

Introduction to Information Security
Prof. Dilip. Ayyar
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 56

Now, we look at the OS security capabilities Linux versus Windows.

(Refer Slide Time: 00:10)

OS Security Capabilities: Linux vs. Windows

- A qualitative assessment of operating system security is subjective and your "mileage may vary" based on present and past experience
- A true comparison between Windows and Linux on the values of the inherent security of each operating system is hard to obtain, and the matter is extremely contentious among both security professionals and computer hobb



A qualitative assessment of the operating system security is subjective and your mileage may vary based on present and past experience. A true comparison between windows and Linux on the values of inherent security of each operating system is hard to obtain and the matter is extremely contentious among both security professionals and computer hobbists. What it basically means is, if you take the case of my example throughout my life I have been working on Linux and Mac OS X. So, I do not like to work on windows system for varied reason.

So, my assessment of windows may be totally different than what another person's opinion may be, again it is not to say that windows is bad or windows does not have security, like I mentioned earlier windows also has got security built in unfortunately the network administrators or system administrators do not know how to use the full features of windows thereby leaving the system compromised and based on user experience, if you are going to log down windows completely you may probably get the same opinion of windows as a user and say may be Ubuntu where this system does not give me what is expected, because I need everything to be open.

So, again it depends on the past experience and when you are comparing the security features it is totally different. In Linux for example, root takes it all is the principle. So, as long as you secure root and keep you are system up to date you should not have any problem. Whereas, windows because it is widely used and it is since it is the most popular operating system for non technical users as well as there are several softwares, there are several applications which were made for windows and which may not run on different flavors of Linux or Mac OS X for that matter. So, it becomes difficult to judge which is a better OS.

Now, if you are using say tally for example, through wine installed in Linux tally works, but then organizations may hesitate to use tally on wine because of support issues, tally themselves have Mac OS X version if I am not wrong. So, again it depends on the organization, it depends on the perception, it depends on what the organization require and how they are going to secure the infrastructure.

(Refer Slide Time: 03:21)

OS Security Capabilities: Linux vs. Windows (continued)

- Because there are many more Windows systems in the world, there are simply more targets available for attack
 - Windows a richer and more attractive target for malware developers
 - Windows monoculture; because Windows systems are all tightly binary-compatible, a single successful attack can affect a large fraction of them
- The security differences between Windows and Linux is heavily debated and the security track record of both operating systems has proven Linux has fewer serious vulnerabilities
 - Also Linux derives its security from the underlying Unix design philosophy




The simple fact is because there are so many more windows systems in the world, they are simply more targets to attack or there are more targets available for the hackers to attack. Windows has a richer and more attractive target for malware developer, because he knows that if you propagates at Malware or every managers to install a malware it will spread then windows monoculture, because windows systems are all tightly binary compatible, a single successful attack can affect a large number of them or large fraction of them.

The security differences between windows and Linux is heavily debated and the security track record of both OS's have proven that Linux has lesser serious vulnerabilities also Linux derives it is security from the underline Unix design philosophy.

(Refer Slide Time: 04:25)

OS Security Capabilities: Linux vs. Windows (continued)		
	Windows	Linux
Malware	<ul style="list-style-type: none"> • As of 2009, well over 2 million malware programs target Windows • Botnets: networks of infected computers controlled by malicious persons - with more than one million computers have been witnessed • Once malicious software is present on a Windows-based system, it can sometimes be incredibly difficult to locate and remove • As such, users are advised to install and run anti-malware programs • In the event of rootkit infection, users may have to resort to reformatting the system's hard disk and re-installing Windows 	<ul style="list-style-type: none"> • As of 2006, more than 800 pieces of Linux malware had been discovered • Some malware has propagated through the Internet. • However, in practice, reports of bonafide malware presence on Linux-based systems are extremely rare • Antivirus Tools like ClamAV and Panda Security's DesktopSecure for Linux do exist



If you see the malware statistics, you will see as of 2009 over 2 million malware programs targeted windows. Now, as of 2006 more than 800 pieces of Linux malware had been discovered. So, where is 2 million and where is 800 there is of course, the time lag of 3 years, but even then even if you double it, it is only 1600 pieces whereas in windows it is 2 million. Botnets, networks of infected computers controlled by a malicious persons with more than 1 million computers have been witnessed; that means, Botnet attacks have occurred on windows.

Once the malicious software is present on a windows based system it can sometimes be incredibly difficult to locate and remove. So, lot of malware removing programs itself are malware you often get when you browse some sight download this particular malware detection kit free of cost. So, one thing we have to understand in life as well as in security is nothing comes free everything is at a cost. If I am give you something if I am giving you something's free then what is my objective, so it is much more than money for it is much more than crime to exploit it is something else.

So, users are advised to install and run anti malware programs, windows now 7 and 8 all have in built malware detecting programs. Now, when you come to Linux side some of the malware programs for Linux have propagated through the internet, but in practice

reports of bonafide malware presence on Linux based systems are extremely rare. Aniware tools like ClamAV and Pandas securities desktop secure for Linux do exist. So, like I mentioned I mean using clam for a very long time before it was a text based version. Now, you have clam which can install on you are Webmin you can do all the configuration, schedule it as a Cron job. So, you can do several things with clam also.

(Refer Slide Time: 06:50)

OS Security Capabilities: Linux vs. Windows (continued)

Open Vs. Closed	Windows	Linux
	<ul style="list-style-type: none"> •Claims its platform is more secure because of a comprehensive approach to security using the Security Development Lifecycle •However, because Windows is closed-source, only Microsoft-employed programmers can fix bugs •Recent Windows versions have some security vulnerabilities detected 	<ul style="list-style-type: none"> •Claims its platform is more secure because all of its code is reviewed by so many people that bugs are detected •Anyone with programming experience is free to fix bugs and submit them for inclusion in future releases and updates •However such an approach has indeed produced several vulnerabilities, although this is a rare case



Here, is an very interesting debate open versus closed. Now, windows claims at it is platform is more secured, because of comprehensive approach to security using security development life cycle. But, because windows is closed only microsoft employers can fix the bugs. Now, new versions of window recent versions of windows like 7 or 8 have some security vulnerabilities detected. Now, when you take the open source claims that it is platform is more secure, because all of it is code is reviewed by so many people that the bugs are detected quickly anyone with programming experience is free to fix bug and submit them for inclusion in future releasing and updates.

But, such an approach has indeed produced several vulnerabilities although it is a very rare case, sometimes you fix a bug and then it gives rise to another bug. So, it is a very rare case, because it is reviewed and so many rounds of testing are done or iterations of testing are done before it is actually a release candidate. So, there are both positive and negative aspects of open and closed systems.

(Refer Slide Time: 08:15)

OS Security Capabilities: Linux vs. Windows (continued)

Response Speed	<ul style="list-style-type: none">•There are claims that closed source offers a faster and more effective response to security issues•However, critical bug fixes are released only once a month after extensive programming and testing, and certain bugs have been known to go un-patched for months or even years	<ul style="list-style-type: none">•Bugs can be fixed and rolled out within a day of being reported (often within hours), though usually it takes a few weeks before the patch is available on all distributions
-----------------------	---	---



Then, the response speed or time in windows there are claims that close sources offers a faster and more effective response to security issues, but critical bug fixes are released only once a month after extensive programming and testing and certain bugs are known to go un-patched for months or even years, but in the case of open source bugs can be fixed and rolled out within a day of being reported often within hours though it usually takes a few weeks before the patch is available on all distributions.

(Refer Slide Time: 08:54)

OS Security Capabilities: Linux vs. Windows (continued)

User Accounts	<ul style="list-style-type: none">•In Windows Vista, all logged-in sessions run with standard user permissions, preventing malicious programs from gaining total control of the system•Processes that require administrator privileges can be run using the User Account Control framework.•For standard users, this presents a credentials dialogue that requires the password of a member of the administrators group (who are listed)•For users who are already logged in an administrator, only confirmation is necessary•The first user account created during the setup process is automatically a member of the administrators group•The majority of users did not change to an account type with fewer rights, meaning that, in Windows versions prior to the introduction of UAC, malicious programs would have full control over the system•However the security of the User Account Control is not guaranteed to prevent malicious programs and users from unlimited access in Windows	<ul style="list-style-type: none">•Users typically run as limited accounts, having created both administrator (root) and at least one user account during installation•In most Linux distributions, there are commands (su, sudo) that will temporarily grant elevated permissions to processes that need it•In practice, this can be very dangerous, as any error can lead to severe damage to the system•New frameworks such as PolicyKit seek to rectify this problem• However, as of Feb. 2009, PolicyKit is not in widespread use.
----------------------	---	---



When we come to user accounts in vista and are though all logged in sessions are run with standard user permission, preventing malicious programs from gaining total control of the system. Whereas, in open source users typically run as limited accounts having

created both administrator or root and at least one user account during installation. Then in windows processes that require administrative privileges can be run using the user account control framework.

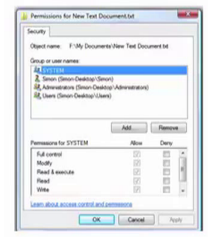
In most Linux distributions there are commands like su and sudo that will temporarily grant elevated permissions to processes that require it. Here, in the case of windows for users who are already logged in as administrator only confirmation is necessary here new framework such as policy kit seeks to rectify the problem of this, but as on February 2009 policy kit in open sources is not in wide spread use.

Now, coming back to windows for standard users this presents a credentials dialogue that require a password of a member of a administrative group which are listed that is for the user account control framework. And then, the first user account created during the set up process is automatically a member of the administrative group, the majority of users did not change to an account type with fewer rights meaning that in windows version prior to the introduction of UAC, malicious programs would have full controlled over the system.

However, the security of the user account control is not guaranteed to prevent malicious programs and users from unlimited access in windows. So, one of the things that we have to note or learn here is these second last point under windows, the majority of the users did not change to an account type with fewer rights, once I am administrator equivalent why would I deprecate my privileges or why would I bring down my privileges. So, most of the time the users continue to use that administrator account, unless otherwise it is domain joint.

(Refer Slide Time: 11:19)

OS Security Capabilities: Linux vs. Windows (continued)

Windows: File System Permissions	<ul style="list-style-type: none">•The DOS based Windows ME, Windows 98, Windows 95, and previous versions of non-NT Windows only operated on the FAT file system and did not support file system permissions•Windows NT and subsequent NT-based versions of Windows use NTFS-based Access Control Lists to administer permissions, using tokens•On Windows XP and prior versions, most home users still ran all of their software with Administrator accounts, as this is the default setup upon installation•The existence of software that would not run under limited accounts and the cumbersome "Run As..." mechanism forced many users to use administrative accounts•However, few organizations have taken advantage of the richness of the Token based system of NTFS which can be applied to almost all NT operating system objects	File system permissions on a Windows Vista system. 
---	---	---

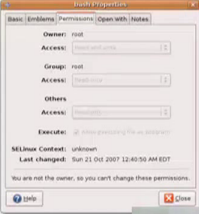



In windows file system permission the DOS based windows ME, windows 98, 95 previous version of non-NT mp windows only operated on the FAT file system and did not support file system permissions, but windows NT and subsequent NT based versions of windows use NTFS based access control list to administer permissions using tokens on XP and prior versions most home users still ran all their software with administrator accounts as this is the default setup upon installation.

The existence of software that would not run under limited accounts and the cumbersome run as mechanism forced many users to use administrative accounts. So, that was one of the reason why many users were forced to use administrative accounts. But, few organizations have taken the advantage of the richness of the token based system of NTFS which can be applied to almost all NT operating system objects.

(Refer Slide Time: 12:30)

OS Security Capabilities: Linux vs. Windows (continued)


Linux: File System Permissions	•Linux has a traditional Unix-like “user, group, other” approach to file system permissions at a minimum •This approach is extended by Access Control Lists on some file systems •There are some specific to Linux frameworks such as AppArmor and SELinux which add even finer-grained controls over which users and programs can access certain resources or perform certain operations •Some distributions use them out of the box	File system permissions on an Ubuntu Linux system running GNOME 
---	--	---



In under Linux file system permission, Linux has a traditional Unix like user group other approach to file system permissions at a minimum, this approach is extended by access control lists on some file systems, there are some specifics to Linux frameworks such as apparmor and SELinux which add even finer grained controls over which the users and programs can access certain resources or perform certain operations some distributions use them out of the box Ubuntu uses them out of the box fedora has gone SELinux installed suse hass got; so, the concept of user group and other is uniformly followed or the permissions have being assigned based on that criteria.

(Refer Slide Time: 13:30)

Conclusion

- Security is a perennial concern for IT administrators
 - Managers need a framework to evaluate operating system security
 - The challenge in evaluating Windows and Linux on any criteria is that there is not a single version of each operating system
 - Users need to keep in mind that there are philosophical differences in the design of Linux and Windows
 - The ability to make either operating system more secure varies depending on architectural design
 - The Windows operating system is designed to support applications by moving more functionality into the operating system, and by more deeply integrating applications into the Windows kernel
 - Linux differs from Windows in providing a clear separation between kernel space and user space
- 

We come to the conclusion of Linux and windows security. Now, security persay is a

perennial concern or a problem for IT administrators. So, the managers need a framework to evaluate the operating system security, the challenge in evaluating windows and Linux on any criteria is that there is not a single version of each operating system, like we said windows started from 95, 98, ME, XP 7, 8 in between vista. Now, even if you take a particular distribution of Ubuntu it is started from 7, 8, 9, 10, 10. something, 11, 11.something, 12, 12.something, now you can 14.04.1.

So, because of that there is not a single version of the OS. So, it becomes difficult, users need to keep in mind that there are philosophical differences in the designs of Linux and windows. One of the fundamental differences windows is monolithic and Linux is not the ability to make either operating system more secure varies depending upon the architectural design requirement of the company.

The windows OS system is designed to support applications by moving more functionality into the operating system and by more deeply integrating applications into the window kernel, Linux differs from window in providing a clear separation between the kernel space and the user space. With that we will end the topic on windows and Linux security and we will look at some security baselines.

(Refer Slide Time: 15:34)

Objectives

- Disable nonessential systems
- Harden operating systems
- Harden applications
- Harden networks



So, we will look at the security baselines now, what are the objectives, one, these are again base lines disable nonessential systems or services, harden the operating system, harden the application, harden the networks including the security infrastructure.

(Refer Slide Time: 15:57)

Disabling Nonessential Systems

- First step in establishing a defense against computer attacks is to turn off all nonessential services
- Disabling services that are not necessary restricts what attackers can use
 - Reducing the attack surface
 - Hardening the operating system



The first is disabling nonessential systems. So, the step in establishing a defense against computer attack is to turn off all nonessential services. Disabling services that are not necessary restricts what an attackers can use; it is by reducing the attack surface and hardening the operating systems. Now, when you talk about services Telnet is the service. So do you need Telnet for doing you are day to day operations no, so disable Telnet.

On suppose you are running a web server which runs on port 443 or HTTPS, do you need any other port open for public no you do not, so you turn off. Similarly, for my SQL or for ORACLE, you change from the default port and put it on some other port for that you disable that default port. So, when a attacker sees from outside he will not know what surface is actually running on what port. So, basic idea is you turn off nonessential services first.

(Refer Slide Time: 17:14)

Disabling Nonessential Systems

- Operating systems use programs that run in the background to manage different functions
- In Microsoft Windows, a background program, such as Svchost.exe, is called a **process**
- The process provides a **service** to the operating system indicated by the **service name**, such as AppMgmt



Now, operating systems use programs that run in the background to manage different functions. In Microsoft windows a background program, such as svchost.exe is run; it is a process. The process provides a service to the operating system indicated by the service name, such as app management or application management.

(Refer Slide Time: 17:38)

Viewing Services

Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	99	2:43:24	16 K
System	8	00	0:00:44	212 K
smss.exe	144	00	0:00:00	380 K
csrss.exe	168	00	0:00:22	2,712 K
WINLOGON.EXE	188	00	0:00:01	436 K
services.exe	216	00	0:00:01	6,572 K
LSASS.EXE	228	00	0:00:00	1,348 K
IEXPLORE.EXE	280	00	0:02:30	29,324 K
svchost.exe	404	00	0:00:00	5,504 K
SPOOLSV.EXE	444	00	0:00:00	6,672 K
DefWatch.exe	472	00	0:00:00	2,388 K
svchost.exe	492	00	0:00:01	8,212 K
MDM.EXE	516	00	0:00:00	2,740 K
Rtvscon.exe	520	00	0:00:16	19,124 K
prtg4.exe	648	00	0:00:00	464 K
prtg4.exe	652	00	0:00:05	5,644 K
resproc.exe	712	00	0:00:00	972 K
motask.exe	724	00	0:00:00	3,332 K
wingmt.exe	764	00	0:00:06	548 K



You can see from this slide it is svchost is somewhere in the between, it is the running, internet explorer is running, LSASS you know by now what it is.

(Refer Slide Time: 17:52)

Disabling Nonessential Systems

- Users can view the display name of a service, which gives a detailed description, such as “Application Management”
- A single process can provide multiple services
 - To view these services:
 - Go to Computer Management
 - Double-click on Services and Applications
 - Double-click on Services



So, users can view the display name of a service which gives a detailed description, such as the application management. A single process can provide multiple services, now to view these services most of you will know it, but even then go to the computer management, double click on services and application, double click on services.

(Refer Slide Time: 18:17)

Disabling Nonessential Systems

The screenshot shows the Windows Computer Management console. The 'Services' folder is expanded, and the 'Application Management' service is selected. A red circle highlights the service name, and a red box highlights the 'Display Name' column header. The 'Description' column for 'Application Management' is also highlighted with a red box.

Name	Description	Startup Type	Service Type	Display Name	
Application Management	Provides s...	Manual	LocalSystem	Application Management	
ASP.NET State Serv...	Provides s...	Manual	.ASPNET	ASP.NET State Service	
Automatic Updates	Enables th...	Manual	LocalSystem	Automatic Updates	
Background Intellig...	Transfers f...	Manual	LocalSystem	Background Intelligent Transfer Service	
ClipBook	Supports C...	Manual	LocalSystem	ClipBook	
COM+ Event System	Provides a...	Started	Manual	COM+ Event System	
Computer Browser	Maintains a...	Started	Automatic	LocalSystem	Computer Browser
DefWatch	Started	Automatic	LocalSystem	DefWatch	
DHCP Client	Manages n...	Started	Automatic	LocalSystem	DHCP Client
Distributed Link Tra...	Sends notif...	Started	Automatic	LocalSystem	Distributed Link Tracking Service
Distributed Transac...	Coordinate...	Manual	LocalSystem	Distributed Transaction Coordinator	
DNS Client	Resolves a...	Started	Automatic	LocalSystem	DNS Client
Event Log	Logs event...	Started	Automatic	LocalSystem	Event Log
Fax Service	Helps you ...	Manual	LocalSystem	Fax Service	
FTP Publishing Service	Provides F...	Started	Automatic	LocalSystem	FTP Publishing Service
IIS Admin Service	Allows adm...	Started	Automatic	LocalSystem	IIS Admin Service
Indexing Service	Indexes co...	Disabled	LocalSystem	Indexing Service	
Internet Connectio...	Provides n...	Manual	LocalSystem	Internet Connection Sharing (ICS)	
IPSEC Policy Agent	Manages I...	Started	Automatic	LocalSystem	IPsec Policy Agent
Logical Disk Manager	Logical Disk...	Started	Automatic	LocalSystem	Logical Disk Manager
Logical Disk Manage...	Adminstrat...	Manual	LocalSystem	Logical Disk Manager	

So, you know what all services are running, so you can see that the applications management is running, it is not started yet.

(Refer Slide Time: 18:26)

Disabling Nonessential Systems

- A service can be set to one of the following modes:
 - Automatic
 - Manual
 - Disabled
- Besides preventing attackers from attaching malicious code to services, **disabling nonessential services** blocks entries into the system



A service can be set to one of the following modes in windows, automatic, manual or disabled. Besides preventing attackers from attaching malicious code to services, disabling non essential services blocks entry into the system. Now, hardening we already seen it is the process of reducing vulnerabilities, a hardened system is configured and updated to protect against attacks, there are three broad categories of items that should be hardened, one is the operating system, the applications that the operating system run and the networks.

(Refer Slide Time: 19:04)

Hardening Operating Systems

- You can harden the operating system that runs on the local client or the **network operating system (NOS)** that manages and controls the network, such as Windows Server 2003 or Linux

http://searchwindowssecurity.techtarget.com/featuredTopic/0,290042,sid45_gci1069557,00.html?bucket=REF

<http://www.microsoft.com/technet/security/prodtech/windowsxp.mspx>



You can harden the operating system that runs on the local client or the network operating system that managers and controls the networks, such as windows server 2003

or 2008 or 12 or a Linux system, there is a link provided here. So, you can go through the link which will give you some of the hardening measure that have to be done. Microsoft has got a good bit of documentation, you can also type in Google or search in Google hardening a Linux, Ubuntu Linux or a red hat Linux you will get lot of resources.