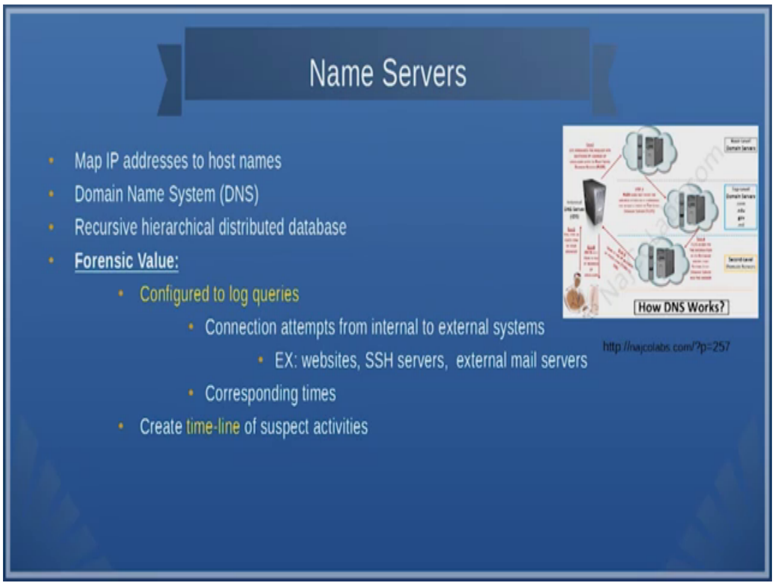
Information security - IV

Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 36
Technical Fundaments for Evidence Acquisition – 2

Hi there, welcome to this module on network forensics. We are continuing with where we left off in the last session. In the last session we were looking at DHCP servers and forensic value that we obtain from the DHCP servers.

(Refer Slide Time: 00:37)



Name Servers

- Map IP addresses to host names
- Domain Name System (DNS)
- Recursive hierarchical distributed database
- **Forensic Value:**
  - Configured to log queries
    - Connection attempts from internal to external systems
      - EX: websites, SSH servers, external mail servers
    - Corresponding times
  - Create time-line of suspect activities

http://najcolabs.com/?p=257

We move on to the next part where we looked at name servers ok. Name servers usually called as domain name servers, domain name systems ok. They convert the IP address to hostname and vice versa hostnames to IP address ok. So, the idea with domain name system is that instead of having numerics as IP address we would like to have names which represents something. For example, instead of having 192 dot 168 dot 0 dot 5 we can say that this is some xxx dot com, where xxx could be some company name. For example, we have nptel dot ac dot in, which is the domain name of NPTEL.

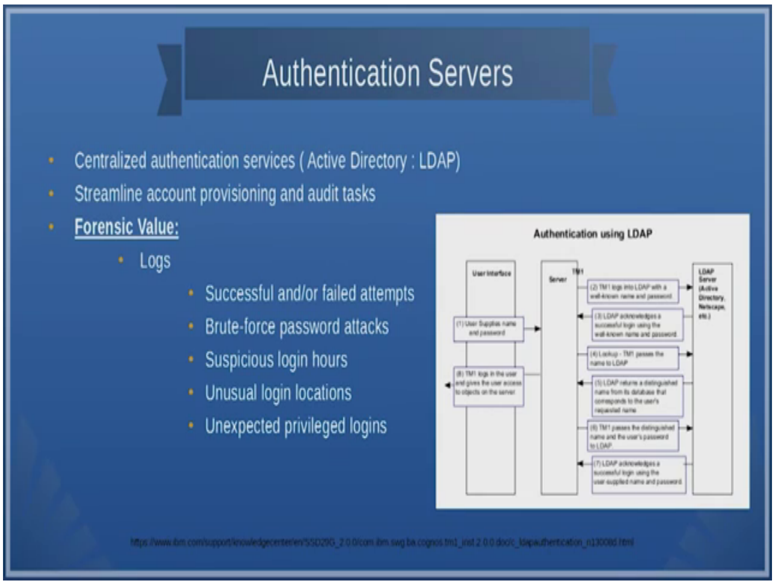
Now, the name servers are actually hierarchical in nature and as shown in the figure on the right hand side we can see how the names of work. Suppose I just want to find out the IP address of some domain name. What happens is that it sends it to the next level of domain in server it tries to find identify a the domain name with the in the current cash either in the switch or the router that you have usually it would be the routers. If the router does not act like a domain in server then it goes to the next higher level domain name server and if that does not address then it goes to the higher next higher level domain name server and the answer percolates all the way back down.

What is the forensic value of this domain name service? The first thing that you can look at is whether the domain name servers are configured to lock the queries. That means, if a mission attaches itself to a network and I want to go to a particular domain I will type that let us say http slash slash www dot some domain dot com or dot g o dot i n whatever.

Now, at this point of time the request goes to the gateway. And gateway if it is a domain name server is just response if it has the answer average sends to the higher level. Now, any request such request can be logged and so a connection atoms that are made from the internal to the external systems. For example, websites or ssh servers, say crucial servers or external mail servers etcetera can be got from the loggs that are provided by the name servers ok. And this helps in actually creating a timeline of the suspect activity. Suppose I go to website which I am not supposed to go then if I type the website name then what happens is that it the logger of logs at what time I try to access that website. So, this gives a clue on what time we try to atom something.

So, the next is the authentication servers ok. Usually if you have a centralized authentication services for example, authentication server where you can log in and then the login credentials are validated etcetera ok. Usually many of the organizations have active directory or some elda based servers. Now, these servers actually authenticate the user whether they want to login to a machine or a or a or network etcetera.

(Refer Slide Time: 03:54)



Authentication Servers

- Centralized authentication services (Active Directory : LDAP)
- Streamline account provisioning and audit tasks
- **Forensic Value:**
  - Logs
    - Successful and/or failed attempts
    - Brute-force password attacks
    - Suspicious login hours
    - Unusual login locations
    - Unexpected privileged logins

Authentication using LDAP

User Interface

Server

TM1

LDAP Server (Active Directory, Netscape, etc.)

(1) User Supplies name and password

(2) TM1 logs into LDAP with a well-known name and password

(3) LDAP acknowledges a successful login using the well-known name and password

(4) Lookup - TM1 passes the name to LDAP

(5) LDAP returns a distinguished name from its database that corresponds to the user's requested name

(6) TM1 passes the distinguished name and the user's password to LDAP

(7) LDAP acknowledges a successful login using the user-supplied name and password

(8) TM1 logs in the user and gives the user access to objects on the server

https://www.ibm.com/support/knowledgecenter/en/SSD29G_2.0.0/com.ibm.swg.ba.cognos.tm1_inst.2.0.0.doc/c_ldapauthentication_n13006d.html

So, the advantage of these kind of this along with say I mean you have some radius (Refer Time: 04:06) those kind of servers. Along with this what you can do is you can log the authentication details.

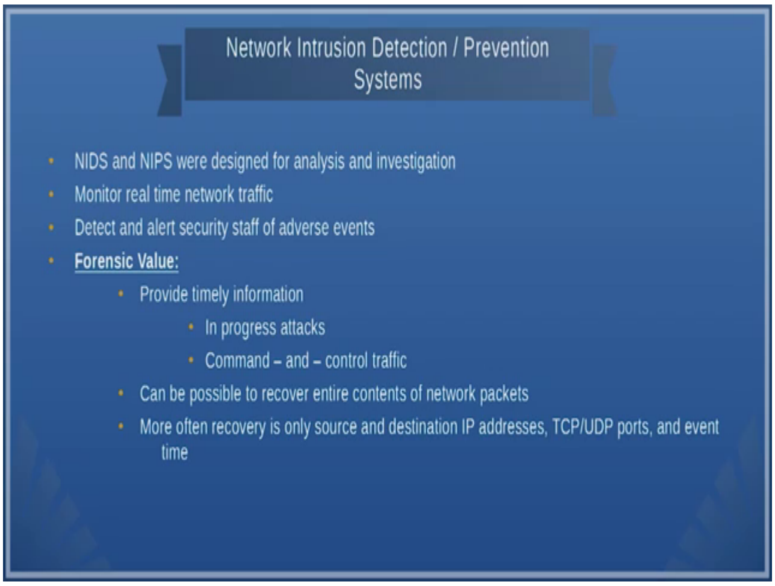
For example, if I want to login to my organization network then I have a username and password. So, that is username and password get validated. I mean if I have thousands of machines I cannot have a local database where in the local machine I cannot store my validation credential. So, I just have to store it in a common directory services, this is exactly what the directory services provided. They also provide authentication authorization and sometimes I mean an accounting also. So, all the 3 logs can be very very useful. For example, if you unsuccessfully try to authenticate it will be actually logged in the authentication service and if you try to use a brute force password attack it will be try it logged in the authentication servers.

As a practical example if you actually connect to the internet website of some bank let say you actually try to put your username and then try to give a password. Now, if you give a wrong password if you if you see in many of the banks they do not let you more than 2 or 3 atoms I think three atoms is standard that they allow. Now, after you fail in the 3 atoms actually your account my get locked know all these things are done with help of a authentication server. So, you on the right hand side you can just see how an authentication server works this very high level. So, the authentication servers the logs that is given by the authentication servers actually can give you lot of information.

For example, if you are working out of office hours and you your logging in from locations which are not authorized for example, I mean you say I am on vacation, but I try to login from some other location ok. All these things can be logged and this will help in forensics.

Sometimes you are not allowed have some kind of a privilege login. Say for example, kind of root you are not supposed to login as root into any of the machines, but (Refer Time: 06:18) has logged in as root into any of the machines. So, this will also be logged by the authentication server and sometimes I mean these are logged by local servers also that someone has tried to get root access etcetera. In this way the authentication servers have provide a huge amount of forensic value with their log fix.

(Refer Slide Time: 06:44)



Network Intrusion Detection / Prevention Systems

- NIDS and NIPS were designed for analysis and investigation
- Monitor real time network traffic
- Detect and alert security staff of adverse events
- **Forensic Value:**
    - Provide timely information
        - In progress attacks
        - Command – and – control traffic
    - Can be possible to recover entire contents of network packets
    - More often recovery is only source and destination IP addresses, TCP/UDP ports, and event time

The next device that we are going to look at is the network intrusion detection and prevention systems. So, now, this is actually a security device ok. So, this was this device was done exactly for the purpose of network forensics and these devices have very high processing capability also. So, this devices actually monitor real time traffic and if you find any suspicious traffic or flow ok, they actually raise an alarm and they can be configured I mean all these things ok, let us be clear. It is the work of the system administrator to configure these devices correctly many of the security lapses happened because the devices are not configured properly or they provide some kind of a loophole because almost all the organizations which with supply the security devices also include as and when any of the attacks happen.

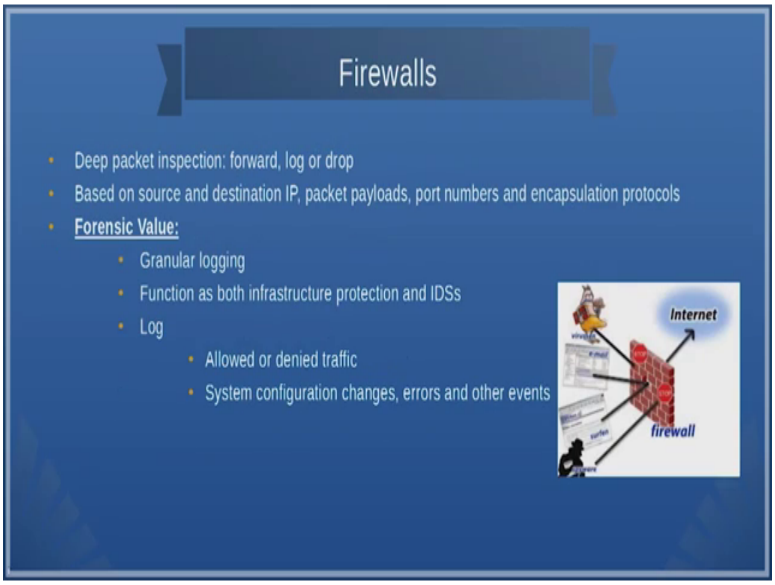
Now, in many of the cases that has happened people the real problem with security was not the that the patch or the fix was not available, it was actually that people did not upgrade those fixes. So, similarly here you can have any type of improve systems you can all technologies that is available, but if you in the human user finally fails to apply those technology then they security loopholes occur ok.

And especially this network intrusion detection prevention systems actually what they were mostly based on some kind of pattern analysis and then packet filtering etcetera. Usually what they do if you can actually configure these machines using command line, we will be looking at some of these commands later, but as this sessions the coming up sessions tells you I mean how we in general do the forensics I mean or how we in general collect the data ok.

And look at this we are now, looking the most into software mostly into software, but will also fine later see that there are some software tools, I mean sorry we are looking mostly into hardware and we can also see that we will have some software tools which you can use that works along with (Refer Time: 08:52) to acquire all these information.

See sometimes this intrusion detection prevention system can recover entire contents of network packets also. More often recovery is only source and destination IP address and as I talk to you in the last class mostly it will be about metadata. Because storing all the data is extremely difficult unless the network investigator has clues that there is something really happening in the network you do not want to store all the data that you want to trace. You just want to get those data that is very very important for the incident to establish the incident or to find out whether the incident has occurred. So, and that can mostly be recovered using the metadata that we have.

(Refer Slide Time: 09:50)



Firewalls

- Deep packet inspection: forward, log or drop
- Based on source and destination IP, packet payloads, port numbers and encapsulation protocols
- **Forensic Value:**
  - Granular logging
  - Function as both infrastructure protection and IDSs
  - Log
    - Allowed or denied traffic
    - System configuration changes, errors and other events

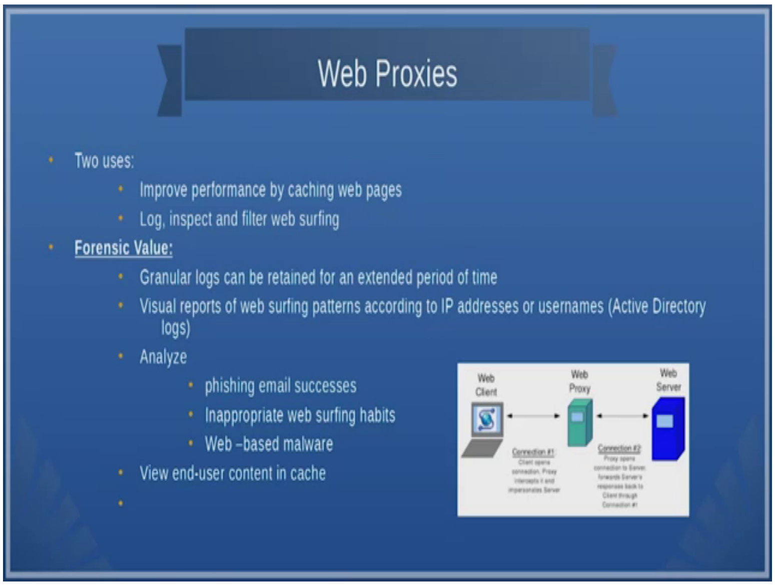
Internet
firewall

The next security gadget which can provide you good amount of information is your firewall ok. Usually firewalls can provide deep packet inspection. So, what do I mean by deep packet inspection? I told you that intrusion prevention and detection systems actually look at the metadata; that means, headers and other information that has firewalls can actually go into the packet. You can if possible it can also find out what is the data that is being transferred.

So, usually we again use firewalls to filter packets based on the source and destination IP addresses it can also give you information on what all the encapsulated protocol etcetera. The advantage of firewalls is that it provides a granular lagging logging you whether you want course granularity or fine granularity you can actually specified in the firewalls and the firewall logs you can use based on what is that where you are in the investigation phase ok. And firewalls also protect as a intrusion detection systems ok. The advent, what you can do with firewall is that once I configure the firewall it can log whatever the allowed or denied a traffic flows and it can also log system, configuration changes errors and other events.

So, firewalls and intrusion detection this systems together, actually these are the two critical components if you want to do network forensics or whatever it is, these are the two critical components which you have to look into very deeply to understand what has happened ok. This does not mean that the other components are not useful, but you you have to give priority to especial this firewalls application level server web servers and application level firewalls, the network level firewalls and of course, web proxies which we are going to see now, ok.

(Refer Slide Time: 12:00)



Web Proxies

- Two uses:
  - Improve performance by caching web pages
  - Log, inspect and filter web surfing
- **Forensic Value:**
  - Granular logs can be retained for an extended period of time
  - Visual reports of web surfing patterns according to IP addresses or usernames (Active Directory logs)
  - Analyze
    - phishing email successes
    - Inappropriate web surfing habits
    - Web –based malware
  - View end-user content in cache

Web Client
Web Proxy
Web Server
Connection #1:
Client opens connection. Proxy intercepts it and impersonates Server
Connection #2:
Proxy opens connection to Server, forwards Server's responses back to Client through Connection #1

So, web proxies provided two functions, one is the obviously, increase the performance of or the lesson the time that is taken to visit a website. This is does by caching the frequently are most often visited web pages. One of the things you might happen is that suppose the webs page on the server has changed and your web proxy has cached it there that is a possibility that there could be a difference in the web pages that you see there you to do something known as a force the resync of the web pages ok.

But in general web proxy is a very useful because they act like a doorway when a person browsers the web this web proxies servers a doorway. Therefore, we can put lot of security measures in the doorway to ensure that that malign I mean software malignant software whatever it is does not get into the network ok.

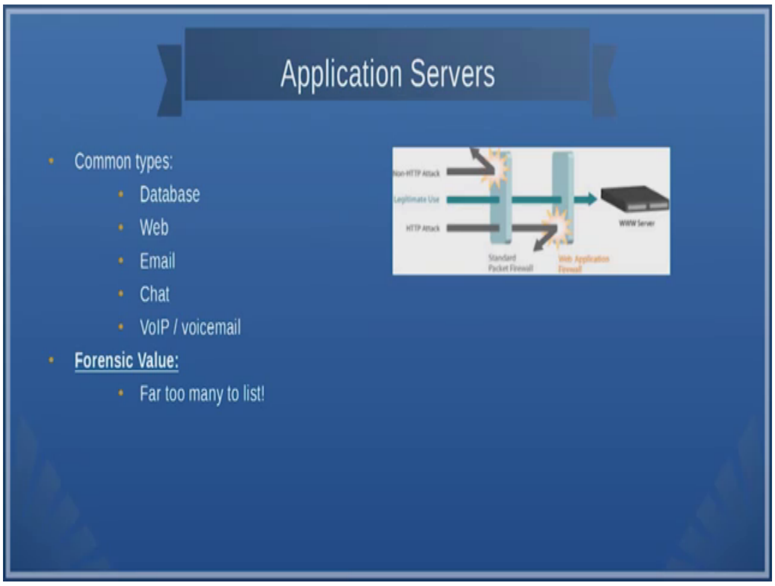
The advantage of web proxies that it can log what are the sites you are going, what are the activities that are happening in the http packets etcetera, it can inspect the packets and it can even filter the brackets ok. So, what we can do is we can put some sort of filters. So, it block certain websites for example, many organizations block facebook and twitter during their official working hours and all this things can be done with the web proxies ok, and sometimes you I mean people usually bypass it ok. So, anyway I mean.

So, the forensic value of web proxies that the granular logs can be stored for a long period of time and many of the proxies actually provide a beautiful visual report of what is the uses search pattern etcetera. For example, I mean if user everyday in the morning whether he comes in looks into facebook first before he logs into the official servers etcetera all this things can be monitored.

The other things that we can do is that we can analyze whether the phishing emails success are there, inappropriate web surfing habits as I told you, web based malware if there is anything is this proxies can ensure that you can block all those things are at least log all those things.

The user usually looks of the contents of the cache that is stored in the web proxies, but anyway I am since as I told you before it provides a single point door where for the data traffic or the http traffic to go out. You can actually log lot of information with this web proxies. And finally, we have this application servers.

(Refer Slide Time: 14:45)



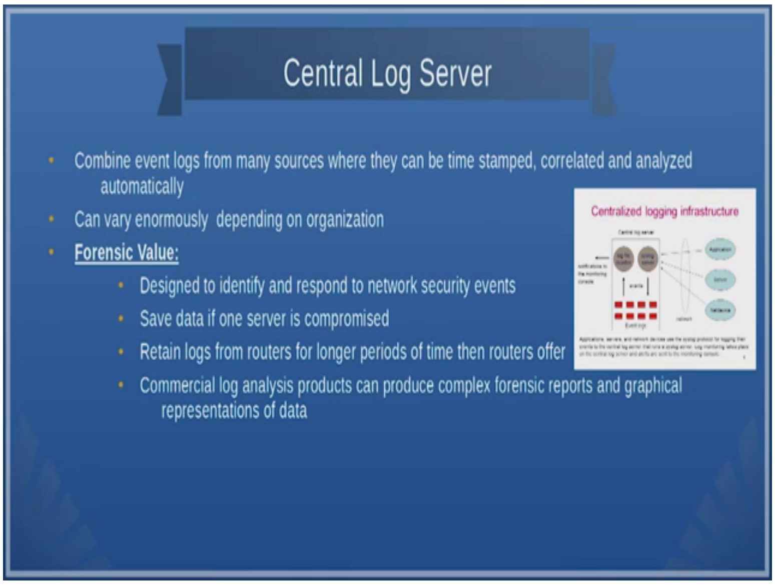
Application Servers

- Common types:
  - Database
  - Web
  - Email
  - Chat
  - VoIP / voicemail
- **Forensic Value:**
  - Far too many to list!

So, the application server are database servers, the web server, the email, the chat server, the voice over IP voice mail servers, etcetera and these forensic value are very very important because these actually store the end results, and if you look at this there is a difference between the standard packet firewall and application level firewall. So, if you look at what is happening is it so, if you look at non http attack then it I mean we were showing it is an example here. So, if you look at non http attack it is just get bounds off by the standard packet firewall whereas it its http attack then it gets bounds off by the web application firewall.

So, so this is actually two levels, you have one level where you filter almost all the packets then if that escapes ok, you can filtered using the web firework anyway. So, coming back to application servers the logs of these application servers are very important. So, one question that arises how much log data do I collect ok, and how much do I preserve, and for what period do I preserve depends on what country you are in many countries manded that it should have it for about 10 years etcetera; that means, the amount of data with speed and the storage etcetera it will be massive.

(Refer Slide Time: 16:10)



Central Log Server

- Combine event logs from many sources where they can be time stamped, correlated and analyzed automatically
- Can vary enormously depending on organization
- **Forensic Value:**
  - Designed to identify and respond to network security events
  - Save data if one server is compromised
  - Retain logs from routers for longer periods of time then routers offer
  - Commercial log analysis products can produce complex forensic reports and graphical representations of data

Applications, servers, and network devices use the syslog protocol for logging their events to the central log server that runs a syslog server. Log monitoring takes place on the central log server and alerts are sent to the monitoring console.

The next is the central log server. Usually as I told you before the use of the central log server is generally when I want to send all the logs to a particular location and then do some sort of analytics on this ok. So, what we do with the central log server is that you can combine event logs from any of the sources and you can just get this time stamped and correlated analyzed automatically.

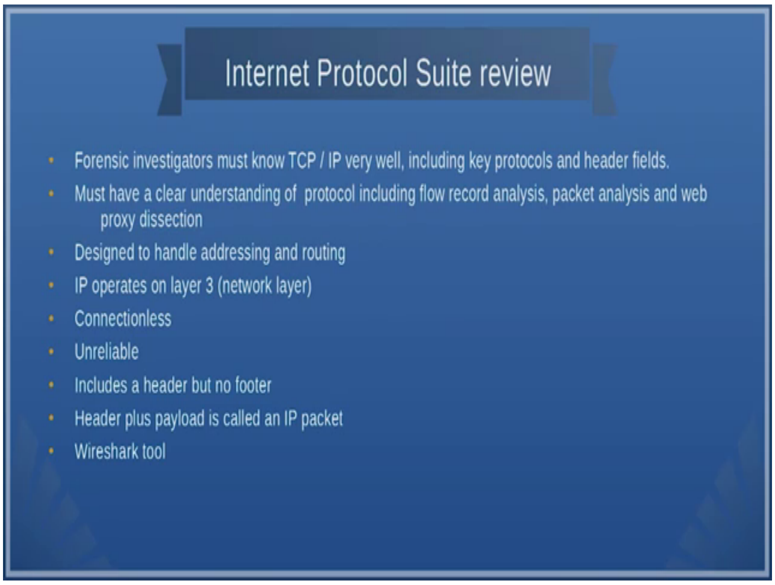
So, this central log server will have massive data, not only will it have massive data you also have to have a lot of good algorithms to get correlation and analysis as well as some accent visualization ok. And this it all depends whether do you want to have a centralized logging or decentralized logging and only if the incident occurred then I collect all this data together all these things are based on what your organization is planning to have as the vision mission or whatever it is ok, or policy ok.

So, coming back to forensic value of the central log servers ok, so this central log servers actually are used to find out how a security lapses happened and why it has happened etcetera and this usually should be replicated because if a person who attacks a central log server almost can delete all the evidence that is that you did you save ok. And sometimes the advantage of having a central log server is router may not have enough memory or space to save all the logs. So, you just push many of those logs not only router any of the other devices that we have seen until now, you pushed it logs and then store it in a central log server ok.

And there are lot of commercially available products which can provide complex forensic reports and graphical representation of data. So, this is more or less I mean you will have you are going to have huge amount of data and then you are going to analyze the data and then present the results ok. So, this is needs to be very powerful server with large amount of storage if you are if you are looking at really looking at centralized logging ok.

Until now, we are looked at what is the kind of hardware device and then and then we also looked at what is the forensic value that is provided by hardware devises. Let us briefly look at the internet protocol suite ok. So, because when whatever attack security attacks happens finally, you will be looking at what happened to the protocols ok.

(Refer Slide Time: 18:47)



Internet Protocol Suite review

- Forensic investigators must know TCP / IP very well, including key protocols and header fields.
- Must have a clear understanding of protocol including flow record analysis, packet analysis and web proxy dissection
- Designed to handle addressing and routing
- IP operates on layer 3 (network layer)
- Connectionless
- Unreliable
- Includes a header but no footer
- Header plus payload is called an IP packet
- Wireshark tool

So, if the internet protocol will be able to identify from where the data are the attacker originated the data etcetera ok. So, if you are if you want to do network forensics you need to completely understand the TCP IP including the options and ports and then the data etcetera ok, especially the header fields ok. And the other point with internet protocol suite is that if you look at internet protocol TCP and other protocols in TCP IP etcetera they actually slice the packets and then sends the packets.

Now, this is it sends it via common medium different package can travels to the common medium. So, it be able to identify one from which machines the packet originated to the flows ok, flows a group of packets which arise from say the same machine and the same user you can call it as a flow.

So, you should be able to understand how flows can be segregated from packets because many of these analyzers packet analyzers they actually dump all the packets and you from the packets you should be able to capture using some kind of a filters you will be able to capture the flows ok. One of the example. Something is come up, something is come up in the screen. What is that? Suddenly (Refer Time: 20:37) show it from that it contains.

Ok, fine. So, let me start let me start from this internet protocol ok. Until now, we have seen lot of hardware devices that we are looking for forensic value. The most important among all these device you can attach all these devices, but then we need the internet protocol suite we need understand internet protocol suite. Internet protocol suite is essentially the TCP IP and UDP, I mean of course, there are other protocols also, but the a forensic investigator must completely understand the key protocols that are use in the internet ok. For example, if you want to decrypt voice and things like that you should have an understanding of sip. Suppose you want to look at email then you understand how snm, smtp works and these protocols run over TCP and IP therefore, you should have a thorough understanding of TCP and IP.

There are two things that you should know one is the packet level analysis. Packet level analysis tells you I mean what are all the packets that went through a particular machine. Then there is a slow level analysis where the slow level analysis tells you how the packets are related ok. So, some related packets becomes a flow and so many of these software which look at dumping the packets and writing into a file of while acquiring the packets ok, acquiring the data.

So, what they what these software do is that they just write everything to a file. Now, from this file we should be able to analyze through filtering what are all the flows etcetera ok, and then dissect them. So, essentially you try to find out this belong to this these packets these group of packets belong to this flow say for example, ftp these group of packets belong to voice, these group of packets belong to let us say video or mails etcetera .

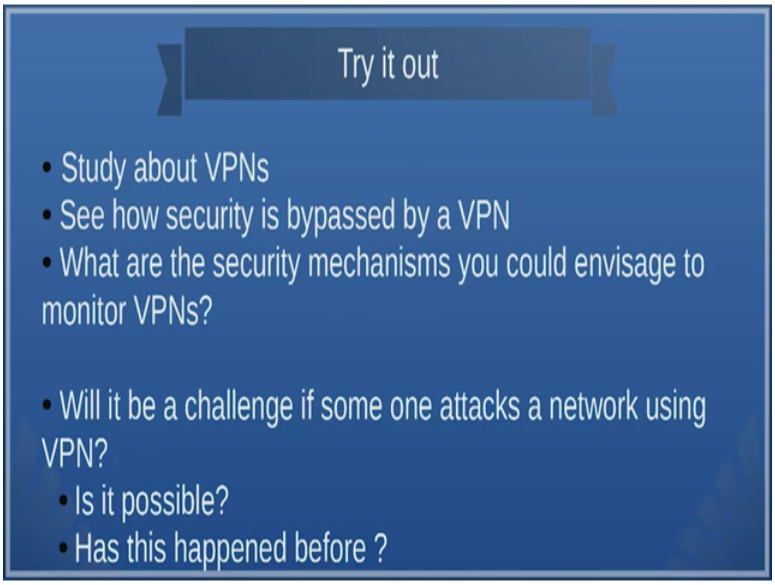
Now, after you group it in this way then you have to identify associate a user with one of these flows. So, this is a very long process so, but anyhow unless you have a good understanding of TCP IP suite you will not be able to do this activity ok.

So, IP operates a the network layer of course, UDP is a connection less protocol and TCP is a connection oriented protocol, ok. So, sometimes an IP within IP that is packets can be tunneled, so you should also look at how tunneling works etcetera. One of the widely used tool I mean I mean which we will also see is the wireshark tool which we can show that it puts the wireshark tool is used to monitor what is happening within the local net ok, and similar tools if you deployed on a router it will be able to monitor what is happening in all the interfaces.

So, essentially extension of dumping the packets, whether you are going to dump it in this machine or you are going to dump it any of the hardware that is shown or you are going to look at logs.

So, there are many ways in which you do it, one is you look at the log files or you just dump all the packets and then analyze the packets later etcetera. We will be looking more closely at the wireshark tool. Now, I thing we have been talking for too long. So, one of the excess that you could try out is something called virtual private networks ok.

(Refer Slide Time: 24:15)



Try it out

- Study about VPNs
- See how security is bypassed by a VPN
- What are the security mechanisms you could envisage to monitor VPNs?

- Will it be a challenge if some one attacks a network using VPN?
  - Is it possible?
  - Has this happened before ?

So, these VPNs are created for security purposes ok. So, it is VPNs are private networks over the public internet. Now, try go to the web take a look at what VPN and how security is implemented in a virtual private network.

Now, you can also look at what are all the problems yeah forensic investigator could face when she is trying to analyze someone who is connected through a VPN. So, how do you if one of the first problems is how do you collect a log, because in a VPN there is a end to end encryption between the routers. So, if I am sitting in between I will be only getting encrypted packets and VPNs are usually used within an organization to connect organizations that are geographical separate ok.

So, you should look at how what are all the security mechanisms, then VPN virtual private network at what layer and what are all the challenges if someone attacks in network using VPN that is using VPN ok. First of all is it possible, one of the attacks is that if I take away all the links by doing a dos attack then VPN will also save ok, and you can also find out whether has this happened before etcetera.

Now, this is for your interest because hearing too much of theory and then trying to see about a new technology and then trying to study how secure it is or how to break the security in that, that will give you a very very good perspective of this acquisition as well as the forensic value. We will look at some traffic acquisition software in the next session.

Thank you.