**Introduction to Information Security**

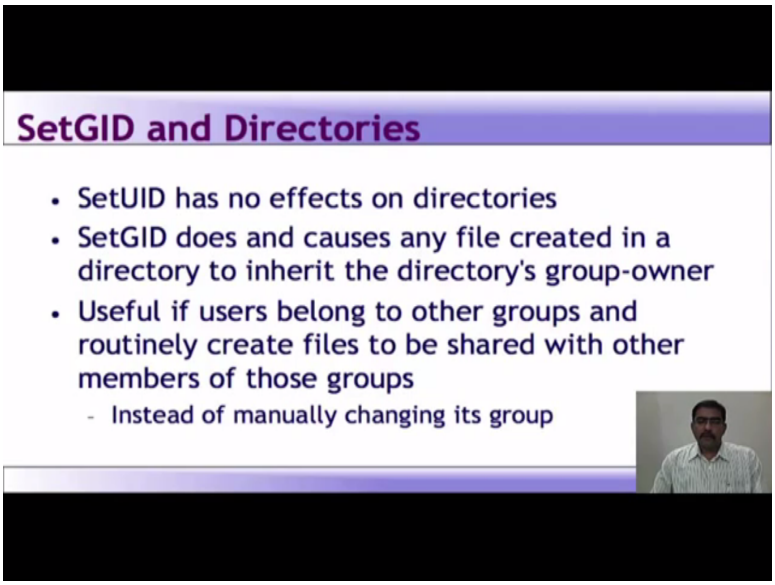
**Prof. Dilip H. Ayyar**

**Department of Computer Science and Engineering**

**Indian Institute of Technology, Madras**

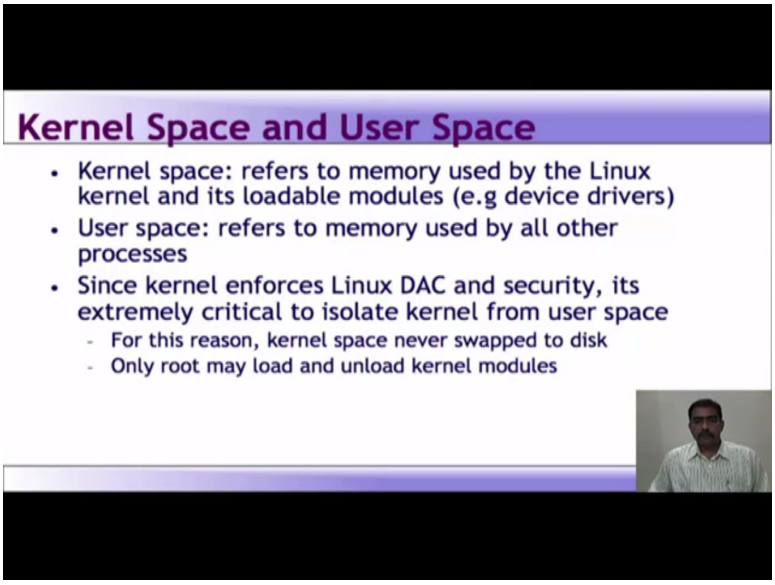
**Lecture - 53**

(Refer Time Slide: 00:10)



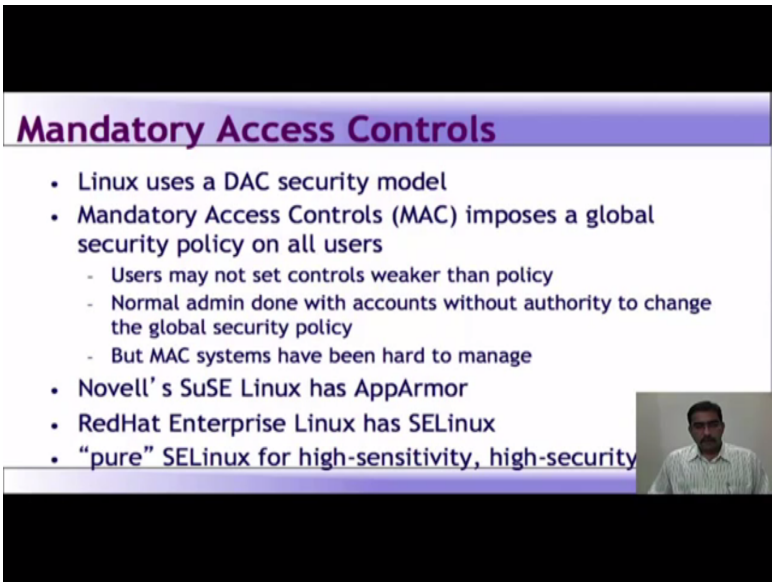

Setgid and directories, the setuid has no effect on the directories, setgid does and causes any file created in a directory, to inherit the directory's group-owner. It is useful, if users belong to other groups, and routinely create files to be shared with other members of the group, instead of manually changing its group. So, that is the difference. So, that is the correlation, between setgid and directories.

(Refer Time Slide: 00:43)




Then, we have discussed before, about kernel space and user space kernel. Space refers to memory used by Linux kernel, and the loadable modules, like you have device drivers. The user space refers to memory, used by all other processors. Since, kernel enforces Linux dac end security, it is extremely critical to isolate the kernel from user space. For this reason, kernel space never is never swapped to the disk, only root may load and unload kernel modules.

(Refer Time Slide: 01:25)



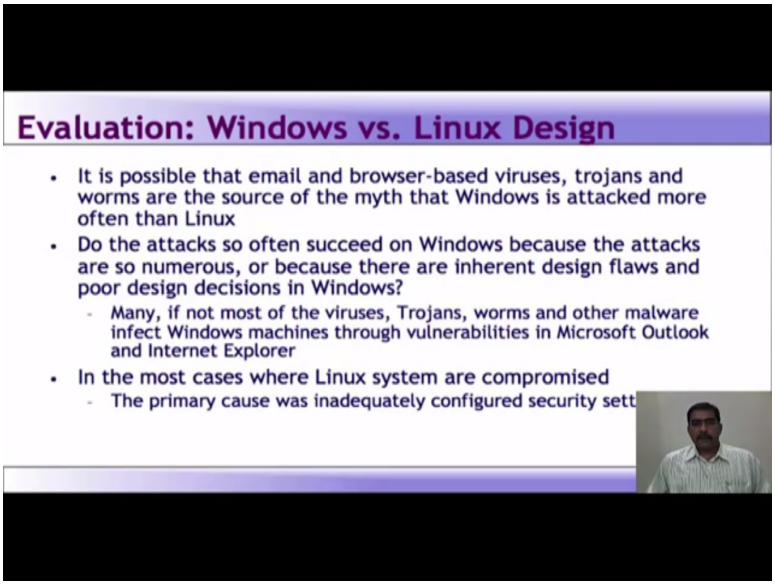

Mandatory access control, now discretionary access control module, we have seen the owner of a given system object, can set whatever access permission on that resource, he or she likes, right. So, that is dac security model. The user, who creates a file on the mac system, mac is

mandatory access control system, generally may not set access controls on that file, that are weaker than the controls, dictated by the system security policy.

In mac based system, the only thing is that the super user account is used for maintaining the global security policy. Day to day system administration is performed using accounts, that lack or do not have the authority to change the global security policy. Now, as a result, it is impossible to compromise the entire system by attacking any one process. To create an effective global security policy, requires detailed knowledge of the intended behavior of the application.

So, the mac systems have been very hard to manage. Now, furthermore the more restrictive, the security controls are on a given system, it will be less convenient, for the users to operate on. So, there should be a proper balance between security, and usability. So, nowthe mac or mandatory access controls impose a global security policy, we have already discussed that. Novell's suse Linux has got apparmor, red hat enterprise has seLinux. Now, pure seLinux for high sensitivity, high availability that is what se means.

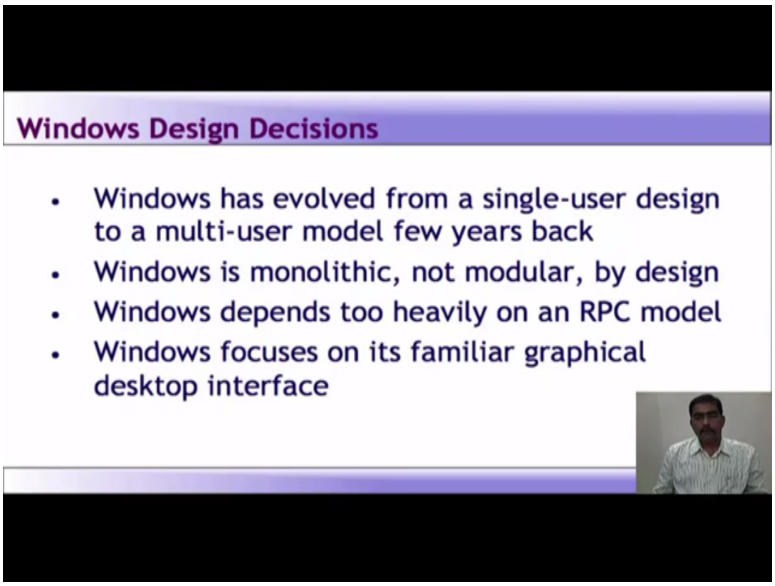
(Refer Time Slide: 03:20)




Now, let us look at the evaluation between windows and Linux designs. Now, it is possible that email, and browser based viruses, Trojans, and worms are a source of myth, that windows attack more often, than Linux. Do the attacks, so often succeed on windows, because the attacks are so numerous, or because there are inherent design flaws and poor design decision, in windows.

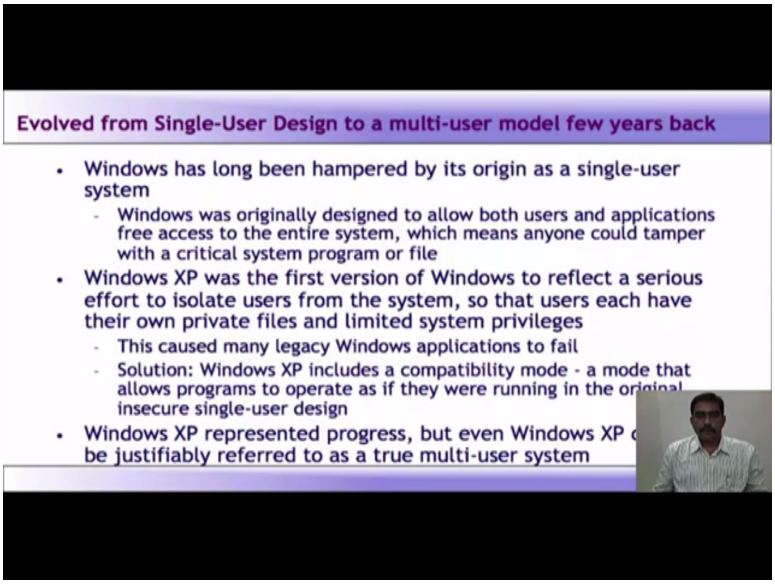
Many if not, most of the viruses, trojans, worms, and other malware infect windows machine, through vulnerabilities in Microsoft outlook, and internet explorer application. In most cases, where the Linux systems are compromised the primary cause of was inadequately, configured security settings.

(Refer Time Slide: 04:13)




Windows has evolved from a single user design, to a multi-user module few years back. Windows is monolithic, means it is not modular by design. Windows depends too heavily on the rpc module, we will see, what is rpc, windows focuses on its familiar graphical desktop user interface.

(Refer Time Slide: 04:35)




Now, what does it means, that it has evolved from a single user design to a multi user module few years back. Windows has long been hampered, by its origin as a single user system. So, when it was windows a few years back, say it is excellent for a desktop. Windows was originally designed, to allow both users and applications, free access to the entire system, which means, anybody could tamper with critical system and put on an attack file.

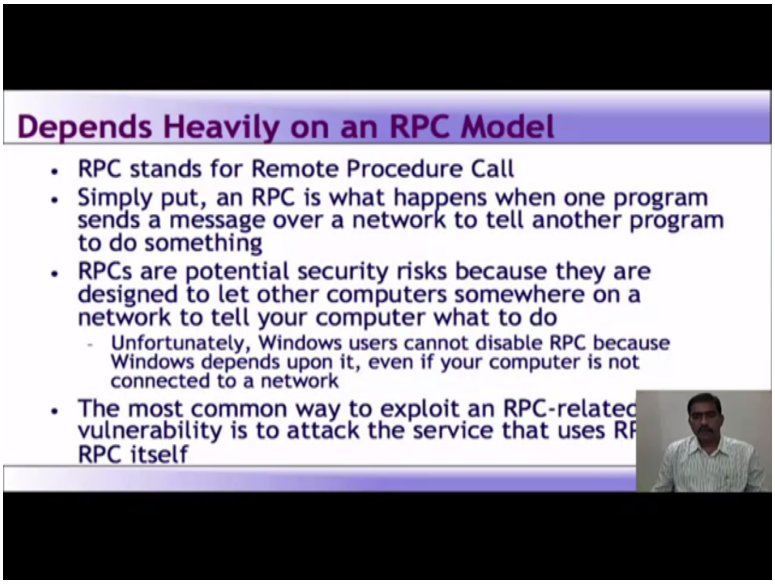
XP was the first version, of the windows to reflect a serious effort to isolate, the users from the system, so that the users each have their own private files, and limited system privileges. This caused many legacy window applications to fail. So, what the solution was windows xp includes a compatibility mode, a mode that allows program to operate as if, they were running the original insecure single user design. Xp represented progress, but even xp could not be justifiably referred to as a true multiuser system.

(Refer Time Slide: 05:45)


Now, again when we spoke about monolithic by design, and it is not modular, but what does it mean, monolithic design means one where most features are integrated into a single unit. So, Microsoft successfully makes competing products irrelevant, or it makes the competing products irrelevant, by integrating more and more of the services they provide, into the operating system.

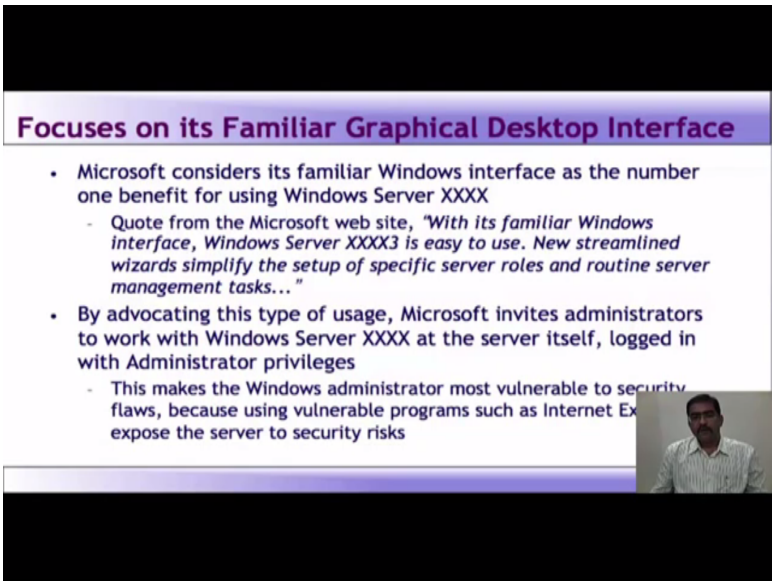
But, this approach creates a monster of inextricably interdependent services. Interdependencies side effect is also there, every flaw in the piece of the system is exposed through all of the service, and applications that depend on it. Then, it is unstable by nature, when you design a system, which has too many interdependencies you introduce numerous risks, when you change one piece of the system. So, it affects the entire system itself. Thus monolithic system tends to make security vulnerabilities more critical, than they need to be.

(Refer Time Slide: 06:47)




They depend very heavily, on the rpc module, rpc stands for remote procedure call. Simply put an rpc is what happens, when one program sends a message over the network to tell another program, to do something. Rpc's are potential security risks because, they are designed to let other computers, somewhere on the network, tell your computer what to do. So, unfortunately windows users cannot disable rpc, because windows depends on rpc, even if you computer is not connected to the network rpc is required for windows. The most common way to exploit an rpc related vulnerability, is to attack that use the rpc not rpc itself.

(Refer Time Slide: 07:45)

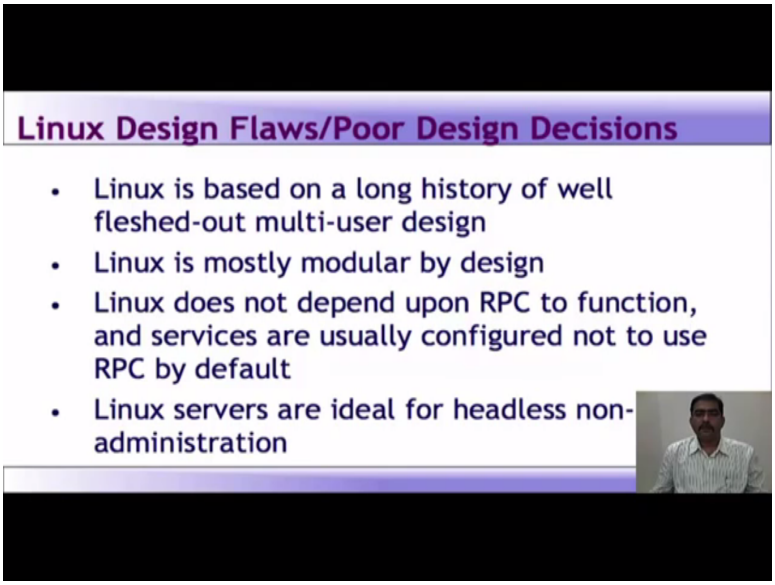



The focuses, windows focuses on its familiar graphical interface, Microsoft considers its familiar windows interface, as the number one benefit of using a windows server, whatever

version. Now, there's support from Microsoft website, with its familiar windows interface, windows server whatever version it is easy to use. New streamline result simplify, the setup of specific server roles, and routine server management tasking.

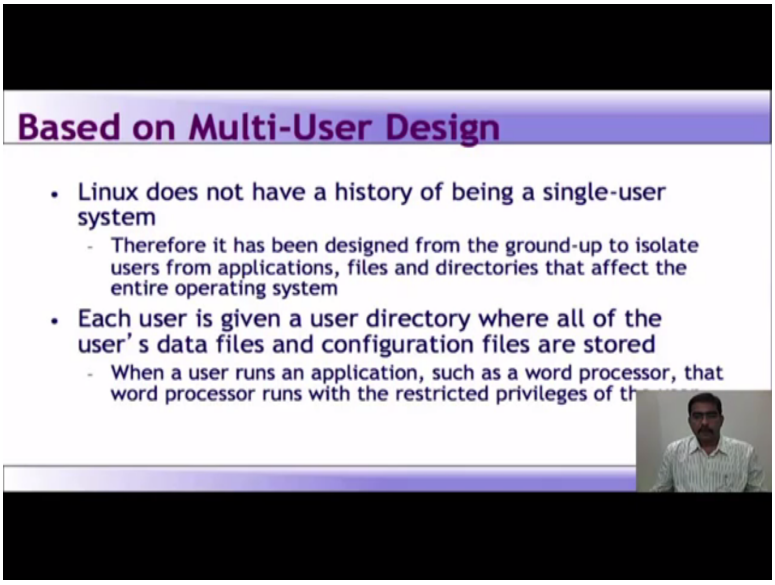
Now, by advocating this type of usage, Microsoft invites, administrators to work with the windows server at the server level itself, logged in with the local administrative privileges. This makes windows administrator, most vulnerable to security risks, because using vulnerable programs such as ie, exposes the server to security risks.

(Refer Time Slide: 08:34)




When you come to Linux design flaws, or poor design decisions, Linux is based on a long history of well flushed out multiuser design. Linux is modular by design, Linux does not depend on rpc to function, and services are usually configures not to use rpc, by default. Linux servers are ideal for headless non-local administration, what is what does that mean.

(Refer Time Slide: 09:05)

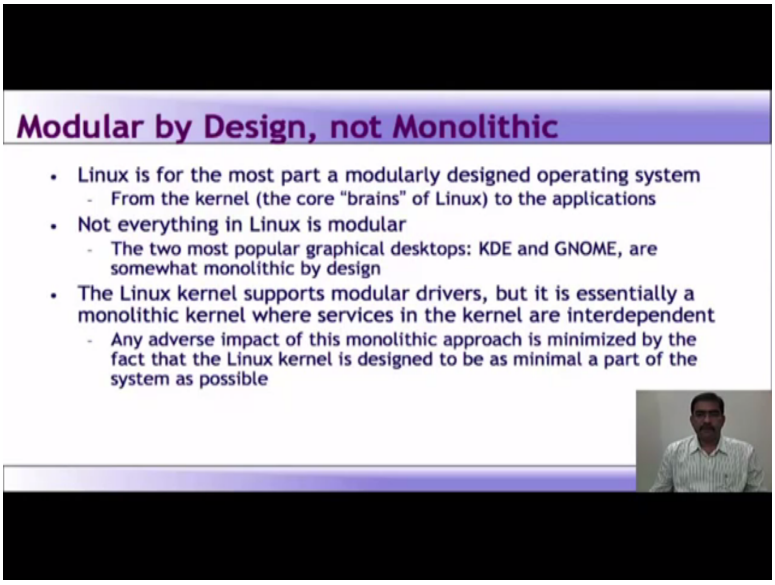



Linux does not basically have a history, of being a single user system. Therefore, it has been designed from ground up, to isolate the user from applications, the files, and the directories, that affect the entire operating system. Each user is given a user directory, where all of the, user data files and configuration files are stored. When a user runs an application, such as a word processor, the word processor runs with a restricted privilege of the user.

Now, what is important here is, Linux provides almost all capabilities, such as rendering of jpeg images, as modular jpeg images. As a result, when a word processor renders a jpeg image, that jpeg rendering functioning will run with the same restricted privileges, as the word processor itself. If there is a flaw in the jpeg rendering routine, a malicious hacker can only exploit this flaw, to gain the same privilege as the user, thus preventing potential damage.

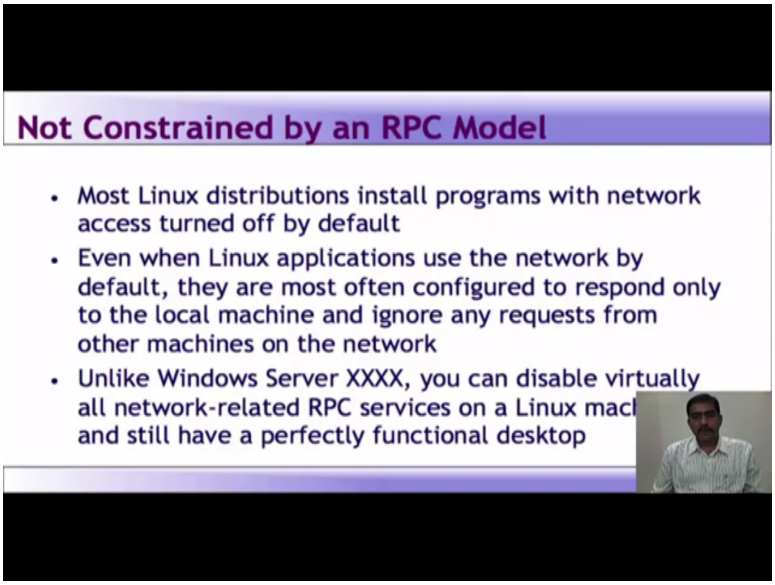
That is the benefit of modular design, and it follows more closely the spherical energy, of an ideally designed operating system. Given these default restrictions in the modular nature of Linux, it is nearly impossible to send an email to a Linux user, that will infect the entire machine with the virus.

(Refer Time Slide: 10:40)



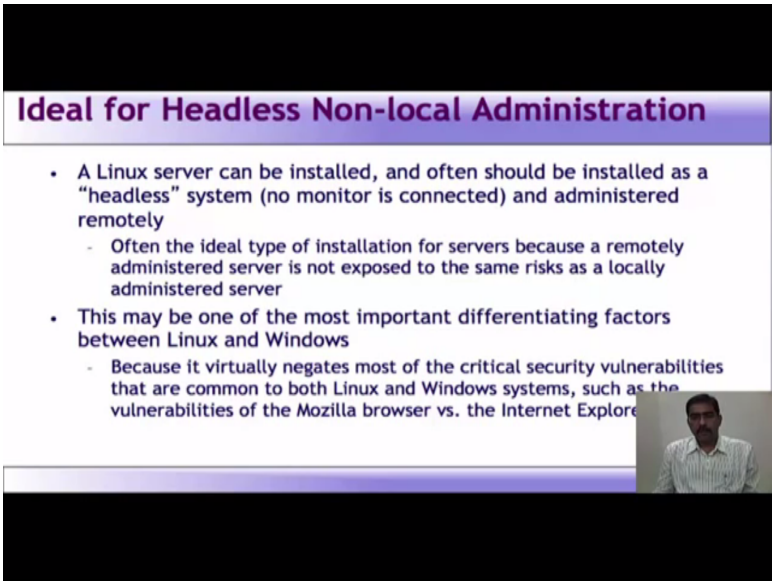

Linux is for the most part, a modularly designed operating system, from the kernel to the applications. Kernel is again, we emphasize the code or bridge of Linux. Not everything in Linux, is also modular. There are two most popular graphical desktops, gnome and kde, they are somewhat monolithic by design. The Linux kernel supports modular drivers, but it is essentially a monolithic kernel, where services in the kernel are interdependent. And advanced, or adverse impact of this monolithic approach, is minimized by the fact that Linux kernel is designed, to be as minimal a part of the system as possible. Now, there is Linux follows, a so called philosophy all most to the point of fanaticism, whenever a task can be done outside the kernel, it must be done outside the kernel. This means that almost every useful feature in Linux, now useful here is as specified by the end user. It is feature that does not have access, to the vulnerable parts of the unit system it is not constrained by an rpc model.

(Refer Time Slide: 11:59)




So, most Linux distribution installed programs are with network access, turned off by default. So, even when Linux applications use the network, they are most often configured to respond only to the local machine, and ignore any request from other machines on the network. Unlike windows server, you can disable virtually all network related rpc service, on the Linux machine, and still perfectly have a good functional desktop.

(Refer Time Slide: 12:31)

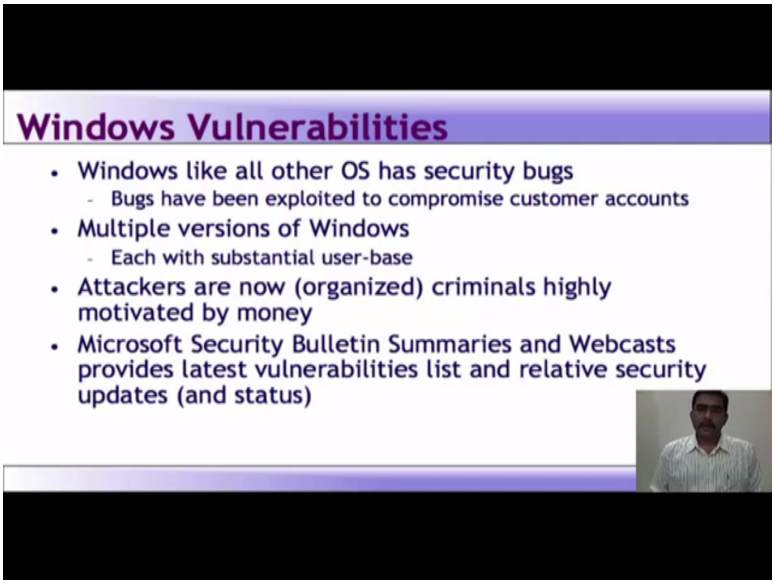



It is ideal for headless non-local administration, now a Linux server can be installed and often should be installed as a headless system, which is no monitor connected, no key board

connected, no mouse connected and administered remotely. Often, the ideal type of installations for servers, because a remotely administered server is not exposed to the same risk, as locally administered server.

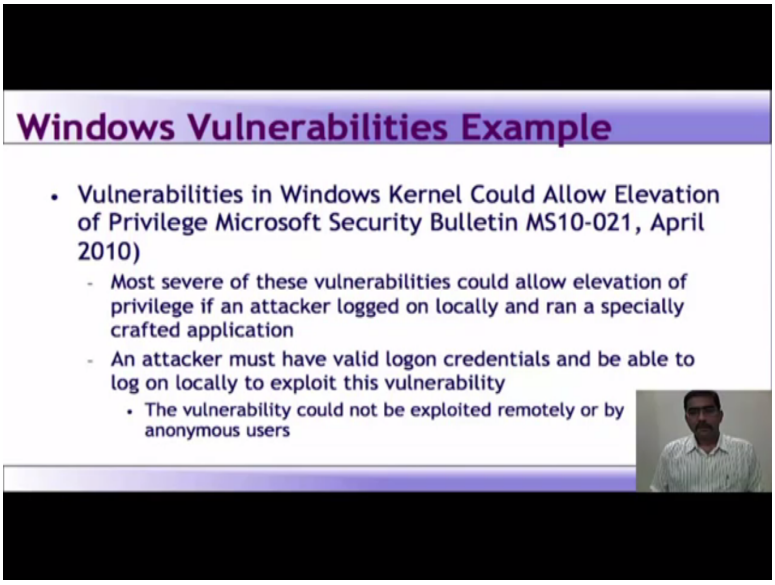
This may be one of the most important differentiating factors, between the Linux, and windows, because it virtually negates most of the critical security vulnerabilities, that are common to both Linux, and windows system, such as vulnerabilities of the Mozilla browser, versus the internet explorer browser. So, you cannot run a Mozilla browser on a server. Let us take a look at windows vulnerabilities.

(Refer Time Slide: 13:25)




Some of them at least, windows like any other os, has security bugs. Bugs have been exploited to compromise customer accounts. There are multiple versions of windows, and each of the versions with a substantial user base, and attackers are now more organized, or they are organized criminals. They are highly motivated by money. Microsoft security bulletin summarize, and webcasts provide latest vulnerabilities list and relative security updates and status.

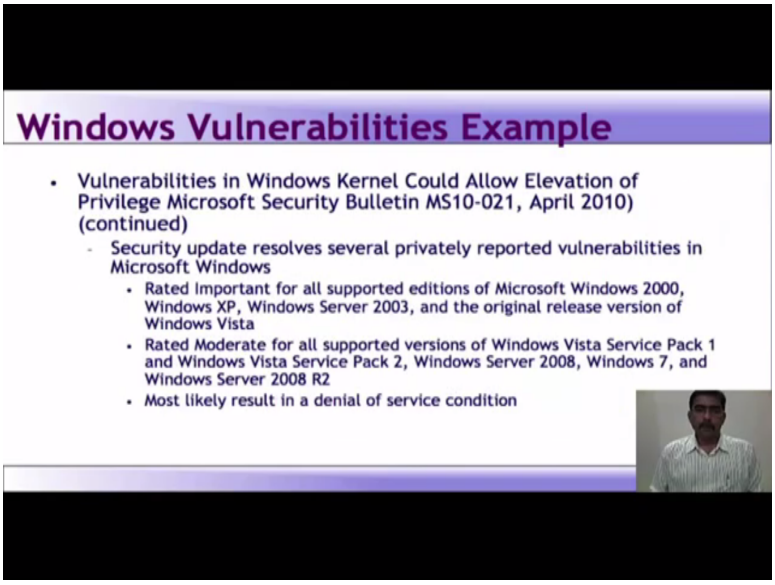
(Refer Time Slide: 14:03)




Now, some example we will look at what kind of vulnerabilities are coming, vulnerabilities in windows kernel could allow elevation of privileges, that is in 2010, what this particular vulnerability does. Most severe of these vulnerabilities could allow elevation of privileges, if an attacker logged on locally, and ran a specifically crafted application.

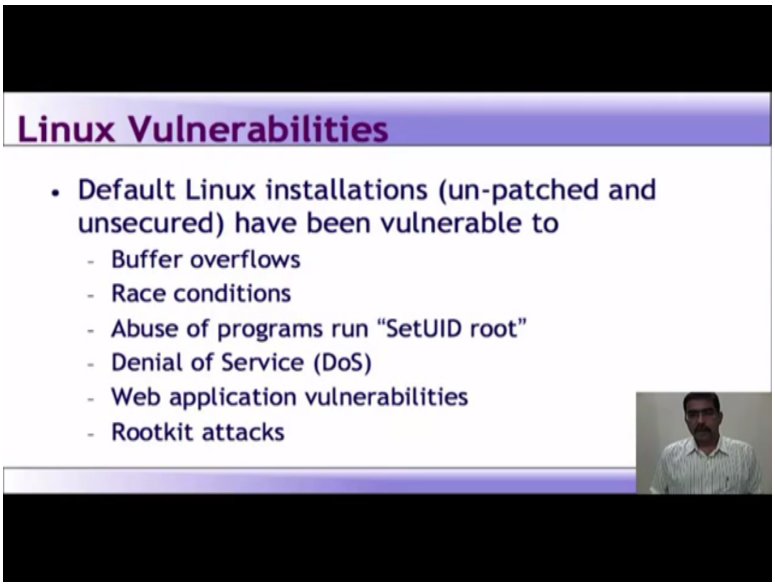
An attacker must have a valid log on credential, and should be able to log on locally to exploit this vulnerability. This vulnerability could not be exploited remotely, or by anonymous users. Now, this is where the fundamental difference, between windows and Linux come in. The system administrators in a windows system log on locally, use it like a desktop, install untrusted applications, introduce unknowingly viruses, trojans or other malware into the system. So, this is exactly an example of why an headless system is required.

(Refer Time Slide: 15:15)




Another Vulnerability in windows kernel, could allow elevation of privileges security updates, resolves several privately imported vulnerabilities in Microsoft windows. Now, here, what basically happens is the denial of service condition, and this particular vulnerability affects, almost all versions of windows that is, vista service pack 2, server 2008, windows 7, Microsoft windows, release , r2. So, again most likely it will result in a denial of service condition.

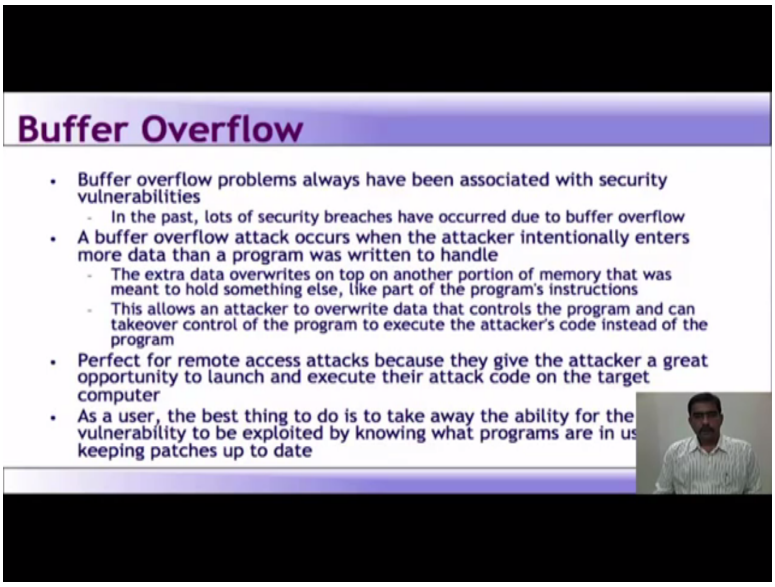
(Refer Time Slide: 15:48)




Linux vulnerabilities, now default Linux installation that is un-patched, and unsecured systems have been vulnerable to buffer overflows, race conditions, abuse of programs that is run setuid and a run setuid, denial of service, web application vulnerabilities. Why web

application vulnerabilities have come here is, because most of the web servers which are running the big ones, run on some version of Linux, then rootkit attacks, we will look into all of those, first let us look into buffer overflow.

(Refer Time Slide: 16:21)

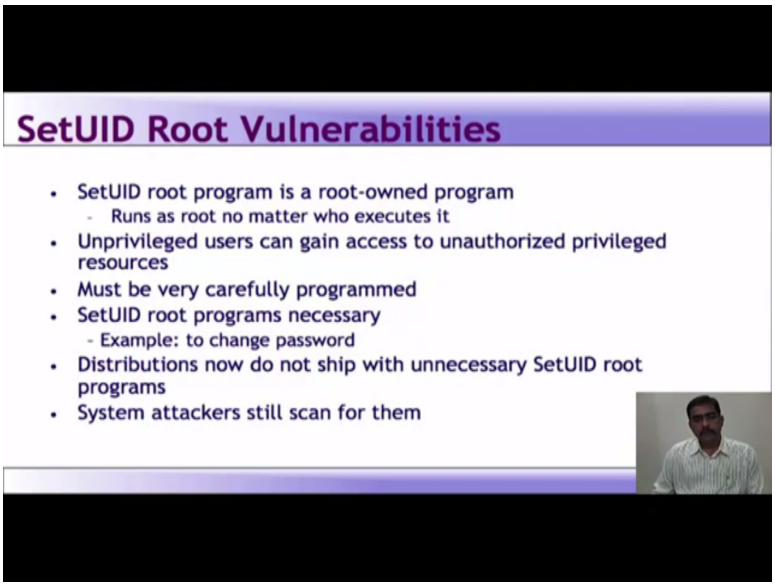



What is a buffer overflow, buffer overflow occurs when attackers intentionally enters more data, than a program is able to handle, that is what a buffer overflow means. As a user, the best thing to do is, to take out the ability for the vulnerability to be exploited, by what is known as patching the system properly, and to know what programs are in use. So, buffer overflow have always been associated with, security vulnerabilities. In the past, lot of security breaches, have occurred due to buffer overflow.

Now, it occurs when the attacker intentionally enters more data than a program is able to handle, we have seen that, the extra data overrides on top of another portion of the memory, that was meant to hold something else, like a part of the program's instruction. This allows the attacker to overwrite data, that controls the program, and can take over control of the program, to execute the attacker's code, instead of the original program.

It is perfect for remote access attacks, because they give the attacker, a great opportunity to launch, and execute their attack code on the target computer. Now, as user the best thing to do is, to take away the ability, for the vulnerability to be exploited, by knowing what program is, are in use, and by keeping the patches up to date, we have already discussed this.

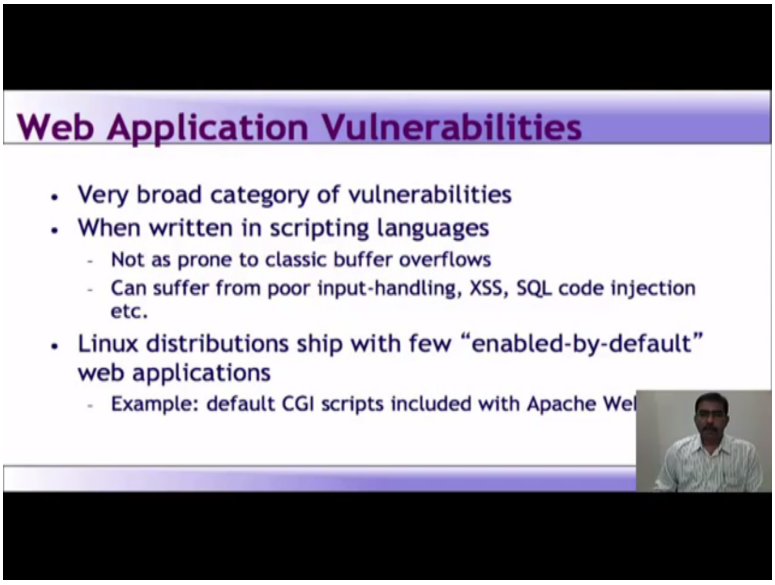
(Refer Time Slide: 18:01)




We will look at setuid root vulnerabilities, as we discussed earlier, when setuid permissions bit is set, the programs will run with the privileges of the user, that owns it rather than, those of the process or user, that is executing it. So, setuid root program is a root-owned program, runs as root, no matter who runs it, or who executes it. If setuid root program can be exploited or abused in any way.

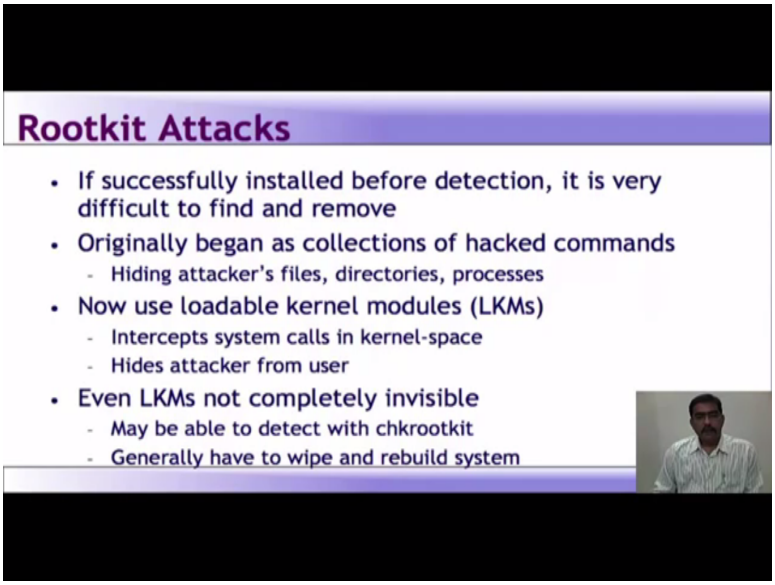
For example, if it can be exploited via a buffer overflow, or a race condition, then the unprivileged user can gain access to unauthorized privileged resources. So, running setuid is necessary for program, which needs to be run by unprivileged users. Yet, it must provide such users, with access to privilege functions, but after changing their password, which requires changes to the protected system file. So, such programs required must be programmed very carefully, due to the history of abuse, again setuid root programs major Linux distributions, no longer ship with the unnecessary setuid root, but system attackers can still scan for that.

(Refer Time Slide: 19:25)




Then is the web application vulnerabilities, it is a very broad category of vulnerabilities, as we know web applications are written in scripting languages, such as php, pearl, java. So, it may not be prone to classic buffer overflow, but it can suffer from poor input handling, including xss, sql code injection, and Linux distribution ship with few enabled by default web applications, like default cgi script, included with the apache web server.

(Refer Time Slide: 20:02)

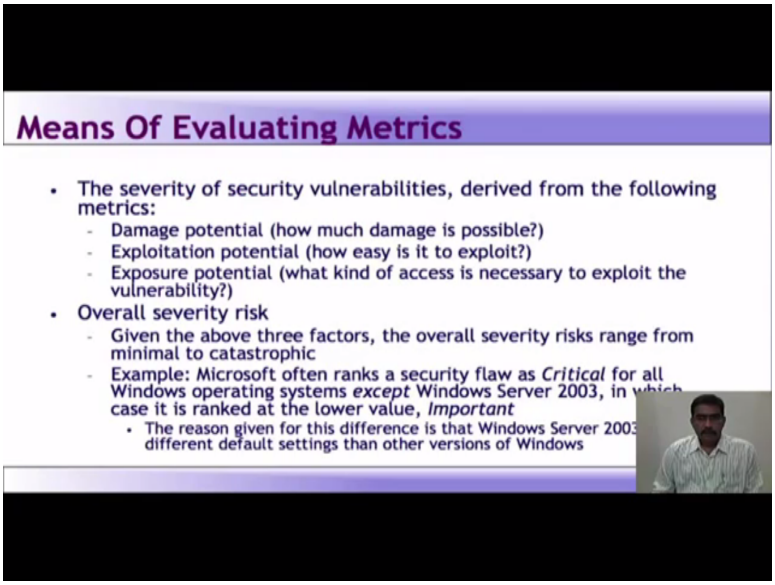



Then comes the rootkit attacks, this is a kind of attack which allows an attacker to cover his or her tracks typically after a root compromise. So, once you get root, then you try to erase your track from the system, so it allows the attacker to tower his or her track which occurs

after a root compromise. Now, rootkits began as a collection of hacked replacements, for some common missed commands, like ls that behaved like legitimate command.

That they have replaced except for hiding an attackers file directly are possible for example, if a attacker were able to compromise or replace a Linux system ls command, with a rootkit version of ls, then anyone executing the ls command to give files, and directory would see everything except that attackers files and directories. Now, since the advent of lkm's loadable kernel modules rootkits, have more frequently taken the form of lkm's, so an lkm rootkit covers the track of an attacker in a kernel space. And intercepts system calls pertaining to any users attempt, to view the intruders resources. Luckily, lkm rootkits are not completely invisible. Many traditional lkm rootkits are detectable with script chk rootkit. It is available at www.chk.rootkit.org. However, the attackers can get far enough if at all, they compromise the system then we will have to wipe, and rebuild the entire system.

(Refer Time Slide: 22:17)

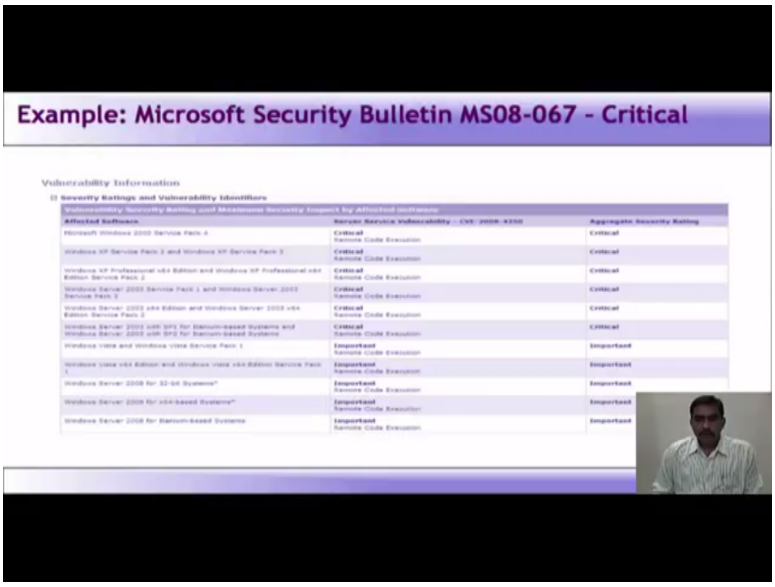



Now, what are the means of evaluating metrics between windows and Linux, the severity of security vulnerabilities, are derived from the following metrics. And what is the damage potential, how much damage is possible on the system, exploitation potential, how easy is it to exploit, exposure potential, what kind of access is necessary to exploit the vulnerability.

Then the overall severity, given the above 3 factor, that is damage potential, exploitation potential, and exposure potential, the overall risk rate from, minimal to catastrophic. Now, if you take an example, windows or Microsoft often runs a security flaw as critical, for all

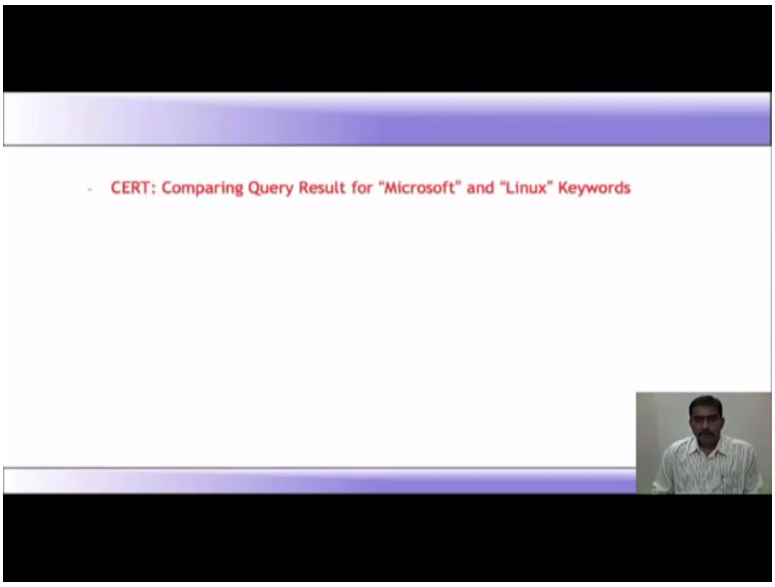
windows operating system except the server 2003 in which case, it is ran at a lower value which is important. The reason given for this difference is that, 2003 has a different default setting, than other versions of windows.

(Refer Time Slide: 23:21)



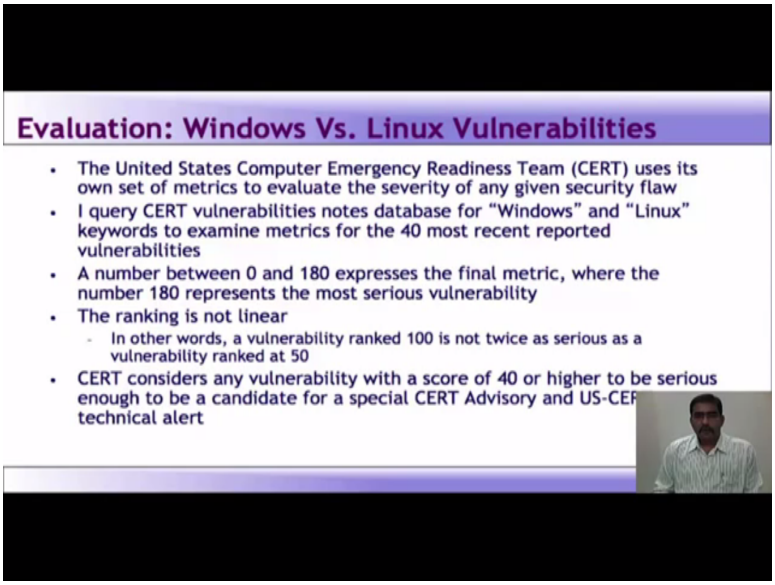

This is an example, of a Microsoft security bulletin, where the vulnerabilities are listed. You can see this critical remote code execution, critical remote code execution, important remote code execution, we have etc. The aggregate severity rate rating, critical important, so this security bulletin looks like this.

(Refer Time Slide: 23:45)



Now, computer emergency response team CERT, comparing query results for microsoft, and Linux keywords.

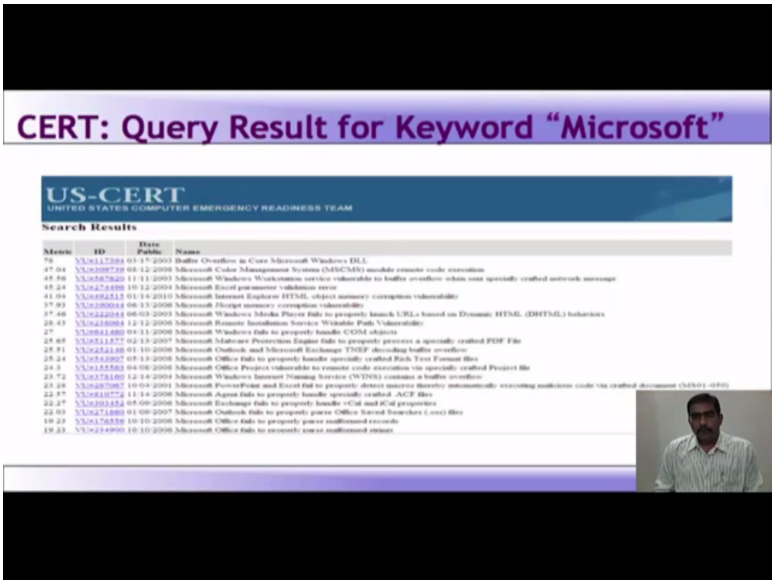
(Refer Time Slide: 23:53)




So, when you are evaluating windows versus Linux vulnerabilities, the us computer emergency readiness team uses its own matrix, to evaluate the severity of any given flaw. Now, I query cert vulnerability notes database for windows, and Linux keywords to examine metrics for the 40 most recent reported vulnerabilities, a number between 0 and 180 expresses the final metric, where the number 180 represents, the most serious vulnerability.

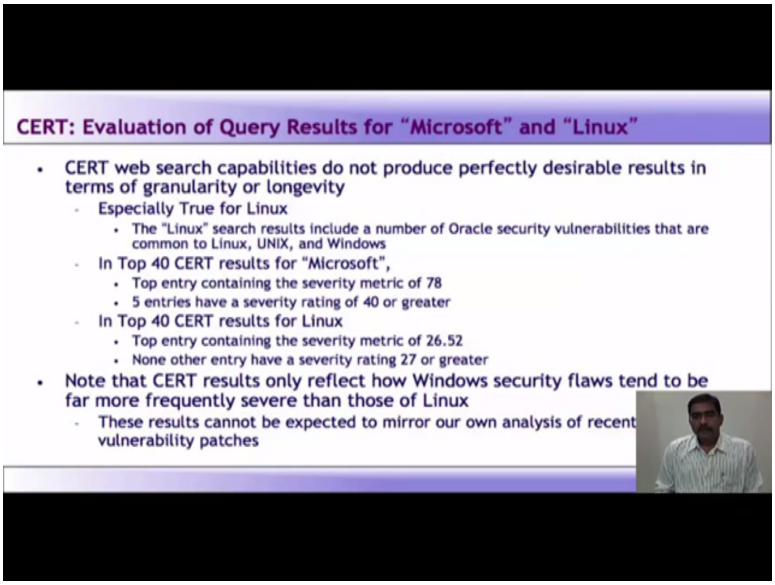
This ranking is not linear, in other words, a vulnerability ranked 100 is not twice as serious, as vulnerability ranked 50. So, you get the point there. CERT considers any vulnerability with a score of 40 or higher, to be serious to be candidate for special cert advisory, and us cert technical alert.

(Refer Time Slide: 24:50)




Now, when you do a query result for microsoft, it lists out all the potential vulnerabilities I have taken from the last, from the oldest to the new ones. So, I have taken a pretty old one, for the presentation here. Similarly, when I do it for Linux, I get a similar thing.

(Refer Time Slide: 25:10)




Cert web search capabilities do not provide, or produce perfectly desirable results, in terms of granularity, or longevity. It is especially true for Linux, because a Linux cert result includes a number of oracle security vulnerabilities, that are common to Linux, unix and windows. So, in top 40 cert result for windows, the top entry containing the severity metric of 78, there were five entries, which had a severity rating of 40 or greater and in top 40 cert results for Linux, the top entry containing the severity metrics of 26.52.

No other entry has a severity rating of 27 or greater. So, you can see the difference. Note that the cert results only reflect how windows security flaws, tend to be far more frequently severe, than those Linux. These results cannot be expected to mirror our own analysis of frequent or recent, vulnerability patches.