


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

Lecture – 55

(Refer Slide Time: 00:10)

Network Access Controls

- Network a key attack vector to secure
- Libwrappers & TCP wrappers a key tool to check access
 - Before allowing connection to service, tcpd first evaluate access control
 - Defined in /etc/hosts.allow
 - Defined in /etc/hosts.deny



Then comes your network access control. Network is a key attack vector to security. So, you can say in a Linux system it is one of the most important attack vectors in the network. Now, network access control that is the controls that restrict the access to the local resources based on IP address of the network system, attempting to access them, are there for the import tool in Linux security. Now, Libwrappers and TCP wrappers are also key tool to check access.

You can go to the net and find out what is a wrapper. If you need more definition. So, before allowing connection to the service TCPD first evaluates the access control. It is defined in this particular file/etc/hosts.allow or in a/etc/hosts.deny. Now, when this comes I will relate a particular example for you. In network access control we were in a audit of a corporate environment with more than three thousand users.

Now, once we have gone for the audit we were made to wait for a couple of hours because the people in the IT department did not want to have someone come and pinpoint that they were wrong. So, audit is always a hated job because nobody in the organization would like to be audited. You yourself me myself would not like to be audited because we do not like

somebody coming and telling us that we are wrong. So, similarly, in this organization we went. So, we were made to wait for two hours.

Now, I got impatient. So, the place where we were sitting that was the work table where the person who had working there was absent for a long time. There were desktops everywhere and this particular desktop was also there on this table. Now, the reason that they gave us is it will take us a long time to configure because we have to give your laptop an access to actually get connected to our network.

We do mac based filtering. So, then what happened is we tried to connect the laptop it could not connect to the network, the DHCP was nor assigning an IP address. So, the system in place was a dell, dell has a habit of putting even the affix in the mac id on the desktop. So, the process became very simple. So, all you have to do is copy that mac id replace the mac id in my laptop and plug in the network. Immediately we got access we were able to get the IP scheme what the DHCP server address is what is the gateway address.

We started working on that system. Now, after another hour the guys from IT came and said your access is ready. So, then for that we told him that we already got an access an hour back, we took it. Now, this is what happens when we talk about network access control you need to really secure your system. So, that these kind of incidents also do not happen. Now, the advantage for the company or the positive thing that happened for the company is, since we were security auditors ourselves.

The objective was not to exploit the system or to bring down their services. The objective was to show them that this could be possible. And to show them that we can take access irrespective of whether you are going to give it or not. So, we continued with our job. So, this is very important when you design networks that not only your user access on the local systems or on the servers, but the network access controls also have to be implemented thoroughly. It has to be analyzed it has to be tested and then it has to be implemented.

(Refer Slide Time: 04:27)

Using iptables for “Local Firewall” Rules

- Also have the very powerful **netfilter** Linux kernel native firewall mechanism and **iptables** user-space front end
- Useful on firewalls, servers, desktop
- Typically for “personal” firewall use will:
 - Allow incoming requests to specified services
 - Block all other inbound service requests
 - Allow all outbound (locally-originating) requests
- Do have automated rule generators
- If need greater security, manually configuration required




Then using IP table for local firewall rules. This is again in case of Linux, Linux kernels native firewall mechanism is net filter, and IP table. Now, you can configure IP filter or IP tables or net filter on the server. You can configure it on the desktop also. Now, generally what it does is for a personal firewall use it will allow the incoming respect or request to the specified services. It will block all other inbound service request it will allow all outbound or locally originating request.

Now, there are automatic rule generators also because it becomes difficult to configure each and every item. If you need greater security, if it is a very high security area then you need to manually configure the services, the ports that you need to allow or deny.

(Refer Slide Time: 05:40)

Antivirus Software

- Historically Linux not as vulnerable to viruses
- Windows targeted more due to popularity
- Prompt patching of security holes more effective for worms
- Viruses abuse users privileges
- Non-privileged user account
 - Less scope of being exploited
- Growing Linux popularity means growing exploits
- Hence antivirus software will be more important
 - Various commercial and free Linux A/V



Then comes the antivirus software. Now, historically Linux was or is not as vulnerable to virus as their windows counterpart. Windows was targeted more due to the popularity due to the market share because so many users of windows are there. And then from patching of security holes has more effective for worms, virus abuses user privileges we have seen all this in domain 3. Then you should use only non-privileged user account. So, then the chances of being exploited are remote.

Now, as the popularity of Linux also grows, means the exploits will also grow. So, you need an antivirus software that will be required for your Linux. Traditionally anybody running on a Unix system, Linux system including myself we used to install clam antivirus on the server just to be able to be on the safe side. And also to satisfy the requirement of the auditors who come to the organization, that do you have have an antivirus software installed, we tell them no we are using Linux. So, there is not much threat in Linux for having an antivirus software. So, then they put a non-compliance. So, then to satisfy the auditor's requirement to satisfy the regulatory requirement and also nowadays since Linux is growing in popularity to secure the system lot of antivirus software both freeware and commercial are available for Linux.

(Refer Slide Time: 07:24)

User Management

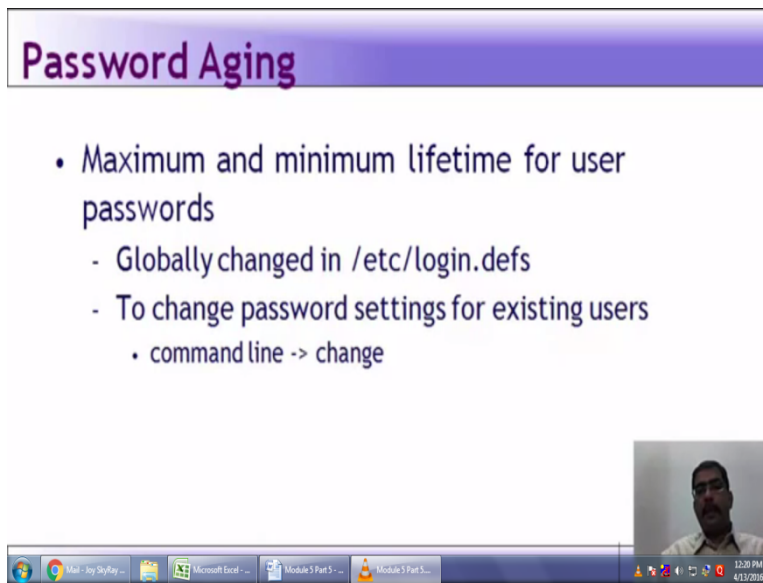
- Guiding principles in user-account security:
 - Be careful setting file / directory permissions
 - Use groups to differentiate between roles
 - Use extreme care in granting / using root privileges



When it comes to user management we will have to follow certain principles, certain practices guiding principles in user account security is be careful when you are setting the file and directory permission. Use groups to differentiate between roles. Use extreme care in granting or using root privileges. Now, we have seen in the previous slides that how a file permission can be given whether it is read access write access execute access for the owner, for the group, for others so we have seen all that.

So, you need to be clear on what permissions you will give to what user under what group. So, and most important thing again the root takes it all principle you will have to keep in mind and say use extreme care in granting or using the root privileges

(Refer Slide Time: 08:21)



Password Aging

- Maximum and minimum lifetime for user passwords
 - Globally changed in /etc/login.defs
 - To change password settings for existing users
 - command line -> change

The password aging we need to set maximum and minimum lifetime for user passwords. Like we discussed a little while earlier whether it is going to be 15 days force change, 30 days, 45 days or 60 days. Generally the practice followed for admin accounts is every 15 days. If it is a bank for the user account it is every 30 to 45 days. If it is normal user account in a corporate it may be 60 days depending on the criticality of the information.

In Linux it is globally changed in /etc/login.defs. To change the password setting for existing users in command line you can put the change. Now, if you really need to learn more about Linux. That is people who are not aware of the Linux operating system, what I would suggest is the most easiest Linux to learn is Ubuntu. So, download a copy of Ubuntu have a VM setup on your system. Install your Ubuntu server or Ubuntu desktop play around with it.

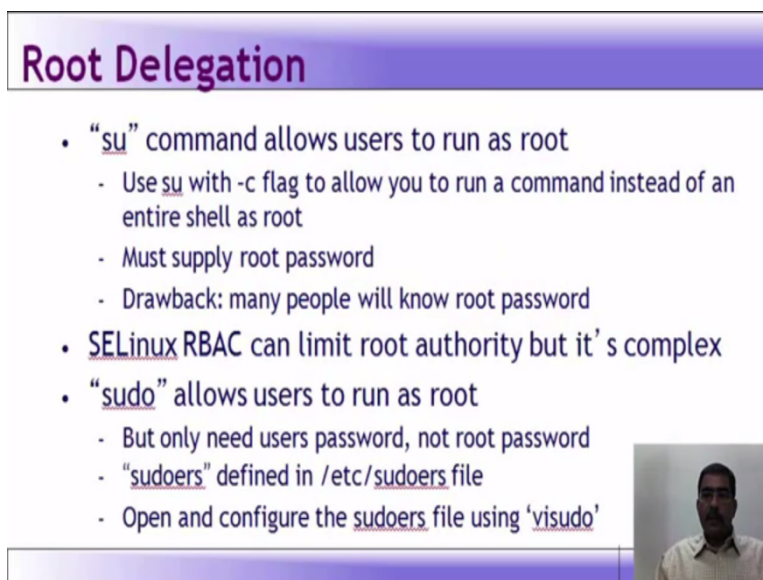
I would recommend a text based version because you will come to know about the command that are used in Unix, which is very important to work with Unix. You need to remember a lot of commands. So, you try it out. So, that you will come to know what the security features are available in Linux. And how you can setup when you install how you can setup the security features. And there are abundant tutorials available on the net for Ubuntu.

The user community has put in a of documentation on different aspects how to install different files, how to delete, how to uninstall, how to install the antivirus, webmin. So, many resources are available on the net. So, I would suggest if you have not worked with Linux or if you are novice user of Linux you have to get started with installing a VM and practicing

because in information security you will definitely encounter a lot and lot of systems which work on different flavors of UNIX or Linux.


So, you need to atleast know how you go and use the logs on a server. How you will go and check whether the root is enabled. So, the fundamental things of Unix you will have to learn to be successful in the information security field especially on text based servers.

(Refer Slide Time: 11:06)



Root Delegation

- “su” command allows users to run as root
 - Use su with -c flag to allow you to run a command instead of an entire shell as root
 - Must supply root password
 - Drawback: many people will know root password
- SELinux RBAC can limit root authority but it's complex
- “sudo” allows users to run as root
 - But only need users password, not root password
 - “sudoers” defined in /etc/sudoers file
 - Open and configure the sudoers file using 'visudo'




Now, root delegation is another aspect, su command it allows the users to run as root. So, if you use su the minus c flag it allows you run a command instead of an entire shell as root. So, you must provide a root password for you to do that for a su. The drawback is many people will know the root password if you are going to allow this. Now, se Linux rbac rule based access control can limit the root authority, but it is very complex. Now, there is another command called sudo which allows users to run as root, but you need only the users password and not the root password sudoers are defined in the etc sudoers file.

You can open and configure the sudoers file using vlsudo, but again when you are editing the sudoers file you will have to be really careful on whom you are giving the permission and what level of permission you are giving. So, that the system is not compromised.

(Refer Slide Time: 12:14)

Logging

- Linux logs using syslogd or Syslog-NG
 - Writes log messages to local/remote log files
- Syslog-NG preferable because it has:
 - Variety of log-data sources / destinations
 - Much more flexible “rules engine” to configure
 - Can log via TCP which can be encrypted
- Change default logging settings on both
- Log files careful management
 - Balance number and size of log files
 - Rotate log files and delete old copies - logrotate



Now, we will in login Linux logs in using syslogd or syslog-ng. It writes the log messages to a local or remote log files. Like we discussed again a SIEM tool is basically a log management tool with additional capabilities of analyzing the logs correlating the logs and giving a report. Nice fancy report based on bcids’s based on ORs or based on other regulatory standards. Now, you need to have a SIEM tool because it simplifies the aspect.

The syslog work on port 514. So, does the SIEM tool. So, the syslog-ng is preferable because it has a variety of log data sources or destinations. It is much more flexible rules engine to configure. So, you need to suppose you have a syslog server installed. You need to send the data or the logs from your routers your firewalls your manage switches the servers and some of the critical desktops.

So, you need to have a wide variety or flexibility for the rule engine to be configured. The syslog-ng is preferred for that because it is flexible. Then you will have to change default login settings on both the server and the syslogng. Then log files management. So, you will have to balance the number and size of log files again like we discussed earlier. What needs to be logged is more important whether you need to log only the success entries, only the failure entries, success and failures, system errors application errors network errors. So, you need to actually balance the number and size of the logins.

In a typical organization like a bank which say around 400 to 500 branches spread throughout India. Assume that they are enabling logs of oracle or MS sql or the operating system logs,

your router logs, firewall logs, switches logs. So, the average consumption per day in terms of log requirement will itself be more than 5 to 6 GB. I have myself seen that a few years back, may be three or four years back, when you enable even the minimalistic configuration to be logged, it used to actually take around 3 to 4 gb of space. So, you need a large data bank or storage space to store the log. So, there are lot of issues in that. So, you need to be careful on you will have to balance the number and size of the log files. Then you will have to rotate log files and delete the old copies, which is the log rotate. Logging itself is not a proactive control because log only tells you about the things that have already happened. It is an aftermath or it tells you what has already occurred. So, that you can already prevent it from recurring again, but effective log helps to ensure that the event in the event of a system failure system administrators can more quickly and accurately identify the cause and therefore, accordingly focus on recovery and remediation effort. So, that is why you need login one is to find out whether any unusual activity is happening. Secondly, in the event of a system failure you can actually read the logs and decide what exactly went wrong and why the system went down. So, login is a very crucial aspect.

(Refer Slide Time: 16:10)

Application Security (Hardening)

- A large topic
- Many security features are implemented in
- Similar ways across different applications
- Sub-topics
 - Running as unprivileged user/group
 - Running in chroot jail
 - Modularity
 - Encryption
 - Logging



Application security or hardening when we talk about it, it is a very large topic. Many security features are implemented in similar ways across different platforms. Now, the sub-topics under hardening will be running as a unprivileged user or group, running in chroot jail then the modularity of features, encryption, the login.

(Refer Slide Time: 16:42)

Running As Unprivileged User/Group

- Every process “runs as” some user
- Extremely important user is not root
 - Since any bug can compromise entire system
- May need root privileges, e.g. bind port
 - Have root parent perform privileged function
 - But main service from unprivileged child
- User/group used should be dedicated
 - Easier to identify source of log messages



So, running as an unprivileged user, every process runs as some user whether it is a system process, whether it is a user process it runs as some user under some account. The extremely important user is not root always. Since any work can compromise the entire system. So, if it is running under root you can be rest assured that one bug or one compromise will bring down the entire system. The system may need root privileges for example, to bind a port, then can have root parent performed privileged function, but main service from unprivileged child.

Say you are installing a particular software. You install it as root, but assign the process or the task of running it to another user, who is not root. The user and group used should be dedicated, that is for certain process and applications. It is easier to identify the source of log messages. So, that is why you need to run it as a separate user or group. So, that you will say that from this particular user on this particular group this particular event has happened. So, it is very easy to identify from logs.

(Refer Slide Time: 18:05)

Running in “chroot” Jail

- “chroot” confines a process to a subset of /
 - Maps a virtual “/” to some other directory
 - Directories outside the chroot jail aren't visible or reachable at all
 - Contains effects of compromised daemon
- Complex to configure and troubleshoot



Running in chroot-jail, chroot confines a process to a subset of root. So, it maps a virtual root to some other directory directories outside the chroot jail are not visible or reachable at all. It contains effects of compromised daemon it is complex to configure and troubleshoot. Now, for example, if a FTP daemon serves files from a particular directory let us say/IP some IP x.x.x.x/FTP/public. There should not be any reason for that daemon to have access to rest of the file systems. So, it should be confined to that particular path.

(Refer Slide Time: 18:51)

Modularity

- Applications running as a single, large, multipurpose process can be:
 - More difficult to run as an unprivileged user
 - Harder to locate / fix security bugs in source
 - Harder to disable unnecessary functionality
- Hence modularity a highly prized feature
 - Providing a much smaller attack surface
- cf. postfix vs sendmail, Apache modules



The modularity when we see application running as a single large multi-purpose process can be more difficult to run as an unprivileged user. It is harder to locate or fix security bugs in the source. It is harder to disable the unnecessary functionality. So, the modularity is a high priced feature, providing a much smaller attack surface. Now, if you take for example postfix versus send mail or the apache modules you will understand about modularity.

(Refer Slide Time: 19:29)

Encryption

- Sending logins & passwords or application data over networks in clear text exposes them to various network eavesdropping attacks
- Hence many network applications now support encryption to protect such data
 - SSL and TLS protocols in OpenSSL library used
- May need own X.509 certificates to use
 - Can generate/sign using openssl command
 - May use commercial/own/free CA

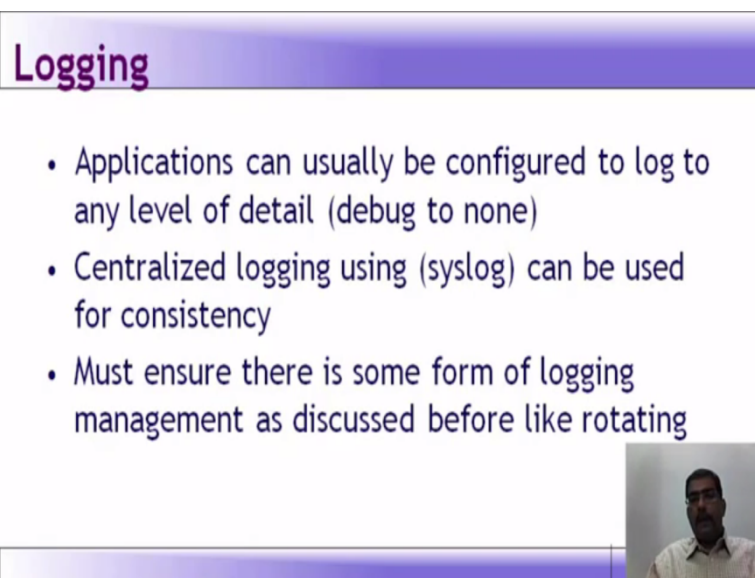


Encryption, sending the logins and passwords or application data over the network in clear text exposes them to various network eavesdropping attack. So, that means clear text in the

sense, it is not encrypted it goes in plain text. Using eavesdropping attack suppose we use a wireshark for sniffing the traffic or some other tool. So, many network applications now support the use of SSL and TLS protocols in the open SSL library used.


Open SSL itself is prone to a vulnerability which can be fixed. I think most of you will know what the vulnerability is I will ask an assignment question on open SSL vulnerability. You may need to own x.509 certificate to use it can generate our sign using the open SSL command. It may be a commercial or it can be your own or it can be a free certification or from a certificate authority.

(Refer Slide Time: 20:33)



Logging

- Applications can usually be configured to log to any level of detail (debug to none)
- Centralized logging using (syslog) can be used for consistency
- Must ensure there is some form of logging management as discussed before like rotating



Again, we come back to a bit of logs. Applications can be configured to log at any level or detail. debug is to none. None is no login, centralized login using syslog can be used for consistency. Now, why I have put syslog is even it is for a small network you can use syslog. If it is for a large network and you need support in managing or fine tuning it you need to go for an SIEM tool. And you must ensure there is some form of login management as discussed.

Like rotating you should have you should have proper policies. You need to know what devices you are going to configure. So, the SIEM basically does again the task of collection. It collects all the logs correlation arranges in order off the device and in a time stamp fashion. Analyzes; it analyzes the log or it presents the logs in a more readable fashion. And then it

reports it based on industry requirement or regulatory requirement it will give you a nice good looking report with lot of graphs lot of pie charts.