Introduction to Information Security

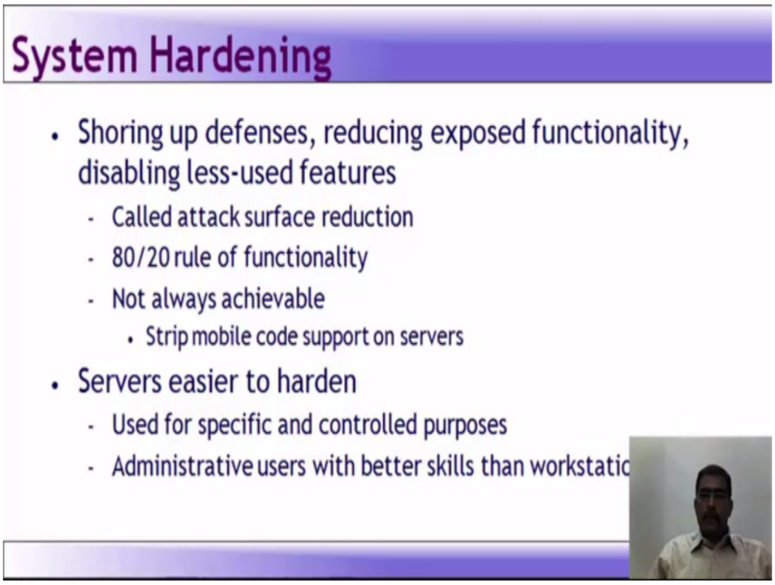
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture- 54

(Refer Slide Time: 00:10)

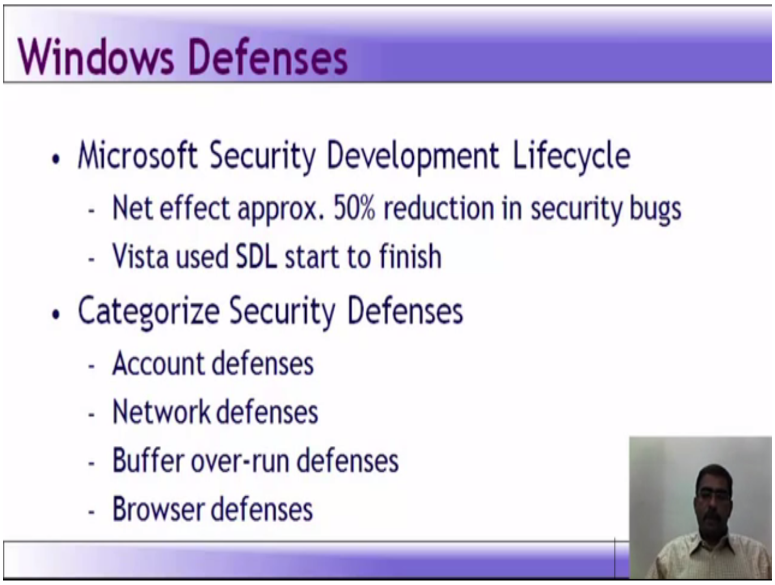


System Hardening

- Shoring up defenses, reducing exposed functionality, disabling less-used features
  - Called attack surface reduction
  - 80/20 rule of functionality
  - Not always achievable
    - Strip mobile code support on servers
- Servers easier to harden
  - Used for specific and controlled purposes
  - Administrative users with better skills than workstatic

System hardening, shoring up defenses, reducing exposed functionality, disabling less or lesser frequently used features. In Microsoft it is called attack surface reduction, then apply the 80/20 rule of functionality. What it means is reduce the amount of functionality exposed to untrusted users and disabling the fewerly used features. The concept is simple, 80/20 rule of functionality apply 80/20 rule to the features that you are going to enable, if the feature is not going to be used by eighty percent of the population, then the feature should be disabled by default. Now, this goal is not always achievable as disabling too many features will make the product really unusable for the users, or non-technical users.

(Refer Slide Time: 01:12)

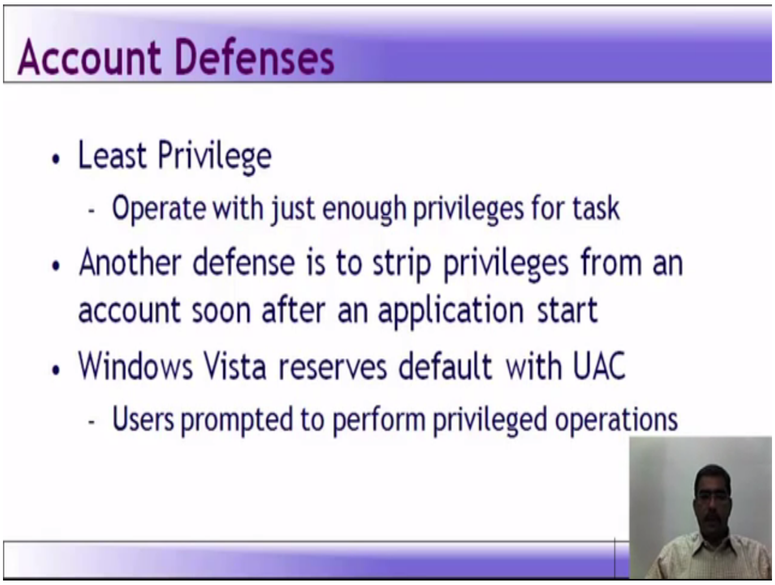


Windows Defenses

- Microsoft Security Development Lifecycle
  - Net effect approx. 50% reduction in security bugs
  - Vista used SDL start to finish
- Categorize Security Defenses
  - Account defenses
  - Network defenses
  - Buffer over-run defenses
  - Browser defenses

Then windows defenses after 2001 Microsoft decided to change the software development process to better accommodate secure design, secure coding, testing and maintenance, with one goal in mind. That is to reduce the number of vulnerabilities in Microsoft product, has it happened? It was a very debatable question, but Microsoft security development lifecycle, the effect of that is net effect approximately fifty percent reduction in security works. And vista onwards it uses or it use the security development lifecycle from start to finish, then categories of security defenses were done. That is categorization of security defenses like account defenses, so they addressed issues related with account, how to better protect an account. Network defenses, how to secure the server due to network vulnerabilities. Buffer over-run defenses, then browser defenses. So, you can see a lot of changes happened from internet explorer 06 to the latest version, where a lot of security features have been incorporated into IE. We will see what is account defenses.

(Refer Slide Time: 02:36)



Account Defenses

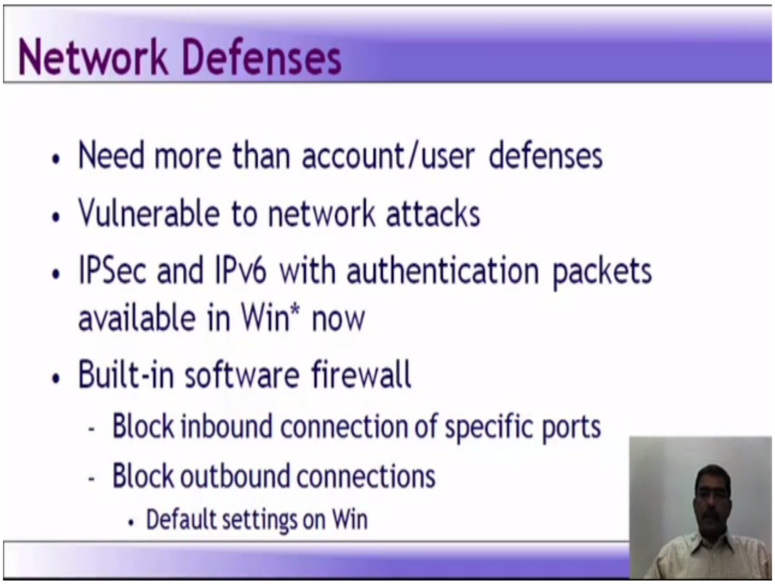
- Least Privilege
  - Operate with just enough privileges for task
- Another defense is to strip privileges from an account soon after an application start
- Windows Vista reserves default with UAC
  - Users prompted to perform privileged operations

It is a principle of least privilege, this principle of least privilege dictates that the users should operate with just enough privilege to get their task done, and nothing more. So, it is a privilege of need to know need to do or rather need to do they have privileges to just accomplish their task, nothing more.

Historically windows xp users operated by default as members of the local administrative group. So, in windows xp, the xp users often operated as the administrator under the local administrator group, this was actually done for application compatibility reasons. In some cases say if the application ran on windows 95 or 98 and could not run on xp, without administrative privileges, the user in xp running as standard user would create a problem. Another defense is to strip the privileges from the account, soon after an application starts.

So, just give the privileges what were required or what was required for starting the application then strip the privileges. Now, from vista onwards vista reserved the default with UAC user access control, users were prompted to perform privilege applications or operations. We have seen in some slides before that it prompts for a dialog you will have to give the administrator password to proceed, now that was started from windows vista onwards.

(Refer Slide Time: 04:21)



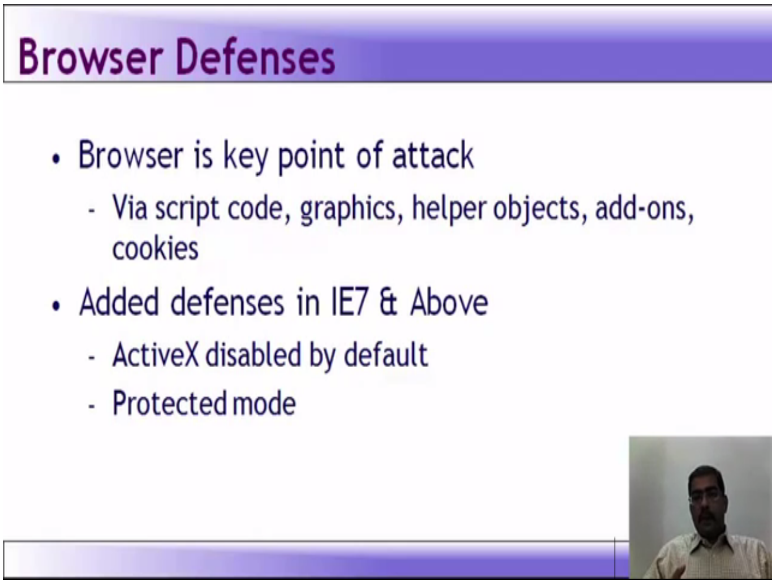
Network Defenses

- Need more than account/user defenses
- Vulnerable to network attacks
- IPSec and IPv6 with authentication packets available in Win* now
- Built-in software firewall
  - Block inbound connection of specific ports
  - Block outbound connections
    - Default settings on Win

Then we see network defenses, we need more than the account or you need to secure the network more than the account, more than the user because it is vulnerable to network attacks. Ipsec, ip security and ipv6 with authentication packets are available in windows now the latest versions. There is a built-in firewall available which blocks the inbound connection on specified ports. It blocks the outbound connections, there are default settings on windows also.

There is one big problem with defenses that focus on user and user accounts, they do nothing to protect the computers from low level network attack. So, we need to have network defenses. Now, starting with the sdlc or secure life cycle of Microsoft they have tried to incorporate all these features into their sdlc process.

(Refer Slide Time: 05:20)

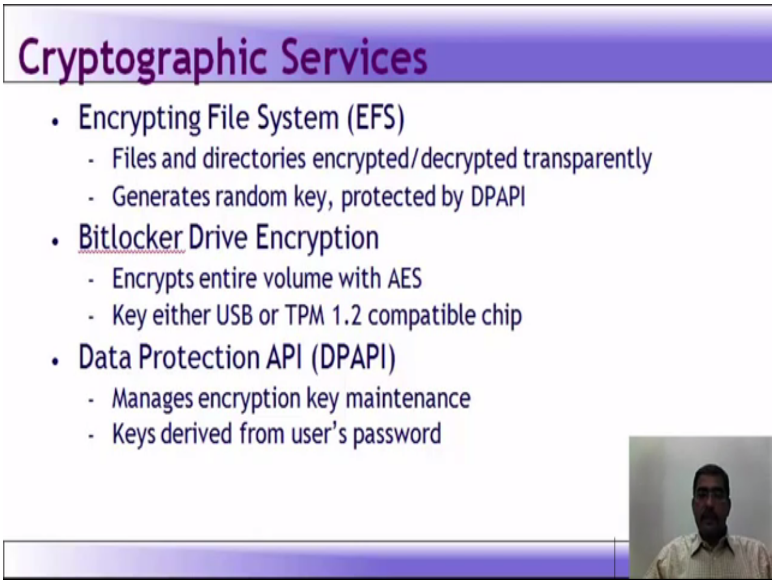


Browser Defenses

- Browser is key point of attack
  - Via script code, graphics, helper objects, add-ons, cookies
- Added defenses in IE7 & Above
  - ActiveX disabled by default
  - Protected mode

Browser defenses, browser is the key point of attack. Now, you can exploit the functionality, via script code, via graphics, via helper objects, via add-ons, cookie manipulation can be done. So, Microsoft added defenses in IE7 and above. You too will notice that in IE7 and above that activex was disabled by default, it runs in a protected mode.

(Refer Slide Time: 05:53)



Cryptographic Services

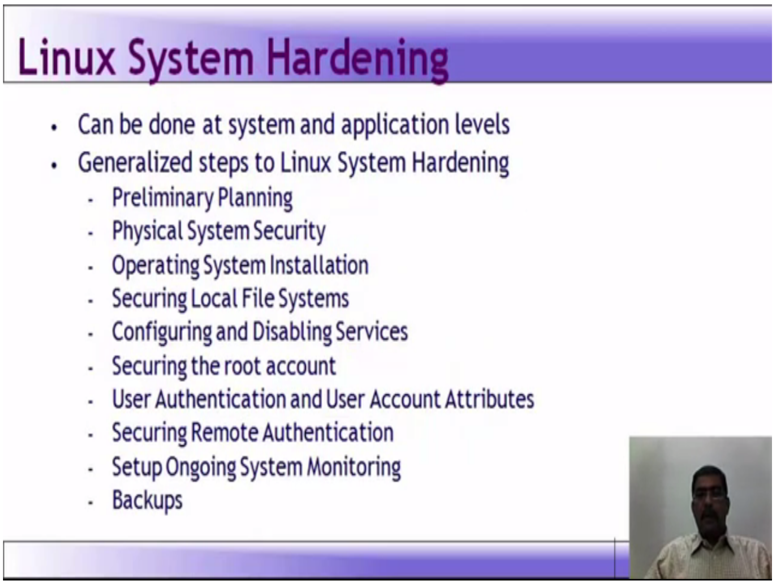
- Encrypting File System (EFS)
  - Files and directories encrypted/decrypted transparently
  - Generates random key, protected by DPAPI
- Bitlocker Drive Encryption
  - Encrypts entire volume with AES
  - Key either USB or TPM 1.2 compatible chip
- Data Protection API (DPAPI)
  - Manages encryption key maintenance
  - Keys derived from user's password

Then came the modification of cryptographic services, that is encrypting file systems. Files and directories encrypted and decrypted transparently, then generation of random key which is protected by DPAPI. Bit locker drive encryption which encrypts the entire volume with AES. Now, the encryption can be either through a USB or through a third party module 1.2

compatible chip. Then data protection API so DPAPI is data protection API, which manages the encryption key maintenance. These are derived from the users password.

This windows after vista includes full fledged cryptographic defenses, such as EFS which we have seen bit locker, data protection APIs, EFS allows files and directories to be encrypted and decrypted transparently for authorized users. At a very high level the EFS works by generating a random encryption key, and storing the key encrypted using the user's encryption key, this key is protected by the data protection API in windows. And the key used by DPAPI is derived from the user’s password. So, these are the changes in the cryptographic side which are incorporated into windows.

(Refer Slide Time: 07:25)



Linux System Hardening

- Can be done at system and application levels
- Generalized steps to Linux System Hardening
  - Preliminary Planning
  - Physical System Security
  - Operating System Installation
  - Securing Local File Systems
  - Configuring and Disabling Services
  - Securing the root account
  - User Authentication and User Account Attributes
  - Securing Remote Authentication
  - Setup Ongoing System Monitoring
  - Backups

Now, we will look at Linux hardening Linux system hardening, it can be done at the system level and the application level. There are generalized steps to linux system hardening, one is you will have to preliminary planning, you will have to plan on what you need to secure, what you need to allow. Then physical system security like we discussed a few slides back, in linux the concept is root takes it all.

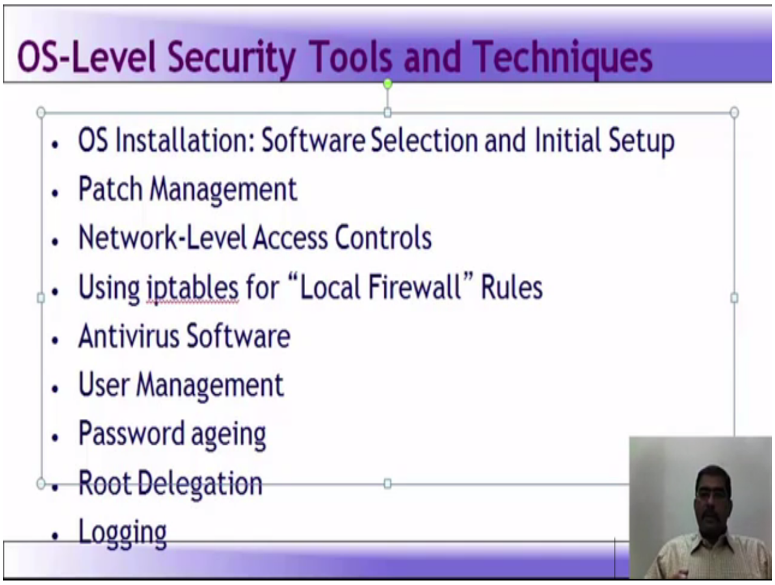
So, you need to a have a proper system security, then how the operating system installation is going to happen, what you need to enable, what you need not install. Then how the local file system will be secured, then how you will configure and disable different services, the services that are not required for users. How do you secure the root account.

So, generally if you see the latest versions of Linux come with root disabled by default, even at the time of installation. So, you need to specifically enable root, if you need root access. And also you can restrict the usage of root using the pseudoer file, then user authentication and user account attributes, how the authentication is taking place, if it is going to be a remote login to a ssh, then do I need a function, such as a token, or a otp to be generated may be install a google api for otp. Then how do you secure remote authentication, this is the same thing I said ssh, if you are going to enable for remote access, which user will get control over or can log in remotely. Root is anyway if you go to the etc/ssh files for the configuration files, the root will be disabled by default.

Then setup ongoing system monitoring, enable logs properly, monitor what is happening in the system. If possible install an SIEM tool security incident and event monitoring tool so that all your logs are correlated, it is analyzed, it is collected, it is stored. And then you can see what is happening do periodic vulnerability assessments on your server, to see whether the patches have been applied properly, whether any new vulnerability had has a potential to exploit the system.

Then of course, the most important thing is back-ups like we discussed in module 3, one who does not archive is condemned to rewrite. So, backups are a very important aspect in the confidentiality, integrity, availability triad. So, if this comes under availability, you need have a backup store it securely, if possible store it in a remote location, or you can have an online backup facility. So, Linux system hard means covers all these points

(Refer Slide Time: 10:40)



OS-Level Security Tools and Techniques

- OS Installation: Software Selection and Initial Setup
- Patch Management
- Network-Level Access Controls
- Using iptables for "Local Firewall" Rules
- Antivirus Software
- User Management
- Password ageing
- Root Delegation
- Logging

Now, in general OS level security tools and techniques, if we are going to see. Then we will have to look at OS installation, how it is going to be installed, what services are going to be allowed. Then how the initial setup is going to be done what kind of documentation is going to be done, then patch management, whether you are going to install only critical patches, which affects security or are you going to fix some bugs also; so patch management is very important.

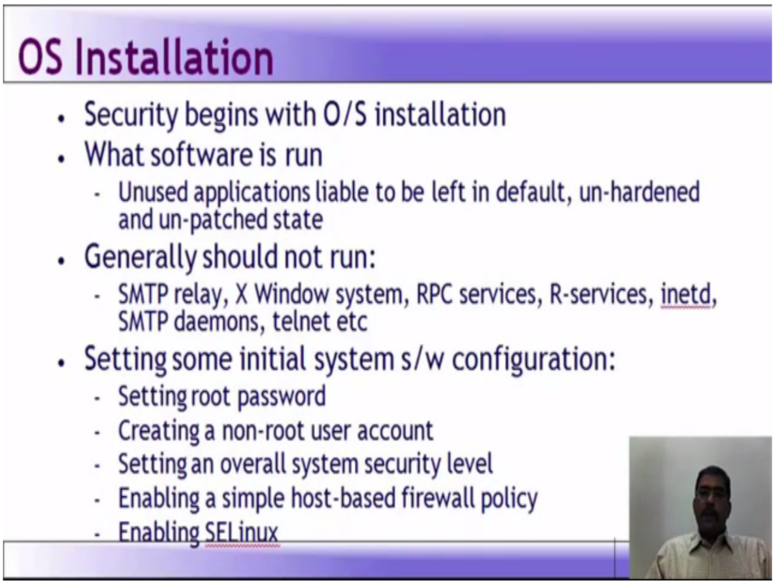
Network level access control, how we are going to give the access to the users is it through an active directory service, is it through a domain or a work group. Now, what kind of resources they can access on the server, whether you want to give the printer access to all the users. Then using ip tables for local firewall rule, this is in case of Linux, whether; ip tables is again inbuilt filter, or a firewall which comes along with Linux system. So, whether you want to configure the ip tables first or local firewall rule, that is to protect from the users within your network. You may have a corporate internet firewall which filters most of the things, but then you may still need to protect your server from being hacked from within your network.

Then in case of windows the antivirus management what kind of antivirus management system you are going to use, whether it is going to be central whether it can be managed from one location, whether the updates from all desktops can be done through the antivirus server. Then comes the user management, how users are going to be assigned what kind of privileges are you going to give them. Then you set password aging, how many days you want to keep the password before you force change, whether it is 30 days, 45 days or it is critical, where it is 15 days.

Then root delegation and root or admin delegation, who is going to get the root delegation, what is his or her background, whether here again the HR policies may come into play, whether a background verification has been done on the admin, whether he is capable of handling the issues. Then of course, the final aspect is login, in most of the systems including desktops in windows, the login is enabled by default. But the size of the logs that are stored on the system are very small because something like less than 512 kb. So, what happens is the systems keeps logging the events and then after once it reaches the threshold of 512 kb it rewrites the event.

So, then what the problem occurs is when you have to do a forensic on that particular system, you will not have the logs because it has been overwritten. So, you need to again design what is the login that you want whether you want to log all events, whether it is a success event, whether it is a failure event, whether errors have to be logged. Now, all these have to be decided before you actually enable login and allocate appropriate space in the system, for the logs to be stored. You can also forward the logs to a syslog server or a SIEM tool, so that your logs are consolidated in one place. And it can be analyzed by security admins so that you get a better understanding on your threat level, or your exposure level. So that you can design or strengthen further security measures.

(Refer Slide Time: 14:35)



OS Installation

- Security begins with O/S installation
- What software is run
  - Unused applications liable to be left in default, un-hardened and un-patched state
- Generally should not run:
  - SMTP relay, X Window system, RPC services, R-services, inetd, SMTP daemons, telnet etc
- Setting some initial system s/w configuration:
  - Setting root password
  - Creating a non-root user account
  - Setting an overall system security level
  - Enabling a simple host-based firewall policy
  - Enabling SELinux

Os installation, security begins with OS installation there is a saying and it is true also that security cannot be retrofitted, once you have setup the devices. So, once the users once the system admin once the network admins are used to a way of working, it is very difficult to restrict or impose security at a later stage. Now, you imagine a organization where p to p file sharing is allowed or they are downloading files freely, the movies, the pdfs the software for their home use everything is being downloaded, and nothing is restricted to the firewall.

Now, suddenly a security auditor comes and this is what is happening you may download virus along with the file, when you are enabling USB in the desktops. Then you there is a likelihood that a malware will be installed, there is also a likelihood or there is a definite impact on the performance of your bandwidth. Now, you are having 20 mbps of bandwidth, but once you restrict all this then you actually need only 10 mbps of bandwidth. So, the top management will say I am saving a lot of money, if I implement all this. So, let me implement all this, but now then you install the firewall configure the rules, you do not allow the download of unnecessary software which is not required for the business.

Suddenly everybody will feel a pinch I was or I am not able to download a file that I want. So, then comes the disgruntled attitude towards the organization, so security is not only designed to be implemented at the time of installation. But also you when you try to retrofit it, or when you try to apply security measures at a later time, it becomes really difficult for the organization because it becomes a people issue, it becomes a process issue, it becomes a technology issue. So, then it becomes very difficult for the users to adapt, so security begins with OS installation.

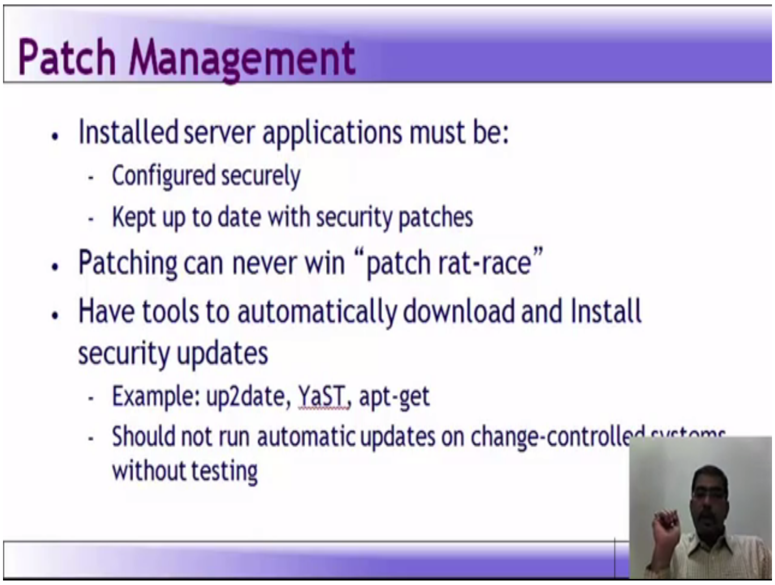
Now, they will have to decide what software is run unused applications are liable to be left in default, it is unhardened in a unpatched state, lets say that media player is there nobody uses in the office because there are no headphone jacks available, or visible out. And there is the updates are not done for the media player, then it could probably or possibly leave a vulnerability in the system.

Then in case of servers you should not run smtp relay, smtp is simple mail transfer protocol. So, relaying should not be allowed so if I am able to remotely log into the web server mail server, and then give a series of commands like ehlo the server name then mail from rcpt to subject data. And then I end it then I can actually impersonate somebody within the organization. So then xwindow system in case of linux so you should not run xwindow system on linux servers. The linux server is the safest when it is run on the text mode.

RPC services we have dealt with it earlier R services in linux, inetd services, smtp daemons Telnet is an absolute no no. Then some initial system software configuration setting the root password, or admin password it should be really strong if you need the root to be enabled. Then creating a non-user or a non-root user account, setting an overall system security level, enabling a simple host based firewall policy like your IP tables enabling SELinux we have spoken about SELinux also. So, linux security system begins at the operating system installation time itself.

Now, one of the most critical system impacting decision, or system admin or the installer has to make what software will run on the system. Suppose I am running a web server based on engine x, why do I need to enable other features like say apache or tomcat, or so it is a decision that the system admin has to make before doing the installation.

(Refer Slide Time: 19:09)



Patch Management

- Installed server applications must be:
  - Configured securely
  - Kept up to date with security patches
- Patching can never win "patch rat-race"
- Have tools to automatically download and Install security updates
  - Example: up2date, YaST, apt-get
  - Should not run automatic updates on change-controlled systems without testing

Then comes the patch management, now the server is installed. The installed server applications must be configured securely it should be kept up to date with the security patches. So, it is not only updating or securing your linux installation, suppose you have installed a web server, you have installed a mail server. So, those also have to be updated and configured securely. If you have mysql you should not keep a simple password just because it is a system in progress.

So, all the ancillary software or the application software that are required to be run should be configured, and kept up to date with security patches. Patching can never win a patch rat-race. Now, there will always be software vulnerabilities that the attackers are able to exploit for some period, before the vendor issues patches for it. It is not like a vulnerability is found today, and the patch is released tomorrow. So, a patch rat-race who wins the race whether it is the exploiter or it is the guy who is developing the software.

So, you need to have a control over, what you are configuring, how you are configuring and whether you are up to date with the patches. Then you should have tools to automatically download and install security updates, example upto date yast apt-gate. Now, apt-gate is a command in Ubuntu or Linux-based systems could not run automatic updates on change control systems, without testing.

Now, all the modern Linux based systems includes tools for automatically downloading and installing security updates. You can actually write a small script that pseudo apt-gate update over a period of time, or you can enable or crone job, or you can install a software like webmin, which can tell you the status of the patches and it will do the update for you automatically.

So, there are several new additions even in linux again webmin is ui based, so it becomes very easy for non-gui users to actually to work on webmin. Whereas, there are several software like webmin available also, webmin is something that I have used personally. So, I am relating this particular instance to webmin and you can even manage your sql configuration, php configuration all those things. So, you need some kind of tools to do this for you so that your job becomes easier, when you are doing the administration of a.