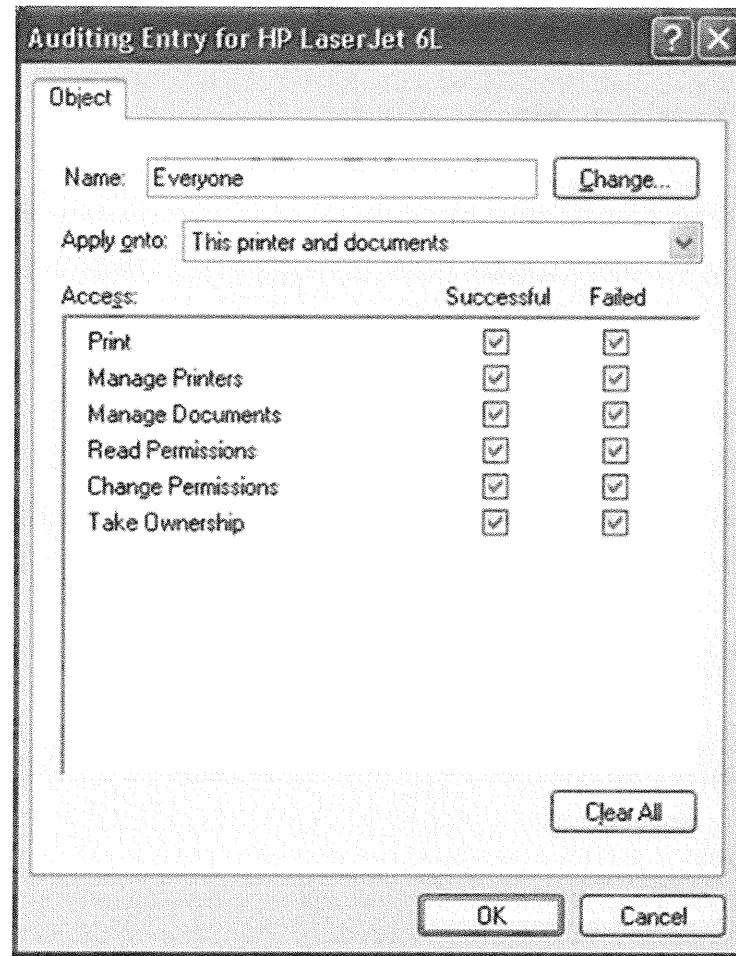
Even if you do enable *Audit Object Access* for both success and failure, nothing extra will be logged. Auditing access to NTFS files/folders, Registry keys, and printers is a two-step process. First, you enable *Audit Object Access* in the computer's audit policy; then you go to the individual files, folders, keys, and printers you want to monitor and configure their *System Access Control Lists (SACLs)*. An object's SACL defines exactly which users and groups should have their interaction with the object logged. Moreover, you can choose exactly what types of interaction will be logged, too.

Let's configure the SACL of an NTFS file as an example. Right-click any NTFS file on your system and go to Properties > Security tab > Advanced button > Auditing tab. The Auditing tab is where you configure a folder or file's SACL. Now, click the Add button and select a user or group whose interaction with this file you want to track. (When in doubt, always audit the Everyone group.) After you select a user/group, a dialog box appears asking you exactly which types of actions you want to monitor, for example, Successful Delete, Failed Read, Failed Execute File, Successful Change Permissions, and so on. The two columns of check boxes for Successful and Failed actions correspond to the auditing of successful or failed events in the *Audit Object Access* policy; if you don't enable one of those categories in the policy, then that category of action (Successful or Failed) simply is not logged, no matter what check boxes are checked in the SACL.



The same is true for registry keys and printers. To audit access to a registry key, open REGEDIT.EXE > Edit menu > Permissions > Advanced button > Auditing tab. For printer icons, right-click the printer > Properties > Security tab > Advanced button > Auditing tab.





If you have no Security tab, then pull down the Tools menu in Windows Explorer > Folder Options > View tab > and uncheck the box at the bottom labeled *Use simple file sharing*.

There are many actions that can be audited, and the list is different whether you are auditing a folder, file, key, or printer (you interact with them in different ways, after all). Importantly, notice that both NTFS and registry SACLs can inherit settings from their parent containers. This is very helpful because, by using inheritance, you can define the audit settings you want at a top-level folder or key and have those settings apply to everything underneath it. If you need to edit those SACLs, you only have to make a single change at the top-level container.

# What Should be Logged?

- Try to anticipate how an attacker might leave a trail and then audit to collect *that* data
- Audit the most valuable data and services
- The more you log, the slower your server's performance, so avoid flooding logs with useless data that no one will ever examine or need
- Apply SACLs with security templates!

SANS Security Essentials – © 2016 SANS

## What Should be Logged?

Don't audit access to the entire hard drive and Registry; this will slow your computer down by more than 50 percent. Beyond that advice, however, only general suggestions can be given because every environment, server, and workstation is different. You should audit what you're interested in! Here are some general suggestions:

- Try to limit the scope of your object auditing as much as possible without missing the data you actually need. The more you log, the slower your machine will run, and the quicker your log files will grow.
- The wealth of your organization resides in its proprietary data, so audit all successful and failed actions of the Everyone group on those files. This would include databases, documents, spreadsheets, source code files, customer lists, scripts, and HTML files on the web servers, Outlook personal storage (.PST) files, and so on. This produces a lot of data, but, if not the jewels of the company, why do object auditing at all?
- Avoid auditing Read/List access, except on the most sensitive files and folders; otherwise, your logs will be flooded with data.
- Avoid auditing Execute actions on binaries, except for administrative tools and other dangerous software, the shortcuts in the Administrative Tools folder. An exception would be for Internet servers where an extremely high level of paranoia is justified, but you still should selectively omit auditing the binaries that you expect and *want* to be executed, for example, script interpreters on IIS.

For the type of server being audited, try to anticipate which files an intruder would most likely access, and make sure to audit those at a minimum.

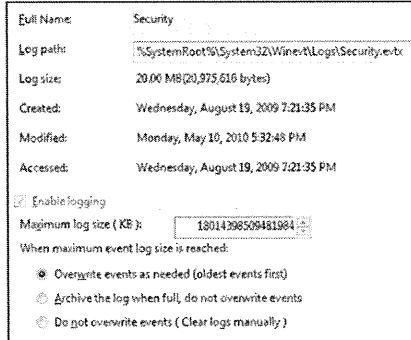
- In general, audit Delete, Create Files/Write Data, Create Folders/Append Data, Write Attributes, and Change Permissions for the %SYSTEMROOT% and %PROGRAMFILES% folders and their subdirectories by the Everyone group. If an application or service writes temporary files to any of those subdirectories instead of using %TEMP%, then prune your SACLs to ignore them selectively.
- Temporary folders are attractive to hackers because it is easier to hide things there, but you must be careful when auditing them. In general, only audit the Change Permissions, Write Attributes, and Write Extended Attributes actions in temp folders to avoid flooding the logs with useless data. In general, it's better to periodically search temp folders for well-known hacking tools than to try to audit all interactions. You also can use DIRUSE.EXE to alert you if any monitored temp folder exceeds X number of megabytes in total content.
- In general, the Take Ownership and Change Permissions actions should be audited on all files, all hard drives.
- Mainly for political reasons, printers should have all their actions audited for the Everyone group. Even busy print servers don't generate more than a few thousand events each day.
- It usually is not worth the effort to configure extensive Registry key SACLs by hand. Configure registry SACLs with security templates that have been designed by others and then customized by you.

### **Security Templates (Again)**

Remember INF security templates? When applied, a security template can reconfigure NTFS and registry SACLs, as well (but not printer SACLs). You should have a separate template for each type of server you will be auditing. The template will have a number of SACLs defined already by the vendor from which you obtained it (Microsoft, NSA, NIST, CIS, and so on) plus all the custom SACLs you've added for your particular environment. Preconfigured templates are especially useful for Registry key SACLs. Exactly which keys have bad default audit settings? How would you know this without weeks of research and effort?

These security templates can be applied, of course, with the Security Configuration and Analysis snap-in, the SECDIT.EXE command-line tool, or Group Policy.

# Log Size and Wrapping Options



- Each log is finite and can be sized separately from the other logs
- Appropriate log size will be determined by the rate of new events and your wrapping options
- Logs are compressed XML and can grow large, perhaps filling all the free space in the volume

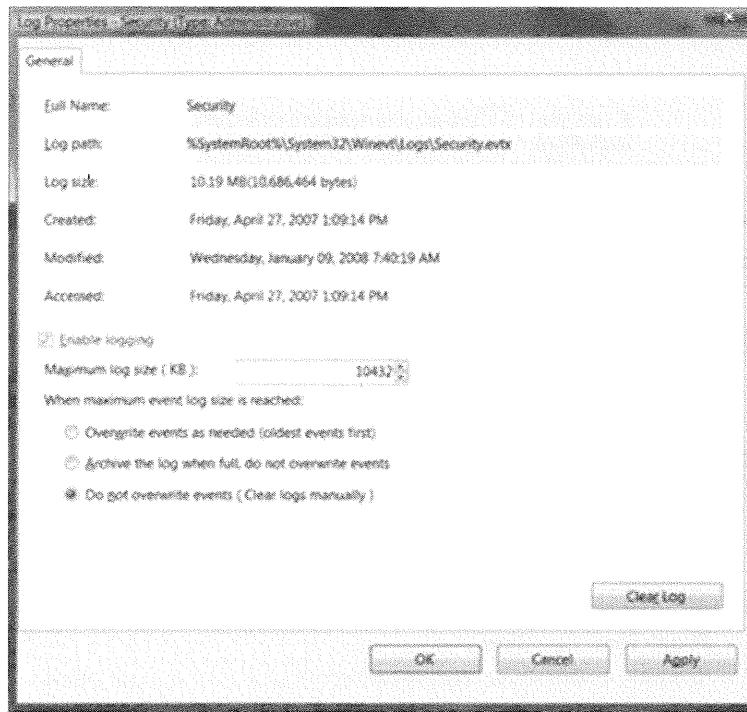
SANS Security Essentials – © 2016 SANS

## Log Size and Wrapping Options

A security template also can be used to set the maximum size and wrapping options for your Event Logs. On Windows XP/2003, the logs are stored in the %SystemRoot%\System32\Config folder, but on Vista and later, look in %SystemRoot%\System32\Winevt\Logs\. The names of the log files are self-explanatory. Event Logs are assigned maximum sizes beyond which they are not permitted to grow. What happens, then, when they fill up?

To change your Event Log size and wrapping options without applying a template, open the Event Viewer from the Administrative Tools folder > right-click a log > Properties > General tab. On Windows XP/2003 each log can be increased in size to a maximum of 4,194,240K (about 4.2GB), but don't try it. On those obsolete Windows systems, the combined size of all log files should never be set larger than 300 MB because there is a well-known problem with their spontaneously dropping event messages once the logs grow larger than 300 MB in total (KB183097). On Windows Vista/2008/7 and later, there's no such problem because the logs are compressed XML, and they can be set to the maximum size of the volume if wanted.

When setting the maximum size, Windows does not reserve the necessary free space. Rather, the log grows on the file system as necessary up to the maximum size or when the drive runs out of free space (whichever comes first). 1 MB of log space holds about 7,500 events. How big should the logs be? Well, set them each initially to at least 50 MB, but the size actually is determined by your wrapping requirements.



When a log file fills to its maximum capacity, that log files wrapping options engage.

There are three wrapping options:

- Overwrite Events as Needed
- Overwrite Events Older than X Days (number of days is configurable)
- Do Not Overwrite Events (Clear Log Manually)

Paranoid environments should always clear the log manually after an application or custom script archives the log. For run-of-the-mill workstations inside the LAN, events can be overwritten as necessary for the sake of convenience. However, for critical servers and systems exposed to the Internet, events only should be overwritten if they are older than X days. On the assumption that you are making full backups once per week, X should be set to 15 days. In general, we want at least two full backups to have archived an event before that event is overwritten. If events are written faster than you can back them up, then you must either make more frequent backups and reduce X, increase the maximum size of the log files, or deploy a log consolidation system. Keep in mind that your adversaries may deliberately attempt to fill your logs to maximum size to try to conceal their activities.

# Log Consolidation

- Consolidate your log data into a central database:
  - **Syslog, HIDS, and Third-party Log Aggregators:**
    - Kiwi, Snare, WinSyslog, Splunk, ArcSight, LogRhythm, and such
  - **Event Viewer:**
    - Right-click the Subscriptions folder > Create Subscription
  - **Free Scripting Tools:**
    - PowerShell Get-WinEvent
    - Solarsoft DumpEvt.exe, Microsoft PsLogList.exe, and others

SANS Security Essentials – © 2016 SANS

## Log Consolidation

Each Windows machine has its own separate Event Logs. Analysis of Event Log data is assisted greatly by having a centralized copy of that data from all the machines one cares about. Also, it's important for security to move event data off of vulnerable systems as quickly as possible because the first thing a skilled hacker might do after compromising a server is to clear its Event Logs.

### Windows Event Collector Service

The built-in Windows Event Collector service is a bit like syslog on Linux, but event log data is sent over SSL, and it uses the Web Services Management (WS-Management) protocol to either *pull* data from monitored systems (collector initiated) or to *push* data from the monitored systems to the collector (source initiated) or both. When a monitored system is offline, its batched-up events will be forwarded to the collector when accessible again.

You can "subscribe" to the Event Logs on remote systems using the Event Viewer tool and going to the Subscriptions container; monitored systems are configured to forward events to your subscriptions through Group Policy (too many steps to summarize here). You can also manage Windows Event Collector settings from the command shell with WINRM.VBS and WECUTIL.EXE, such as on standalone computers. The Windows Event Collector service is built into Windows Vista/2008/7 and later, but WS-Management for Windows XP/2003 can be downloaded and installed, too.

When configured, remote Event Log data is placed into the Forwarded Events log on the collector server. Under the hood, this is the same service and protocol used by Microsoft's System Center Operations Manager (MOM), but you can do it for free yourself if you don't need the bells and whistles.

## **Microsoft System Center Operations Manager ("MOM Server")**

Microsoft System Center Operations Manager (MOM) watches over your servers by continuously extracting their Event Logs and other auditing data, storing that data in a central database, scanning the data for user-definable patterns, raising alerts or initiating user-definable actions when these patterns are found, and providing a set of analysis tools. Of course, it's not exactly free. There are special add-on "Management Packs" for IIS, SQL Server, Exchange Server, domain controllers, and other products.

## **Third-Party Log Collection and Analysis Solutions**

There are many excellent third-party solutions on the market for doing log consolidation and analysis, and some of them are even free to use in smaller environments; for example, Splunk is free when collecting less than 500MB/day of data ([www.splunk.com](http://www.splunk.com)) and can scale up as needed if you pay for the enterprise version. Other well-known products aren't free, such as ArcSight ([www.arcsoft.com](http://www.arcsoft.com)) and LogRhythm ([www.logrhythm.com](http://www.logrhythm.com)) but also have additional analysis and alerting capabilities.

## **Windows Syslog**

There are free and commercial syslog clients and servers for Windows, too. This is especially useful in a mixed Windows/Linux environment. You can forward Windows log data to a syslog server, or a Windows host itself could be the syslog server for all devices. Try a Google search for **Windows Syslog** to show a number of products, and a few popular products in particular are Kiwi Syslog Server ([www.solarwinds.com](http://www.solarwinds.com)), Snare ([www.intersectalliance.com](http://www.intersectalliance.com)) and Adiscon WinSyslog ([www.adiscon.com](http://www.adiscon.com)).

## **Doing It Yourself**

When Event Log data is stored as plain ASCII text, it is easy to compress, easy to search, easy to filter, easy to import into a database, easy...*everything*. If you use syslog, the log files will already be in textual form or you can export them to text files. If you use Windows Event Collector, the logs are compressed XML and can be exported to other textual formats too. It is also possible to query local or remote Event Logs directly and save the resulting data to text files, and there are many options for this:

- **PowerShell CmdLets:** PowerShell has a built-in cmdlet named *get-winevent* that can be used to query local or remote Event Logs, and then other cmdlets, such as *export-csv*, could be used to save to text files. You can also use *get-wmiobject* to query log data through WMI.
- **WMI Scripting:** Custom scripts can use the Windows Management Instrumentation (WMI) interface to dump or clear the contents of event logs as well. See the *Resource Kit* for an example script, or get a free script in the public domain from <http://cyber-defense.sans.org/blog/downloads> that can write Event Log data to a clean comma-delimited text file, clear logs, and sort the data by day/time before writing it to the text file (*DumpEventLog.vbs*).
- **Microsoft PsLogList.EXE:** From the Sysinternals page of Microsoft's website, you can download PsLogList.EXE (<http://www.microsoft.com/sysinternals/>). PsLogList is used to dump the contents of a log to a comma-delimited ASCII text file. The exported logs can be on a local or remote system. PsLogList also can filter the events exported, based on source service, event ID number, time stamp, and other criteria. It can also clear the log after dumping it.
- **SomarSoft DumpEvt.EXE:** DumpEvt (<http://www.systemtools.com/somarsoft/>) can alter the Event Log data as it is dumped so that it will be imported more easily into databases. DumpEvt can also dump only previously un-DumpEvt-dumped data to avoid duplicates, and it can clear logs.

# Forensic Snapshots (1 of 3)

## • Capture the running state of a computer at an instant in time to text files:

- Provide a baseline for before/after comparisons
- Manually detects system compromises
- Document what changes have occurred
- Aid in regular troubleshooting
- Potentially act as legal evidence
- Though not as complete as binary drive and memory dumps, text files are still useful and are much easier to compress, store, search, and share

SANS Security Essentials – © 2016 SANS

### Creating Forensic Snapshots (1 of 3)

For mission-critical internal servers and servers exposed to the Internet, your efforts also should include creating periodic system snapshots. A *system snapshot* is a collection of data that documents the configuration and running state of the machine at a point in time. Its purpose is to provide a baseline against which later snapshots can be compared to detect changes. Presumably, you'll have a *before* snapshot, when you assume the machine is working fine and has not been compromised, and an *after* snapshot, taken after problems began or after a suspected compromise or just because it's time for another audit. The *before and after* snapshots can be compared so that only the differences are listed. This process is useful for troubleshooting, but you mainly want to use these snapshots to detect intrusions, to know how your adversaries have modified our systems (rootkits, Trojans, and so on), and to provide forensics evidence that might be admissible in a court of law.

### What About Raw Binary Memory and Drive Images?

The ideal snapshot of a server might be binary images of its hard drive and raw memory. But ideal for what? Not for doing quick nightly captures, not when storage is in short supply, and not when you want to make analysis easier for beginners who aren't familiar with the latest forensics tools. Binary drive and memory captures are ideal for maximum fidelity and completeness, but that doesn't mean these raw captures are the best for every purpose.

Because the purpose of a snapshot is to provide a baseline for comparison, you want to capture data in a form which easily is compared against other snapshots; you want that data to be highly compressible for long-term storage if necessary; and you want to automate the entire snapshot-making process. What fits the bill? Plain text files produced by custom scripts and command-line tools are perfect for system snapshots.

Through scripts and command-line tools, you can gather almost any type of data you want. It's trivial to redirect this data to text files, and large text files can be compressed to a fraction of their original size.

Store your textual snapshot files in an NTFS folder with compression enabled so that you don't have to monkey around with Zip files or other archive software. The compression will be transparent to your tools.

### **How to Structure the Data**

The purpose of making a snapshot is to have it for later comparison with prior snapshots, hence, the names of the snapshot files and their internal structure should be geared to this end.

The name of the folder containing the snapshot files should include the computer's name, date, and time. You might also want to create different parent folders for different types of machines; for example, you might create folders for different Organizational Units, for external/internal servers of different types, or for whatever categorization scheme will aid in working with the files.

The snapshot data should include a well-formatted README.TXT that includes the computer's name, the date and time, the script used to create the snapshot, the username and domain of the person running the script, and any other identifying information you'll later need.

The body of the snapshot should be divided into files that are labeled uniquely and standardized across as many of the snapshots as possible. In practice, this means you should try to use the same script each time. If you modify the script to gather more data, consider putting the data into a new file or appended to the end of an existing file type. Again, anticipate how file-comparison tools or other auditing scripts will later try to use this data, so make your snapshots as "digestible" as possible to software, that is, make it well formatted and standardized.

# Snapshot Contents (2 of 3)

- File Hashes
- User Accounts
- Group Memberships
- Shared Folders
- Account Policies
- Privileges
- Processes
- Device Drivers
- Service Settings
- Network Configuration
- Listening Ports
- Environmental Variables
- All Registry Values
- All NTFS DACLs
- IIS Configuration Files
- **Anything useful for post-incident forensic analysis!**

SANS Security Essentials – © 2016 SANS

## Snapshot Contents (2 of 3)

Ideally, a snapshot should include all the information necessary to help discover precisely what changes an expert-level intruder with administrative privileges has covertly made to your system. This is almost impossible, but it's the goal to shoot for. Hence, a good snapshot should at least include:

- File hashes, such as with SHA-256, especially of the OS binaries
- All local user accounts, with as many of their properties as possible
- All local groups and their memberships, especially the local Administrators group
- Shared folders, their local paths, and their permissions
- Local audit, lockout, and password policies
- List of all privileges and the various users/groups who have these privileges on the machine
- List of running processes and their properties
- List of drivers and their properties
- Services and their startup settings (Automatic, Manual or Disabled) of all services, running or not
- All networking configuration settings, including IP addresses, the route table, NetBIOS names, DNS/WINS servers, IPSec configuration, firewall rules, and so on
- Environmental variables
- The entire Registry, or at least the keys which control services, drivers, and run commands
- List of all files, or at least the files in %SYSTEMDRIVE%, including their sizes, last-modified dates, and file attributes (especially the hidden files)
- List of all folders with the number of files in each folder and the total number of bytes consumed by all the files in each folder

- Dump of all NTFS permissions, or at least the NTFS permissions of everything under %SYSTEMROOT%.
- If SQL Server is installed, then include lists of all the users and groups who occupy the various "roles" in SQL Server, especially the SysAdmin role
- If IIS 5.0/6.0 is installed, includes a copy of the metabase.
- If IIS 7.0 or later is installed, includes copies of all the XML config files for IIS

In general, anything that is likely to be needed to perform a post-incident forensic analysis of the server should be included in the snapshot. The aim here is to create a baseline for comparison to help the forensic analyst do her job, so it's pre-forensics or forensics preparation because you won't capture a clean baseline *after* the compromise. By having one or more prior snapshots available, you can save your incident handlers and forensic analysts time.

# Snapshot Batch Script (3 of 3)

- Download the latest version of SNAPSHOT.BAT from:
  - <http://cyber-defense.sans.org/blog/downloads>
  - Go to the Downloads link and get the SEC505 zip file
  - The PowerShell version is SNAPSHOT.PS1
- **Simply run SNAPSHOT.BAT as an administrator:**
  - It will create a folder such as *ComputerName-Date-Time*
  - Folder will be filled with text files containing the data, with names such as **Users, Groups, Processes, Drivers, etc.**

SANS Security Essentials – © 2016 SANS

## Snapshot Batch Script (3 of 3)

Below is a sample batch script that can get you started. It produces a snapshot approximately 150 MB in size (or approximately 50 MB compressed) and takes approximately 20 minutes to run on a typical machine. If you disable the lines at the bottom of the script for file hashing and dumping NTFS permissions, though, it finishes in approximately 2 minutes and creates approximately 60 MB of data (or 20 MB compressed).

The SNAPSHOT.BAT script works best on Windows 7, Server 2008, and later. Place the script in a folder where you would like to save the snapshot data. It takes no command-line arguments. The script automatically creates a folder named after the computer and the current time, for example, *ComputerName-Date-Time*. All the output of the script goes into separate files in that folder, for example, Users.txt, Groups.txt, BIOS.txt, Processes.txt, and so on.

You can modify the script as you want. You might want to add tools that are not from Microsoft or that are not free. This script is just an example to get you started. In particular, you may want to edit the commands near the end of the script that create SHA-256 hashes of files and dumps NTFS permissions because these commands require most of the CPU cycles and disk space.

The SNAPSHOT.BAT script can be downloaded from <http://cyber-defense.sans.org/blog/downloads> (in the Downloads section, get the zip file for SEC505). The zip file on that site includes this script and many others, so extract all its contents to a folder and then do a file search for the script you want.

The SHA256DEEP.EXE tool used in the script can be downloaded for free from <http://md5deep.sourceforge.net>. Another free tool in the script, AUTORUNSC.EXE, can be downloaded from <http://www.microsoft.com/sysinternals/>.

```
REM Set FOLDER variable to contain output files. The format for
REM will look like "SERVERNAME-2012-06-05-11-03" (-year-month-day-hour-minute).
FOR /F "TOKENS=1* EOL=/ DELIMS= " %%A IN ('DATE.EXE /t') DO SET STARTDATE=%%B
FOR /F "TOKENS=1,2 EOL=/ DELIMS= " %%A IN ('DATE.EXE /t') DO SET MM=%%B
FOR /F "TOKENS=1,2 EOL=/ DELIMS=/" %%A IN ('echo %STARTDATE%') DO SET DD=%%B
FOR /F "TOKENS=2,3 EOL=/ DELIMS=/" %%A IN ('echo %STARTDATE%') DO SET YYYY=%%B
FOR /F "TOKENS=1,2 EOL=/ DELIMS=:" %%A IN ('TIME.EXE /t') DO SET HH=%%A
FOR /F "TOKENS=1,2 EOL=/ DELIMS=:" %%A IN ('TIME.EXE /t') DO SET MIN=%%B
SET FOLDER=%COMPUTERNAME%-%YYYY%-%MM%-%DD%-%HH%-%MIN%
```

#### **REM Create folder in current working directory**

```
mkdir %FOLDER%
cd %FOLDER%
```

#### **REM Create README file**

```
ECHO SYSTEM FORENSICS SNAPSHOT > README.TXT
ECHO Computer: %COMPUTERNAME% >> README.TXT
ECHO Date: %DATE% >> README.TXT
ECHO Time: %TIME% >> README.TXT
ECHO Batchfile: %CD%\%0 >> README.TXT
ECHO User: %USERNAME%@%USERDOMAIN% >> README.TXT
```

#### **REM MSINFO32.EXE Report**

```
start /wait msinfo32.exe /report MSINFO32-Report.txt
```

#### **REM Computer System**

```
wmic.exe computersystem list full > Computer-Info.txt
```

#### **REM BIOS**

```
wmic.exe bios list full > BIOS.txt
```

#### **REM Environment Variables**

```
set > Environment-Variables.txt
```

#### **REM Users**

```
wmic.exe useraccount list full > Users.txt
```

#### **REM Groups**

```
wmic.exe path win32_group get /value > Groups.txt
```

#### **REM Group Members**

```
wmic.exe path win32_groupuser get /value > Group-Members.txt
```

**REM Password and Lockout Policies**

net.exe accounts > Password-And-Lockout-Policies.txt

**REM Local Audit Policy**

auditpol.exe /get /category:\* > Audit-Policy.txt

**REM SECDIT Security Policy Export**

secedit.exe /export /cfg SecEdit-Security-Policy.txt 1>nul 2>nul

**REM Shared Folders**

wmic.exe share list full > Shared-Folders.txt

**REM Networking Configuration**

ipconfig.exe /all > Network-IPConfig.txt

netstat.exe -ano > Network-NetStat.txt

route.exe print > Network-Route.txt

nbtstat.exe -n > Network-NbtStat.txt

netsh.exe winsock show catalog > Network-WinSock.txt

wmic.exe path win32\_networkadapterconfiguration get /value > Network-NIC.txt

**REM Windows Firewall and IPSec Connection Rules**

netsh.exe firewall show config verbose = enable > Network-Firewall.txt

netsh.exe advfirewall show allprofiles > Network-Firewall-Profiles.txt

netsh.exe advfirewall show global > Network-Firewall-Global-Settings.txt

netsh.exe advfirewall firewall show rule name=all > Network-Firewall-Rules.txt

netsh.exe advfirewall export "Network-Firewall-Export.wfw" 1>nul 2>nul

netsh.exe advfirewall consec show rule name=all > Network-Firewall-IPSec-Rules.txt

**REM IPSec Configuration (XP/2003)**

netsh.exe ipsec static show all > Network-IPSec-Static.txt

netsh.exe ipsec dynamic show all > Network-IPSec-Dynamic.txt

**REM Processes**

wmic.exe process list full > Processes.txt

**REM Drivers**

wmic.exe sysdriver list full > Drivers.txt

**REM Services**

wmic.exe service list full > Services.txt

**REM Registry Exports (Add more as you want)**

```
reg.exe export hklm\system\CurrentControlSet Registry-CurrentControlSet.txt /y  
reg.exe export hklm\software\microsoft\windows\currentversion Registry-WindowsCurrentVersion.txt /y
```

**REM Sysinternals AutoRuns**

```
autorunsc.exe -accepteula -a -c 2>nul 1> AutoRuns.txt
```

**REM Hidden Files with Last-Modified Dates**

```
dir %SYSTEMDRIVE%\ /A:H /S /ON /T:W /N /R > FileSystem-Hidden-Files.txt
```

**REM Files with Last-Modified Dates**

```
dir %SYSTEMDRIVE%\ /A:-D /S /ON /T:W /N /R > FileSystem-Files.txt
```

**REM NTFS Permissions and Integrity Labels**

```
icacls.exe %SYSTEMDRIVE% /t /c /q 2>nul > FileSystem-NTFS-Permissions.txt
```

**REM SHA256 File Hashes**

**REM VERY TIME AND SPACE CONSUMING!**

**REM Add more paths as you wish of course...**

```
sha256deep.exe -s "c:\*" 2>nul > Hashes-C.txt  
sha256deep.exe -s "d:\*" 2>nul > Hashes-D.txt  
sha256deep.exe -s -r "%PROGRAMFILES%\*" 2>nul > Hashes-ProgramFiles.txt  
sha256deep.exe -s -r "%SYSTEMROOT%\*" 2>nul > Hashes-SystemRoot.txt
```

**REM \*\*\*END OF SCRIPT\*\*\***

The uppercase words in percentage signs (for example, %SYSTEMDRIVE%) are environment variables that are translated when the script is run. You can see your variables and their mappings by opening a CMD.EXE command prompt window and executing set. The command-line switches 1>nul and 2>nul redirect standard-out and error-out, respectively, into a black hole so that this data will not be seen.

To gather data from a remote computer, run the script on that remote machine, perhaps with PSEXEC.EXE, and then move the files from the remote computer to the local one, perhaps through the hidden C\$ share.

*But what should you do with all this data?*

# Change Detection and Analysis

- It's hard to detect a compromise because skilled hackers and well-designed malware leave only subtle traces of their intrusions
- There is no magic Perform Forensics button; it takes a human being to understand and analyze all this data
- **Use the snapshot files as a baseline for comparison, along with your logs and other forensic artifacts, to detect malicious changes**



SANS Security Essentials – © 2016 SANS

## Change Detection and Analysis

The whole point of gathering all this snapshot and logging data is to detect covert changes to our systems, explain how the changes were made, stop the spread of further damage, to hopefully repair the damage that already has been done, and to learn what vulnerability made it possible in the first place so that you can prevent it from happening again. If you simply restore the server from last night's backup, why won't it be immediately compromised again? And how do you know your backups don't already contain the compromise?

### Detecting Changes

If hackers have formatted your hard drives, this is easy to detect, but other changes will be invisible unless you specifically look for them. This is where comparing the current snapshot against earlier ones really helps. What's the best way to do the comparison?

You always can do an "eyeball audit" with two copies of Notepad side-by-side, a snapshot in each. But Notepad is an anemic text viewer; you might try the free Notepad++ instead.

But eyeball audits can't be automated. Fortunately, there are other tools that can compare two similar text files and print only their differences. One of these is a built-in tool named FC.EXE. FC works from the command line. It takes two files, compares them, and prints each set of mismatches, along with their line numbers. With the line numbers you can open the files in a text editor and jump straight to that line number. If you want something PowerShell flavored, look at the compare-object cmdlet.

If you'd like a graphical comparison tool, there is WINDIFF.EXE from Microsoft. (And it can work from the command-line, too.) WINDIFF highlights the mismatching lines from the files in different colors, and you can jump back and forth between mismatches easily. Similar free tools with more features are CSDIFF ([www.componentsoftware.com](http://www.componentsoftware.com)) and WinMerge ([www.winmerge.org](http://www.winmerge.org)). In general, there are many file comparison tools available for free or inexpensive purchase ([http://en.wikipedia.org/wiki/Comparison\\_of\\_file\\_comparison\\_tools](http://en.wikipedia.org/wiki/Comparison_of_file_comparison_tools)).

In the end, though, it takes a human being to understand and analyze the data from all these snapshot files, and that'll be true for some years to come. Even when vendors have products that perform "automatic analysis," actually what you're getting is an alert based on host-IDS signatures of some sort, not analysis in the sense of explanation or risk assessment that's customized to your environment. How to perform this analysis is beyond the scope of Security Essentials, but file comparison tools for your snapshot files can at least get you started.

If you want to learn more about Windows forensics, SANS has a number of excellent courses for this, such as FOR408 and FOR508.

# Summary

- **Automation:**
  - PowerShell
  - Resource Kit
  - Third-party Tools
  - Scripting
  - Task Scheduler
- **Auditing:**
  - Policy Compliance
  - Vulnerability Scanning
  - Ongoing Logging
- **Forensics:**
  - Get ready to be compromised!
  - Create baselines for comparison.
  - Gather the artifacts you'll need to understand what's changed.
  - Perform change analysis using automation and scripting.

SANS Security Essentials – © 2016 SANS

## Summary

The purpose of this module was to introduce you to Windows automation, auditing, and forensics. We audit our networks so that we can discover vulnerabilities before the bad guys do. We hope to detect harmful changes. We'll need automation tools so that we don't have to do it all by hand.

Auditing as a process is composed of a variety of activities, including verifying policy compliance and vulnerability scanning. Forensics includes collecting system snapshots, gathering log data, detecting changes, and analyzing how and why those changes occurred. We looked at a script for making snapshots and discussed tools for working with them.

Automation tools and scripts are terribly important to avoid tedium and errors. The more a process can be automated, the more standardized the data gathered, the more useful that data is, and the more consistently the work will be performed.

Windows was designed to be as manageable from the command line and scripts as Microsoft could make it because Microsoft now wants to compete head-on with Linux. PowerShell, the various Resource Kits, and many websites provide wonderful scripts and command-line utilities to help us do more in less time.

We hope that these resources and the skills you are learning now can enable you to secure your networks and expand your professional horizons.

---

## **SEC401 Lab Tools – Windows Security**

---

SANS Security Essentials – © 2016 SANS

### **SEC401 Lab Tools – Windows Security**

This section intentionally left blank.

---

## **Security Configuration and Analysis Tool**

---

SCA is an MMC snap-in that enables administrators to make a wide variety of changes to a system from a single interface.

SANS Security Essentials – © 2016 SANS

### **Security Configuration and Analysis Tool**

The Security Configuration and Analysis (SCA) tool is probably one of the most powerful administrative tools in Windows that most administrators do not know exist. It has the ability to do what so many organizations want to do to their systems but do not know how to begin: baselining.

SCA can make myriad important and relevant changes to a system from a single console.

## SCA Details

- Name: Security Configuration and Analysis
- Operating system: Windows
- License: Part of the OS
- Protocol used: NA
- Category: System configuration
- Description: SCA is a system-configuration tool that enables administrators to quickly make machines conform to predefined system security templates
- URL: <http://www.microsoft.com>

SANS Security Essentials – © 2016 SANS

### SCA Details

The following topics and action items are covered in this section:

- Learning about the Security Configuration and Analysis tool and its many uses
- Examining all of the components available through SCA
- Analyzing your current systems against a default template
- Editing the templates to fit your needs
- Reconfiguring your systems to comply with the template

---

## SCA Background

---

- SCA is a tool built in to the Windows OS, which is used to audit systems against a security template as well as configure them
- Templates can be pushed to Windows devices through GPOs and login scripts
- SCA is an all-or-nothing tool with little protection from errors. You must validate any configuration changes prior to pushing them to a production environment

SANS Security Essentials – © 2016 SANS

### SCA Background

This section intentionally left blank.

---

## SCA Purpose

---

- Audits and configures Windows devices to conform to corporate security and configuration policies
- Eases the burden and task of baselining multiple systems in specific environments as well as rolling out changes that would otherwise require manual system changes on every device

SANS Security Essentials – © 2014 SANS

### SCA Purpose

This section intentionally left blank.

---

## SCA Architecture

---

- SCA is a snap-in for a custom MMC (Microsoft Management Console)
- It comes with many default templates that are provided for free by Microsoft and can be a base for creating custom templates
- You can download additional templates from groups such as NIST and SANS

SANS Security Essentials – © 2016 SANS

### SCA Architecture

When using SCA, you should note a few concerns and limitations. For one, you cannot harden a system and then create a specific template from that system; it only works the other way around. Also, there are no warnings or safeties when applying changes. If you make a mistake or make conflicting changes to your system, you might render a box useless. After a change is made, it is permanent; there is no undo key. The only option you might have is to apply one of the default templates that come with Windows to return the system to its default state. The issue is that any custom edits made to your template are not undone.

## Installation

- Right sweep on screen. From the menu select search, mmc, and click the **mmc**
- Click **Console, Add/Remove snap-in**
- Click **Add** and choose the **Security Configuration and Analysis and Security Templates**
- Click **OK** until you are back to the original MMC

SANS Security Essentials – © 2016 SANS

## Installation

This section intentionally left blank.

---

## Running SCA

---

- You can save the new MMC to the desktop for easy use
- You must have administrative privileges to run SCA



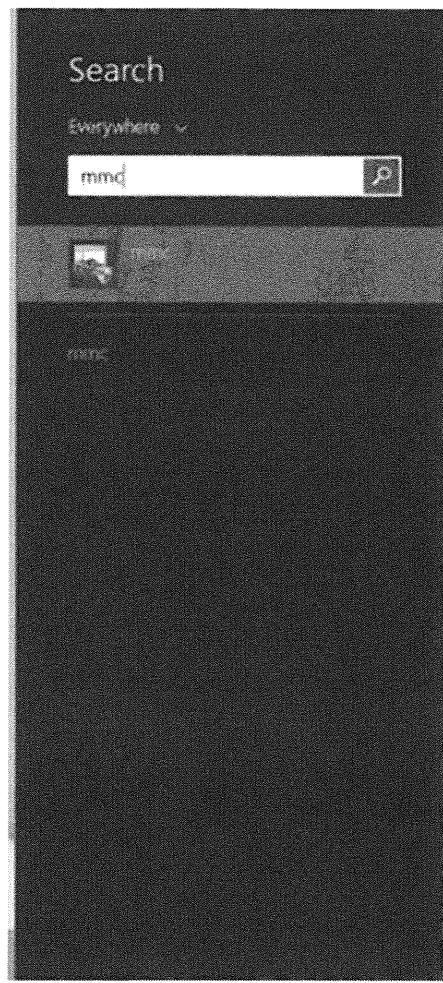
### Running SCA

To install and run SCA, perform the following steps:

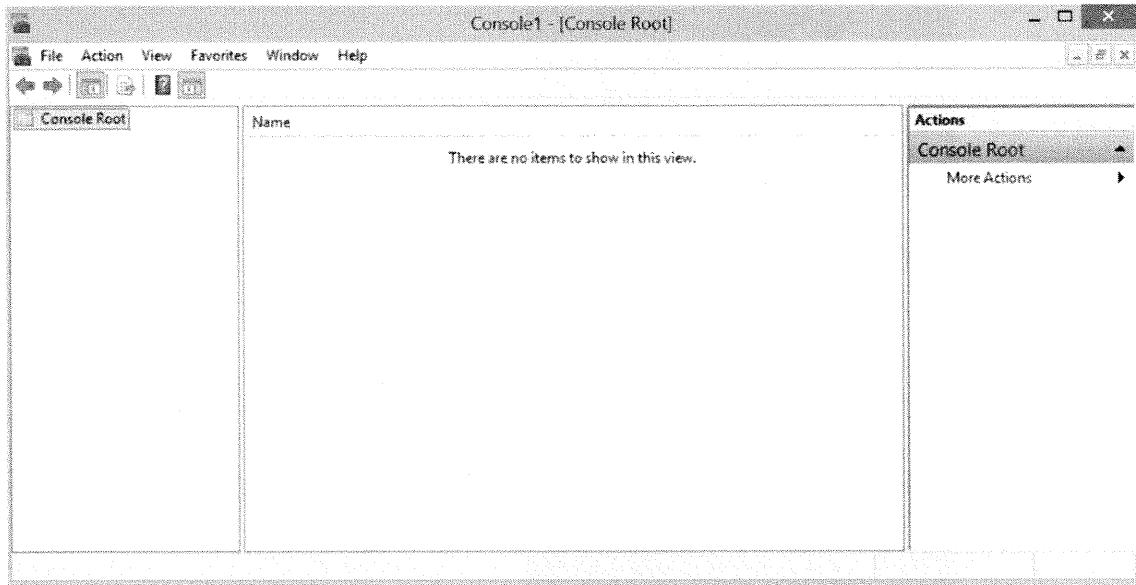
1. A benefit of this tool is that it does not require installation. To begin, sweep from the right side of your screen to pull up the menu.



2. Click *Search*, type **mmc**, and click *mmc*.



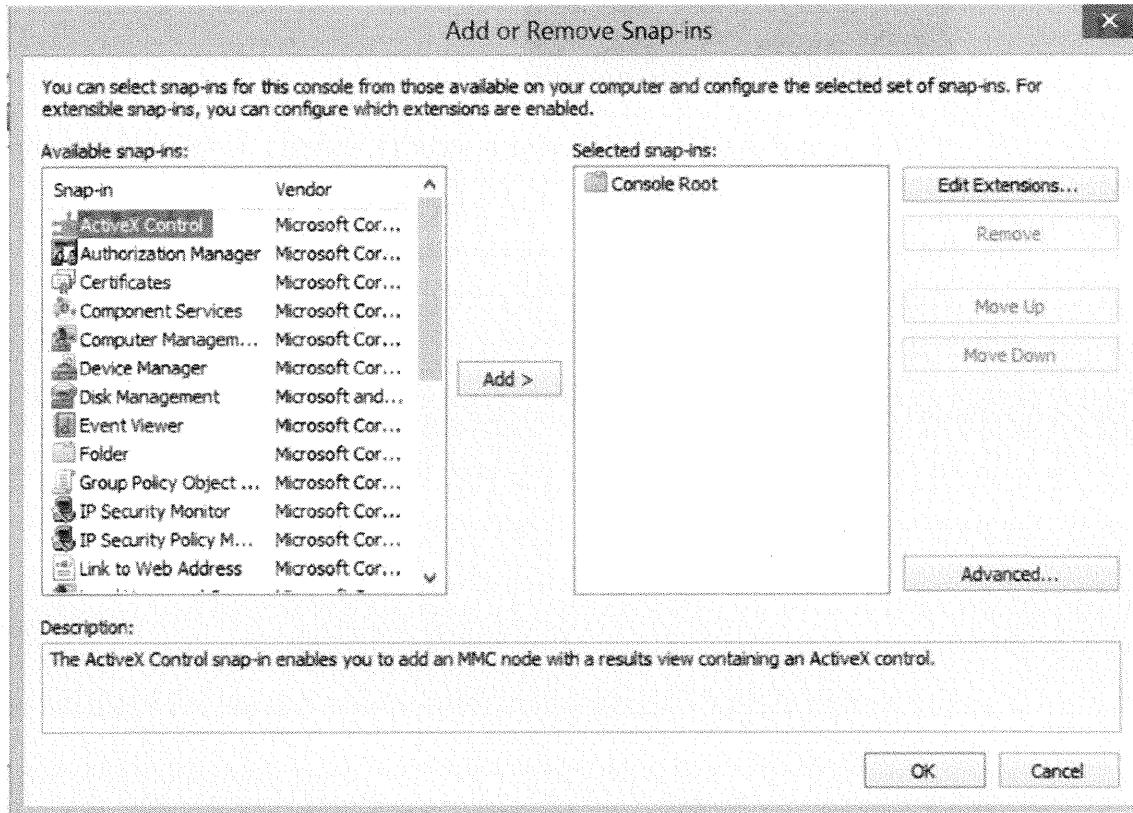
3. If UAC is enabled, you will receive a security warning. If this window appears, click *Yes* to proceed.
4. An MMC window displays. It looks similar to the computer management console, because the computer management console is actually an MMC plugin.



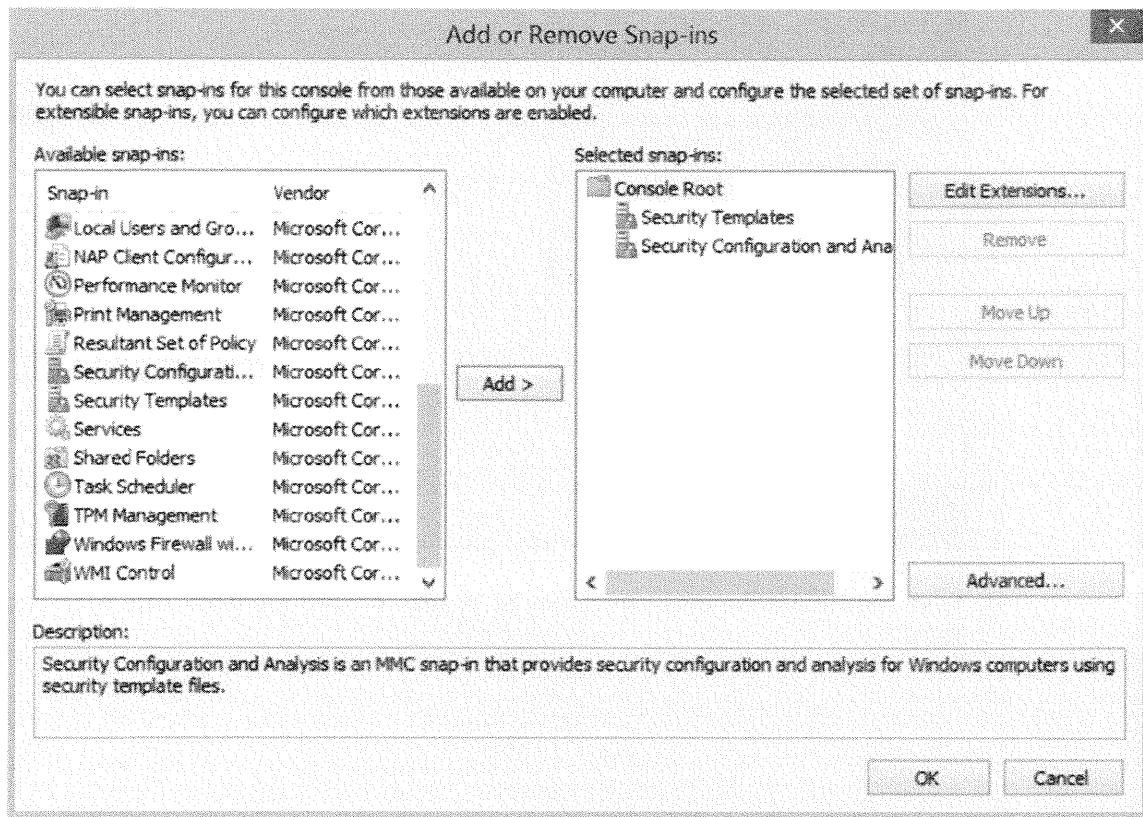
## Adding Plugins to MMCs

To add your own plugins to the blank MMC, perform the following steps:

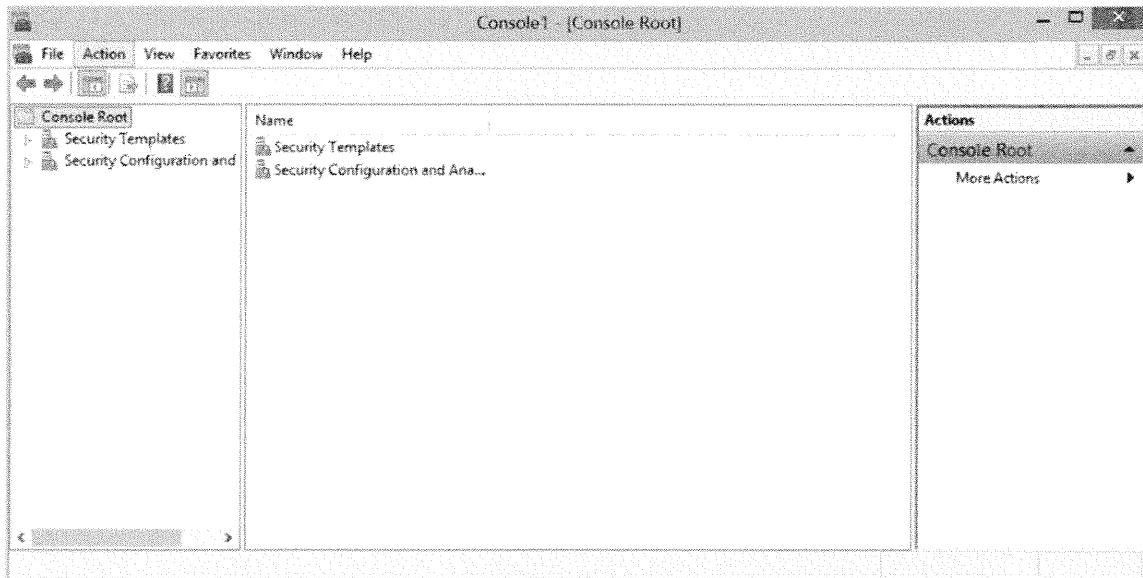
1. Click *Console Root*, and click *File, Add/Remove Snap-in*. The Add or Remove Snap-in window displays.



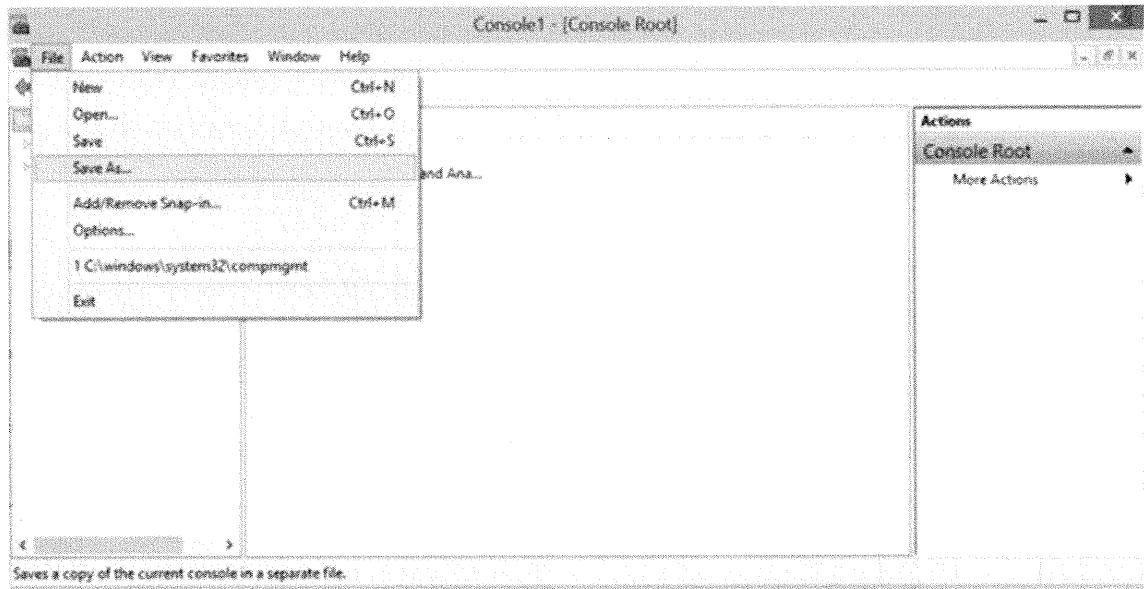
- To add the Security Templates and Security Configuration and Analysis plugins, scroll to the bottom of the list, select each plugin, and click *Add*. After you are done, click *OK*.



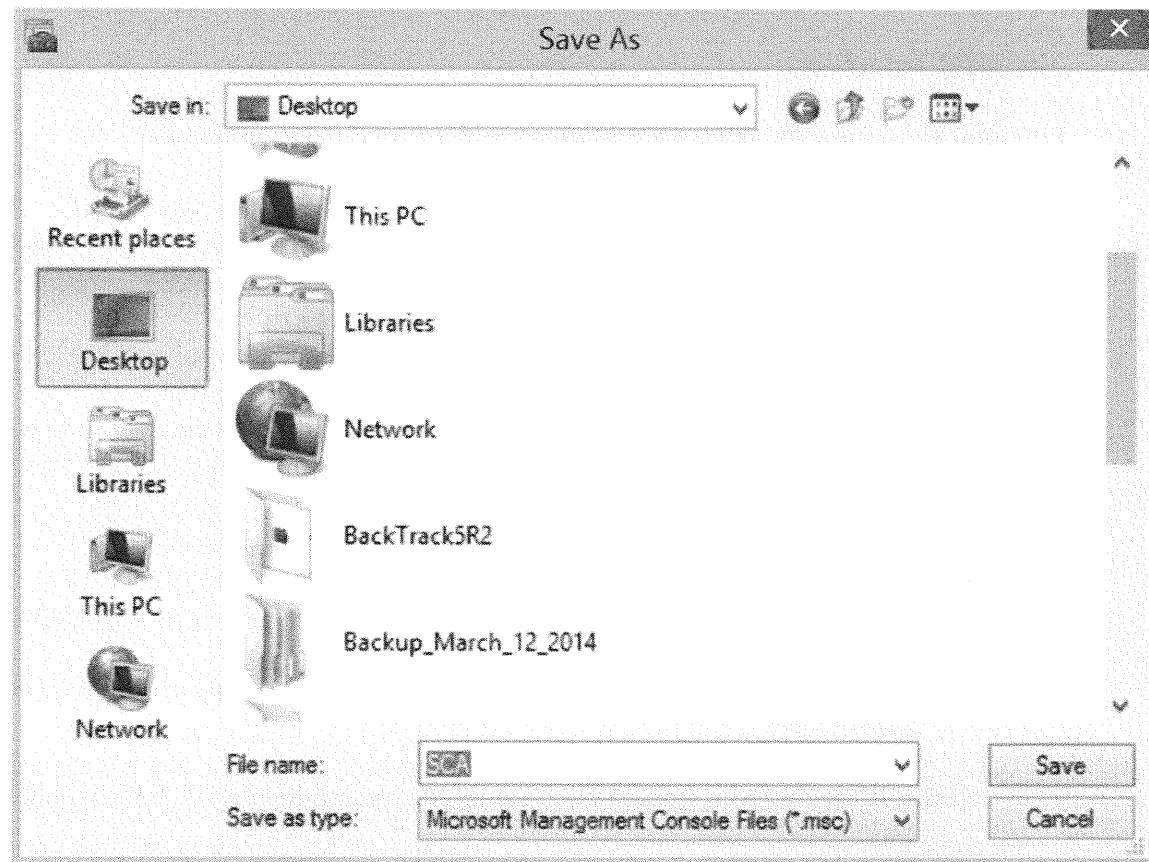
The MMC window displays with the two snap-ins just added.



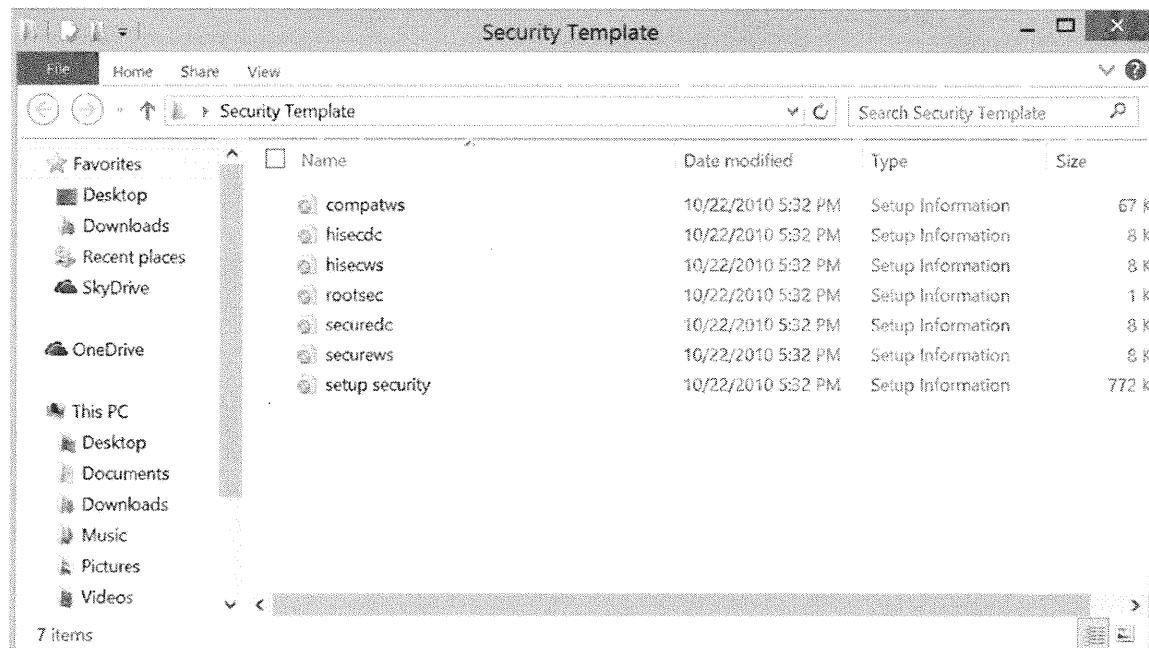
3. Before going any further, you should save your custom MMC setup so you can get back to it later if needed. Click *File, Save As*.



4. Save the file on the desktop. Enter **SCA.msc** for the filename, and then click *Save*.



5. For Windows 8, you have to copy sample templates off your DVD. Insert the Windows 8 DVD into your computer and copy the entire Security Templates directory to your desktop.

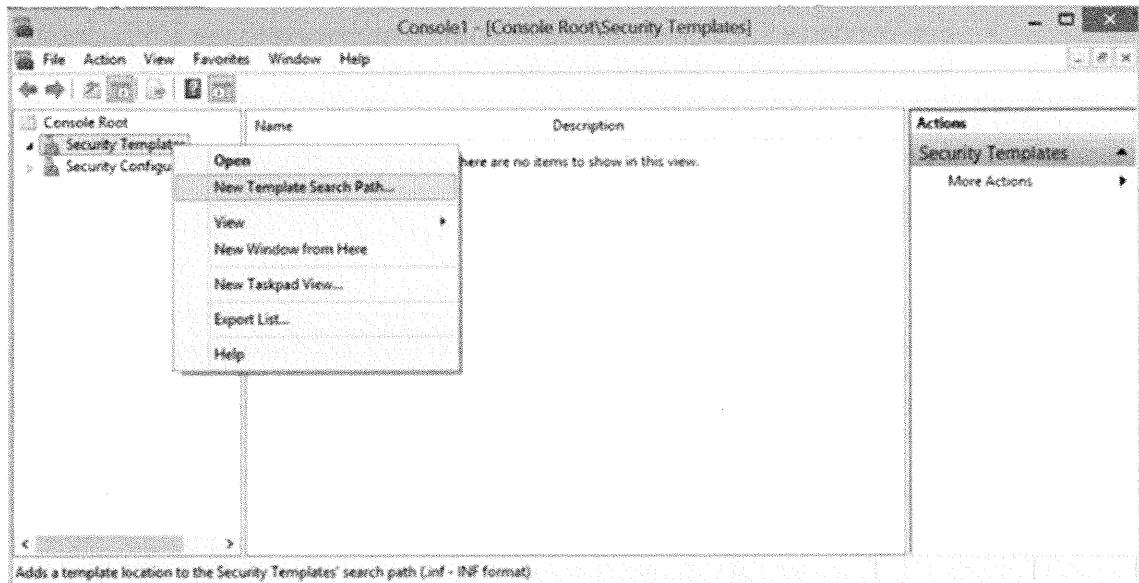


## Microsoft Templates

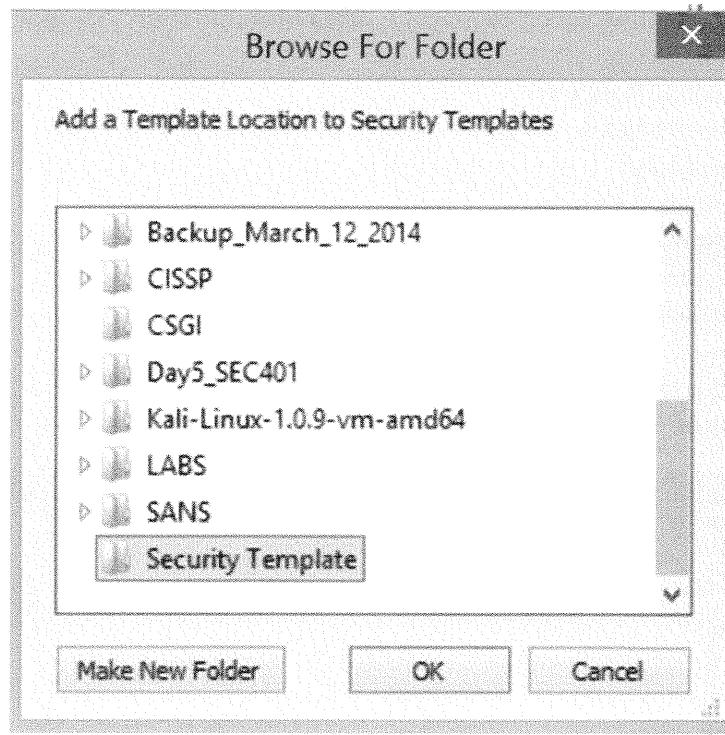
Let's quickly review the purpose behind each of the Microsoft templates:

- **Compatws:** You can use this template so you don't have to place users in the power users group to run certain applications. Basically, it relaxes the restrictions on the users group, which is not considered a good template for secure environments.
- **Hisecdc:** This is the high-security template for domain controllers. It is a good template to use as a baseline for creating a more secure Windows XP environment. This template forces the machine it is applied against to digitally sign all network communications. Because of this, communications with a lower-level Windows client or server might not be possible.
- **Hisecws:** This template is the same as the preceding one except it is for workstations.
- **Securedc and securews:** These templates are provided for secure systems.
  1. To load the templates, right-click *Security Templates* and click *New Template Search Path*.

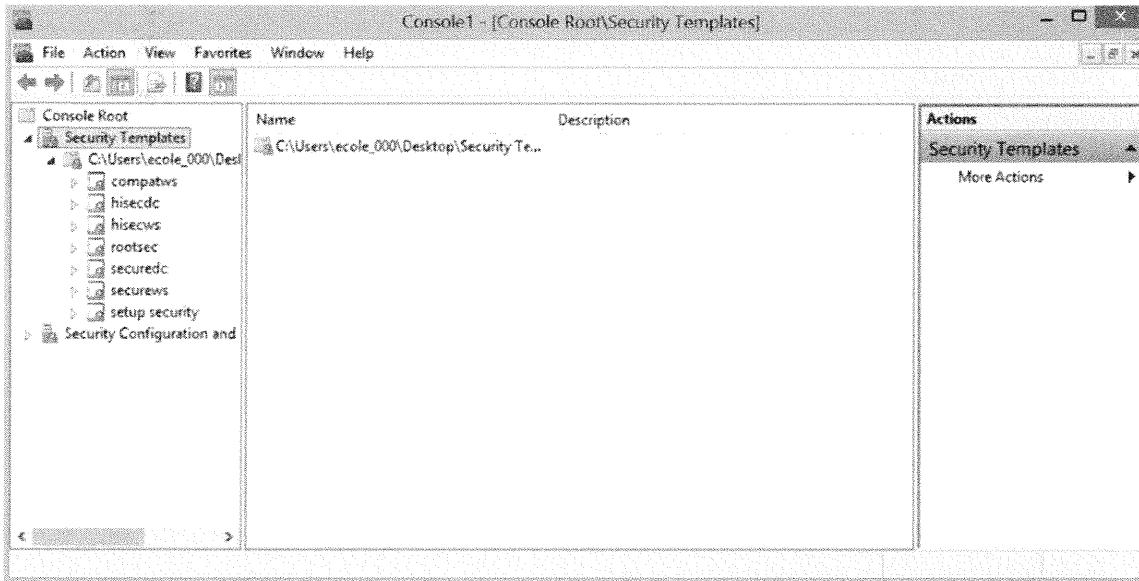
**Note:** If the option is grayed out, you might have to delete the default path that is currently listed.



2. Select the Security Template directory that you copied to your desktop and click *OK*.



3. Click the *arrow* next to Security Templates to show the new directory you just added. Click the *arrow* next to the directory to show all the loaded templates.

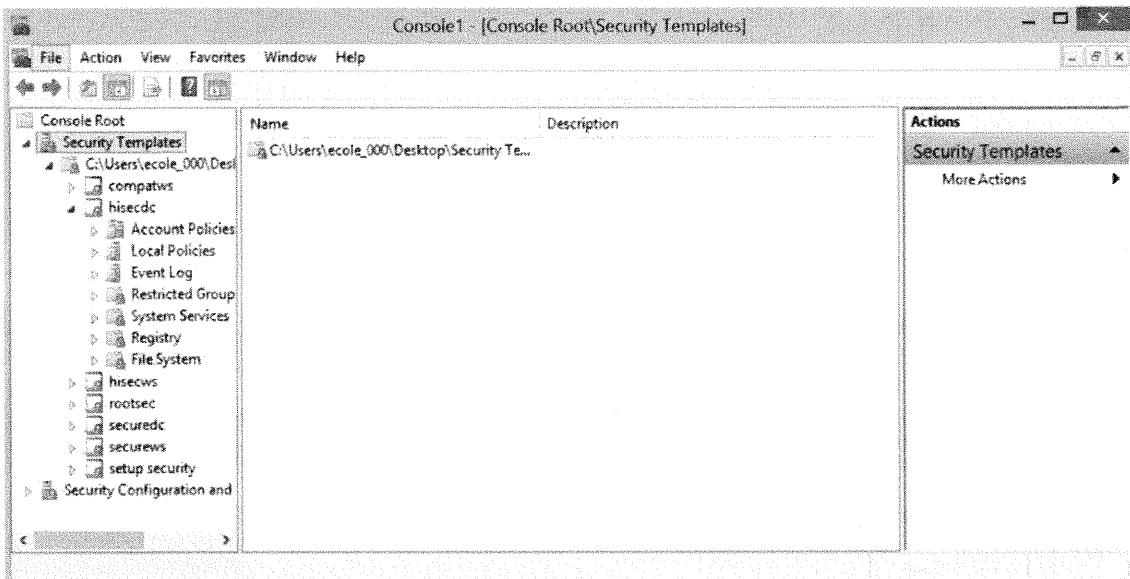


4. Click the *hisecdc* template and click the *arrow* next to it. Normally, this template is for high-security domain controllers, but you will use it for this lab due to the number of changes it provides. You can choose to pick another template if you want.

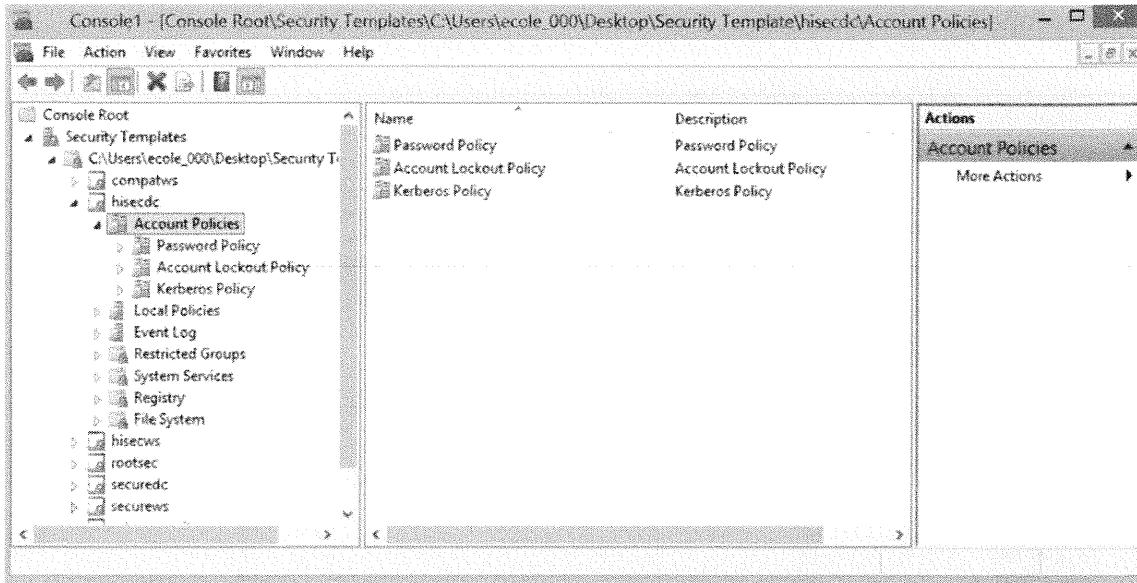
You can manipulate seven main categories of items from this tool:

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System

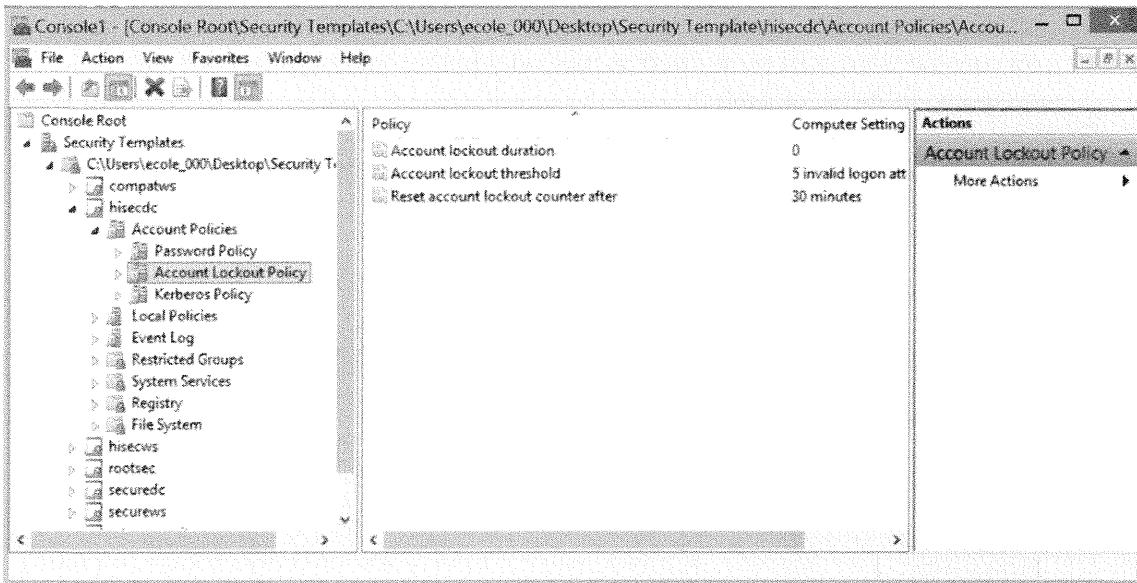
Let's spend a few minutes going through each category and the different subsections of each of these categories.



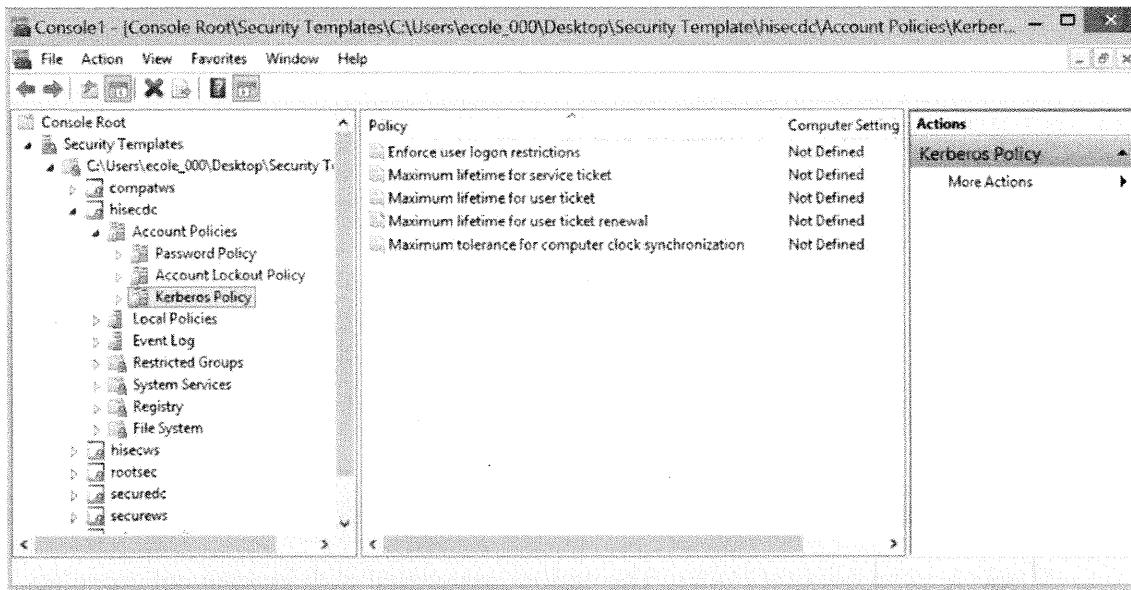
1. To open Account Policies, click the arrow next to it, and then highlight *Password Policy*. From this menu, you can view the template settings with regards to passwords. In the right pane, you see the different settings, which are the template settings, not the computer settings. This template defines strong passphrase requirements.



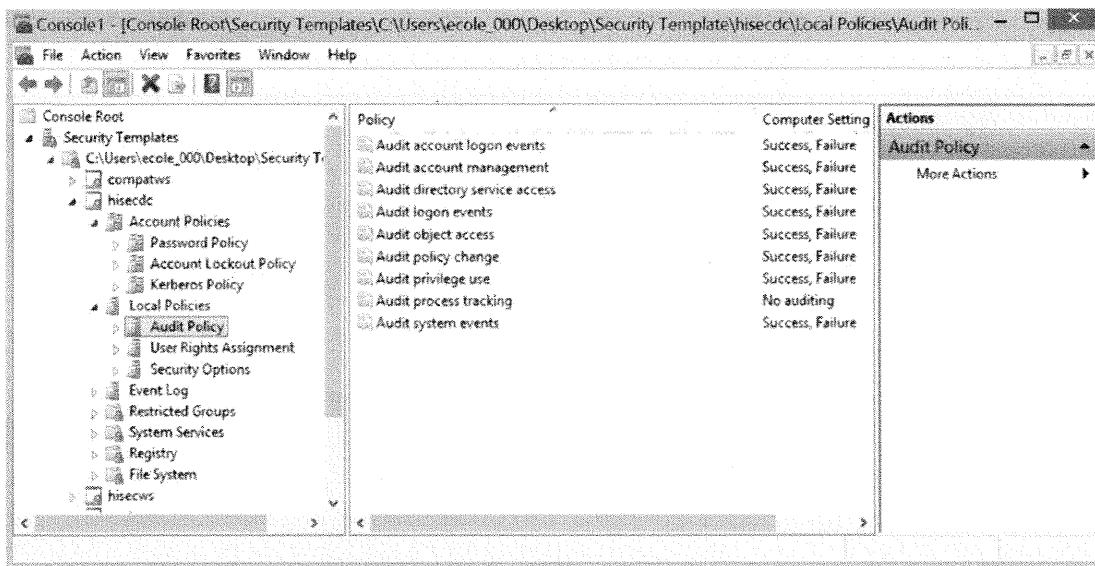
2. Click *Account Lockout Policy*. The options associated with locking out accounts as well as restoring them are displayed.



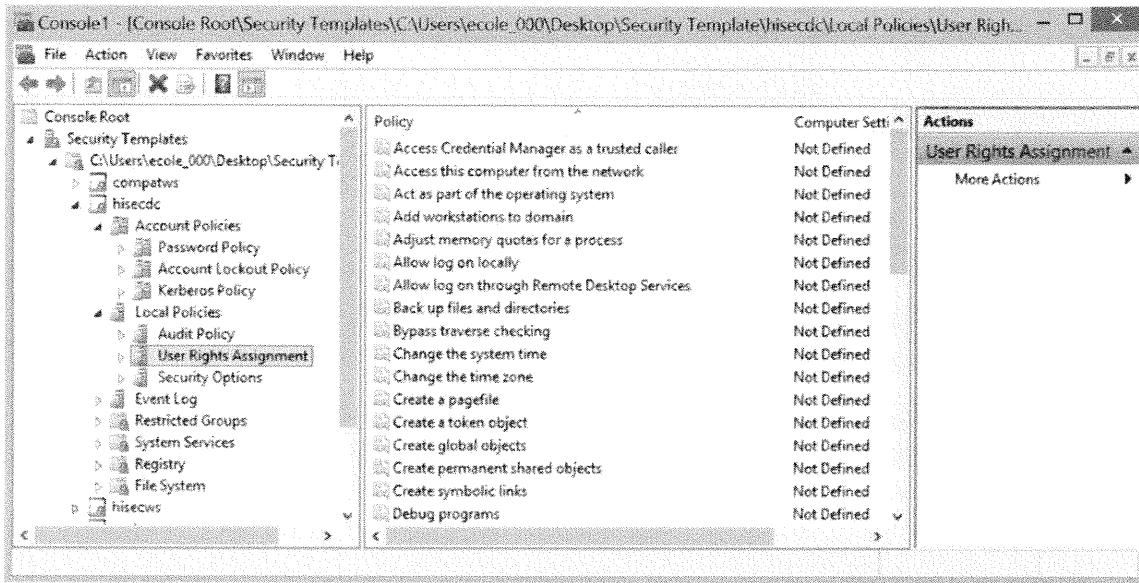
- Click *Kerberos Policy* to display the Kerberos options. Be careful when dealing with Kerberos. If you are part of a mixed network, you might have systems that don't support Kerberos trying to log in to your system. If you set your system to require Kerberos authentication, systems that don't support Kerberos will not properly authenticate to your system.



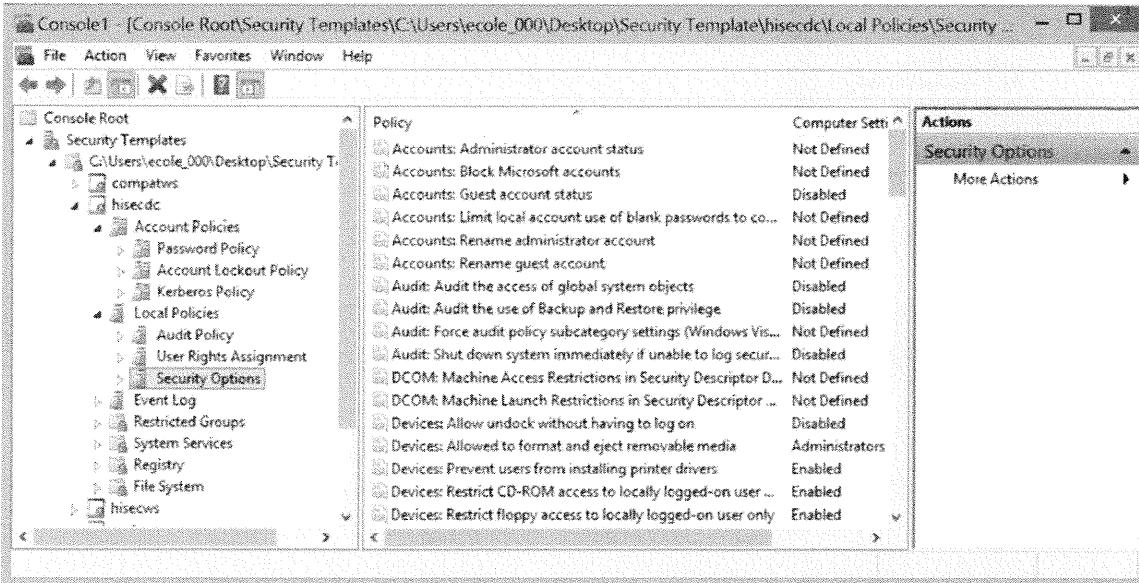
- Click the arrow in front of Local Policies and click *Audit Policy*. By default, auditing is turned on for Windows machines. Under the Audit Policy category, you can see what will be audited as well as whether your system will log successes, failures, or both.



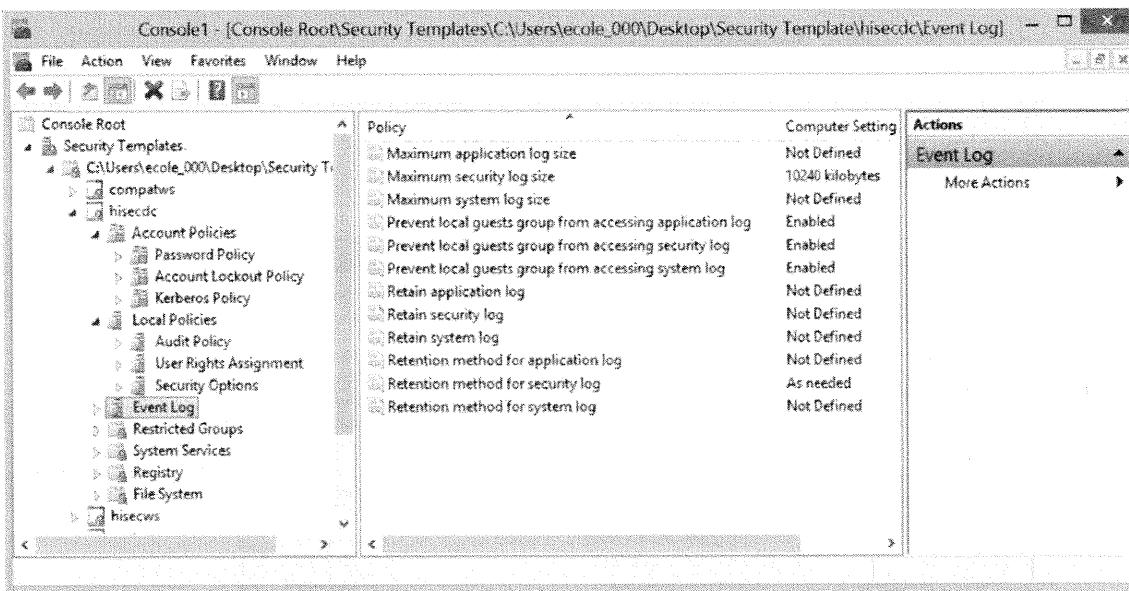
5. Click *User Rights Assignment*. From here, you can define what accounts have certain special rights on the system. For example, you can specify that a particular group or user has the right to force shutdown from a remote system, or you can deny logon locally to specific groups. Undefined means that it is undefined in the template file, not on the actual system.



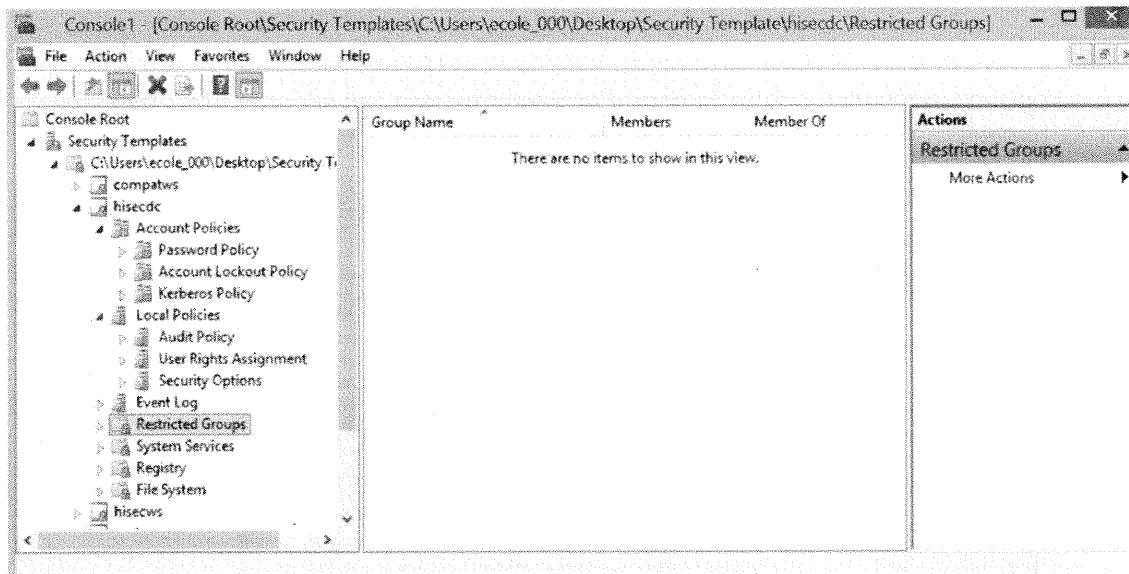
6. Click *Security Options*. From here, you can enable or disable any of the security options available on your system. For example, you can set up a login message banner.



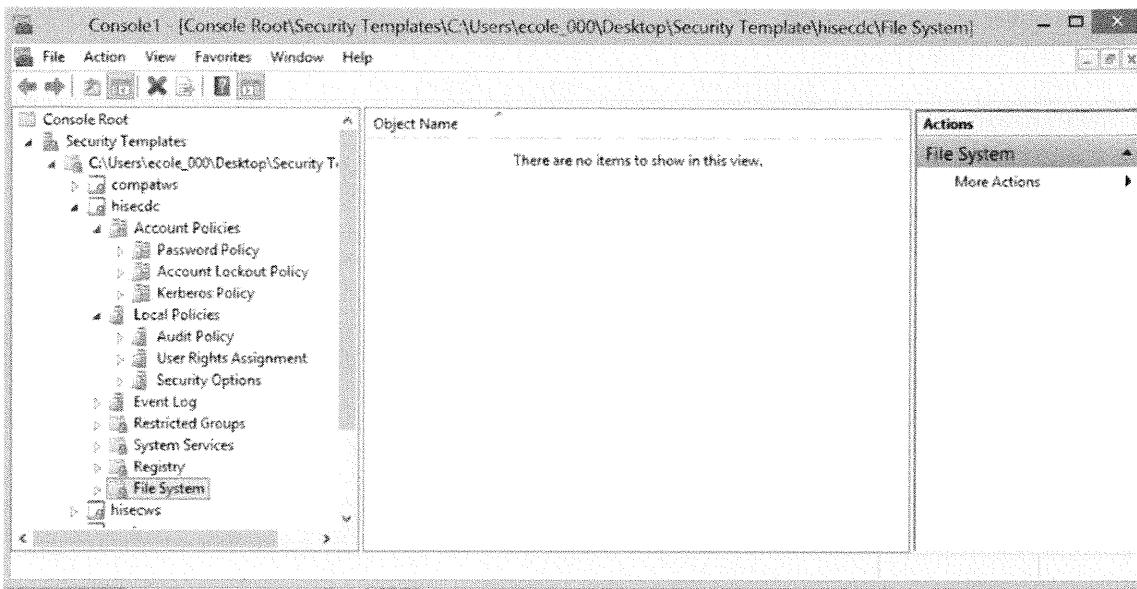
7. Click *Event Log*. From here, you can set the different event log settings such as log size and guest restrictions to your logs.



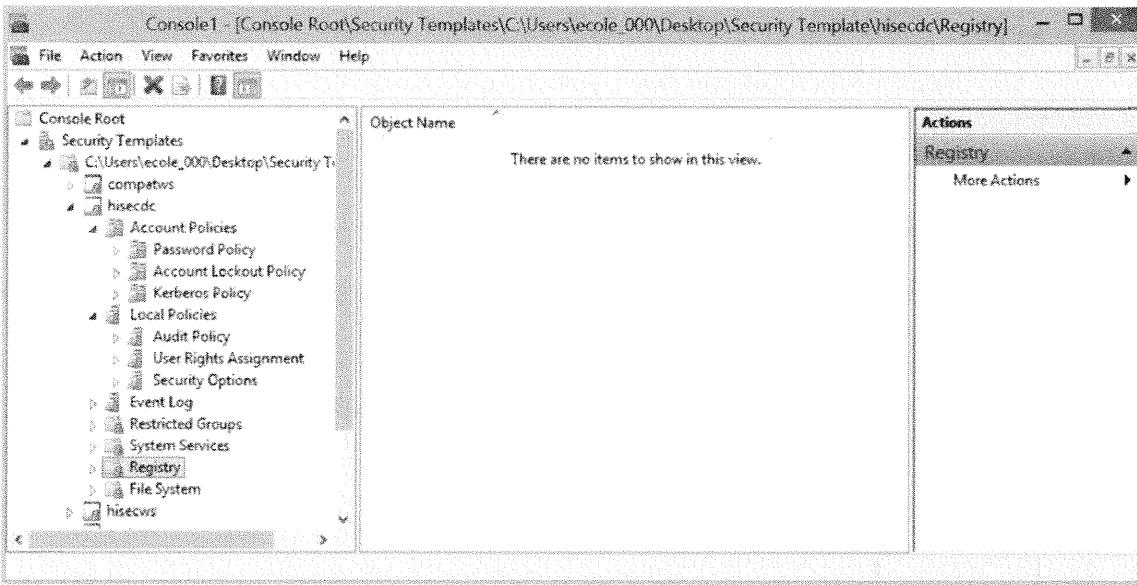
8. Click *Restricted Groups*. Any group placed in the Restricted Groups category cannot add new members. You would need to remove a particular group from the restricted group, add the user, and then place the group back to the restricted group.



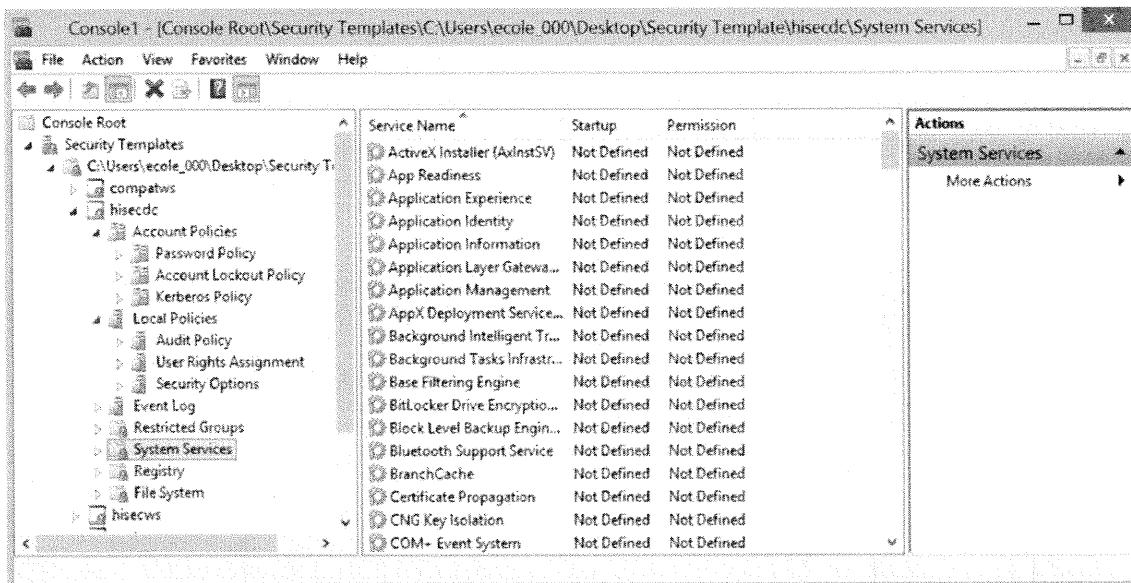
9. You also have the ability to globally change access control lists (ACLs) associated with any file or folder located on your drives. Click *File System*. From here, you can view the entire directory structure on your drive.



10. Click *Registry*. From SCA, you have the ability to set particular permissions to a subset of registry hives and keys.



11. Click *System Services*. From here, you can set the startup mode for each service to Automatic, Manual, or Disabled. You can also set certain permissions.

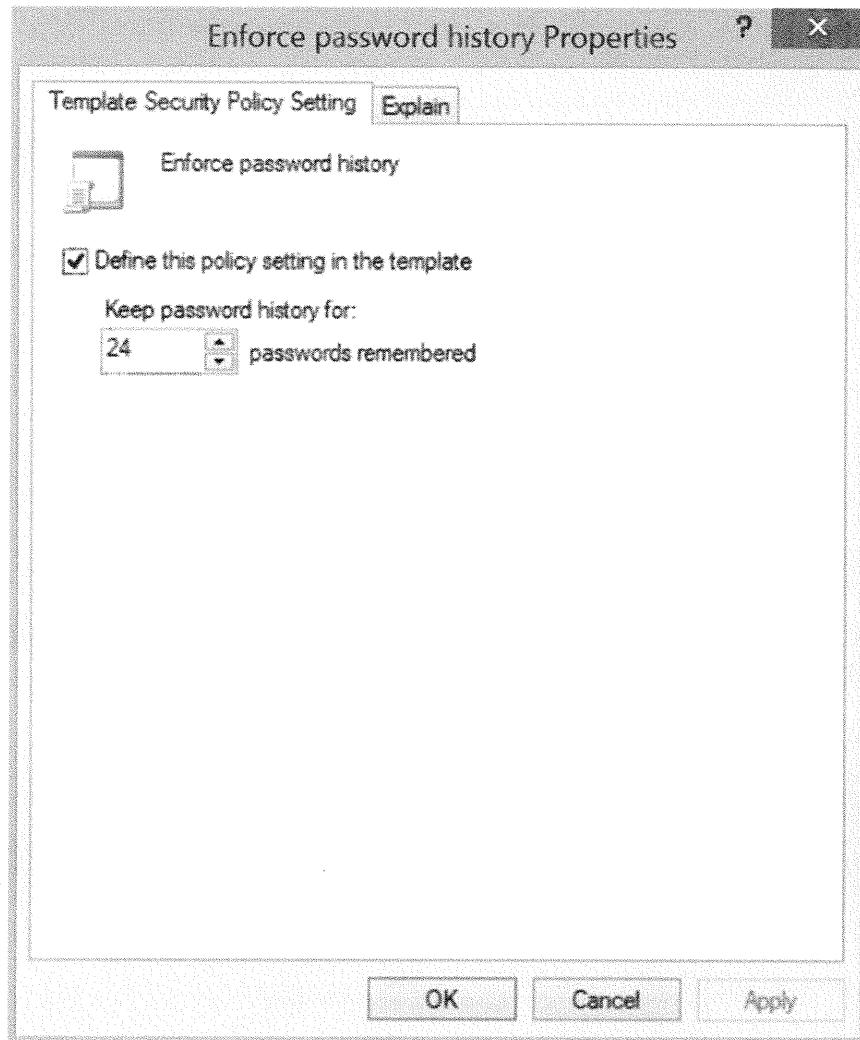


## Modifying Template Settings

This tool has the ability to modify the templates from this screen. To modify any of the settings, simply right-click a particular item in the right pane and click *Properties*, or double-click the item you want to change. From here, you can change the setting to whatever you choose. When you are done, you can either save the changes to the particular template by choosing *File, Save* or save it as a new template by choosing *File, Save As*.

## Defining Policy Settings in Templates

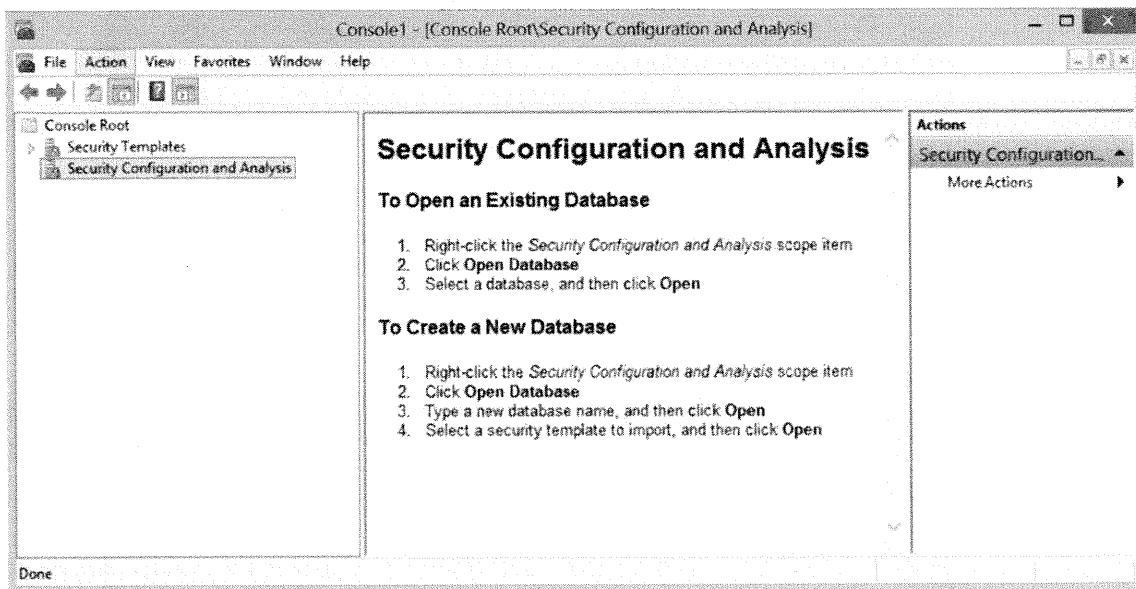
1. In the left pane, click *Password Policy*, and then in the right pane, double-click *Enforce password History*. The Enforce password history Properties window displays. From here, you can choose to define this policy setting in this template, and choose the number of passwords the system remembers before allowing a user to reuse the password.



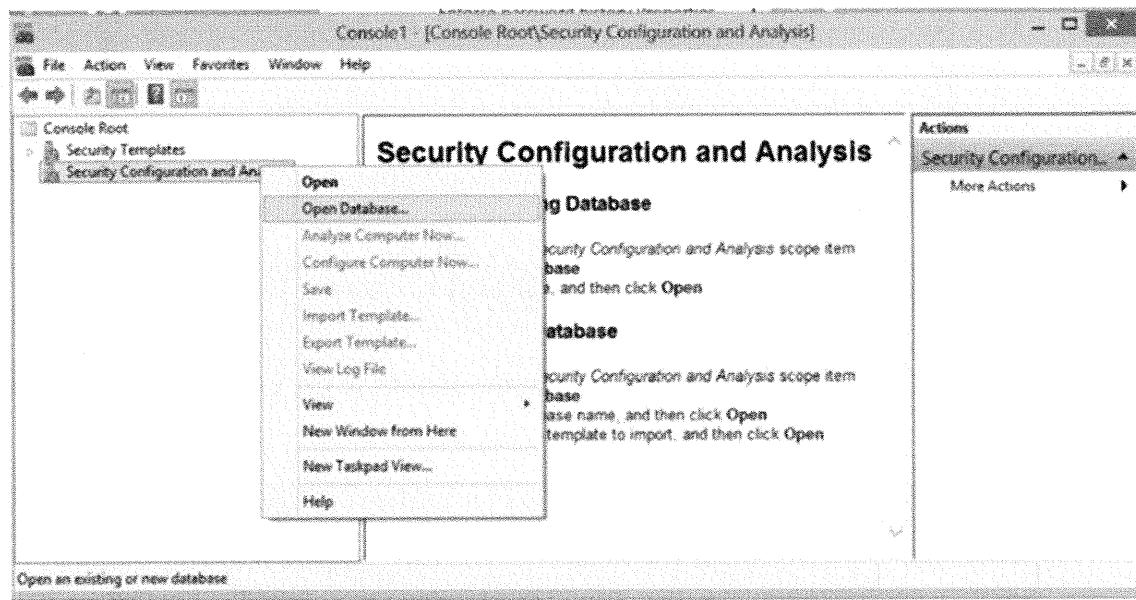
2. Spend a few minutes reviewing each of the options to get a better feeling for the different things you can do.

## Comparing Templates

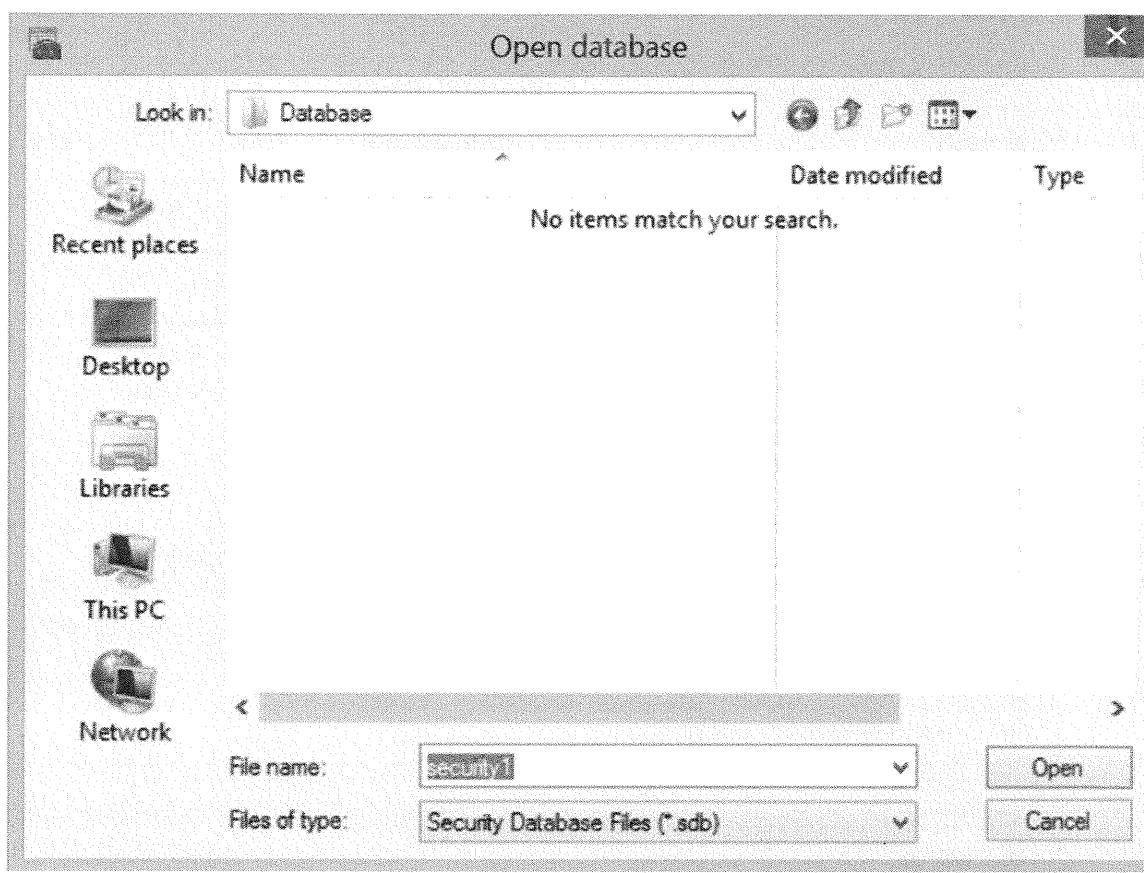
1. Now that you have edited your template, you can compare it to your current system configuration and then bring your system inline with the template. Click *Security Configuration and Analysis*. Microsoft provides some instruction on how to proceed in the right pane.



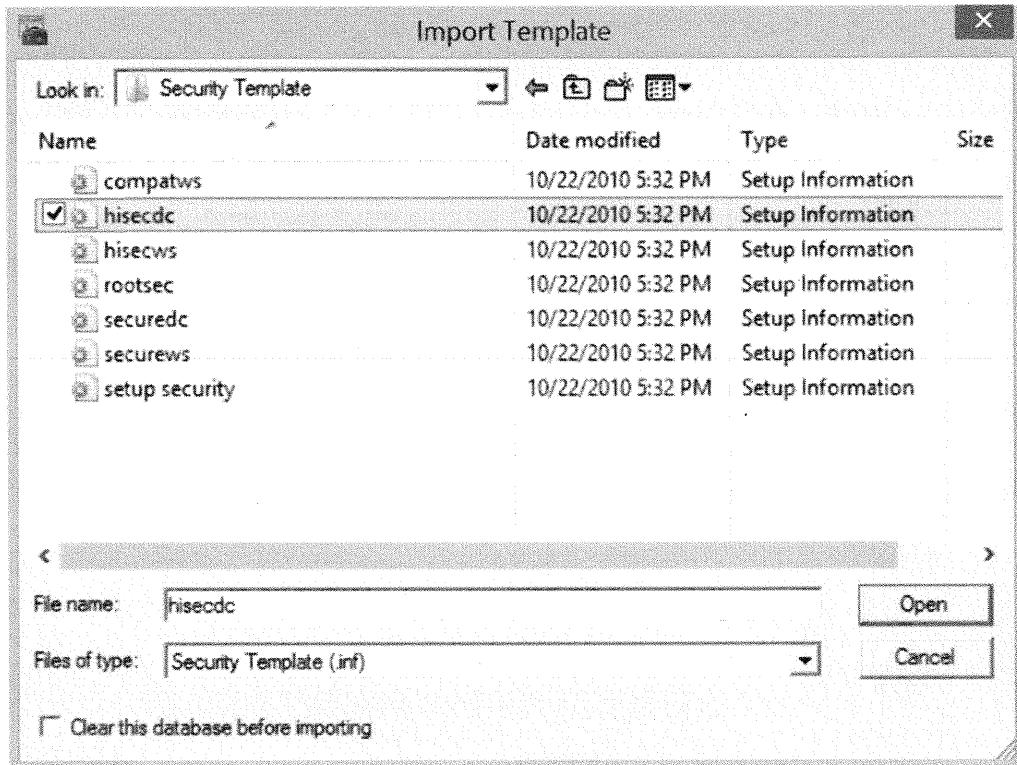
2. To create a new database, right-click *Security Configuration and Analysis* and click *Open database*.



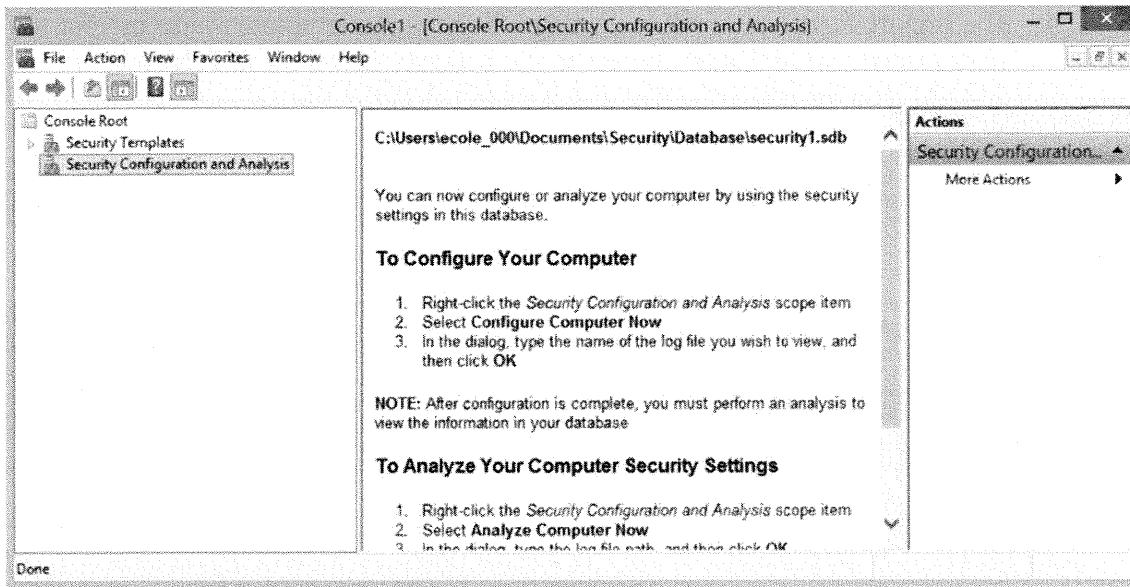
3. After the Open database window displays, in the File name field, type **Security1.sdb** and click **Save** to save to the desktop. Click **Open**.



4. The Import Template window displays. To import a template to use in your tool, click *hisecdc.inf*. Because you saved the Security Template directory to the desktop, you have to go to that directory to select the file.



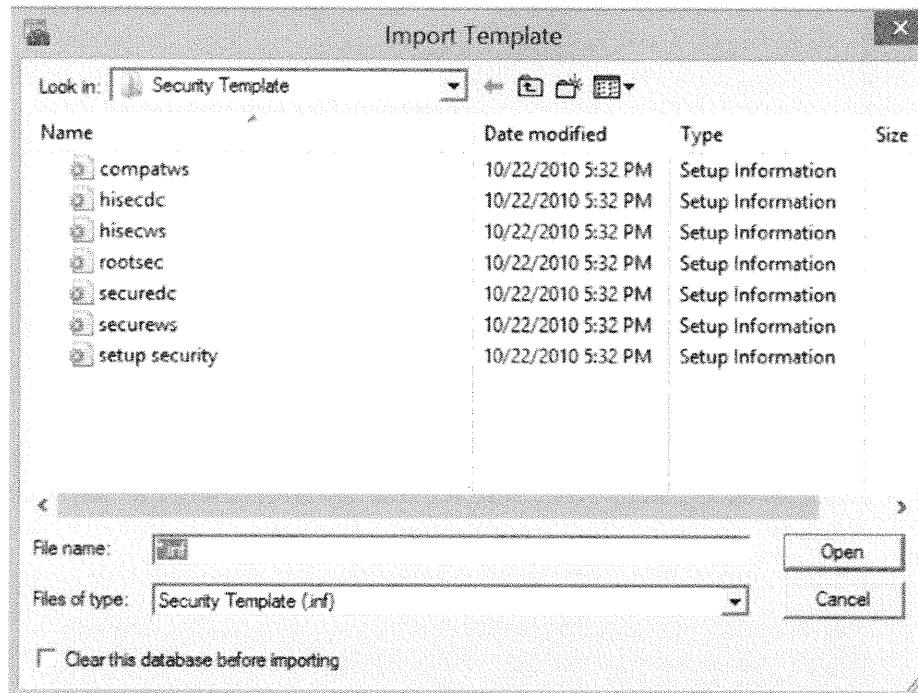
The SCA window reappears with additional instructions on the right-hand side of the screen.



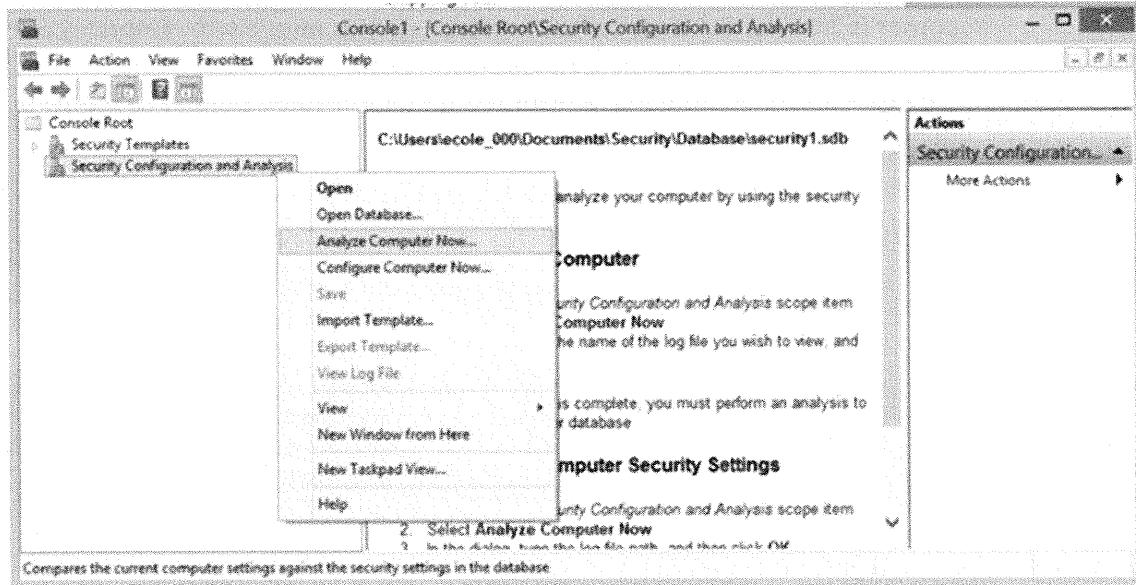
## Merging Templates

1. Before you analyze your systems, you might want to merge two templates. Right-click *Security Configuration and Analysis* and click *Import Template*. The Import Template window displays. If you uncheck the option in the lower left-hand

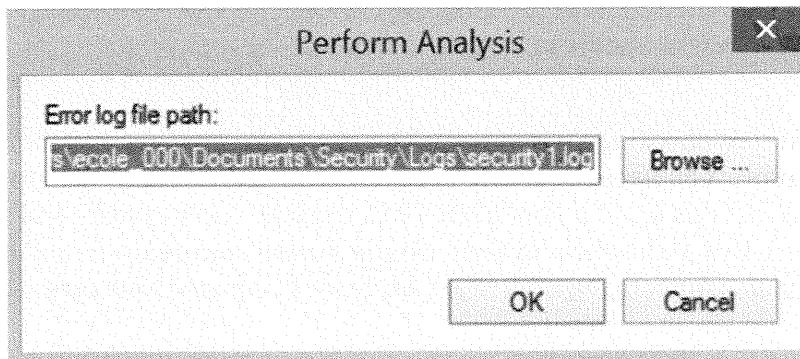
corner (Clear the database before importing), you merge two templates into one. You can then export the merged template. You will not merge any templates now; we just wanted to show you a feature of this tool. Click *Cancel* to return to the main screen.



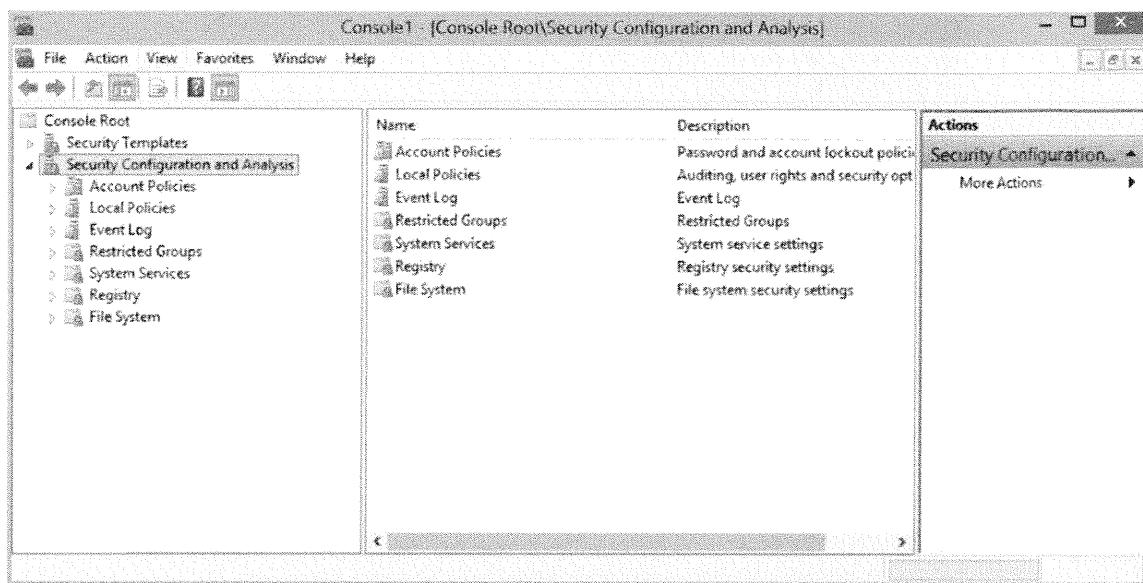
2. Now, you can start checking your system. The right pane changes and shows the database location. You have the ability to blindly configure your system to match your template, but this is not a good idea. First, compare your system against the database. To do this, right-click *Security Configuration and Analysis*, and click *Analyze Computer Now*. Be careful: The *Configure Computer Now* option is right below the option you are choosing.



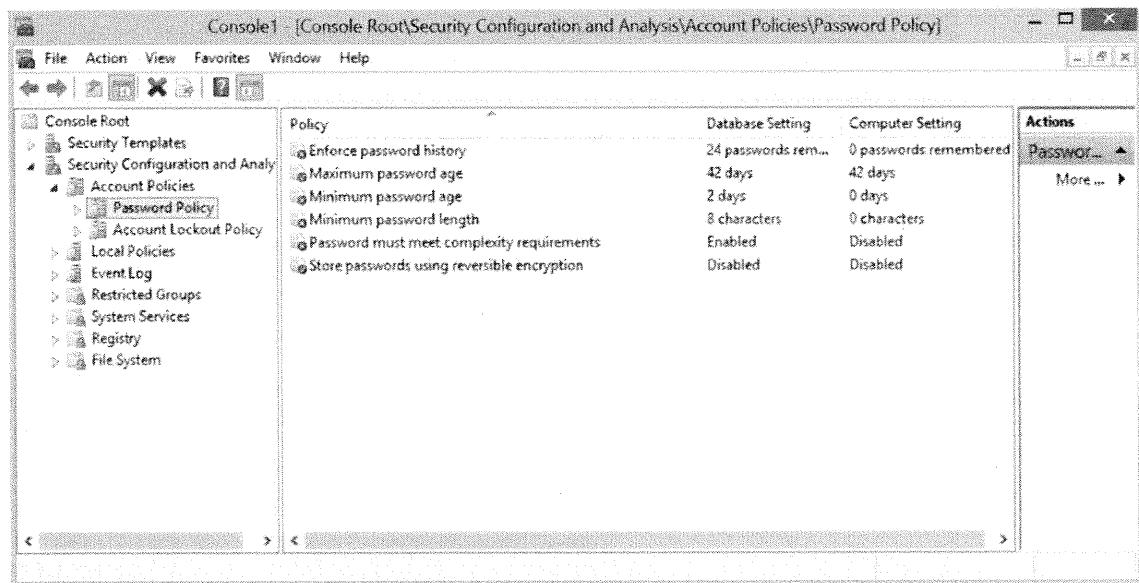
3. The Perform Analysis window displays, which is the only chance you have to cancel a wrong step. Make sure the title bar of this window says, “Perform Analysis” and not “Configure System.” If it says, “Configure System,” click *Cancel*. Leave the default path for the error log and click *OK*.



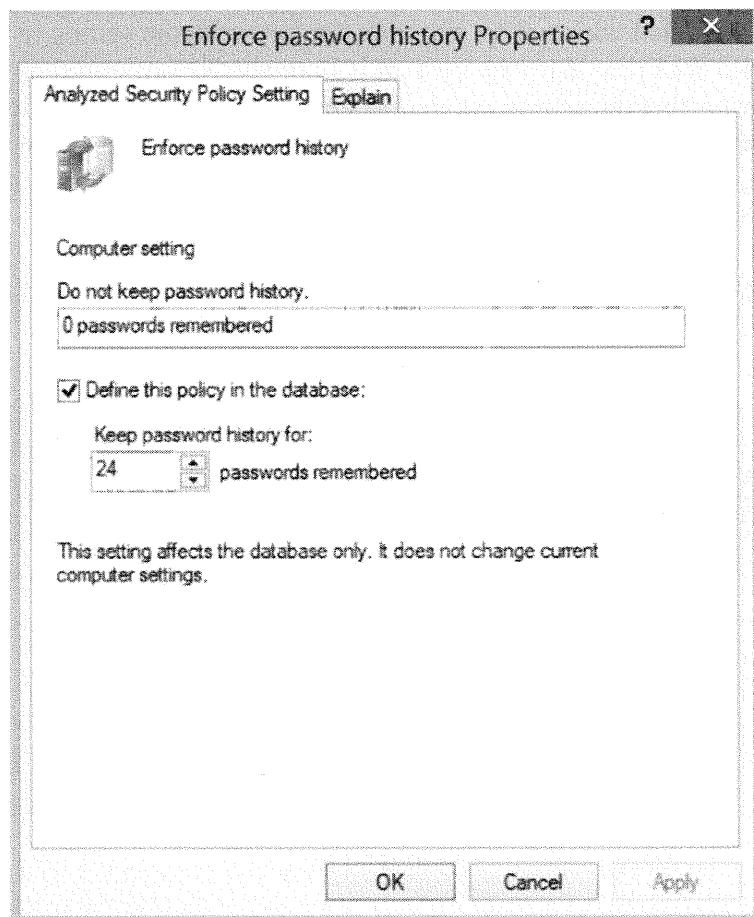
4. The Analyzing System Security window displays. Your system now compares your current settings to those located in the database (which was created from the template you imported).
5. After the analysis is complete, you have the ability to see where your system does not match the template. On the left pane, click the *arrow* in front of Security Configuration and Analysis to expand the categories.



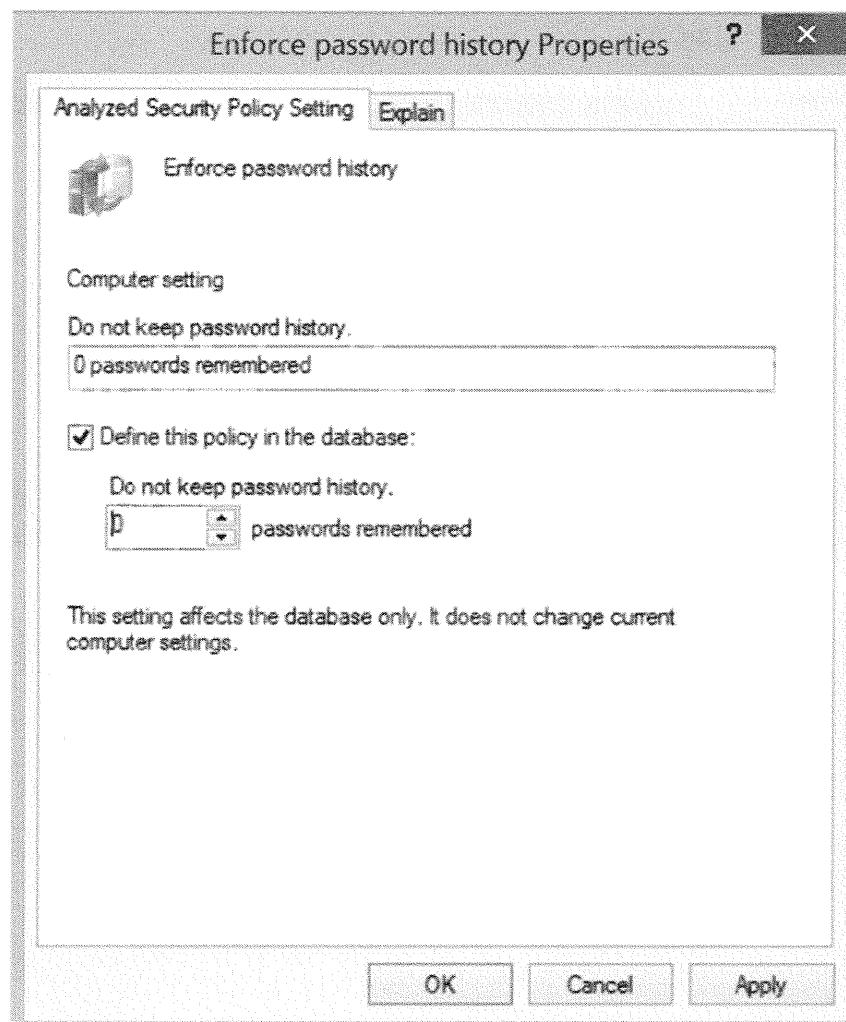
6. You see similar categories to what you saw under Security Templates, except now the comparison of your systems is actually set to what is set in the template. If you click any of the categories in the left pane, you see the same screens you saw before in the right pane with the addition of the Computer Setting information. You see one of three different icons associated with each line item or policy. A red x means that your system does not comply with the setting in the template. This does not mean that your system is improperly configured or has errors; it only means that the setting on your system is different from the template setting. A green checkmark signifies that your system setting is the same as the one defined in the template. A blue box signifies that the particular line item or policy is not defined in the template.
7. Under Security Configuration and Analysis, click *Account Policies*. Click the arrow in front of Account Policies and click *Password Policy*.



8. You still have the ability to make modifications to the template at this point. Double-click *Enforce password history* to display the Enforce password history Properties window. At this time, you can make a change or even undefine it in the template.



9. To see how this works, set the password history to the same value that is on your system. In this case, I am going to set it to 0. If you set it, click *Apply* and then click *OK*.



10. The item that previously had a red x now has a green checkmark, which shows that the changes you make are analyzed on the fly.

The screenshot shows the Windows Security Configuration and Analysis console window titled "Console1 - [Console Root\Security Configuration and Analysis\Account Policies>Password Policy]". The left pane displays a tree view of security policies under "Console Root". The right pane shows a table of password policy settings with columns for "Policy", "Database Setting", and "Computer Setting". A vertical "Actions" pane on the right contains buttons for "PASSWORD..." and "ENFORCE...".

Policy	Database Setting	Computer Setting
Maximum password age	999999999999999999 days	999999999999999999 days
Minimum password age	42 days	42 days
Minimum password length	2 days	0 days
Password must meet complexity requirements	8 characters	0 characters
Store passwords using reversible encryption	Enabled	Disabled
	Disabled	Disabled

---

## SCA Exercise

---

1. Can you make the changes shown in a template one at a time?
2. What is required before you can implement a template in a corporation?
3. What three hives can you edit with SCA?
4. What is the restricted group?
5. What is an MMC?
6. Name a current MMC on your system.

SANS Security Essentials – © 2016 SANS

### SCA Exercise

The following questions are answered in the next section:

1. Can you make the changes shown in a template one at a time?
2. What is required before you can implement a template in a corporation?
3. What three hives can you edit with SCA?
4. What is the restricted group?
5. What is an MMC?
6. Name a current MMC on your system.

---

## SCA Exercise Solutions

---

1. No. You would need to make individual templates for each change you want to make.
2. A corporate policy that permits and approves the changes you are making.
3. Classes\_root, Machine, and Users.
4. You cannot add users to any group in the restricted group. You must remove them from the restricted group prior to adding new users.
5. Microsoft Management Console.
6. Computer management console.

SANS Security Essentials – © 2016 SANS

### SCA Exercise Solutions

The following are the answers to the questions:

1. No, you need to make individual templates for each change you want to make.
2. A corporate policy that permits and approves the changes you are making.
3. Classes\_root, Machine, and Users.
4. You cannot add users to any group in the restricted group. You must remove them from the restricted group prior to adding new users.
5. Microsoft Management Console.
6. Computer Management Console.

### Summary

The SCA tool can be powerful for administrators in controlling the user population's desktop configurations. Through the use of GPOs and other methods, you can push out these templates to multiple users in a single session. Because the templates are not hardware-centric, you can create templates that are relevant to departments or functions instead of machine type. Another possibility is to break up the templates into smaller sections or make only a small number of changes at a time. This ensures that you do not push too many changes to people at a time as well as eases any troubleshooting you might have to perform.

The templates are simply *.inf* files that can be easily viewed and edited in Notepad. It is highly recommended that you spend the time manually reviewing your specific template before implementing, especially if you download a third-party template. Although they cannot contain trojans, they can contain malicious configurations that create insecure situations in your environment.

---

## Microsoft Baseline Security Analyzer (MBSA)

---

MBSA enables you to analyze a system for security.

SANS Security Essentials – © 2016 SANS

### **MBSA (Microsoft Baseline Security Analyzer)**

If you ask network administrators what the most difficult thing about their job is, a majority of them will likely complain about the tasks of patch and security management. If you are managing a network of 100 servers and 2,000 desktops, how can you tell which systems are at which security level without purchasing an expensive third-party system? Microsoft Baseline Security Analyzer (MBSA) can do this. Microsoft BSA is the next stage in the evolution of HfNetChk. Although you can still use the command-line version of this tool, BSA's GUI version makes running it and auditing the results extremely easy.

MBSA has the capability to scan either just the local machine or an entire network of Microsoft-based operating systems. It determines patch and service pack levels, well-known vulnerabilities, and issues with applications (application conflicts, for example), such as Exchange and SQL Server. Though BSA is impressive, it should never replace a properly conducted security audit.

---

## MBSA Details

---

- Name: Microsoft Baseline Security Analyzer (MBSA)
- Operating system: Windows
- License: free
- Protocol used: N/A
- Category: Patches
- Description: Scans a single system or a group of systems to determine patch and service pack levels
- URL: <http://www.microsoft.com>

SANS Security Essentials – © 2016 SANS

### BSA Details

The following topics and action items are covered in this section:

- Learning about Microsoft's BSA and its capabilities
- Identifying the common options used in BSA
- Working through examples of BSA running
- Practicing running BSA against local machines
- Determining the appropriate actions to take after a scan has completed

---

## MBSA Background

---

- One of the biggest problems with any operating system is managing patches
- Depending on the configuration, determining what patch applies to a given system is a difficult task
- Multiply the task of determining patches across multiple systems in an enterprise, and the task becomes unmanageable

SANS Security Essentials – © 2016 SANS

### MSBA Background

This section intentionally left blank.

---

## MBSA's Purpose

---

- Simplifies verifying the security of a system to include patch management
- Performs the following:
  - Searches for appropriate service packs
  - Searches for well-known vulnerabilities
  - Determines conflicts among applications
- Always test a patch in a lab before you put it on a production system

SANS Security Essentials – © 2016 SANS

### BSA's Purpose

When dealing with patch management, there is a cardinal rule that should never be broken: Do not patch production machines without first properly testing the patches in a lab environment, and always have a backup plan. There is nothing worse than getting through a two-hour patching exercise only to realize at 3:30 a.m. that your patching exercise has broken something that you need up and running by 7:00 a.m. the same day.

---

## MBSA Installation

---

- Create a directory and copy the tool
- Run the installation script:
  - Agree to the license
  - Enter in information
  - Accept defaults

SANS Security Essentials – © 2010 SANS

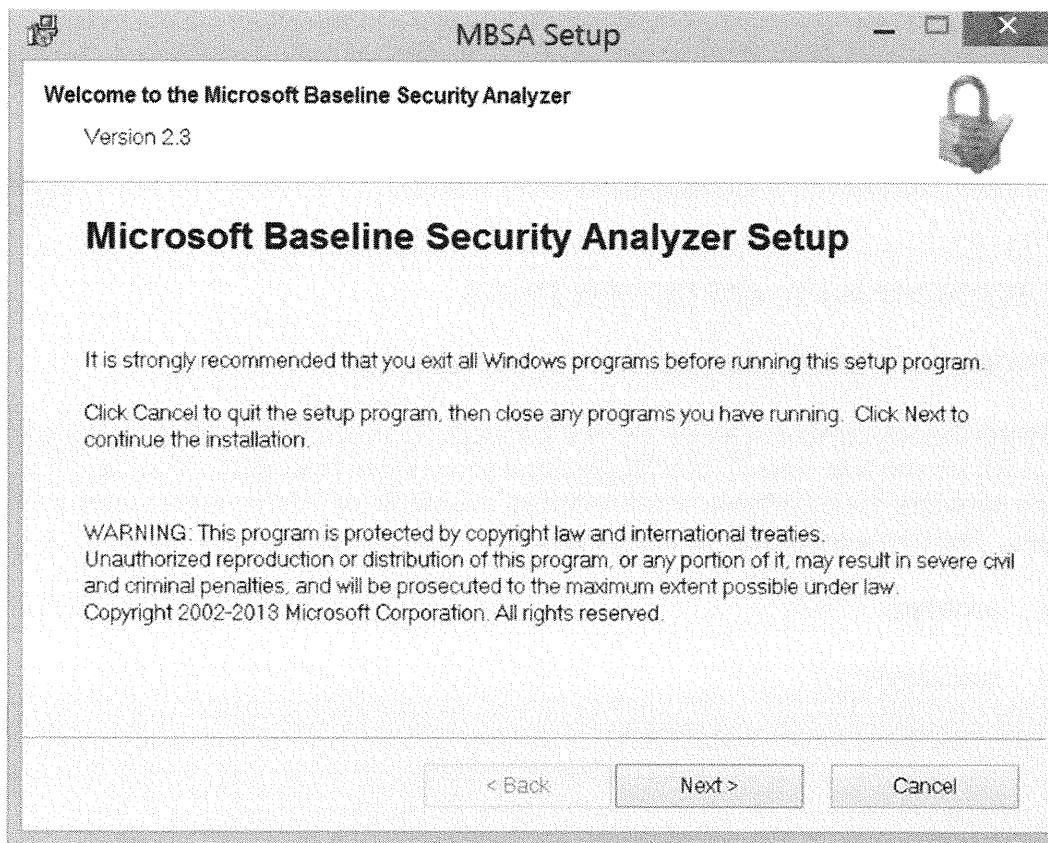
## BSA Installation

To install BSA, perform the following steps:

1. Create the directory in c:\toolsBSA. Copy the E:MBSASetup-x64EN file (where E is the drive letter of your CD ROM) from the provided CD and place it in the c:\toolsBSA directory. Double-click *mbasetup-x64EN* to begin the installation process.

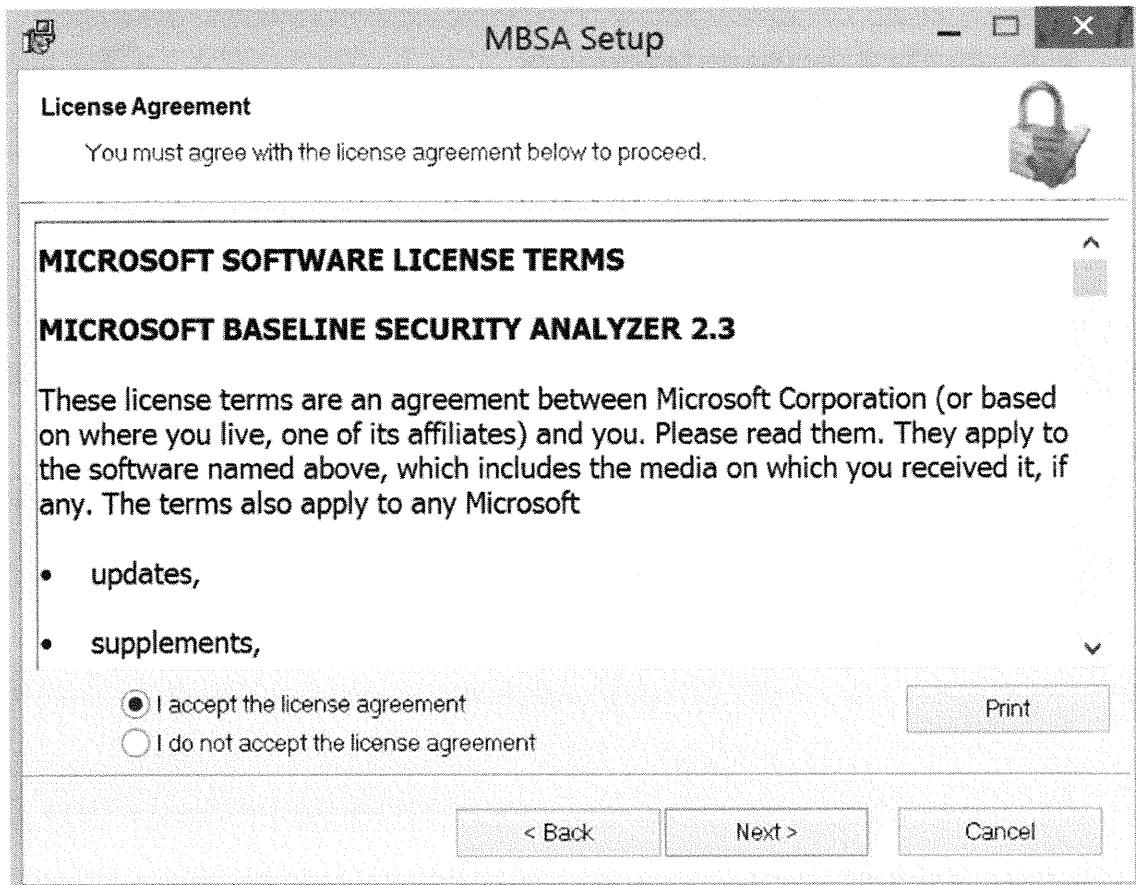
**Note:** If you are using a 32-bit system, you would run either the MBSASetup-x86EN or the MBSASetup-x32-EN installation program.

After the Welcome to the ... Wizard window appears, click *Next*.

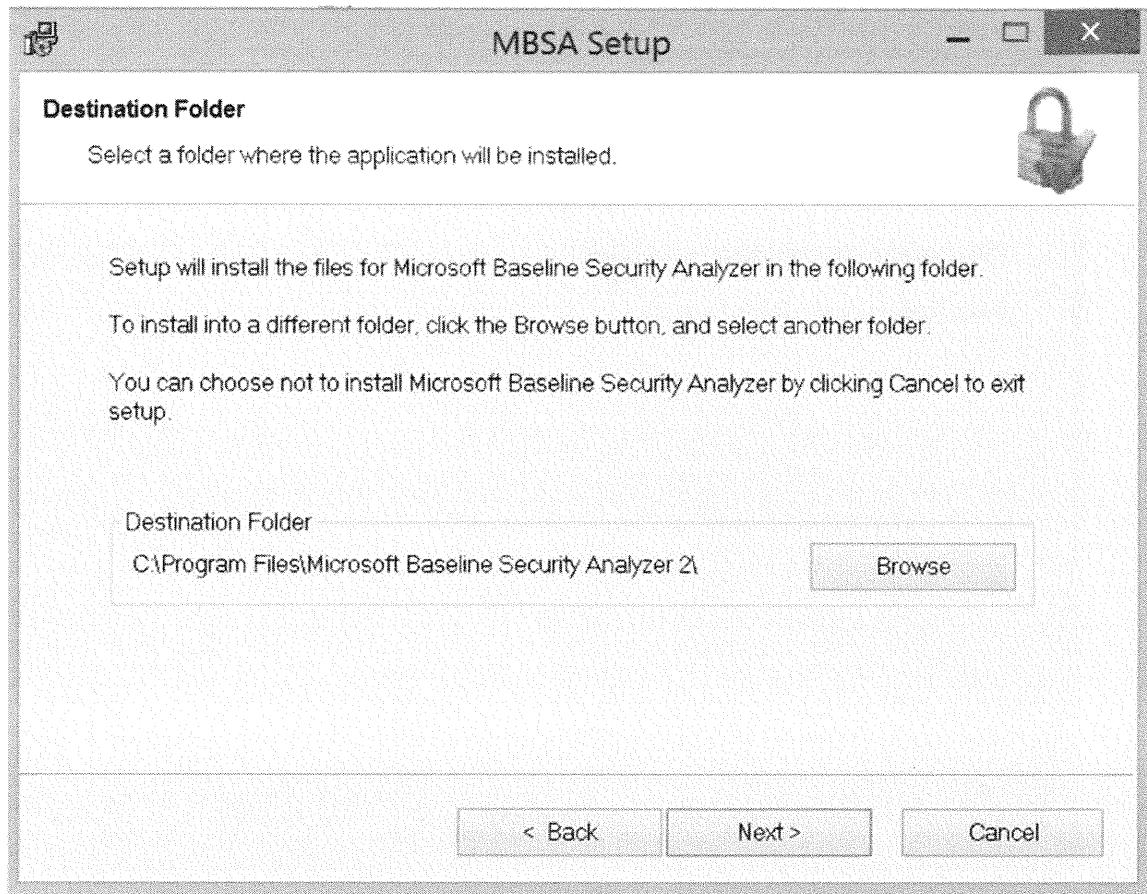


2. After the License Agreement window displays, read the license agreement, and if you agree with it, click *I accept the license agreement*, and click *Next*. If you do

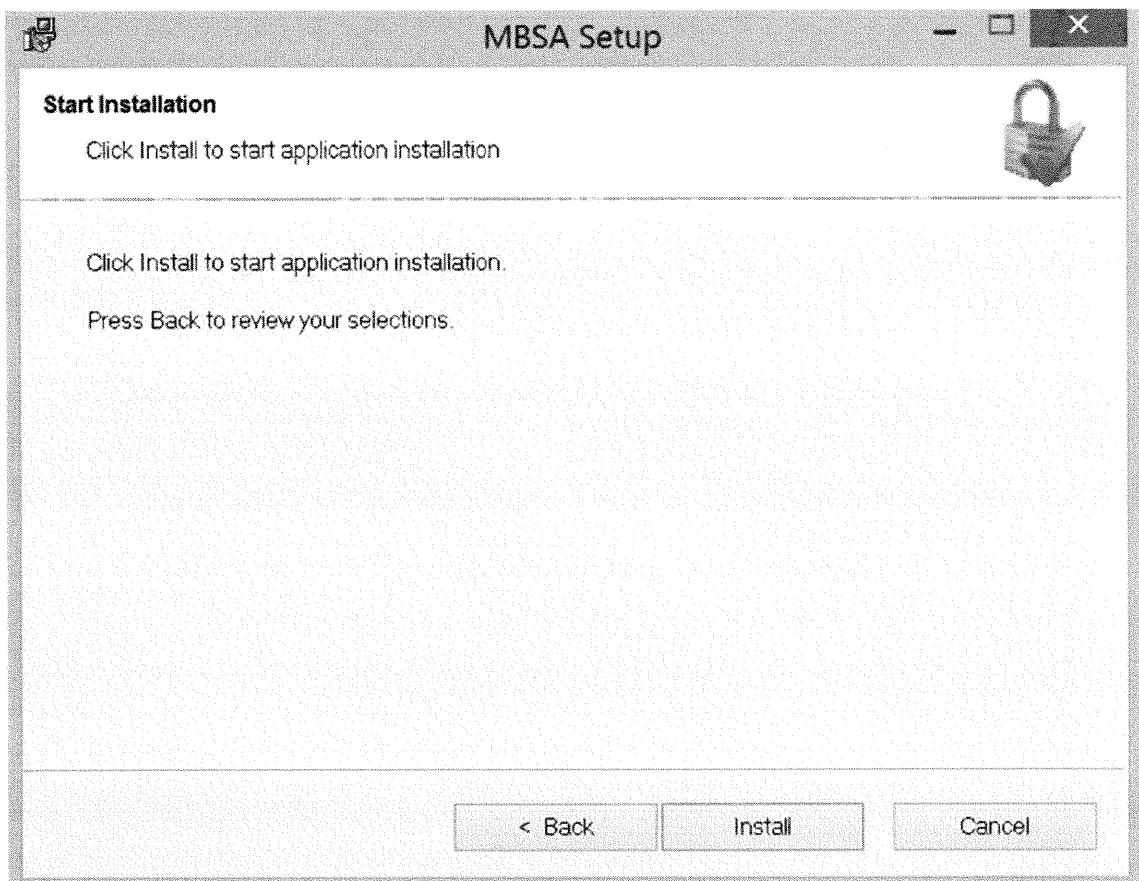
not agree with the license agreement, click *Cancel* and move on to the next chapter.



3. After the Destination Folder window displays, accept the default location and click *Next*.



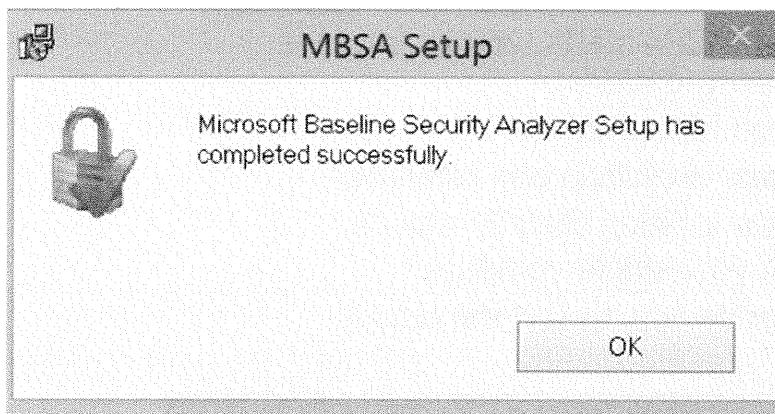
4. After the Start installation options window displays, click *Install*.



5. The Installation window displays. This can take some time depending on your machine.

**Note:** If you are running UAC, select *Yes* to allow the program to install.

6. After the Successfully Installed window displays, click *OK*.



---

## Running MBSA (1)

---

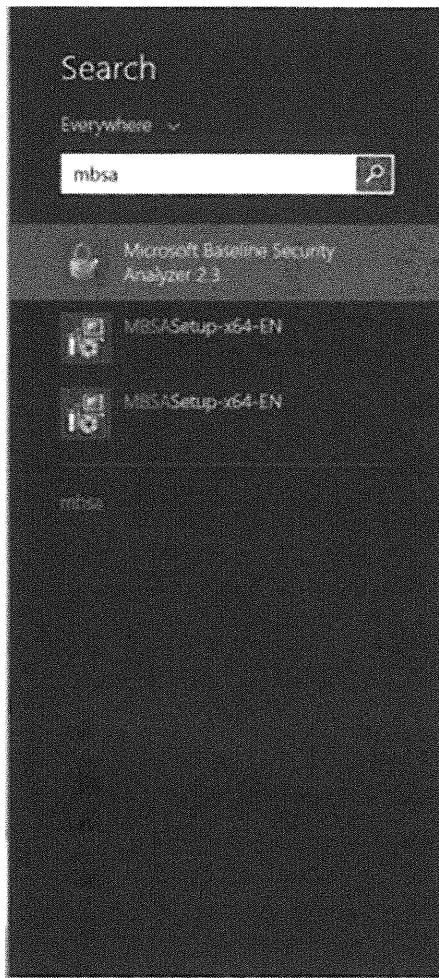
- When MBSA starts, you receive the following options:
  - Scan a computer
  - Scan more than one computer
  - View existing security reports
- Scan your single computer:
  - Decide how to sort the output

SANS Security Essentials – © 2016 SANS

### Running MBSA (1)

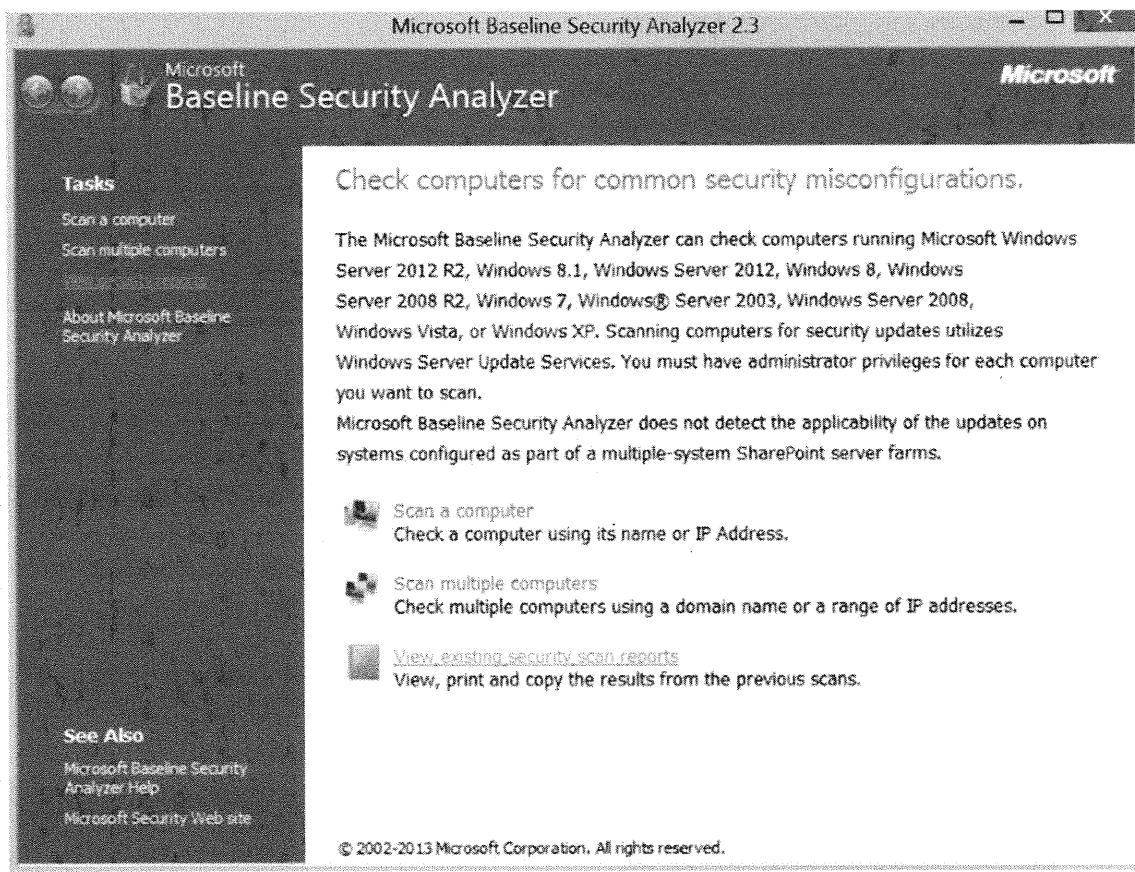
To run BSA, perform the following steps:

1. To start MBSA, right sweep from the desktop to display the Search window. Click *Search*, type **MBSA**, and click *MBSA* to run the program.



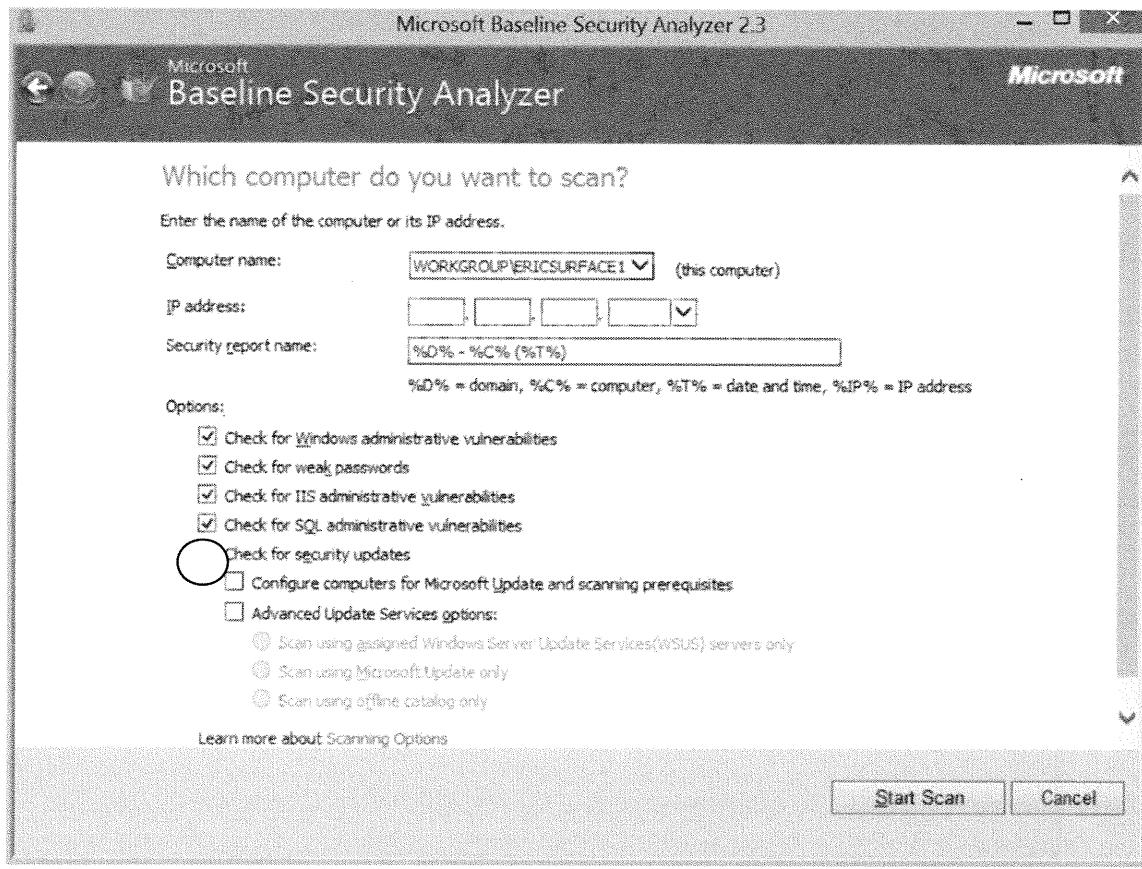
The BSA's Welcome window displays and shows three options (located in the left-hand pane):

- Scan a computer
  - Scan multiple computers
  - View existing security scan reports
2. Because you have not run this application before, the View existing security reports option is grayed out. Click the *Scan a computer* option.

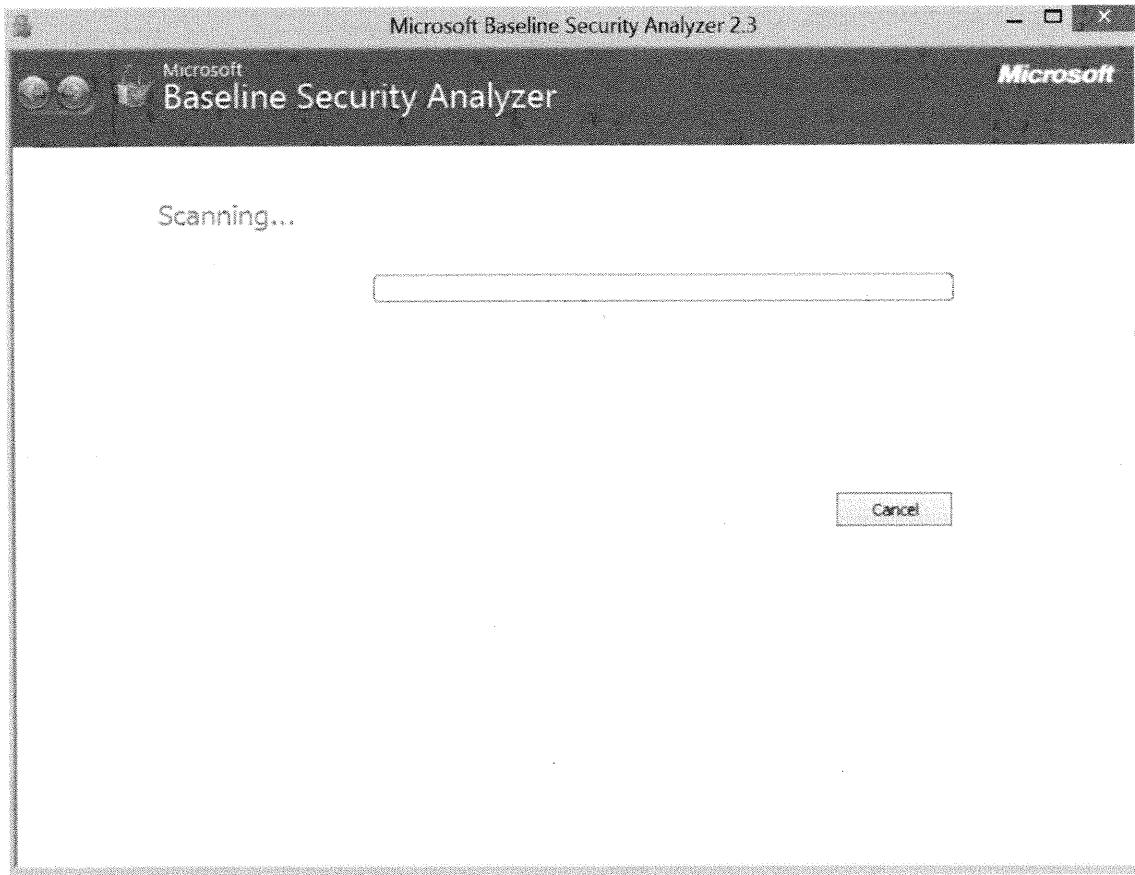


3. The BSA Scan a computer window displays. By default, the local system should already be listed next to the Computer name: field. If there is a specific way you want your reports named, you can change the default rules next to the Security report name field. In the Options section, there is a list of specific tests. For the purposes of this course, you are going to scan for everything. To help organize your work efforts, you can scan with one option enabled at a time, which minimizes the amount of work reported at a time.

**Warning:** Because you are not connected to a network, make sure you uncheck the *Check for security updates* checkbox. Ensure that your system's name is listed, and click *Start Scan*.



The BSA Scanning window displays.



4. After the BSA View Security Report window displays, the results are listed for you to review. By default, the most serious problems are displayed first in the results. You can change the report listing by changing the Sort Order. You can choose one of the following Sort Order options:
  - Issue Name (alphabetical order)
  - Score (worst first)
  - Score (best first)

In the report, you see the following information:

- System name and domain name
- Local IP address
- The name of the report
- Your MBSA version and database version used for scanning
- Your security rating

This report shows a Severe Risk rating. This is obviously not a good result. After the name, domain name, version, and rating information, you see the issues discovered during the scan. Each line represents a particular test that was performed. If the test passes, a green checkmark is displayed under the score column. If the test fails, a red

x appears. If the test did not pass, but the issues are not as serious, an orange x displays.

Spend some time reviewing the issues reported.

The screenshot shows the Microsoft Baseline Security Analyzer 2.3 interface. The title bar reads "Microsoft Baseline Security Analyzer 2.3". The main window title is "Microsoft Baseline Security Analyzer". The content area displays a report titled "Report Details for WORKGROUP - ERICSURFACE1 (2014-11-01 20:25:54)". A warning message states "Security assessment: Severe Risk (One or more critical checks failed.)". Below this, a table provides system information:

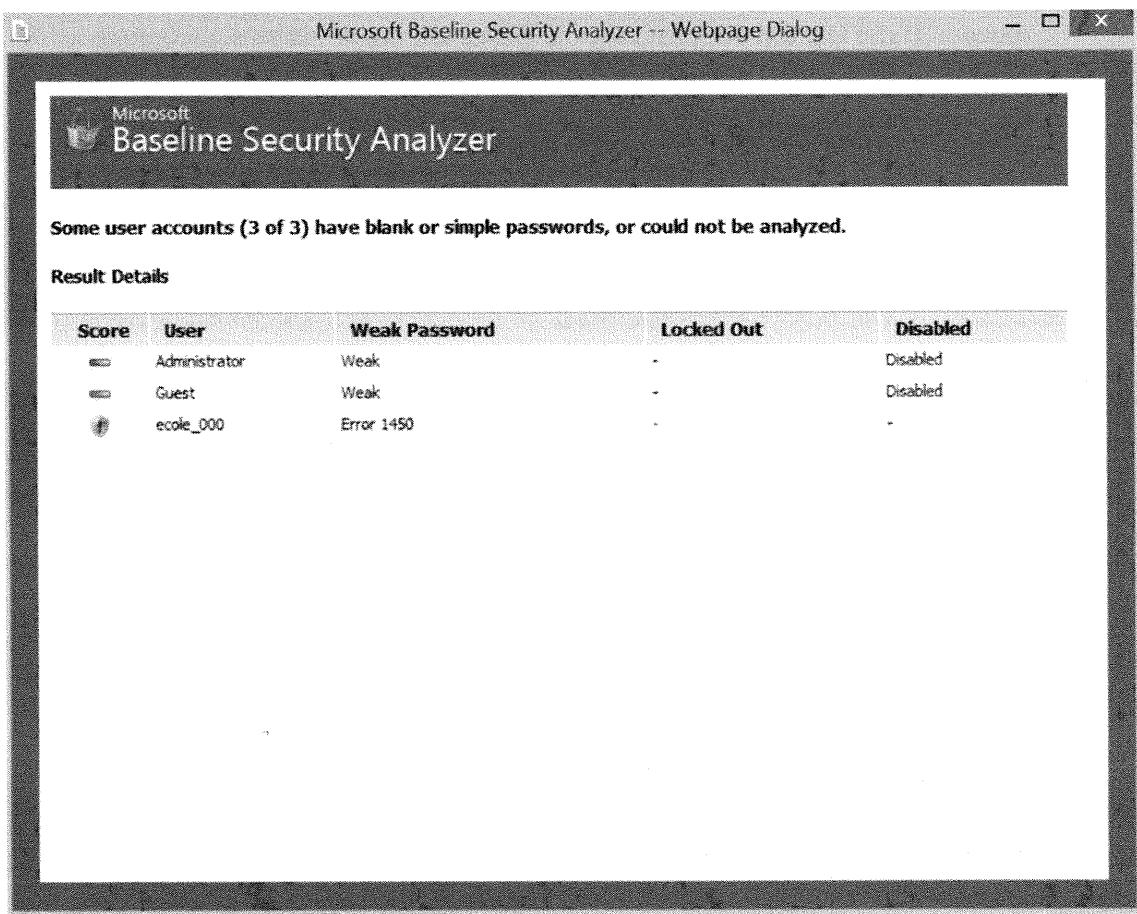
Computer name:	WORKGROUP\ERICSURFACE1
IP address:	192.168.195.1
Security report name:	WORKGROUP - ERICSURFACE1 (11-1-2014 8:25 PM)
Scan date:	11/1/2014 8:25 PM
Scanned with MBSA version:	2.3.2208.0
Catalog synchronization date:	Security updates scan not performed

Below the table, there is a dropdown menu for "Sort Order" set to "Score (worst first)". The section "Windows Scan Results" contains a table for "Administrative Vulnerabilities". The table has columns: Score, Issue, and Result. One entry is shown:

Score	Issue	Result
Automatic Updates	The Automatic Updates system service is not running. What was scanned... How to correct this.	

At the bottom of the window, there are buttons for "Print this report", "Copy to clipboard", "Previous security report", "Next security report", and "OK".

- After you review the report, under the reports section for one of the items, click *Result Details*. You might have to scroll down in the window to see any item that has this link. The BSA Result Details window displays.



6. Go back to the main report and click *How to correct this* for one of the items in the report.

The screenshot shows a window titled "Microsoft Baseline Security Analyzer". The main content area is titled "Local Account Passwords".

**Issue**

Weak passwords are one of the main causes of security breaches. Examples of weak passwords are names of children or pets, or common words found in the dictionary, such as "happy."

It is outside the scope of this tool to check for all possible weak passwords on accounts. Rather, this tool only checks for a few commonly used weak passwords as follows:

- Password is blank.
- Password is the same as the user account name.
- Password is the same as the computer name.
- Password uses the word "password."
- Password uses the word "admin" or "administrator."

This check also notifies you of any accounts that have been disabled, or are currently locked out.

This check is not performed on domain controllers.

For Microsoft® Windows® XP computers that use simple file sharing (includes Windows XP Home Edition and Windows XP Professional computers not joined to a domain), MBSA will not flag local accounts with blank passwords. To help protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network, or for any other logon activity except at the main physical console logon screen.

**Solution**

Adopt a strong password policy. This is one of the most effective ways to ensure system security. For guidance on implementing strong passwords, refer to the articles in the Additional Resources section.

**Instructions**

**To change password policy settings in Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP Professional, or Windows 2000**

1. Open the **Control Panel**.
2. Double-click **Administrative Tools**, and then double click **Local Security Policy**.
3. Double-click the **Account Policies** folder, and then select the **Password Policy** folder.
4. Double-click the policy that you want to change and then specify the new policy setting.

7. If you scroll down through your report, you should come across at least a couple of green checkmarks. According to Microsoft, these represent what you are doing correctly on your system.

The screenshot shows the Microsoft Baseline Security Analyzer 2.3 interface. At the top, it displays the title "Microsoft Baseline Security Analyzer 2.3" and the Microsoft logo. Below the title, there's a section titled "Microsoft Baseline Security Analyzer" with a list of findings:

Updates	installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted.
>Password Expiration	What was scanned How to correct this All user accounts (3) have non-expiring passwords.
File System	What was scanned Result details How to correct this All hard drives (1) are using the NTFS file system.
Autologon	What was scanned Result details Autologon is not configured on this computer.
Guest Account	What was scanned The Guest account is disabled on this computer.
Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
Administrators	What was scanned Result details No more than 2 Administrators were found on this computer.
Windows Firewall	What was scanned Result details Windows Firewall is enabled on all network connections.

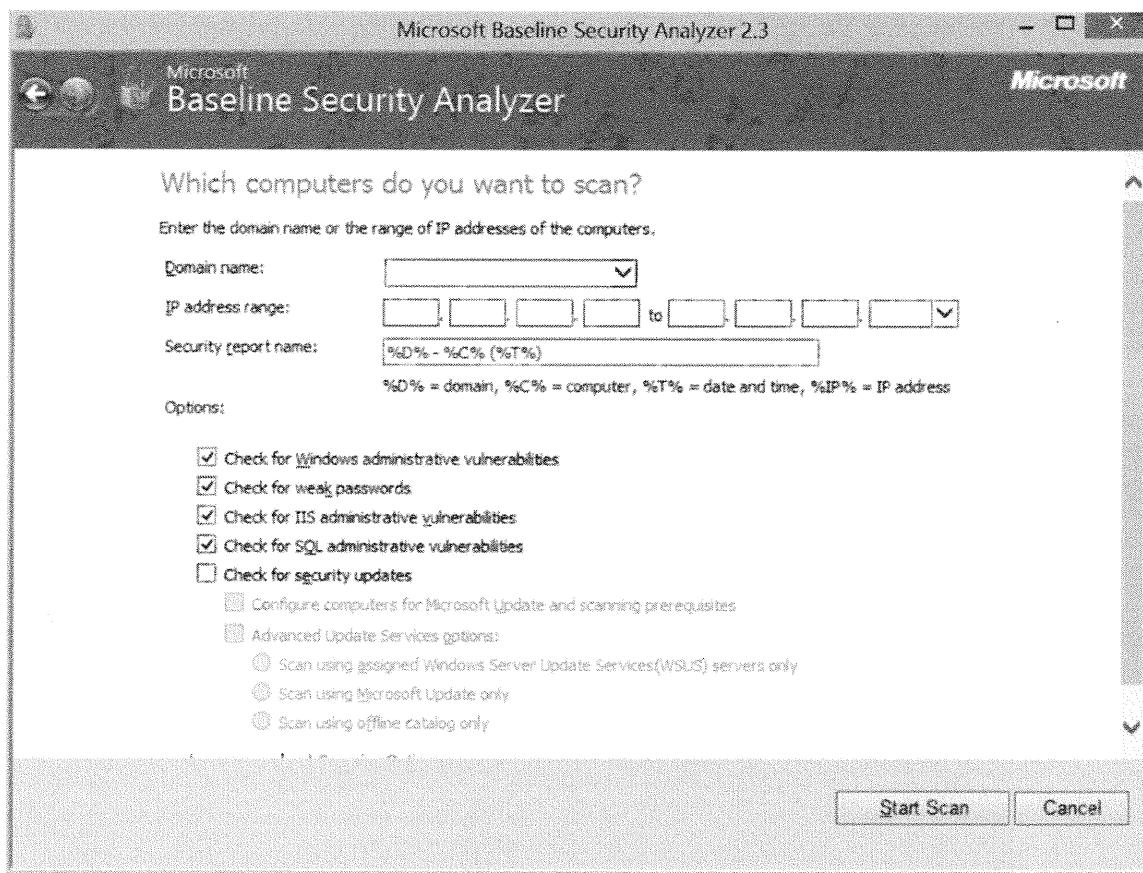
Below this, there's a section titled "Additional System Information" with a table:

Score	Issue	Result
1	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.

At the bottom of the window, there are several buttons: "Print this report", "Copy to clipboard", "Previous security report", "Next security report", and "OK".

## Scanning Networks or Ranges of IP Addresses

You can also use BSA to scan an entire network or range of IP addresses. Before scanning these types of systems, make sure you have the appropriate access and permission to do so. To perform these scans, click *Pick multiple computers to scan* from the left pane. After the BSA picks multiple computers to scan window displays, you can enter the domain name or an entire IP address range. The same options as those used for a single system scan are available. Because you are not part of a network, you do not have the ability to scan other systems.



If you click *Pick a security report to view*, and if you had performed a multiple computers scan, you can go back to previous scans to view the information. This is a great way to track progress on specific systems or networks.

The screenshot shows the Microsoft Baseline Security Analyzer 2.3 interface. The title bar reads "Microsoft Baseline Security Analyzer 2.3". The main header says "Microsoft Baseline Security Analyzer". Below it, there's a message: "Choose a security scan report to view". A note states: "Security reports are located in: C:\Users\ecole\_000\SecurityScans\". There is a dropdown menu labeled "Sort order: Scan date (descending)" and a link "Click here to see reports from the most recent scan only". A table lists two scan results:

Computer Name	IP Address	Assessment	Scan Date
WORKGROUP\ERICSURFACE1	192.168.195.1	Severe Risk	11/1/2014 8:28 PM
WORKGROUP\ERICSURFACE1	192.168.195.1	Severe Risk	11/1/2014 8:25 PM

At the bottom, there are links "Print this report" and "Copy to clipboard". A large "OK" button is at the bottom right.

Now that you have reviewed the various BSA's options, and you have seen the results this tool produces, you are ready for the next level—what BSA is capable of testing.

## Running MBSA (2)

- The following items are scanned for under Windows:
  - Missing Security Updates
  - Expired account passwords
  - File system type
  - If Autologon is enabled
  - If the Guest account is enabled
  - What the settings on the RestrictAnonymous Registry key are
  - How many local admin accounts exist
  - If blank or simple passwords are used
  - If unneeded services are running
  - It will list the shares on the system
  - What auditing feature is enabled
  - Windows version

SANS Security Essentials – © 2016 SANS

## Running BSA (2)

In the Windows check portion of the scan, the following items are scanned for:

- Missing security updates
- Expired account passphrases
- File system type
- If Autologon is enabled
- If the Guest account is enabled
- The settings on the RestrictAnonymous registry key
- How many local admin accounts exist
- If blank or simple passphrases are being used
- If unneeded services are running
- A list of the shares on the system
- Which auditing feature is enabled
- Windows version

In the IIS check portion of the scan, the following items are scanned for:

- If the IIS (Internet Information Server) Lockdown tool was installed and run on the system
- If IIS sample applications are still on the system
- If parent paths are enabled
- If IIS is updated with the latest security updates
- If the Admin virtual folder is in use
- If the MSADC and the Scripts virtual directories are in use
- If IIS logging is enabled
- If IIS is running on a Domain Controller (DC)

In the SQL portion of the scan, the following items are scanned for:

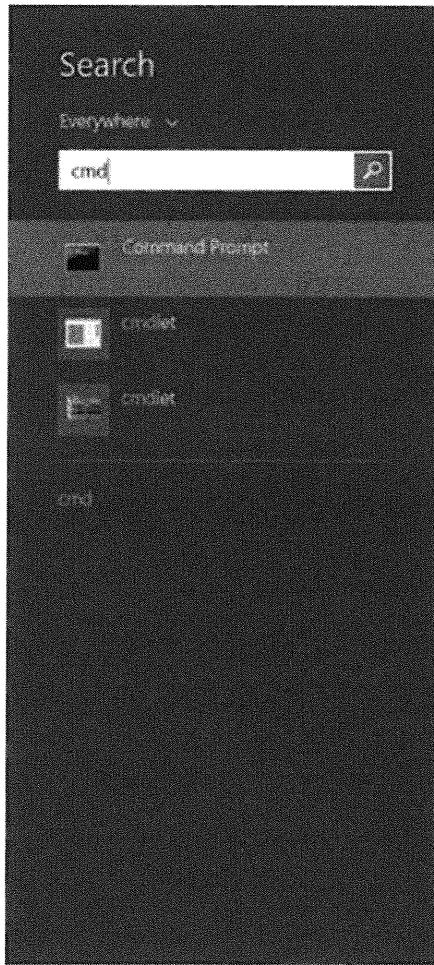
- If the admin group belongs to the sysadmin role
- If the CmdExec role is properly restricted to sysadmin
- If the SQL Server is on a Domain Controller
- If the administrator passphrase is blank or too weak
- Verification of the permissions on the installation folders
- If the Guest account has access to the SQL database
- If the Everyone group has access to the SQL registry keys
- If the SQL service accounts are part of the local admin group
- If the SQL accounts have blank or simple passphrases
- Missing SQL patches and updates
- The Server Authentication mode type
- Number of sysadmin role members

In the desktop applications portions of the scan, the following items are scanned for:

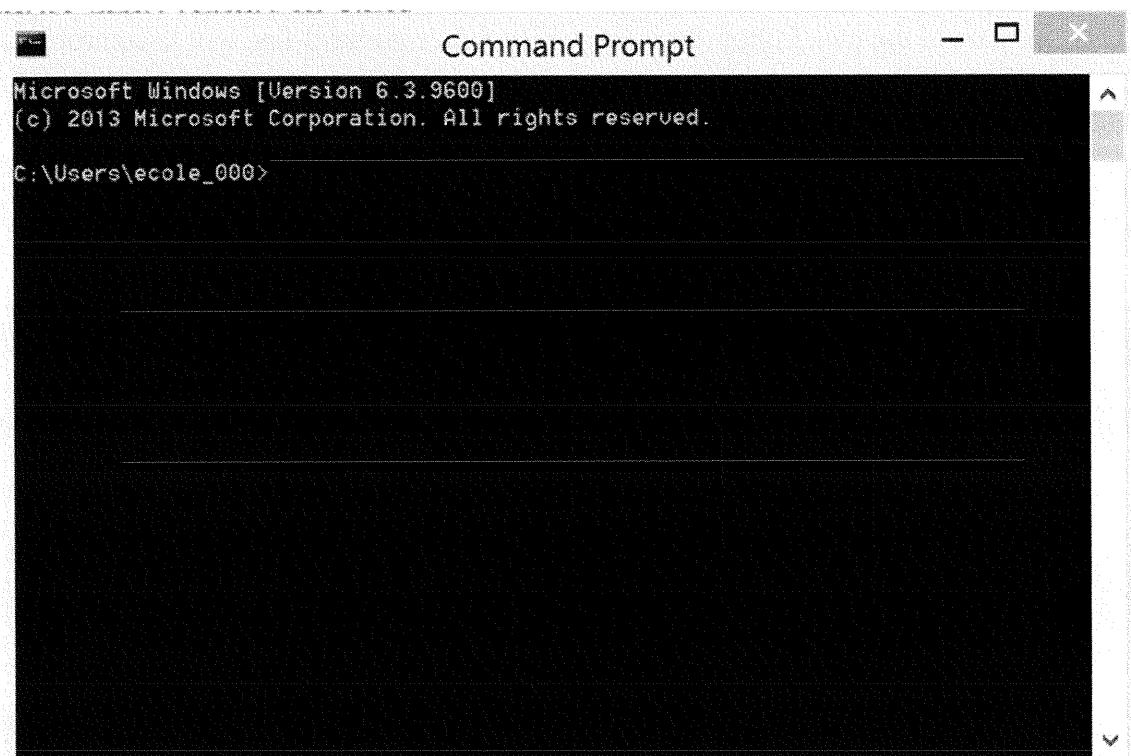
- The IE security zone settings for each user
- Outlook security zone settings for each user
- Office security zone settings for each user

From the GUI tool, you cannot turn on or turn off specific checks for each of the main categories. If you want more control over your scan, you can use the command-line version of the tool. Follow these steps to use the command-line tool to control your test options:

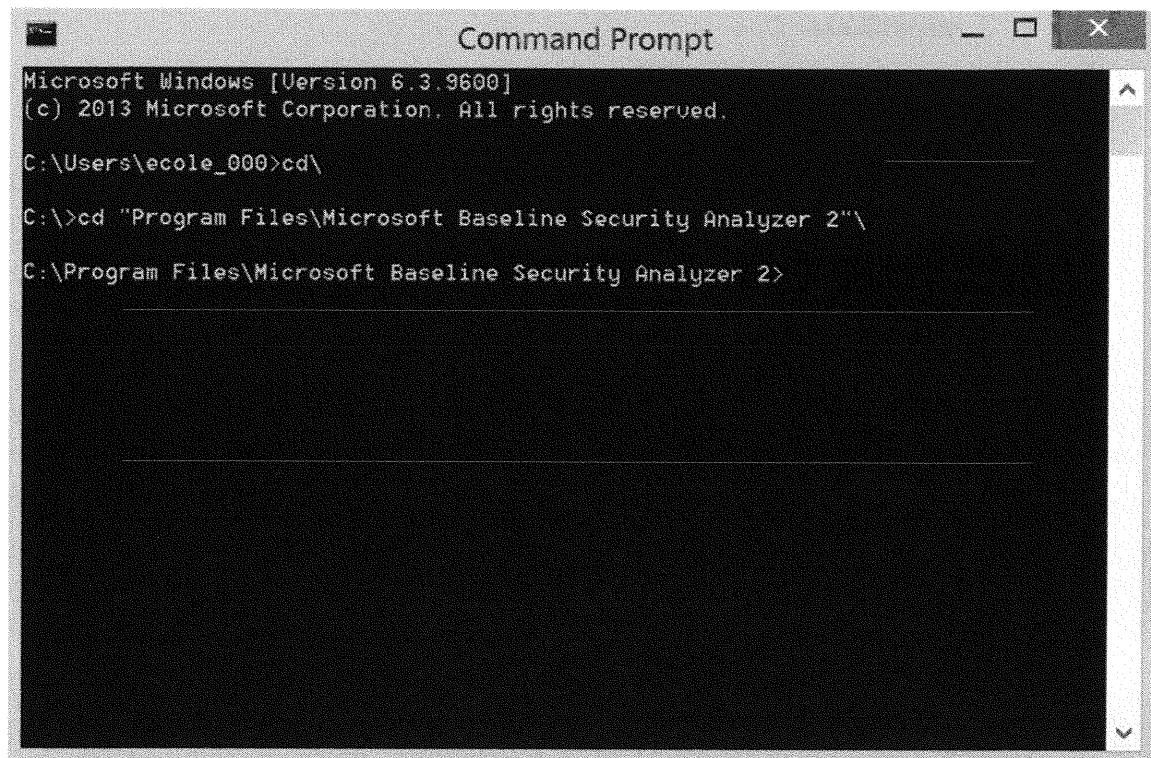
1. Right-sweep to open the menu. Click *Search*, type **cmd**, and click *cmd*. A Command Prompt window displays.



A command prompt displays.



2. Type **cd \** and type **cd Program Files\Microsoft Baseline Security Analyzer 2.**



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window displays the following text:

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

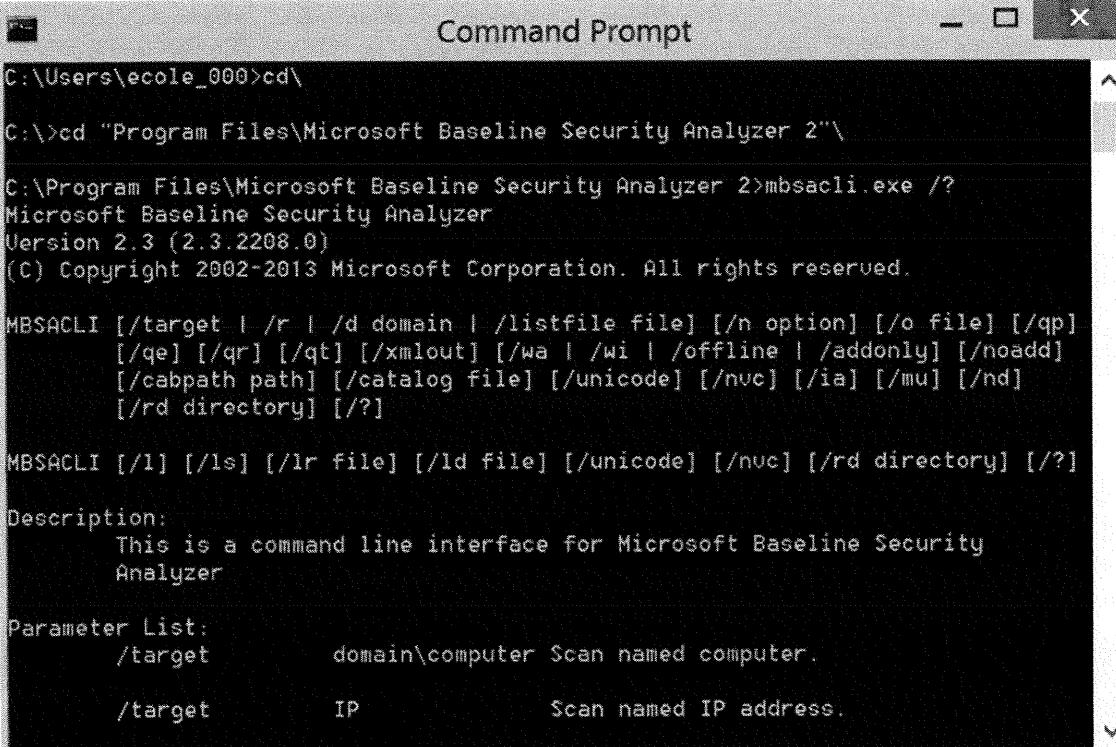
C:\Users\ecole_000>cd\

C:\>cd "Program Files\Microsoft Baseline Security Analyzer 2"\

C:\Program Files\Microsoft Baseline Security Analyzer 2>
```

3. To see the various command-line options available, type the following:

**mbsacli.exe /?**



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "mbsacli.exe /?". The output displays the Microsoft Baseline Security Analyzer 2 command-line interface (MBSA CLI) help text. It includes the version information (Version 2.3 (2.3.2208.0)), copyright notice ((C) Copyright 2002-2013 Microsoft Corporation. All rights reserved.), and detailed descriptions of parameters like /target, /r, /d, /listfile, /n, /o, /qp, /qe, /qr, /qt, /xmlout, /wa, /wi, /offline, /addonly, /noadd, /cabpath, /catalog, /unicode, /nvc, /ia, /mu, /nd, /rd, /l, /ls, /lr, /ld, and /?. Below the help text, there is a "Description:" section explaining what the tool is, and a "Parameter List:" section detailing the /target parameter.

```
C:\Users\ecole_000>cd\
C:\>cd "Program Files\Microsoft Baseline Security Analyzer 2"\

C:\Program Files\Microsoft Baseline Security Analyzer 2>mbsacli.exe /?

Microsoft Baseline Security Analyzer
Version 2.3 (2.3.2208.0)
(C) Copyright 2002-2013 Microsoft Corporation. All rights reserved.

MBSACLI [/target [ /r [ /d domain [ /listfile file] [/n option] [/o file] [/qp]
          [/qe] [/qr] [/qt] [/xmlout] [/wa [ /wi [ /offline [ /addonly] [/noadd]
          [/cabpath path] [/catalog file] [/unicode] [/nvc] [/ia] [/mu] [/nd]
          [/rd directory] [/?]

MBSACLI [/l] [/ls] [/lr file] [/ld file] [/unicode] [/nvc] [/rd directory] [/?]

Description:
  This is a command line interface for Microsoft Baseline Security
  Analyzer

Parameter List:
  /target      domain\computer Scan named computer.
  /target      IP           Scan named IP address.
```

As noted previously, there are several options you can use at the command line. Some of the options, which are helpful for testing and that have greater functionality than their GUI counterparts, are as follows:

- **-t:** This option allows you to control the number of threads that the application uses on your system. You can use from 1-128. The higher the thread count, the faster the scan will run; however, at the same time, it utilizes more resources on your local system.
- **-u:** This option allows you to specify the username with which to scan the remote systems. You need to have administrative access on machines that are scanned. If you are logged into your local box with a non-administrative account, use this option in conjunction with the next flag, -p.
- **-p:** This option allows you to specify a passphrase to use with the username you specify when scanning remote systems.
- **-z:** This option suppresses registry checks. It allows for the scan to perform more quickly, but it does not use the registry to help validate the scanner's findings.

---

## MBSA Exercise

---

1. Who wrote Microsoft's MBSA?
2. Can MBSA run against a network?
3. What level of access do you need on machines that you are scanning?
4. What must you do on your system to run the command-line version from any directory?
5. What option would you use to specify a particular XML file?

SANS Security Essentials – © 2010 SANS

### MBSA Exercise

The following questions are answered in the next section:

1. Who wrote Microsoft's BSA?
2. Can BSA run against a network?
3. What level of access do you need on machines that you are scanning?
4. What must you do on your system to run the command-line version from any directory?
5. What option can you use to specify a particular XML file?

---

## MBSA Exercise Answers

---

1. Shavlick wrote MBSA.
2. Yes, you can run MBSA against a network.
3. You need Administrator access to scan machines.
4. Add c:\Program Files\Microsoft Baseline Security Analyzer to path through your system's environment variables.
5. Use the -x option to specify an XML file.

SANS Security Essentials – © 2016 SANS

### BSA Exercise Answers

The following are the answers to the questions:

1. Shavlick wrote BSA.
2. Yes, you can run BSA against a network.
3. You need Administrator access to scan machines.
4. Add c:\Program Files\Microsoft Baseline Security Analyzer to path through your system's environment variables.
5. Use the -x option to specify an XML file.

## MBSA Summary

- MBSA is a must-have tool for all Microsoft security professionals
- MBSA makes an unmanageable task manageable
- Although MBSA discovers some common vulnerabilities, it is not a comprehensive tool and should not be used as a substitution for audits

SANS Security Essentials – © 2010 SANS

## BSA Summary

BSA can vastly improve an administrator's ability to track patch levels and the basic security of every system in your network. As stated previously, this tool should not be used as a substitution for a true security audit. As the name implies, BSA is best for establishing a baseline of security awareness for your systems.

A limitation of this scanner, and actually most security scanners, is that it cannot actually patch your systems. This task is left for you to do.

---

## CIS Scoring Tool

---

CIS Scoring Tool is an analysis application that assists administrators in determining a system's compliance. It requires Java to be installed.

SANS Security Essentials – © 2016 SANS

### CIS Scoring Tool

You created a secure template using the SCAtool and applied it to your test machine. How can you be sure that everything was properly configured? How can you be sure that you applied all of your patches? Finally, how can you obtain a *score* on how well you did against the template and patching? The answer is the *CIS Scoring Tool*. This tool assists administrators in determining whether their systems are in compliance with particular patches, hot fixes, and corporate templates.

---

## CIS Details

---

- Name: CIS Scoring Tool
- Operating system: Windows 8.x
- License: Membership required
- Protocol used: NA
- Category: System analysis
- Description: CIS lets administrators verify that a machine has properly implemented everything defined in a particular template and determine patch and hotfix compliance for the operating system
- URL: [www.cisecurity.org](http://www.cisecurity.org)

SANS Security Essentials - © 2016 SANS

### CIS Details

The following topics and action items are covered in this section:

- Learning about the CIS Scoring Tool
- Examining all of the options in CIS
- Reviewing the available reports

---

## CIS Background

---

- The Windows CIS Scoring Tool and baselines are the result of a collaboration of many industry experts and organizations
- Templates provided are used to assist administrators who want to establish a baseline for hardening devices through the SCA tool
- CIS enables administrators to score their systems and create specific reports on where the system is lacking compared to a predefined template

SANS Security Essentials – © 2014 SANS

### CIS Background

This section intentionally left blank.

---

## CIS's Purpose

---

- Audits and configures Windows devices against appropriate patch and hot-fix levels and a predefined security template
- Enables administrators to verify that all hot-fix, patch, and template changes were performed correctly on a specified local device

SANS Security Essentials – © 2016 SANS

### **CIS's Purpose**

This section intentionally left blank.

---

## CIS Architecture

---

- CIS is an application that requires installation
- CIS is a tool that simply takes each task out of a template and compares it to the configuration of a local device

SANS Security Essentials – © 2016 SANS

### CIS Architecture

When scoring yourself with CIS, the *score* depends on your level of compliance to the given criteria. It is important to remember that the score does not signify how secure your systems are. It only tells you how well you compare to the template and patching levels specified. You can obtain a maximum score by comparing your system to a weak template; however, your systems can still be vulnerable to a great number of attacks.

---

## Installation

---

- Make sure Java is installed and in your path
- Copy the CIS Scoring Tool directory to the desktop
- Double-click CIS-CAT and follow the prompts to complete the installation

SANS Security Essentials - © 2010 SANS

### Installation

This section intentionally left blank.

---

## Running CIS

---

- Open the CIS-CAT-FULL directory off of the desktop
- Double-click the CIS-CAT Windows batch file



### Running CIS

This section reviews the procedures for installing and running CIS.

### Installation of Java

Following are the steps that will be performed to install Java on a system:

1. To install Java, double-click *jre-8u25-windows-x64*. The Java installation begins. If your UAC is running, select Yes to run the program. On the Welcome screen, click *Install*.

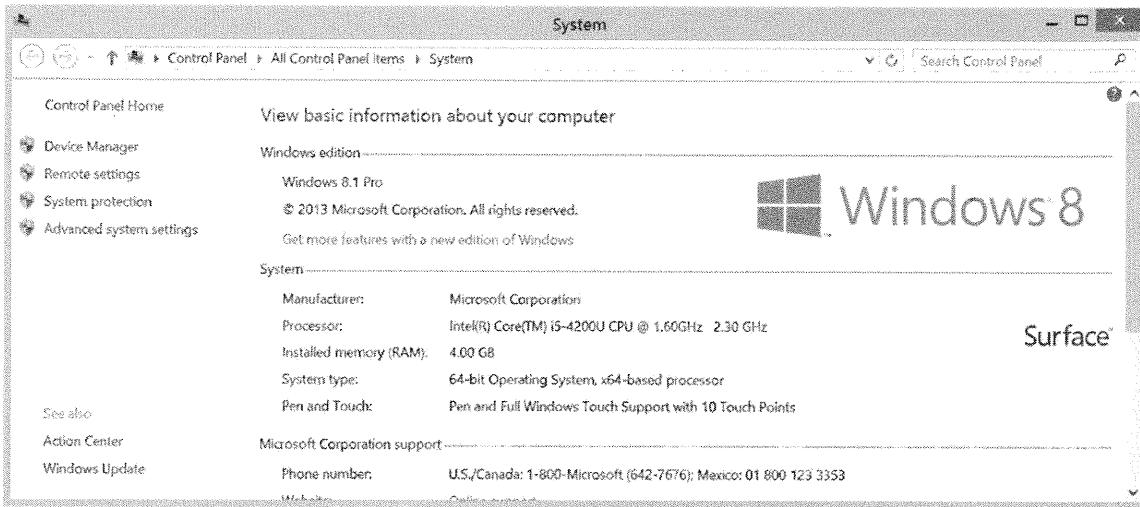


2. When installation is complete, click *Close*.

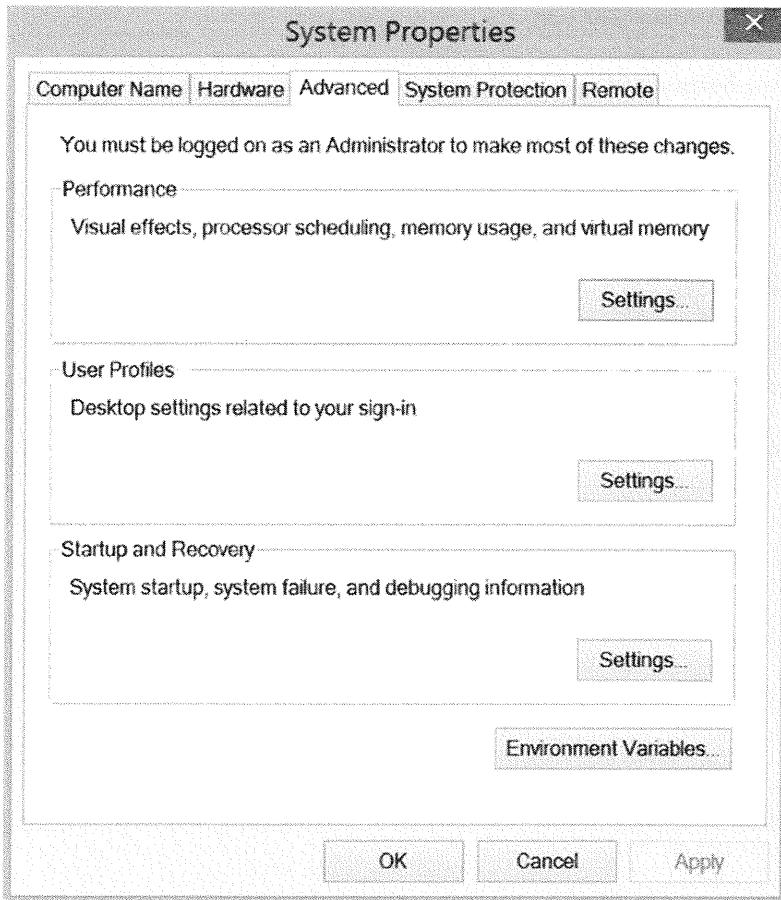


Java is now installed on the system.

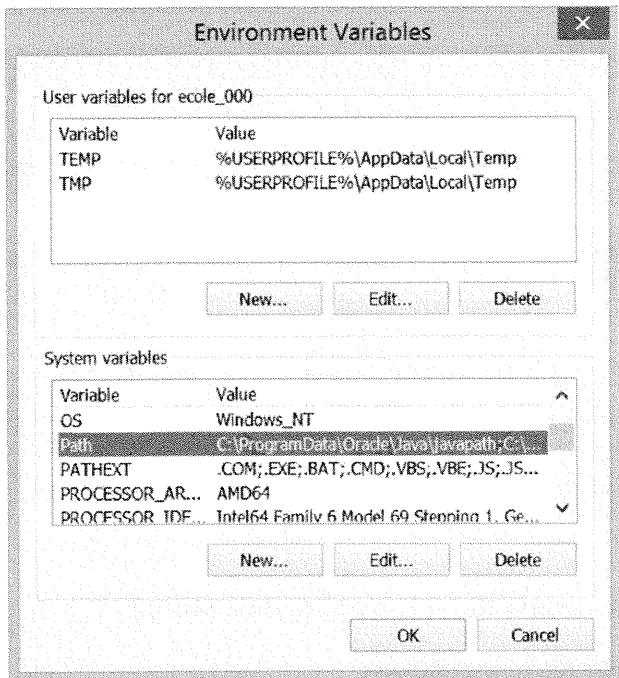
**Warning:** Make sure that Java is installed and listed in your path, because it will be required to run the tool. To update the path, right-click the Windows system in the lower left-hand corner of the screen, and then click *System*.



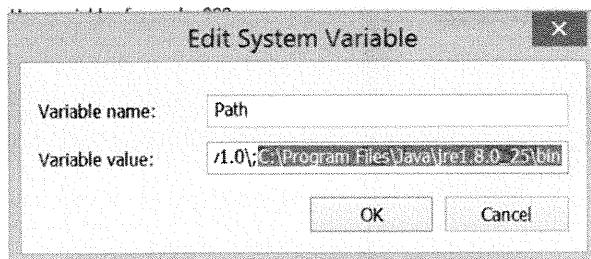
After the screen displays, click *Advanced* to access the Advanced system settings.



Click *Environment Variables*. Under System variables, scroll down and click *Path*.



Click **Edit** and add **C:\Program Files\Java\jre1.8.0\_25\bin** to the end of the line.



Click **OK** to close out all the windows and reboot your system.

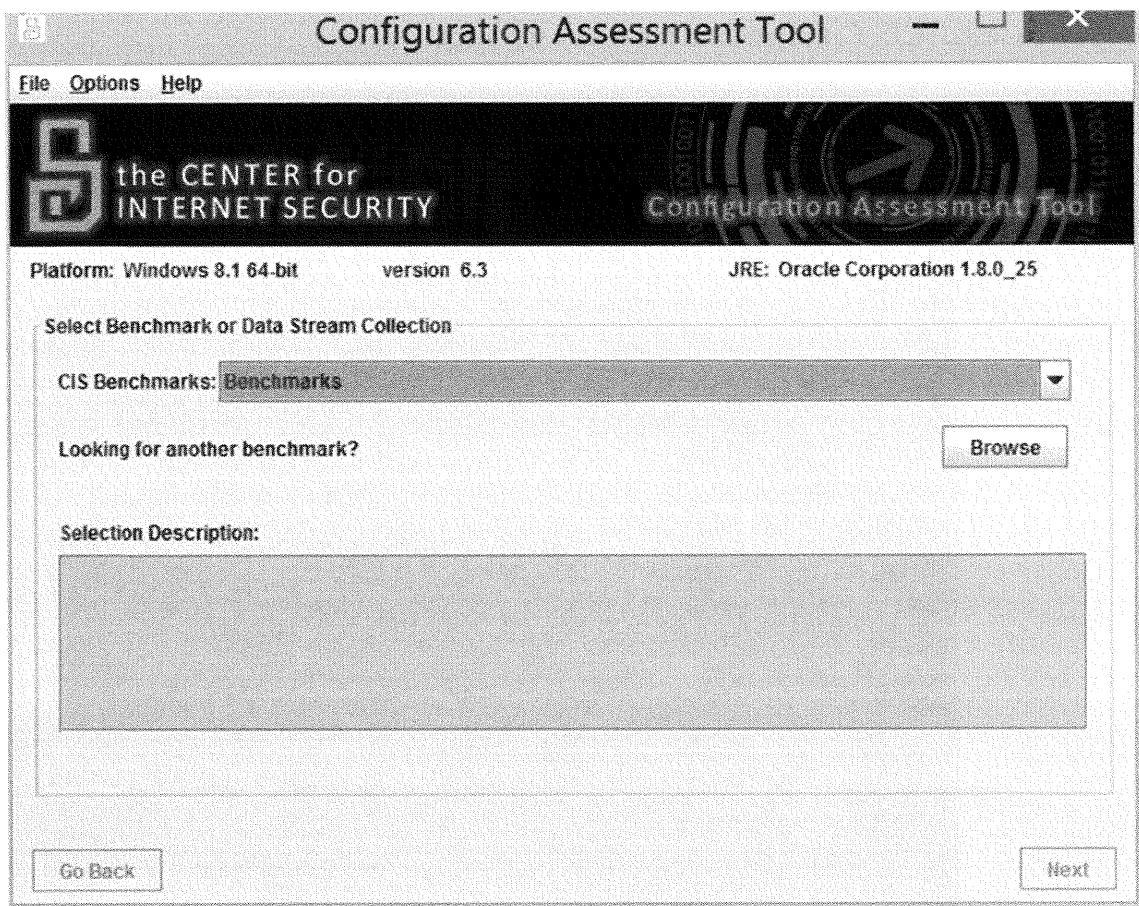
## Installing CIS

To install CIS-CAT, perform the following steps:

1. To begin, from the DVD, copy the *CIS-CAT-Full* directory. Open the directory and double-click the *CIS-CAT* batch file. An initial window opens showing the installation process. If UAC is running, click Yes to continue.



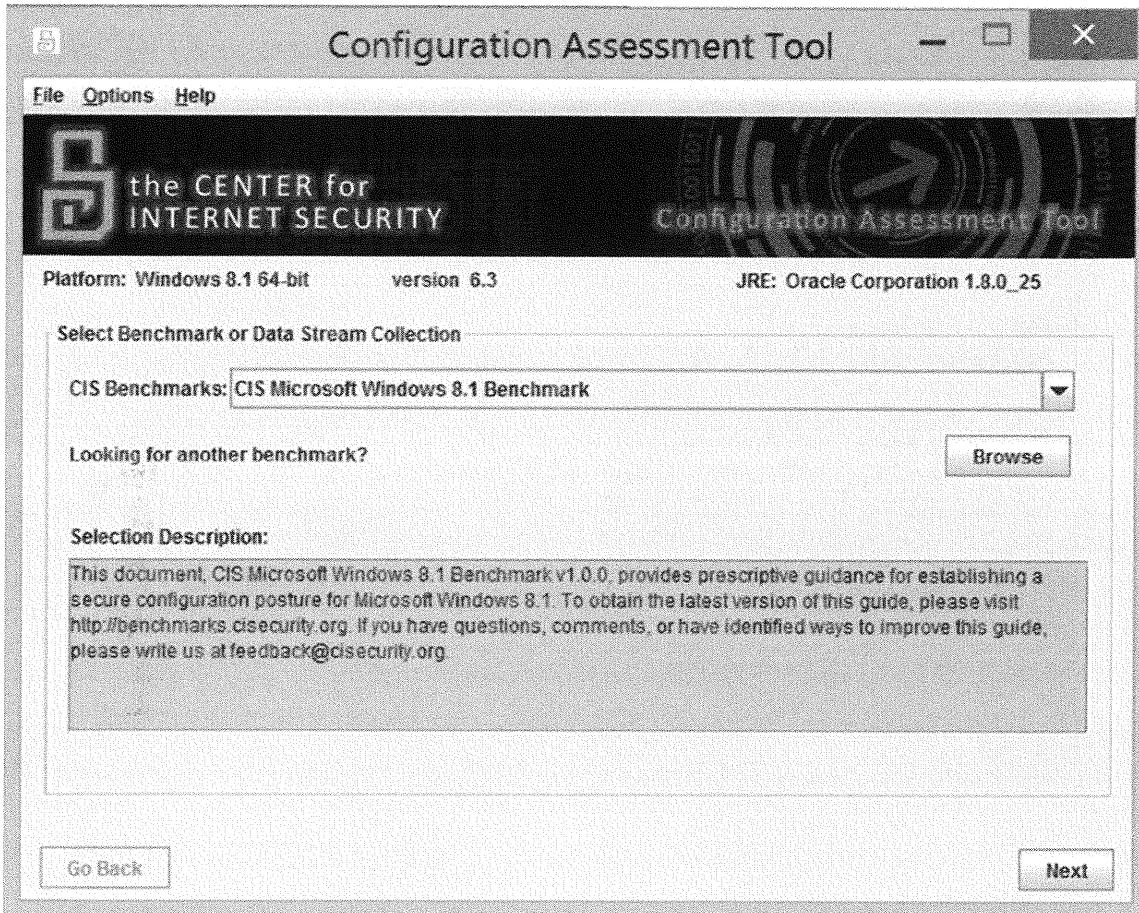
The CIS program starts.



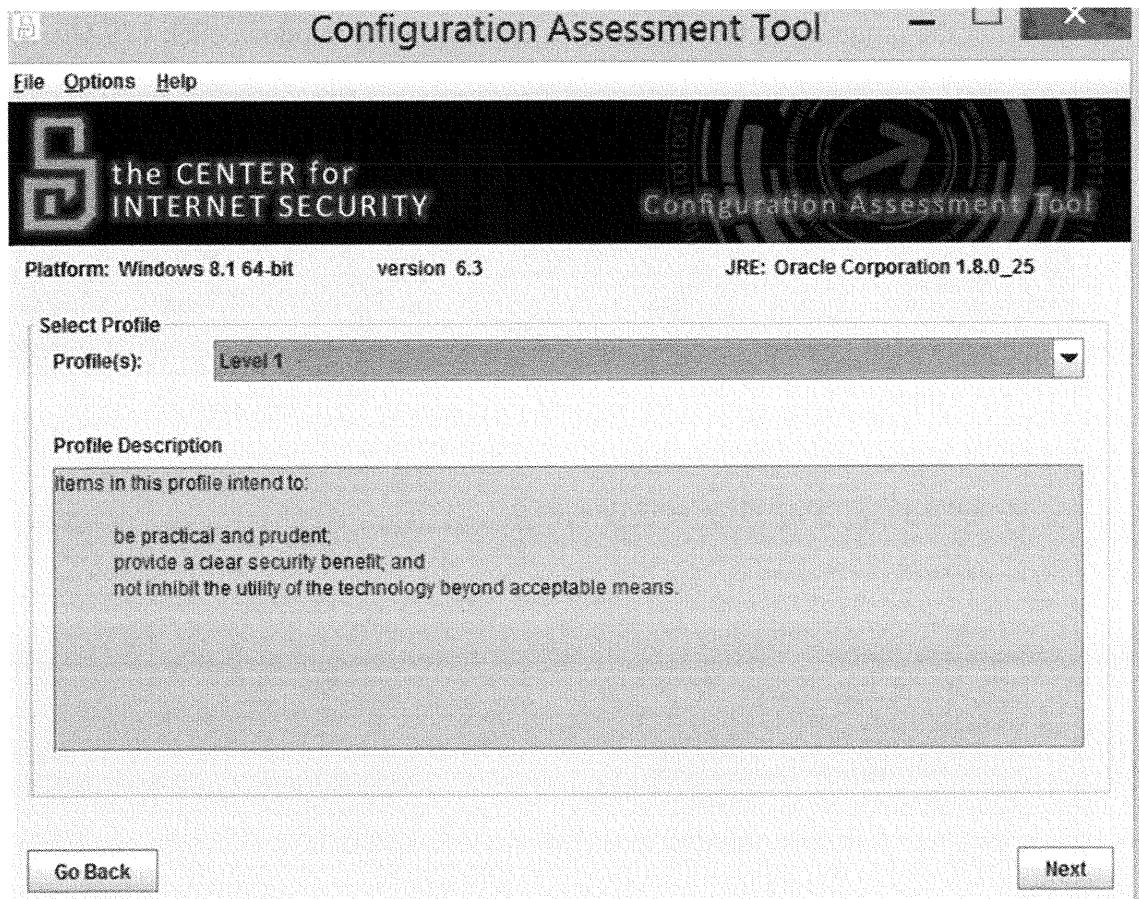
## Running CIS

Following are steps for running CIS:

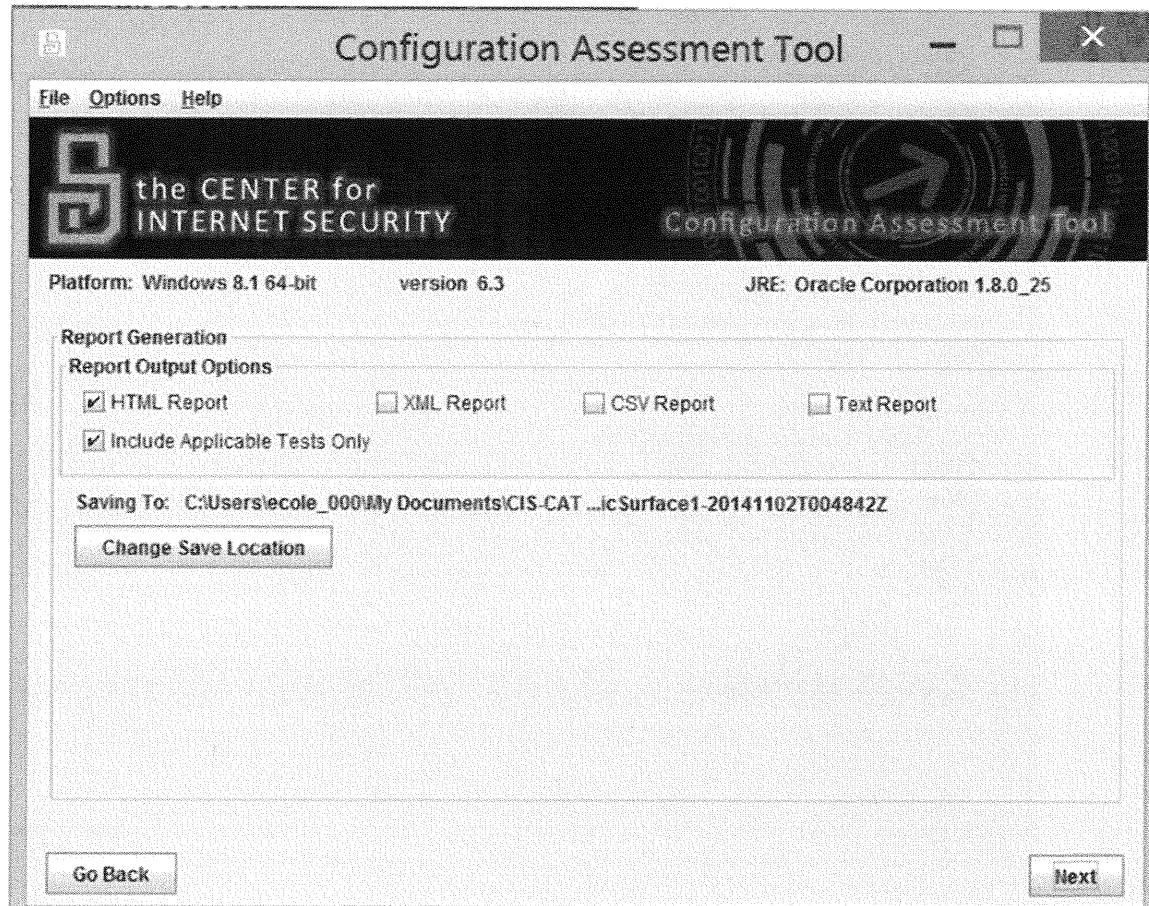
1. After the program starts running, from the drop-down window, click *CIS Microsoft Windows 8.1 Benchmark*. Click *Next*.



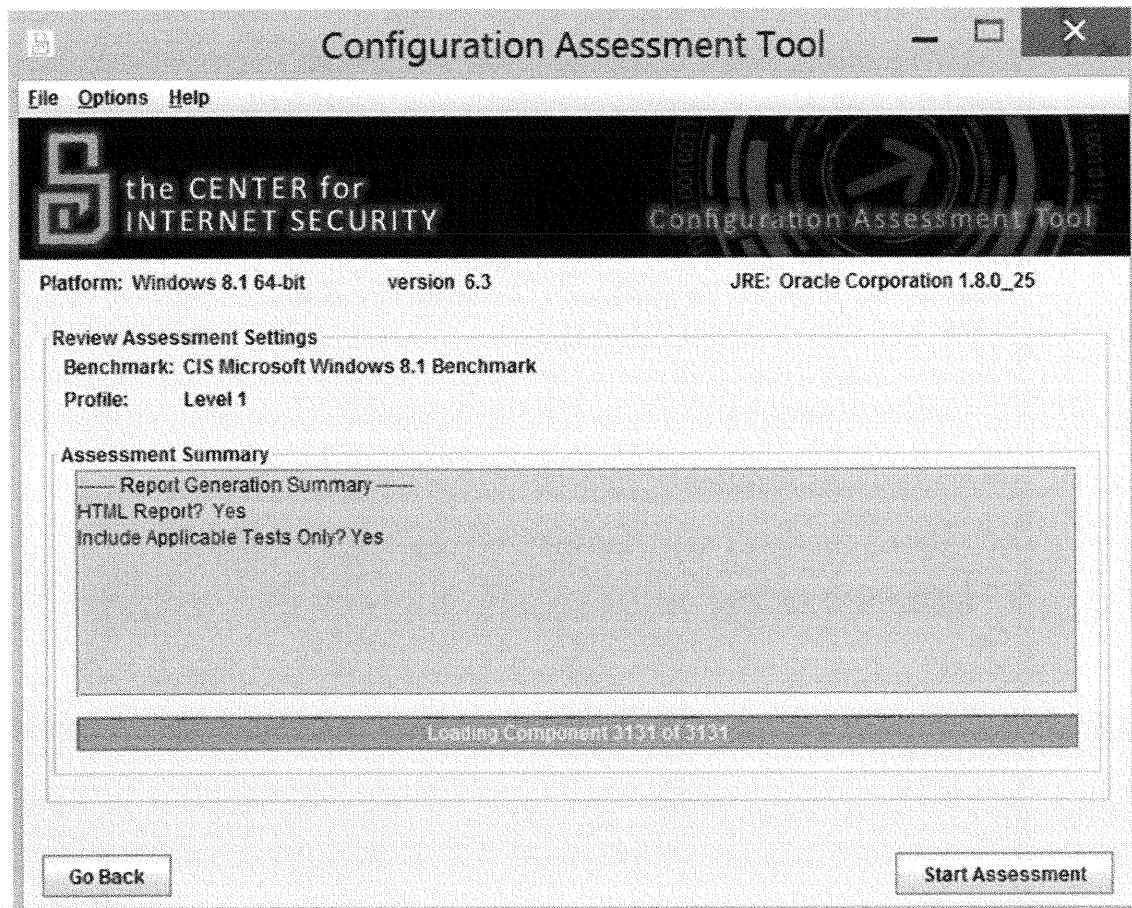
- Under Profile(s), click *Level 1*. Click *Next* to continue. You can review each of the different benchmarks and they should always be tested before they are used in an enterprise environment.



3. Select how you want the reports generated. You should keep the defaults for this lab by clicking *Next*.



4. Review the selections that you made and click *Start Assessment*.

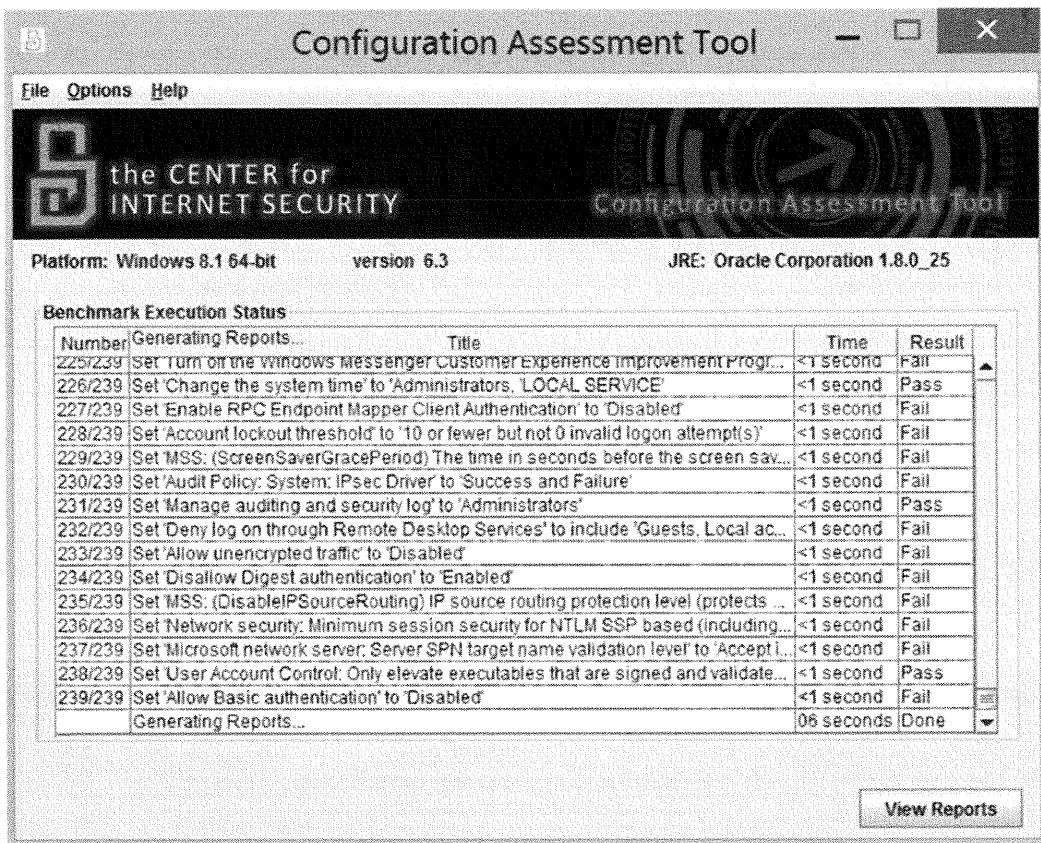


5. The program begins to analyze your system. Please wait for the program to finish. This could take several minutes.

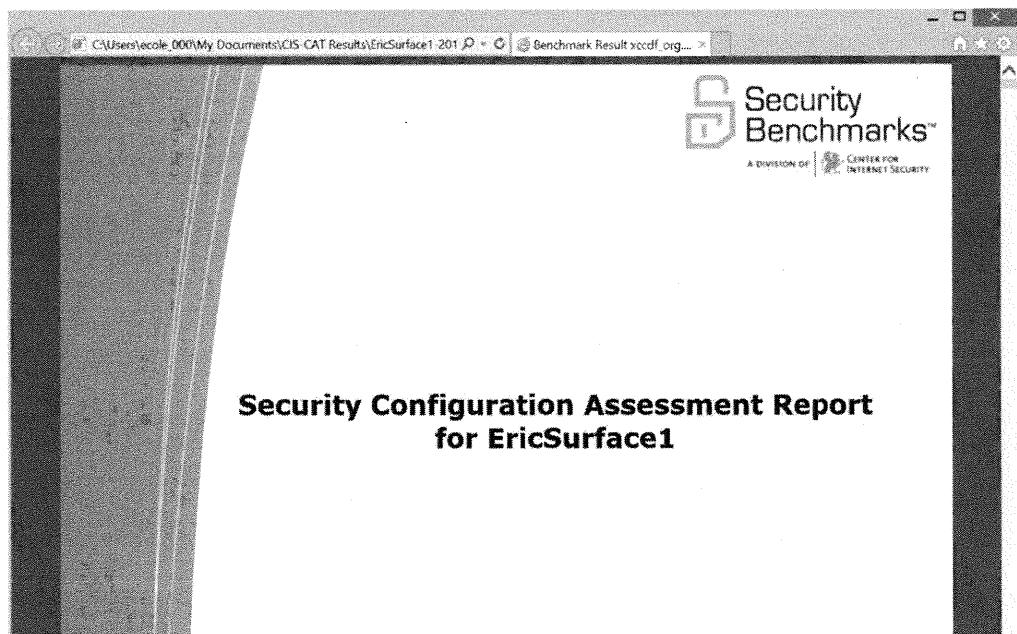
The screenshot shows the Configuration Assessment Tool window. At the top, it displays the title "Configuration Assessment Tool" and the logo of "the CENTER for INTERNET SECURITY". Below the title, it shows the platform as "Windows 8.1 64-bit", the version as "version 6.3", and the Java Runtime Environment (JRE) as "Oracle Corporation 1.8.0\_25". The main area of the window is titled "Benchmark Execution Status" and contains a table with 28 rows of data. The columns in the table are "Number", "Title", "Time", and "Result". The "Time" column consistently shows "<1 second". The "Result" column indicates the outcome of each benchmark: 13/239 is a Fail, 14/239 is a Fail, 15/239 is a Fail, 16/239 is a Pass, 17/239 is a Fail, 18/239 is a Fail, 19/239 is a Fail, 20/239 is a Fail, 21/239 is a Pass, 22/239 is N/C, 23/239 is a Pass, 24/239 is a Fail, 25/239 is a Fail, 26/239 is a Pass, 27/239 is a Pass, and 28/239 is a Pass. At the bottom right of the main area, there is a button labeled "View Reports".

Number	Title	Time	Result
13/239	Set 'Allow Microsoft accounts to be optional' to 'Enabled'	<1 second	Fail
14/239	Set 'Microsoft network client: Digitally sign communications (always)' to 'Enabled'	<1 second	Fail
15/239	Set 'Force specific screen saver: Screen saver executable name' to 'Enabled';scr...	<1 second	Fail
16/239	Set 'User Account Control: Switch to the secure desktop when prompting for elev...' to 'Enabled'	<1 second	Pass
17/239	Set 'Allow unencrypted traffic' to 'Disabled'	<1 second	Fail
18/239	Set 'Windows Firewall: Public: Outbound connections' to 'Allow (default)'	<1 second	Fail
19/239	Set 'WDigest Authentication' to 'Disabled'	<1 second	Fail
20/239	Set 'Do not preserve zone information in file attachments' to 'Disabled'	<1 second	Fail
21/239	Set 'Create symbolic links' to 'Administrators'	<1 second	Pass
22/239	Set 'Prevent the computer from joining a homegroup' to 'Enabled'	<1 second	N/C
23/239	Set 'Audit Policy: Logon-Logoff, Special Logon' to 'Success'	<1 second	Pass
24/239	Set 'Turn off downloading of print drivers over HTTP' to 'Enabled'	<1 second	Fail
25/239	Set 'Turn on PIN sign-in' to 'Disabled'	<1 second	Fail
26/239	Set 'Profile single process' to 'Administrators'	<1 second	Pass
27/239	Set 'Change the time zone' to 'Administrators, LOCAL SERVICE, Users'	<1 second	Pass
28/239	Set 'Audit: Shut down system immediately if unable to log security audits' to 'Disa...'	<1 second	Pass

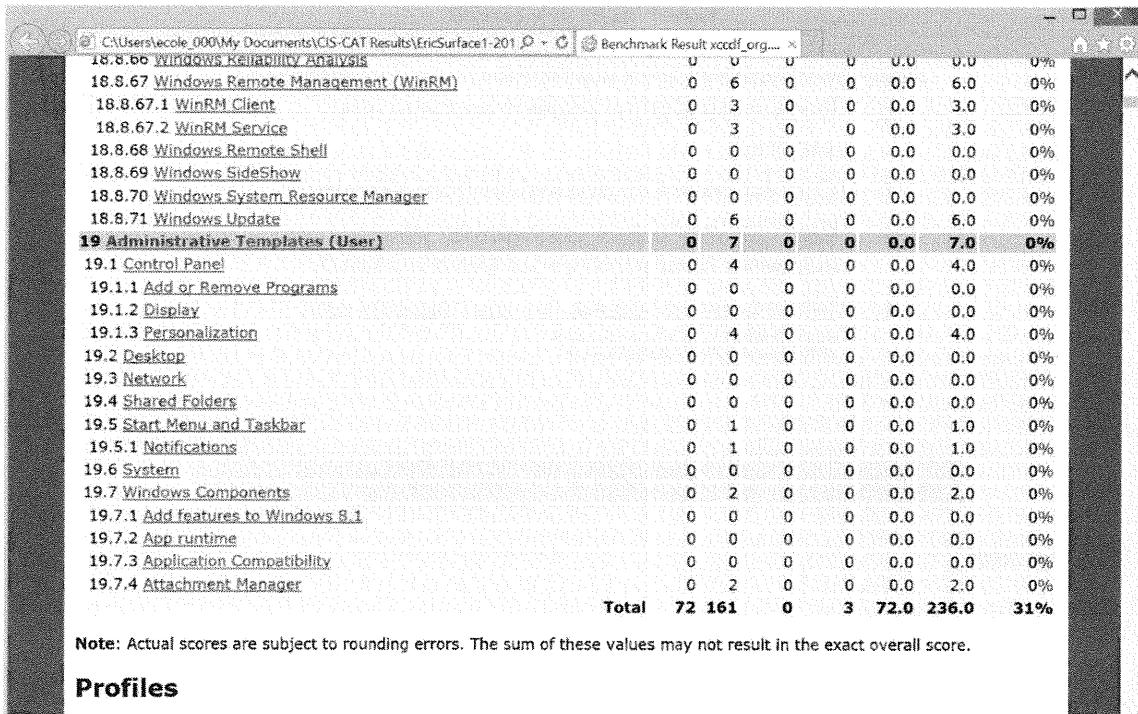
6. Because this is the first time running the program, the only option is to view reports.  
 Click the *View Reports* button.



The report now displays on the screen.



7. Scroll through the results to review your system's overall score.



## Profiles

8. If your system failed a test, you can click the item to find out more details.

**1.1.1 Set 'Enforce password history' to '24 or more password(s)'** Fail

**Description:**

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s).

**Rationale:**

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

**Remediation:**

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s).

```
Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy\Enforce password history
```

9. Spend some time analyzing the report, looking for ways that you can improve your overall security.

---

## CIS Exercises

---

1. Does a maximum score mean you are secure?
2. Can you run CIS against remote devices?
3. Can CIS make any changes to your system's configuration or the template?
4. What level of access do you need to run the CIS Scoring Tool?

SANS Security Essentials – © 2016 SANS

### CIS Exercises

The following questions are answered in the following section:

1. Does a maximum score mean you are secure?
2. Can you run CIS against remote devices?
3. Can CIS make any changes to your system's configuration or the template?
4. What level of access do you need to run the CIS Scoring Tool?

---

## CIS Exercise Solutions

---

1. No. The score simply indicates how well your system compares to the provided templates and patches.
2. No. This particular tool is for local machines.
3. No. This tool is for analysis only.
4. Administrative access is necessary to run CIS.

SANS Security Essentials - © 2016 SANS

### CIS Exercise Solutions

The following are the answers to the questions:

1. No. The score simply indicates how well your system compares to the provided templates and patches.
2. No. This particular tool is for local machines. CIS created other tools for remote scanning.
3. No. This tool is for analysis only.
4. Administrative access is necessary to run CIS.

## CIS Summary

- CIS is an effective tool for determining a system's compliance with specific templates and patches
- CIS can be run only locally
- CIS provides reporting capabilities
- CIS is an excellent tool to use when you set up specific devices versus enterprise-wide deployments

SANS Security Essentials – © 2016 SANS

## CIS Summary

As you can see, the CIS Scoring Tool can be valuable in determining a system's compliance with a specified template as well as current patches. The two limitations that this tool has are that it must be installed and it can run only locally. It can be a helpful resource when you are setting up a particular device rather than an enterprise-wide scale.