Table des matières

Week1 3

Stateless Inspection 3

Stateful Inspection 5

Firewall Filters- IDS and IPS Systems 6

The Difference between IDS and IPS Systems 9

Network Address Translation 9

An Introduction to Local Area Networks 11

Ethernet and LAN - Ethernet Operations 16

Ethernet and LAN - Network Devices 20

Introduction to Basic Network Routing 25

Layer 2 and Layer 3 Network Addressing 26

Address Resolution Protocol 28

Routers and Routing Tables, Part 1 30

Routers and Routing Tables, Part 2 30

Routers and Routing Tables, Part 3 31

Research Network Vendor Training 33

Week 2 33

IP Addressing - The Basics of Binary 33

IP Address Structure and Network Classes 37

IP Protocol and Traffic Routing 39

Introduction to the IPv6 Address Schema 44

Application and Transport Protocols UDP and TCP, Part 1 46

Application and Transport Protocols UDP and TCP, Part 2 50

DNS and DHCP 56

Syslog Message Logging Protocol 61

Flows and Network Analysis 65

Port Mirroring and Promiscuous Mode 66

Next Generation Firewalls - Overview 67

NGFW and the OSI Model 69

NGFW Packet Flow Example and NGFW Comparisons 70

Intrusion Detection and Intrusion Prevention Systems 73

High Availability and Clustering 80

Week 3 84

Data Source Types Part 1 ... 84
Data Source Types Part 2 ... 85
Data Model Types ... 87
Structured Data ... 89
Securing the Crown Jewels ... 92
Leveraging Security Industry Best Practices ... 93
Structured Data and Relational Databases ... 93
Anatomy of a Vulnerability Assessment Test Report ... 95
Securing Data Sources by Type ... 95
Securing Databases Wrap Up ... 97
Data Monitoring ... 97
Data Alerts ... 101
Data Activity Reporting ... 106
Attributes to Include in Logging ... 111
Failed Access Monitoring ... 115
Failed Access Monitoring ... 117
Suspicious Access Events, Part 1 ... 119
Data Breach Feeds ... 122
Data Breach Feeds ... 122
Week 4 ... 123
Introduction to Injection Flaws ... 123
OS Command Injection Part 1 ... 125
OS Command Injection Part 2 ... 128
OS Command Injection Part 3 ... 129
SQL Injection Part 1 ... 131
SQL Injection Part 2 ... 133
Other Types of Injection ... 137
Additional Resources ... 140
Additional Resources ... 140
OWASP Cheat Sheets ... 141
pentestmonkey ... 141
Database Hacker's Handbook: Defending Database Servers ... 141
Software Vulnerabilities ... 141
Common Attacks ... 141
Prevention Measures ... 142

Week1

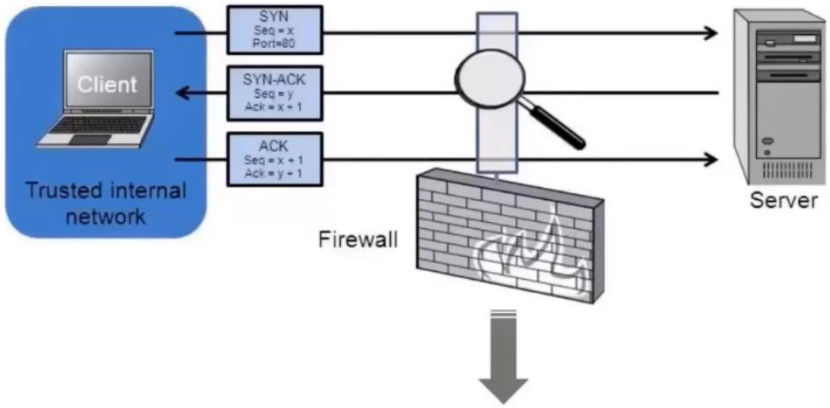
Stateless Inspection

Networking Fundamentals
Basic Concepts of Networking Security

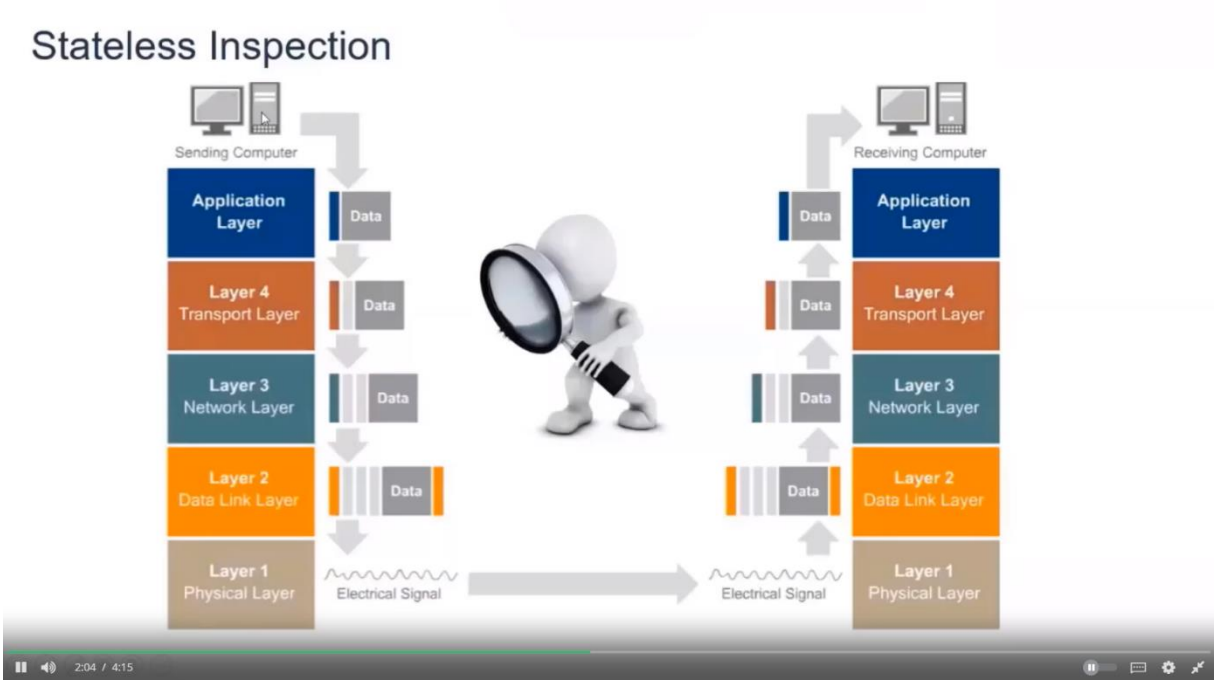
Presented by Ben Briggs
IBM Security

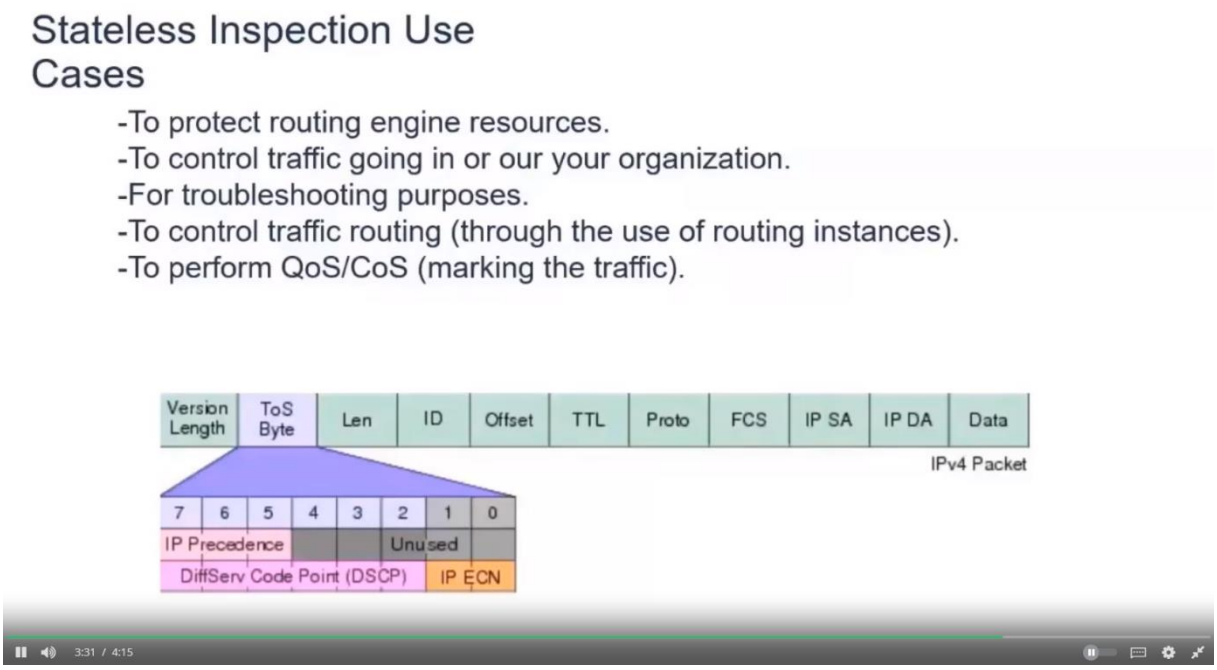
Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security

Stateless Inspection



It does not have a session table

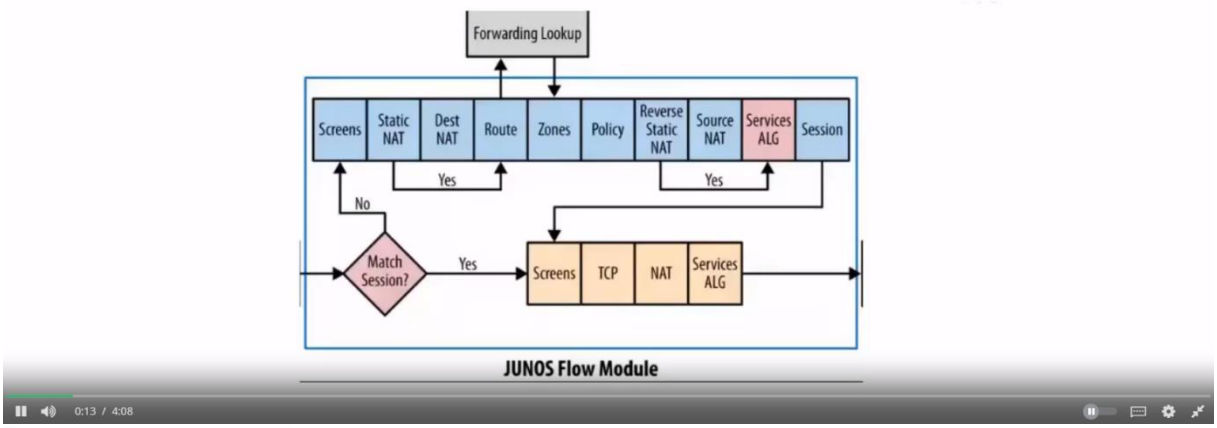




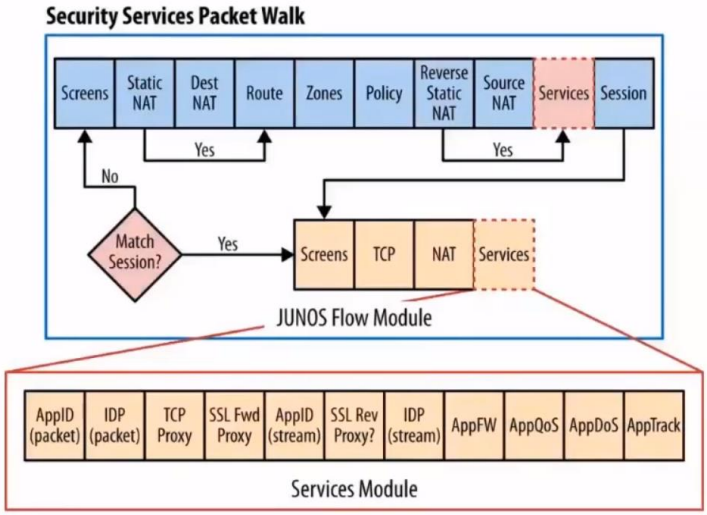
Stateful Inspection

Stateful Inspection

```
user@srx> show security flow session application telnet
Session ID: 57866, Policy name: intrazone-Juniper-SV/4, Timeout: 3394, Valid
In: 172.20.107.10:56290 --> 172.20.207.10:23;tcp If: vlan.107, Pkts: 27, Bytes: 1568
Out: 172.20.207.10:23 --> 172.20.107.10:56290;tcp, If: lt-0/0/0.1, Pkts: 21, Bytes: 1543
```

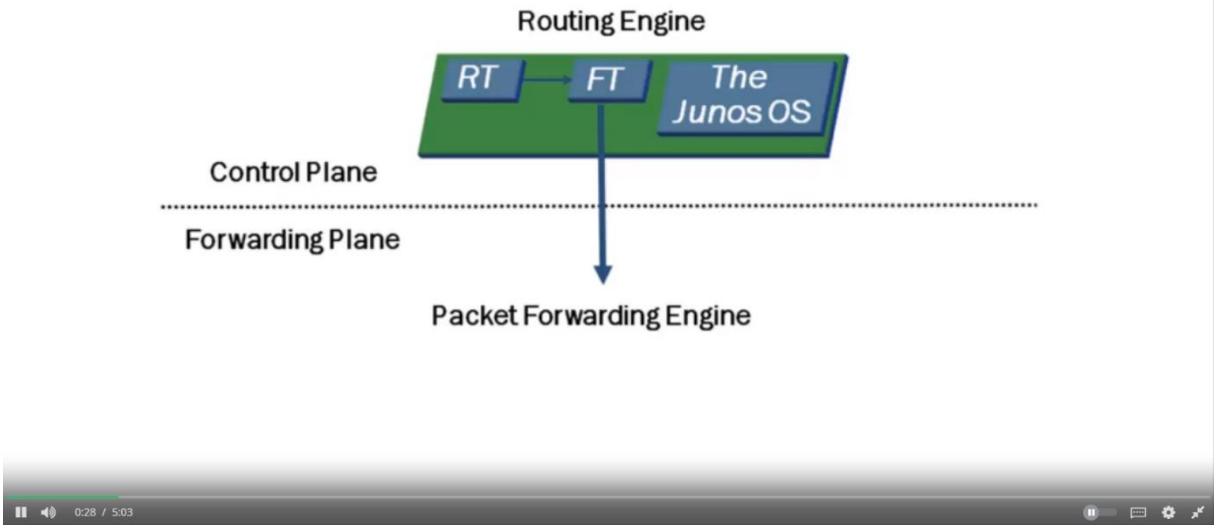


What if we have both types of inspection?



Firewall Filters- IDS and IPS Systems

Firewall Filter (ACLs) / Security Policies Demo…



Intrusion Detection System (IDS)

- An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.
- The IDS is a listen-only device.
- The IDS monitors traffic and reports its results to an administrator.
- Cannot automatically take action to prevent a detected exploit from taking over the system.

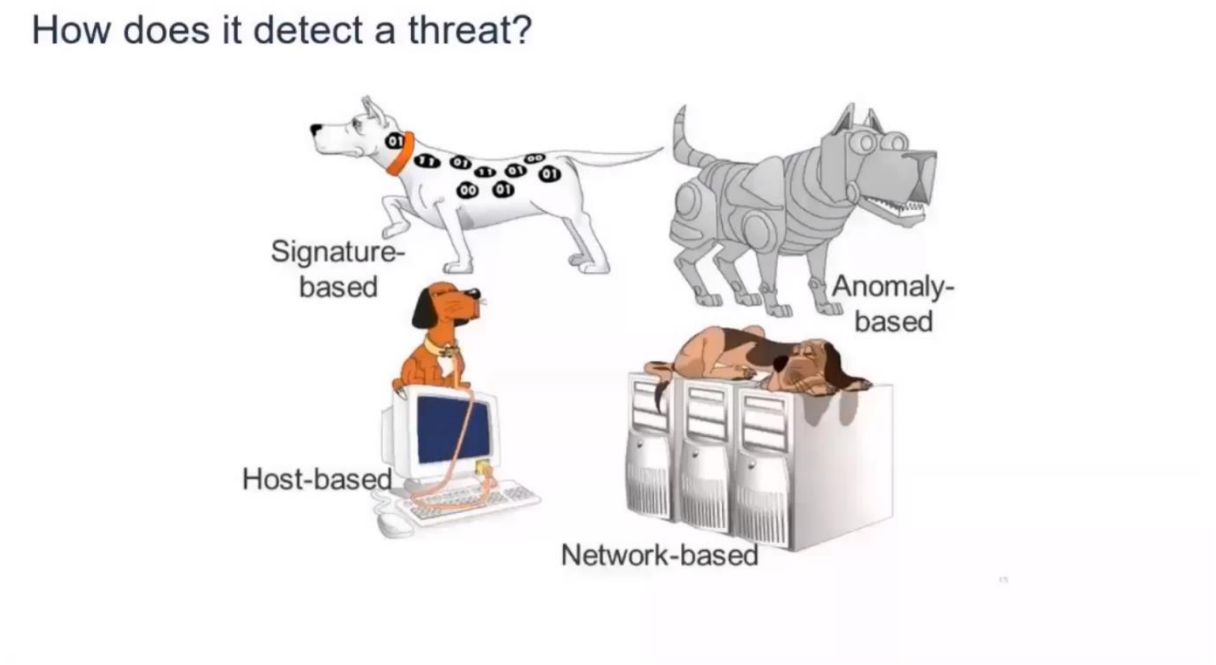
Basics of an Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

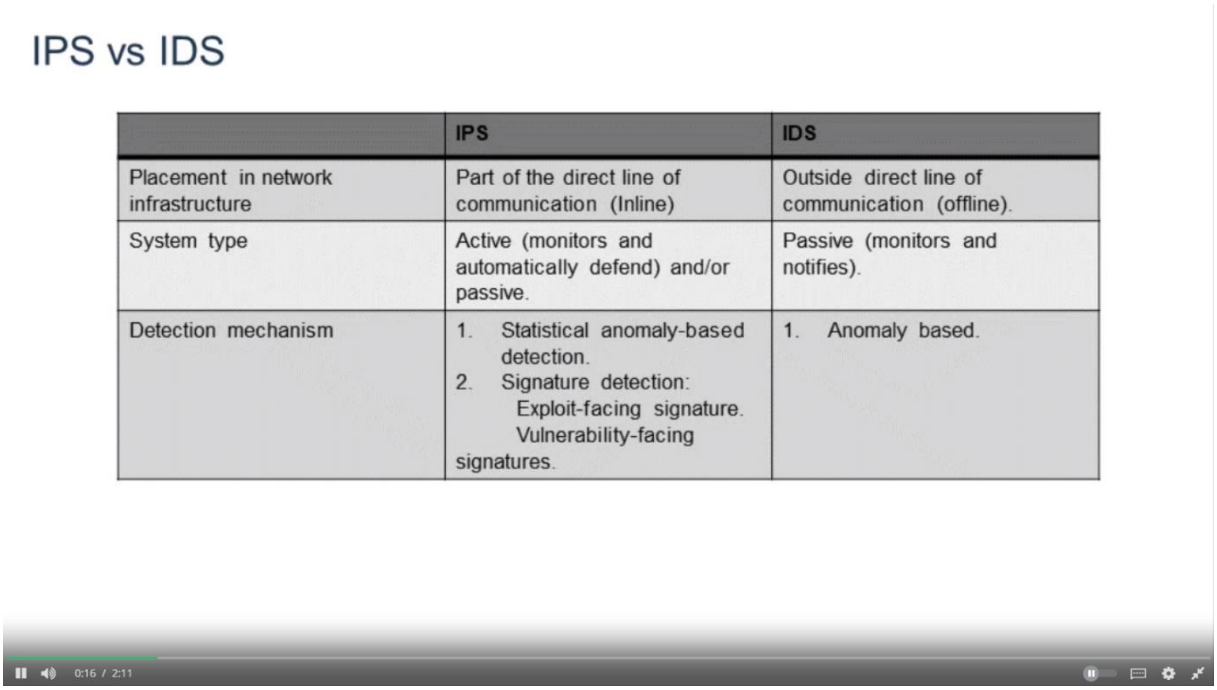
Basics of an Intrusion Prevention System (IPS)

The IPS often sits directly behind the firewall and it provides a complementary layer of analysis that negatively selects for dangerous content.

Unlike the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network.



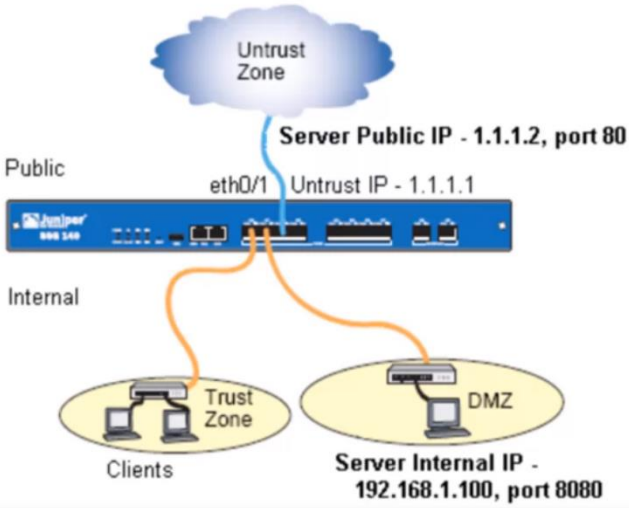
The Difference between IDS and IPS Systems



	IPS	IDS
Placement in network infrastructure	Part of the direct line of communication (Inline)	Outside direct line of communication (offline).
System type	Active (monitors and automatically defend) and/or passive.	Passive (monitors and notifies).
Detection mechanism	1. Statistical anomaly-based detection. 2. Signature detection: Exploit-facing signature. Vulnerability-facing signatures.	1. Anomaly based.

Network Address Translation

Network Address Translation



0:24 / 4:22

Network Address Translation

- Method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
- Gives you an additional layer of security.
- Allows the IP network of an organization to appear from the outside to use a different IP address space than what it is actually using. Thus, NAT allows an organization with non-globally routable addresses to connect to the Internet by translating those addresses into a globally routable address space.
- It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

1:25 / 4:22

Types of NAT

Static address translation (static NAT): Allows one-to-one mapping between local and global addresses.

Dynamic address translation (dynamic NAT): Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.

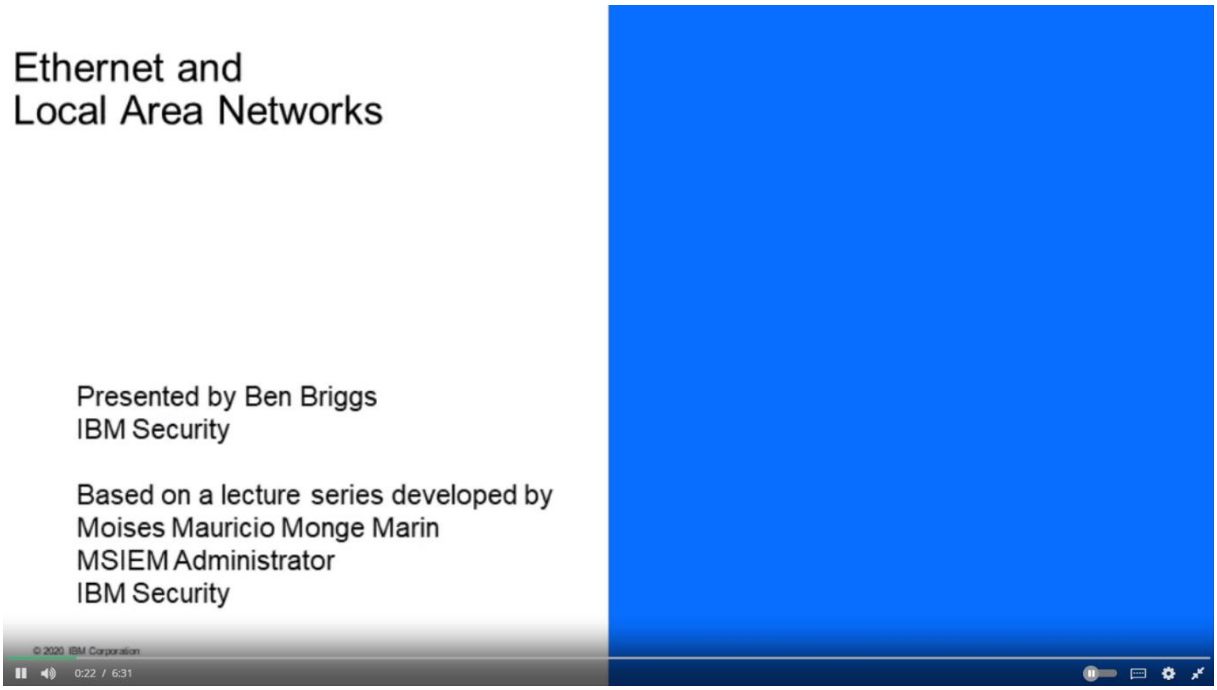
Overloading: Maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). By using overloading, thousands of users can be connected to the Internet by using only one real global IP address.

An Introduction to Local Area Networks

Ethernet and Local Area Networks

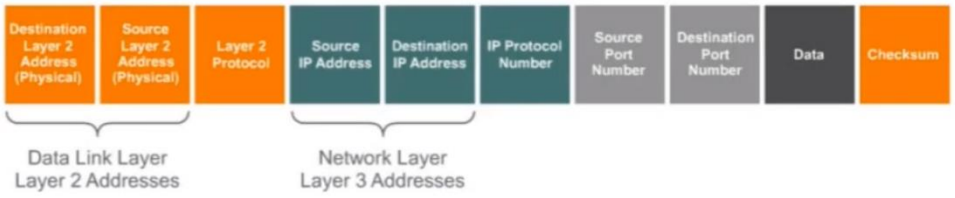
Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security



Objectives

- Describe how Ethernet networks work.
- Differentiate and understand the variety of network devices we have.
- Understand the difference between a collision and a broadcast domain.
- Describe the different ways we have to segment broadcast domains.
- Understand how the Virtual LANs or VLANs work on a Local Area Network.
- Introduce the 2 different addressing schemes we have on today's networks.



Source: https://learningportal.juniper.net/

Network Addressing Part 1

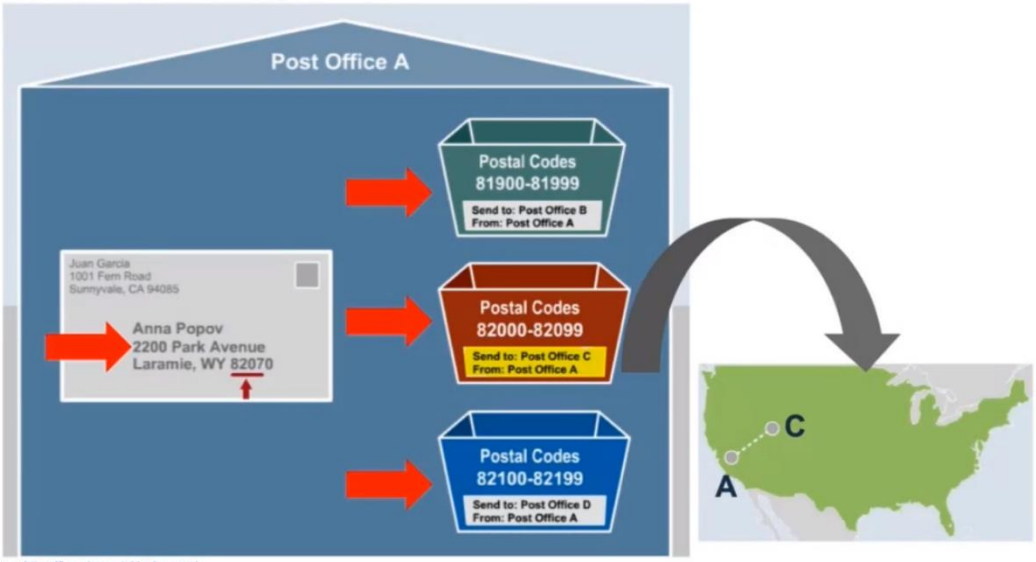
To understand how networks work, is critical to understand the two different types of addressing networks use.

Layer 3 or network layer adds an address to the data as it flows down the stack; then layer 2 or the data link layer adds another address to the data.

Why do we have 2 different addresses?

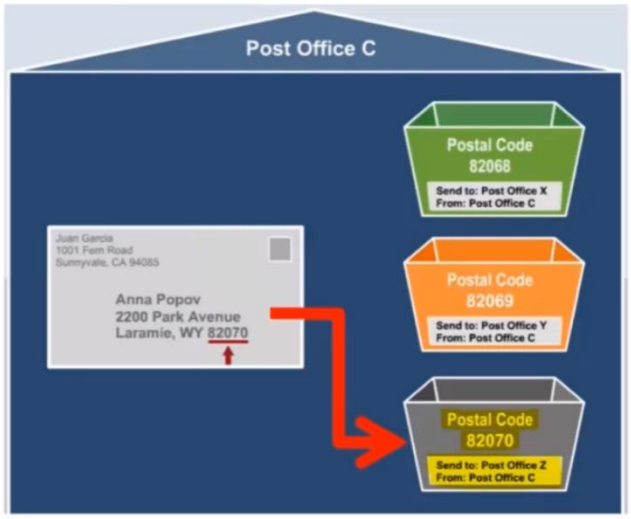
Source: https://learningportal.juniper.net/

Network Addressing Part 2



Source: https://learningportal.juniper.net/

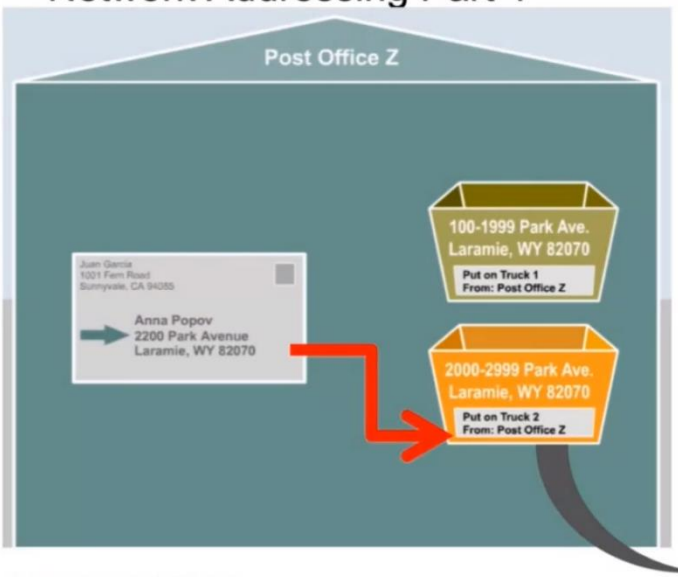
Network Addressing Part 3



Source: https://learningportal.juniper.net/

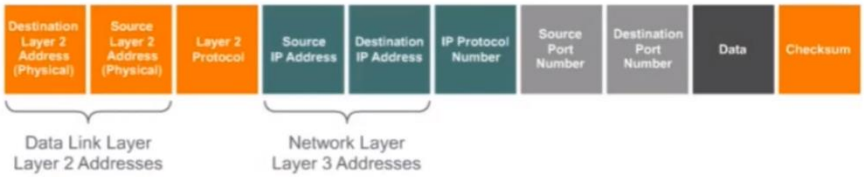
2:42 / 6:31

Network Addressing Part 4



Source: https://learningportal.juniper.net/

Network Addressing Part 5



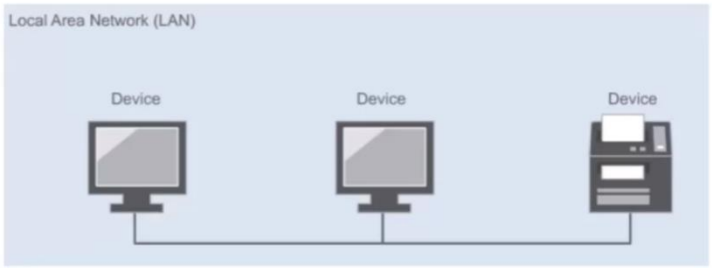
	Layer 2 Addresses	Layer 3 Addresses
		
Also Known As	MAC Addresses Hardware Addresses Physical Addresses	IP Addresses Logical Addresses
Example	00:90:69:9f:ea:46	172.16.12.1
Characteristics	• Identify the stops made along the way • Change with each stop along the route	• Identify the communicating computers or end points • Do not change

Source: https://learningportal.juniper.net/

Introduction to Ethernet Networks Part 2

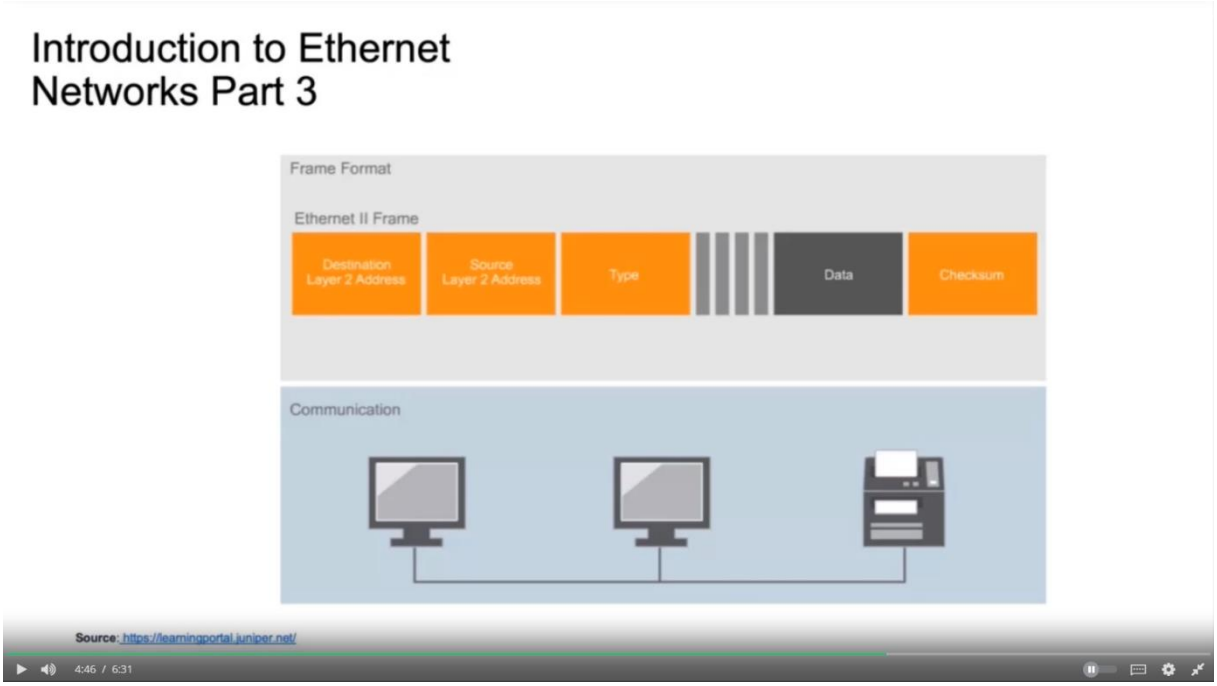
For a LAN to function we need:

- Connectivity between devices
- A set of rules controlling the communication



The most common set of rules is called Ethernet

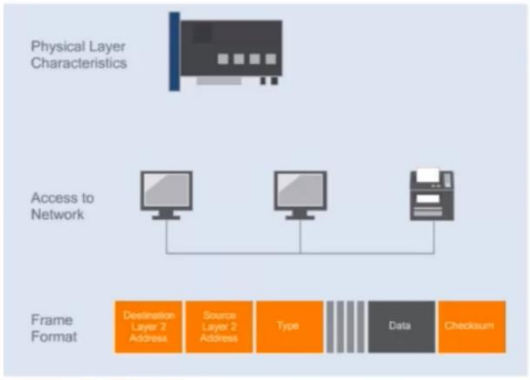
Source: https://learningportal.juniper.net/

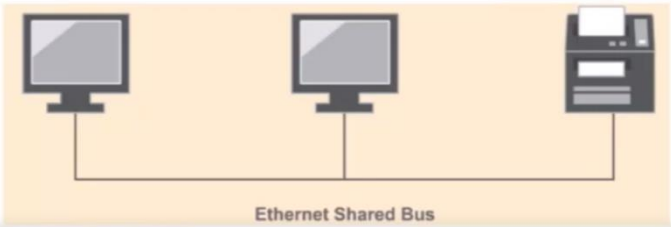


Ethernet and LAN - Ethernet Operations

Ethernet Operations Part 1

Ethernet standards include some components



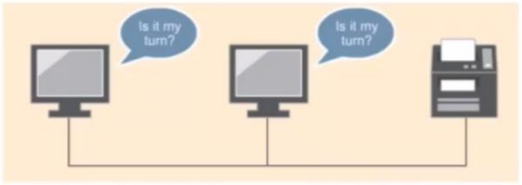


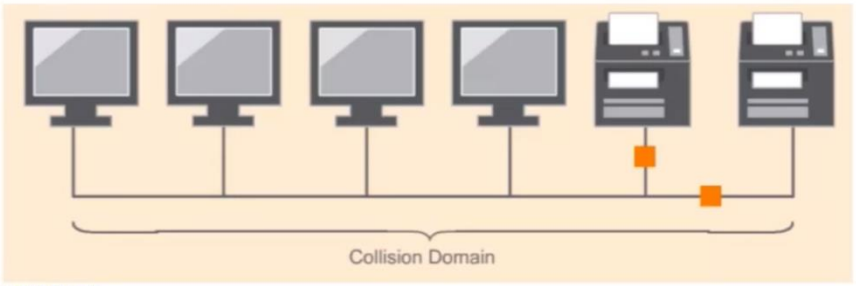
Source: https://learningportal.juniper.net/

0:20 / 4:50

Ethernet Operations Part 3

How do devices know when it is their turn to transmit data?





Source: https://learningportal.juniper.net/

Ethernet Operations Part 4

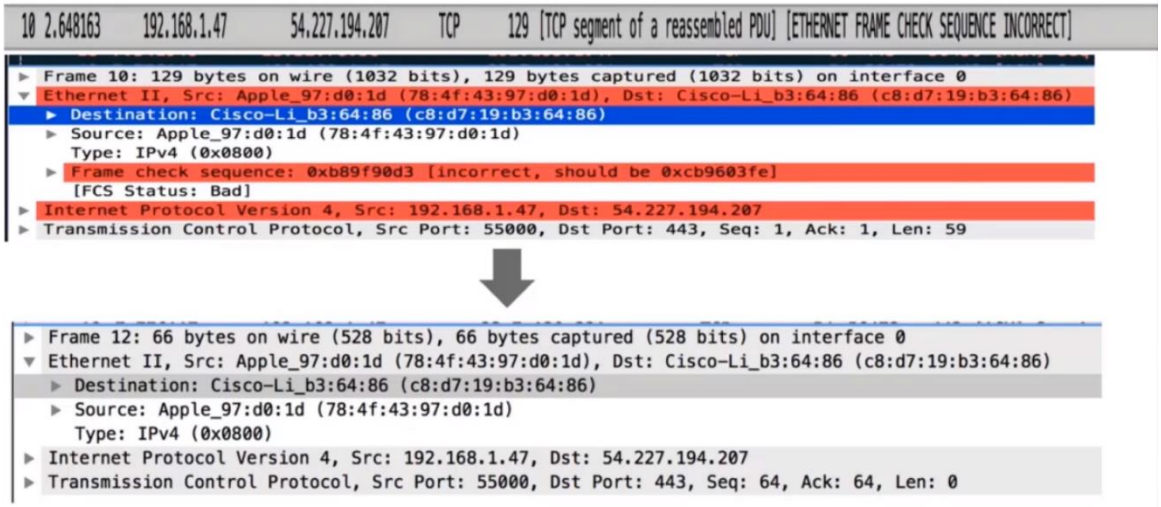
How do devices know when the data is for them?

Destination Layer 2 address: MAC address of the device that will receive the frame
Source Layer 2 address: MAC address of the device sending the frame
Type: Indicates the layer 3 protocol that is being transported on the frame such as IPv4 IPv6, AppleTall, etc.
Data: Contains the original data as well as the headers added during the encapsulation process
Checksum: This contains a Cyclic Redundancy Check to check if there are errors on the data

Source: https://learningportal.juniper.net/

Ethernet Operations Part 5

Are the Preamble and Start Delimiter part of an Ethernet Frame?



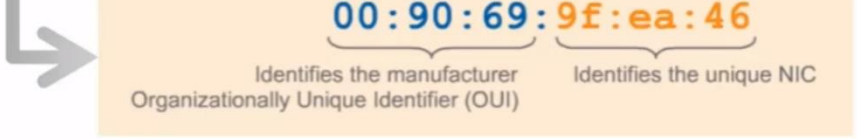
Ethernet Operations Part 6

MAC Address

A MAC address is a 48-bit address that uniquely identifies a device's NIC.
First 3 bytes are for the OUI and last 3 bytes are reserved to identify each NIC.

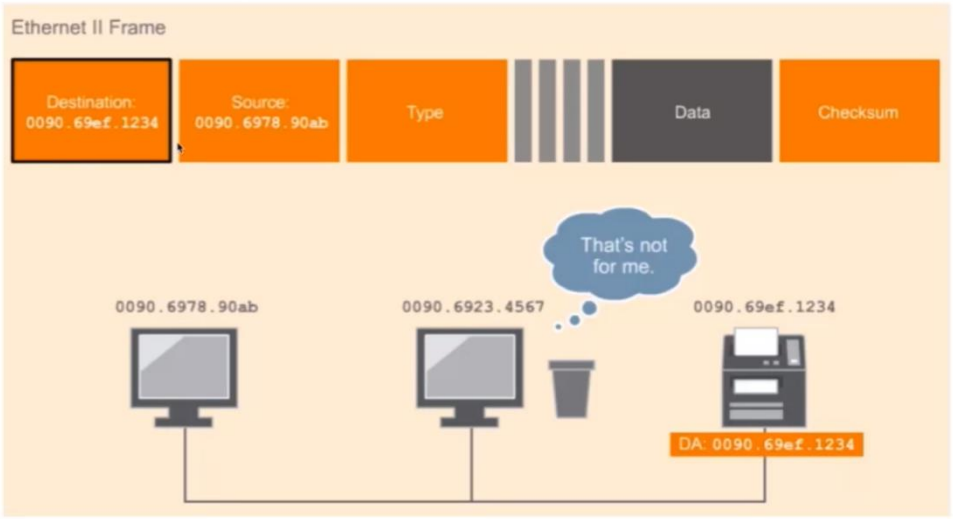
Example:
00:90:69:9f:ea:46

Hexadecimal	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15



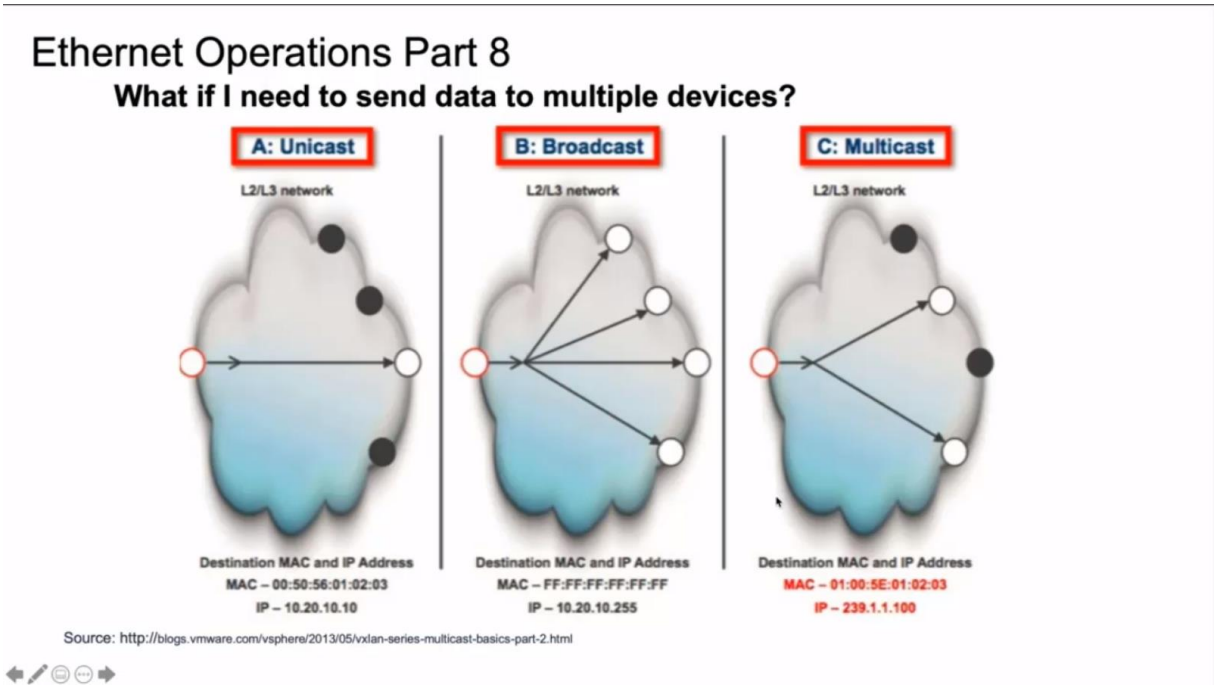
Source: https://learningportal.juniper.net/

Ethernet Operations Part 7

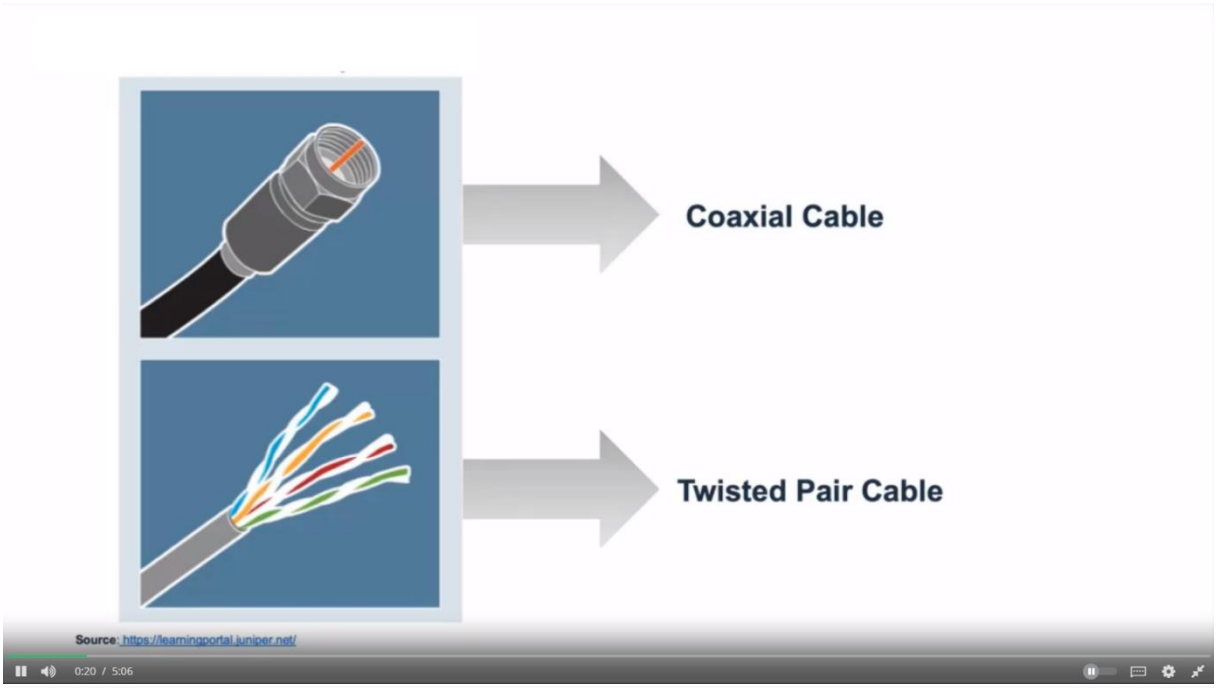


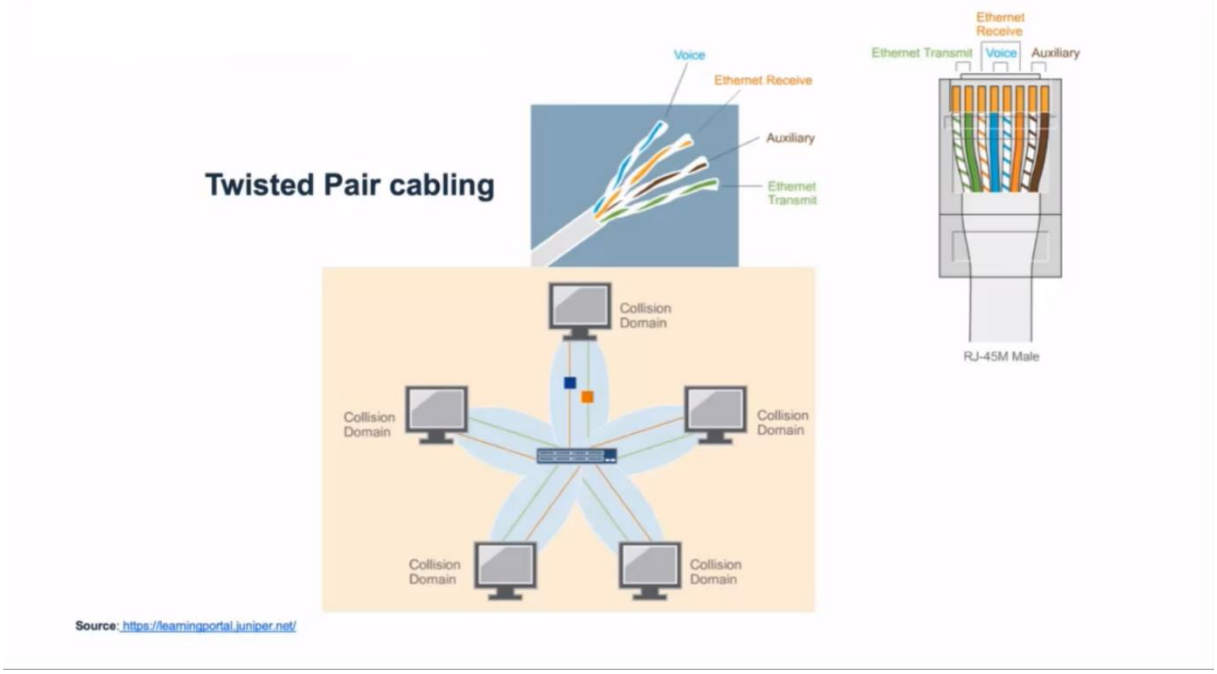
Source: https://learningportal.juniper.net/

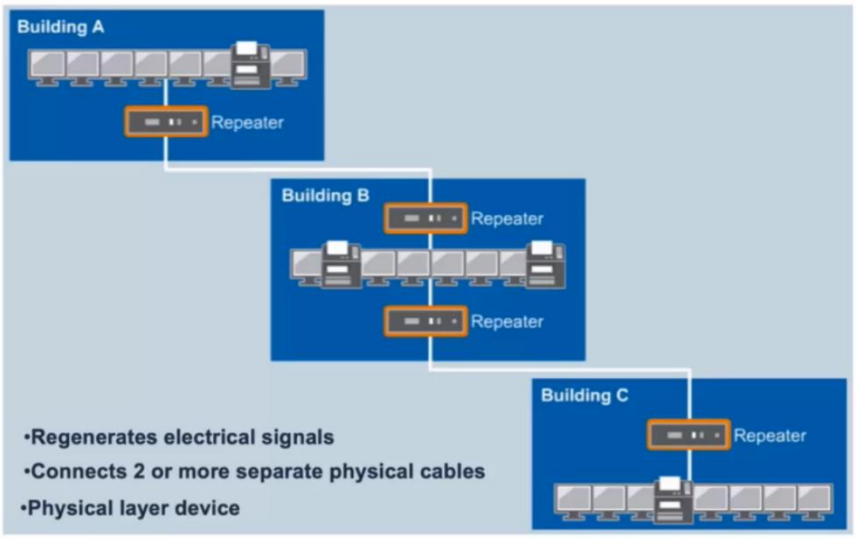
4:03 / 4:50



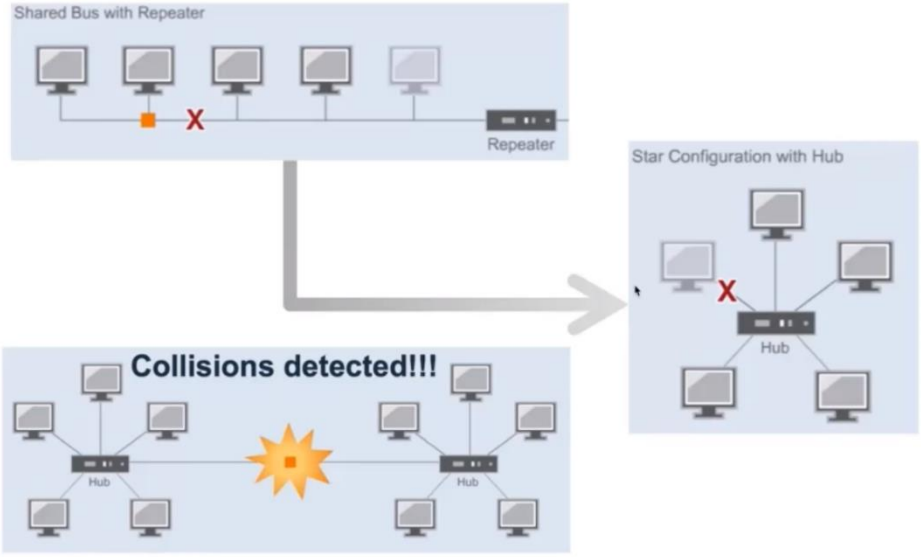
Ethernet and LAN - Network Devices


Coaxial Cable
Twisted Pair Cable
Source: https://learningportal.juniper.net/
0:20 / 5:06

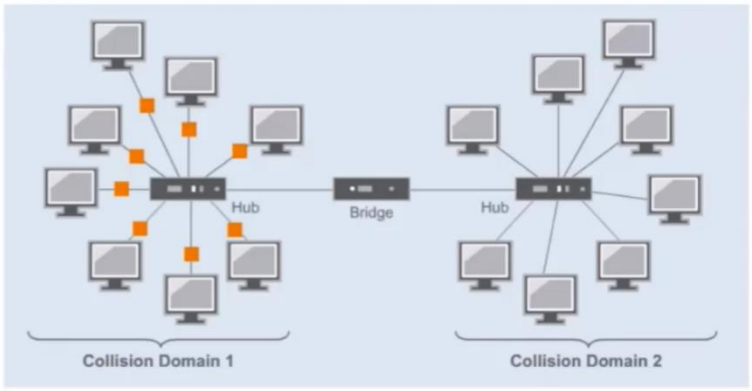

Twisted Pair cabling
Voice
Ethernet Receive
Auxiliary
Ethernet Transmit
Collision Domain
Collision Domain
Collision Domain
Collision Domain
Collision Domain
Ethernet Receive
Ethernet Transmit
Voice
Auxiliary
RJ-45M Male
Source: https://learningportal.juniper.net/

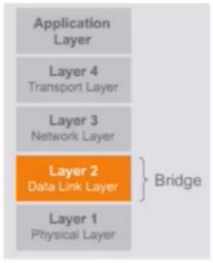


Source: https://learningportal.juniper.net/



Source: https://learningportal.juniper.net/

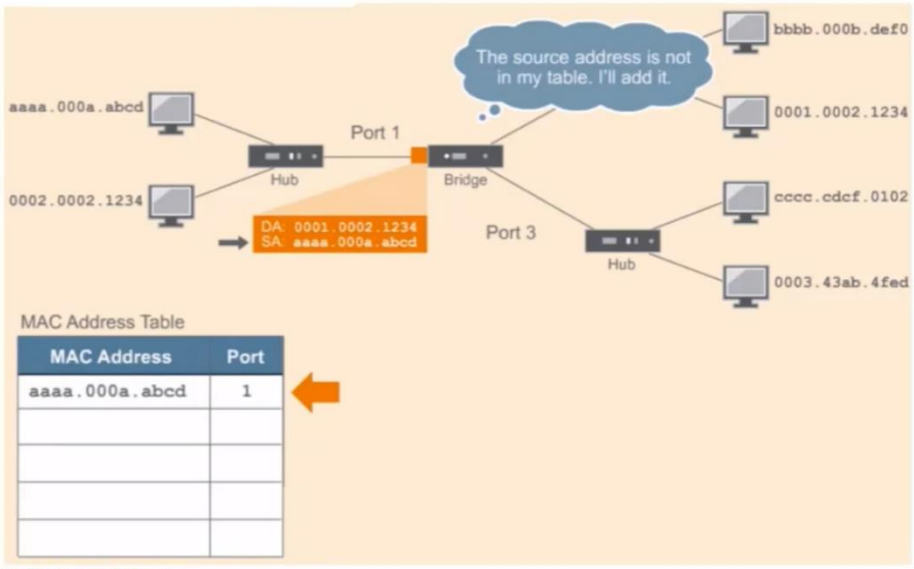




Ethernet bridges has 3 main functions:

- **Forwarding frames**
- **Learning MAC addresses**
- **Controlling traffic**

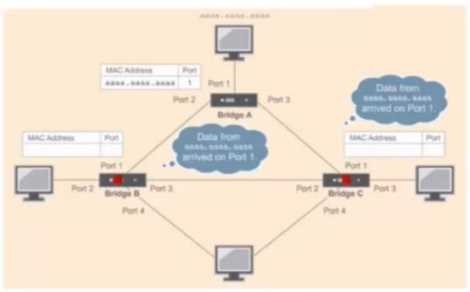
Source: https://learningportal.juniper.net/



MAC Address Table

MAC Address	Port
aaaa.000a.abcd	1

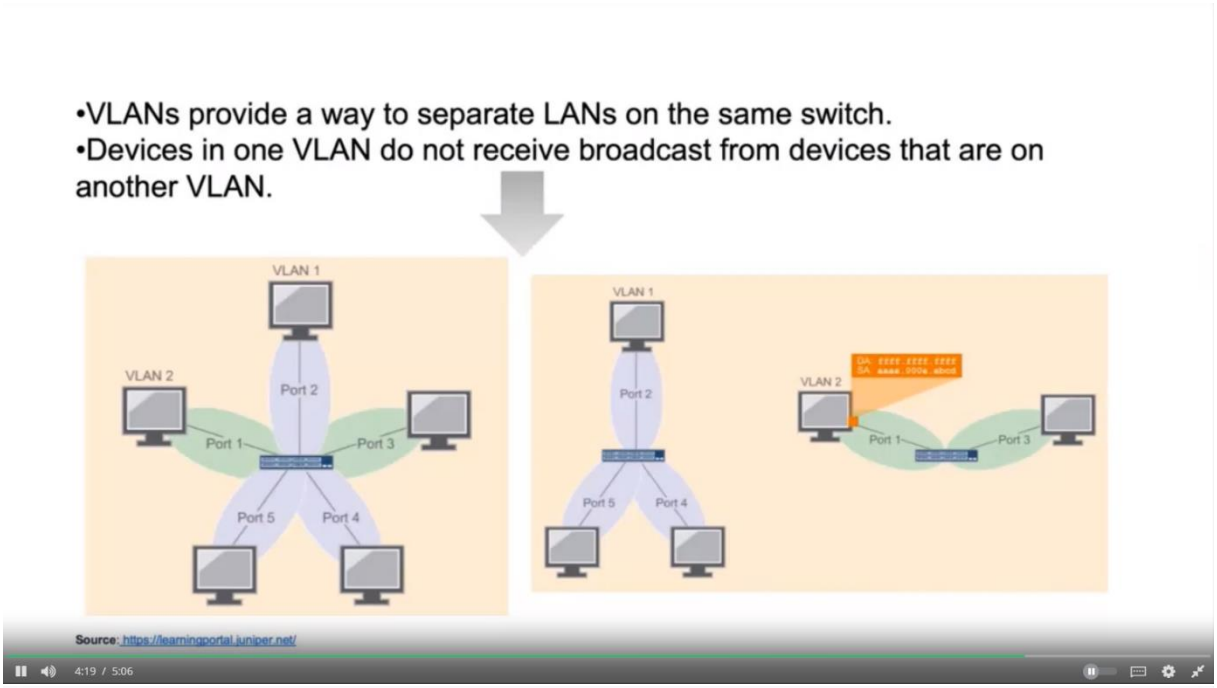
Source: https://learningportal.juniper.net/

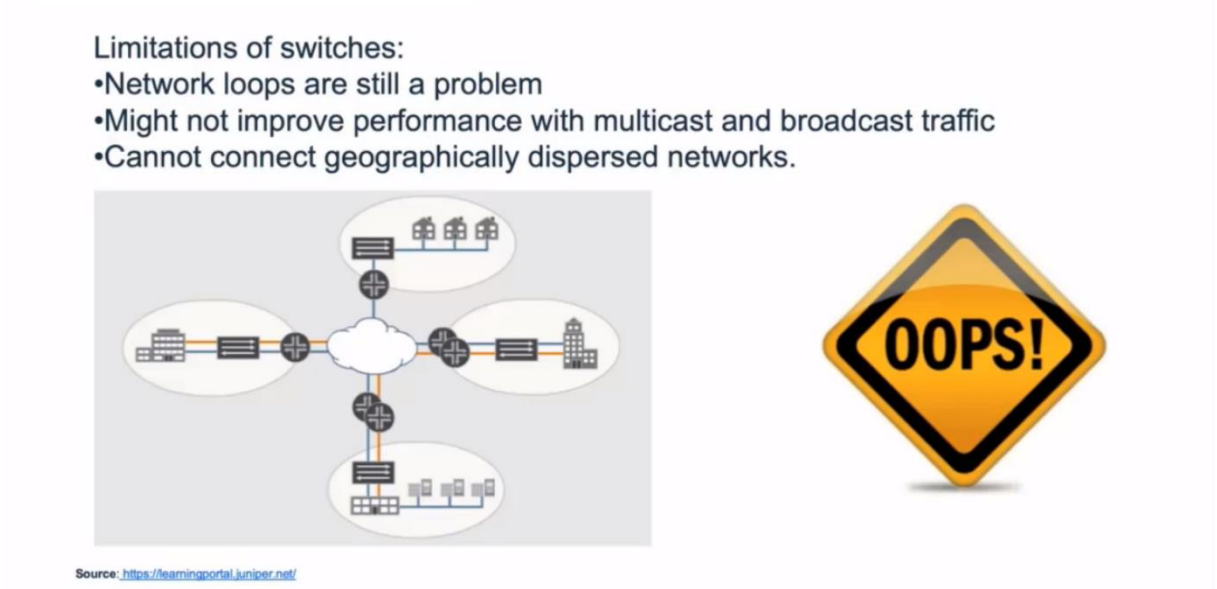


Source: https://learningportal.juniper.net/

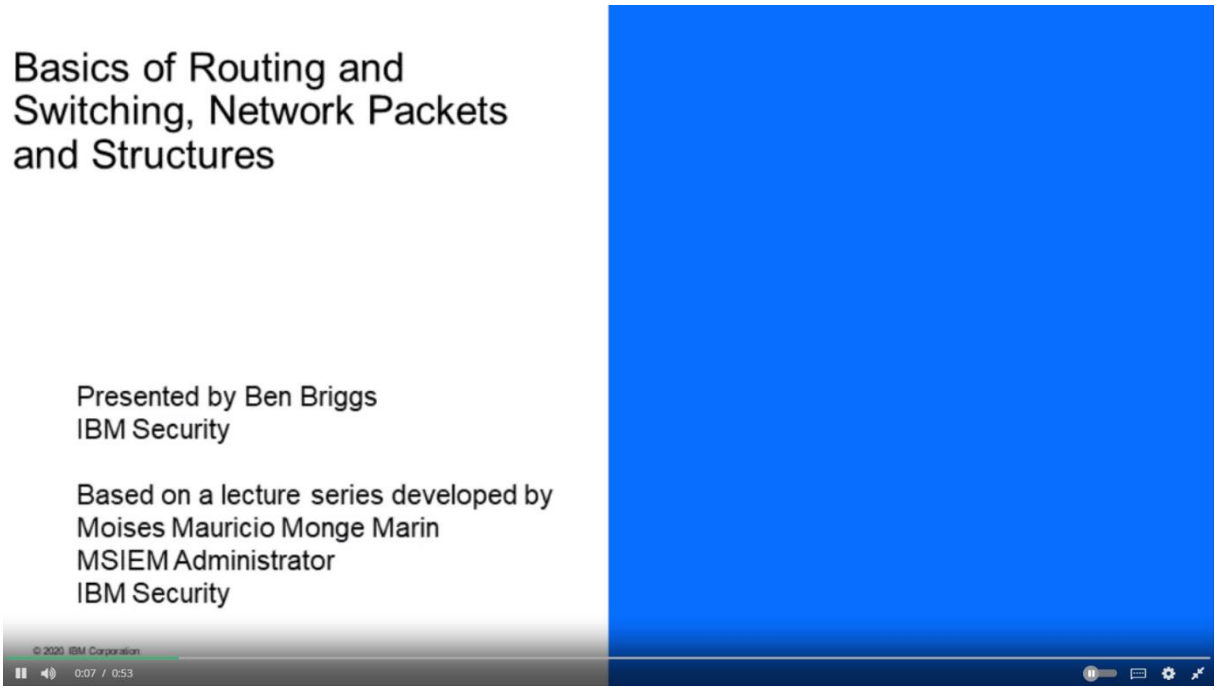
Bridge	Switch
Half-duplex data transmission	Full-duplex data transmission
End-user devices share bandwidth on each port	Each port is dedicated to a single device; bandwidth is not shared
Virtual LANs are not possible	Virtual LANs are possible

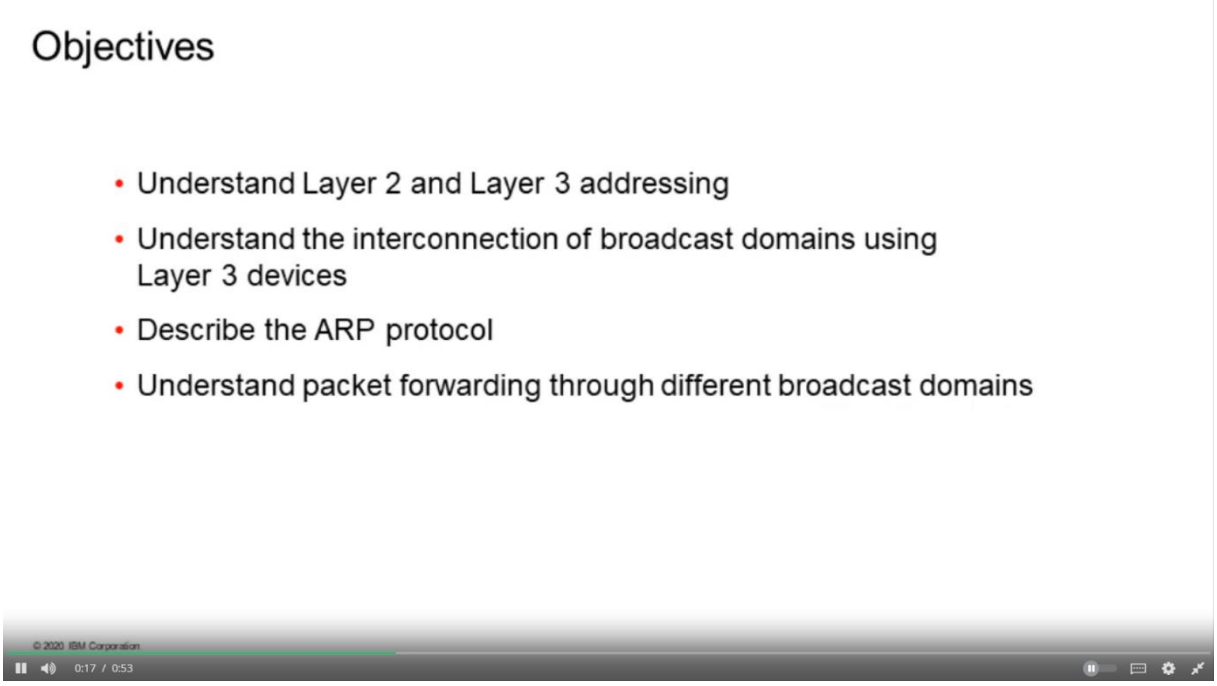
Source: https://learningportal.juniper.net/





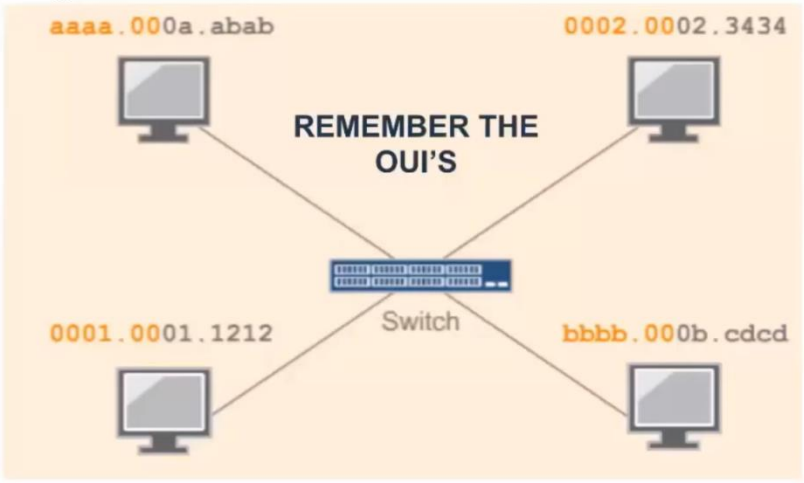
Introduction to Basic Network Routing





Layer 2 and Layer 3 Network Addressing

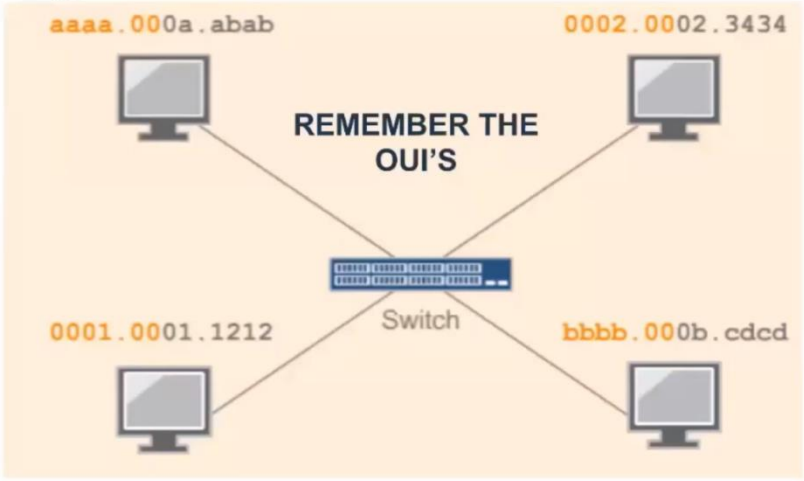
Layer 2 and Layer 3 Addressing



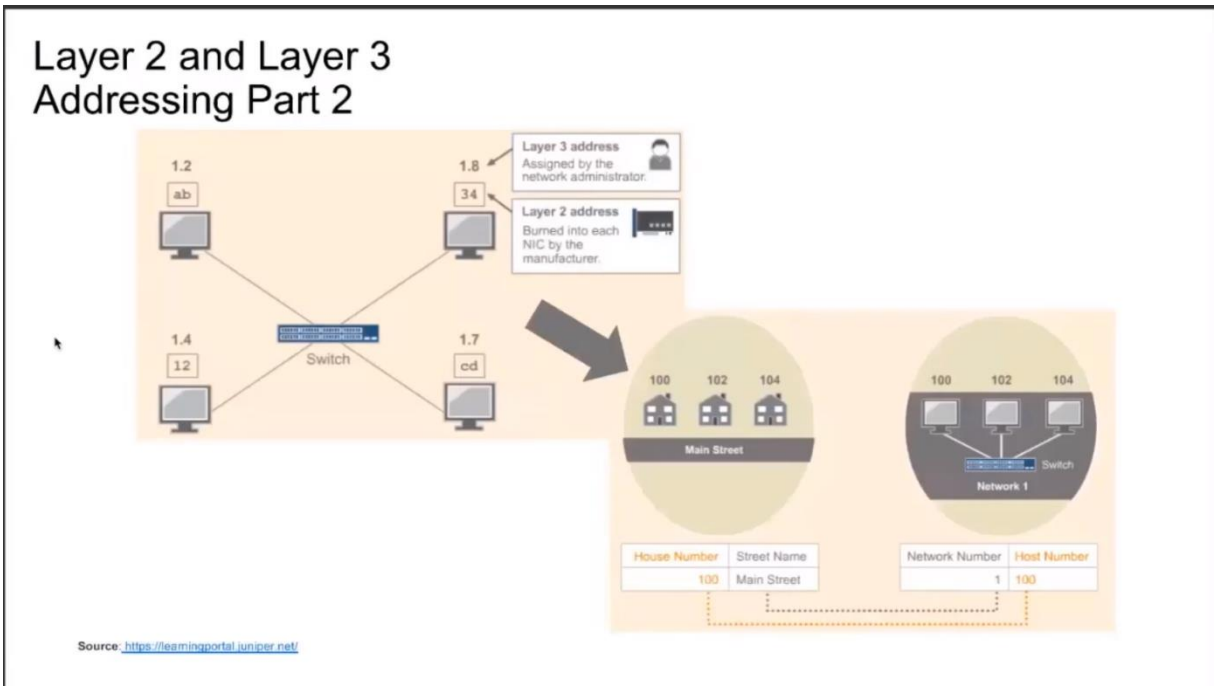
Source: https://learningportal.juniper.net/

0:26 / 5:11

Layer 2 and Layer 3 Addressing

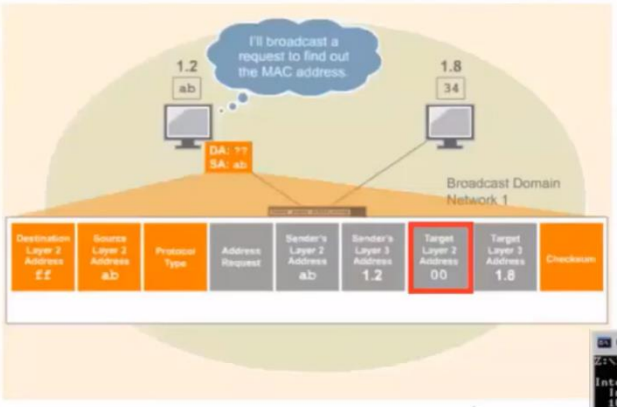


Source: https://learningportal.juniper.net/



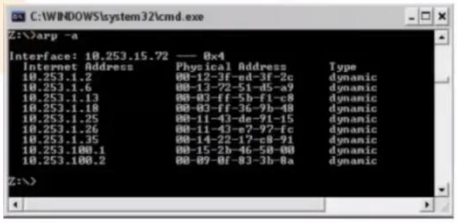
Address Resolution Protocol

Address Resolution Protocol



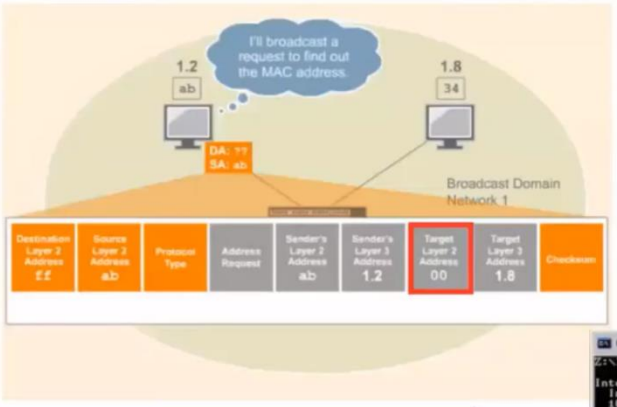
The process of using layer 3 addresses to determine layer 2 addresses is called ARP or Address Resolution Protocol.

ARP TABLE



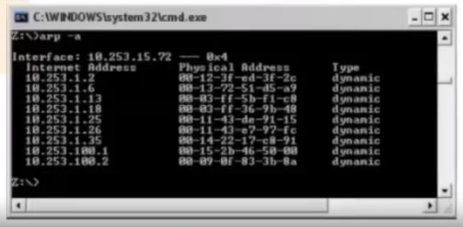
Source: https://learningportal.juniper.net/

Address Resolution Protocol

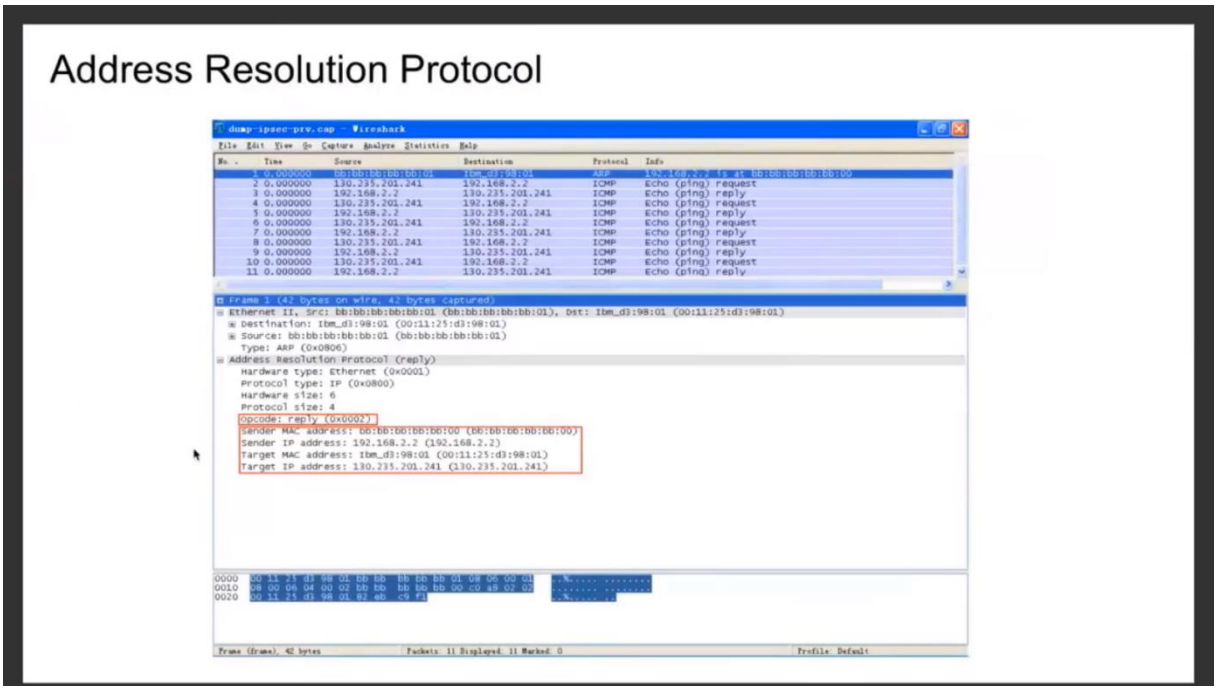


The process of using layer 3 addresses to determine layer 2 addresses is called ARP or Address Resolution Protocol.

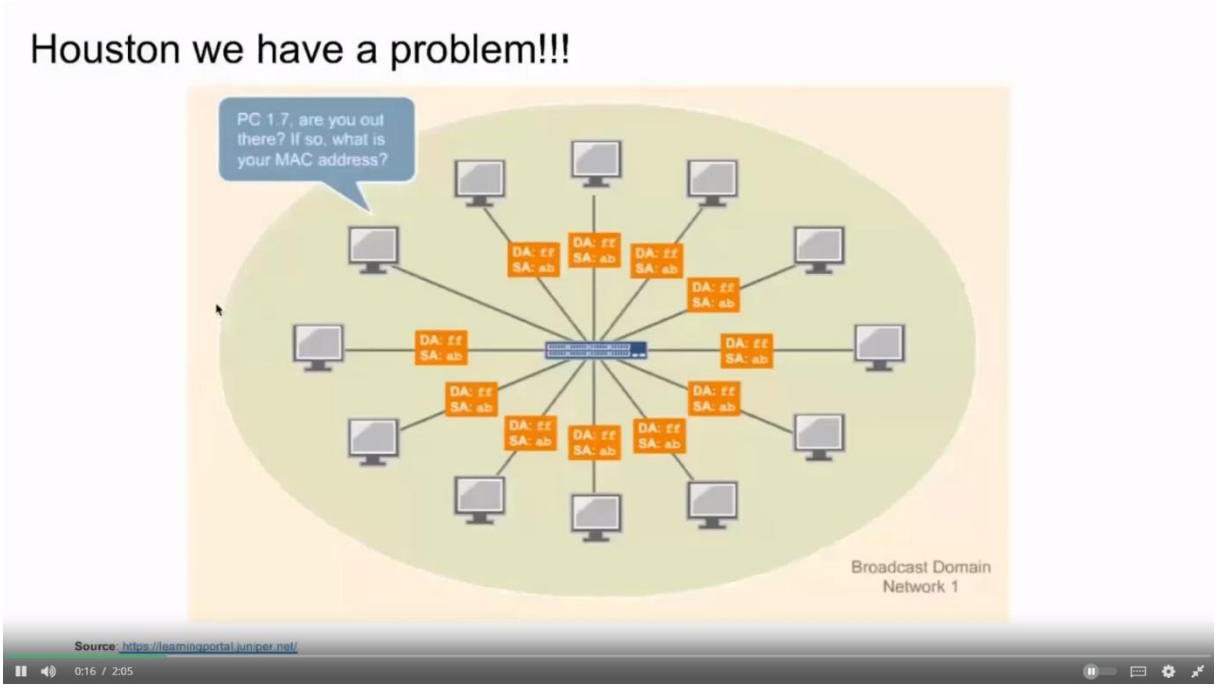
ARP TABLE



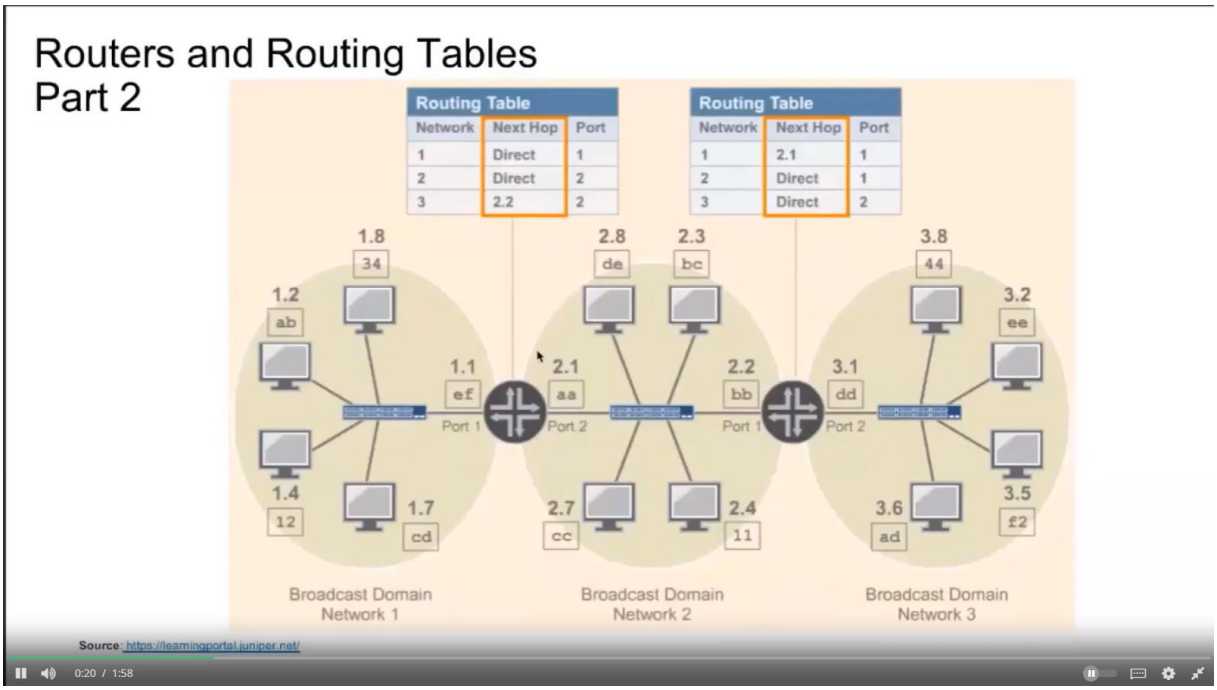
Source: https://learningportal.juniper.net/



Routers and Routing Tables, Part 1

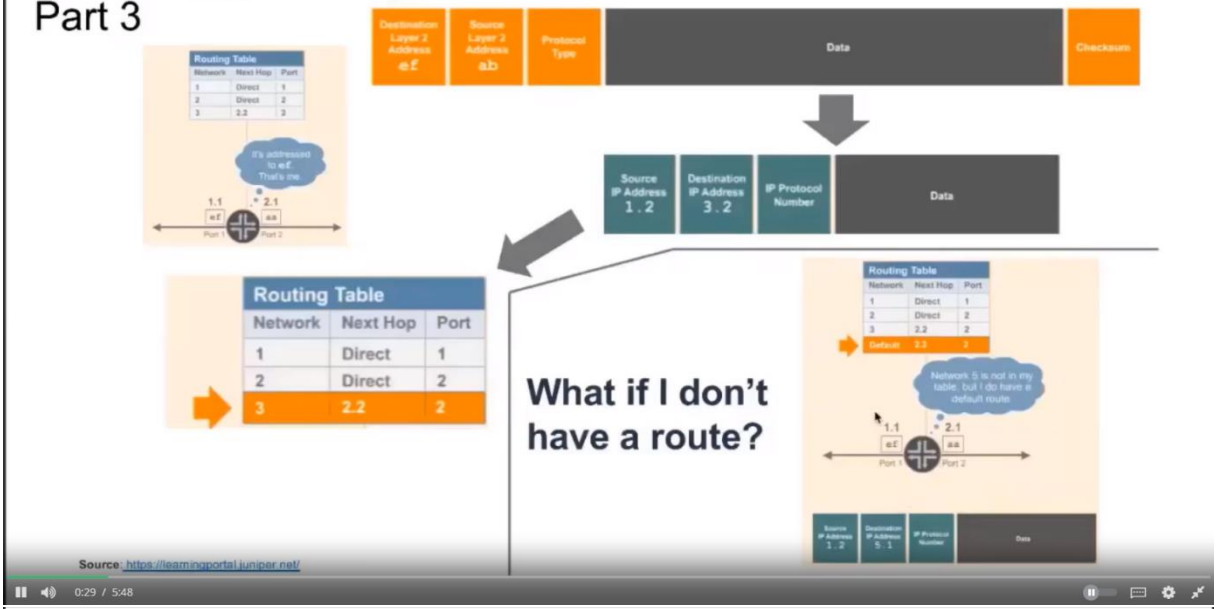


Routers and Routing Tables, Part 2



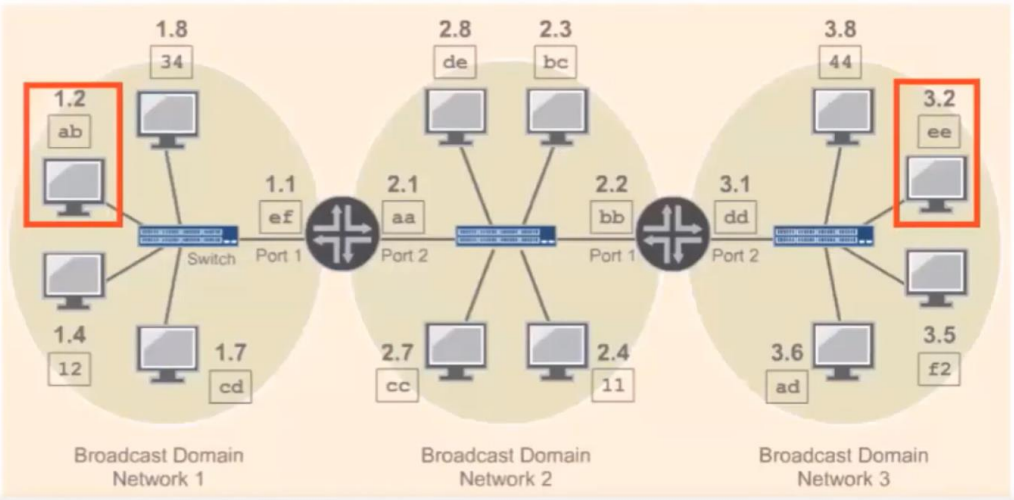
Routers and Routing Tables, Part 3

Routers and Routing Tables
Part 3



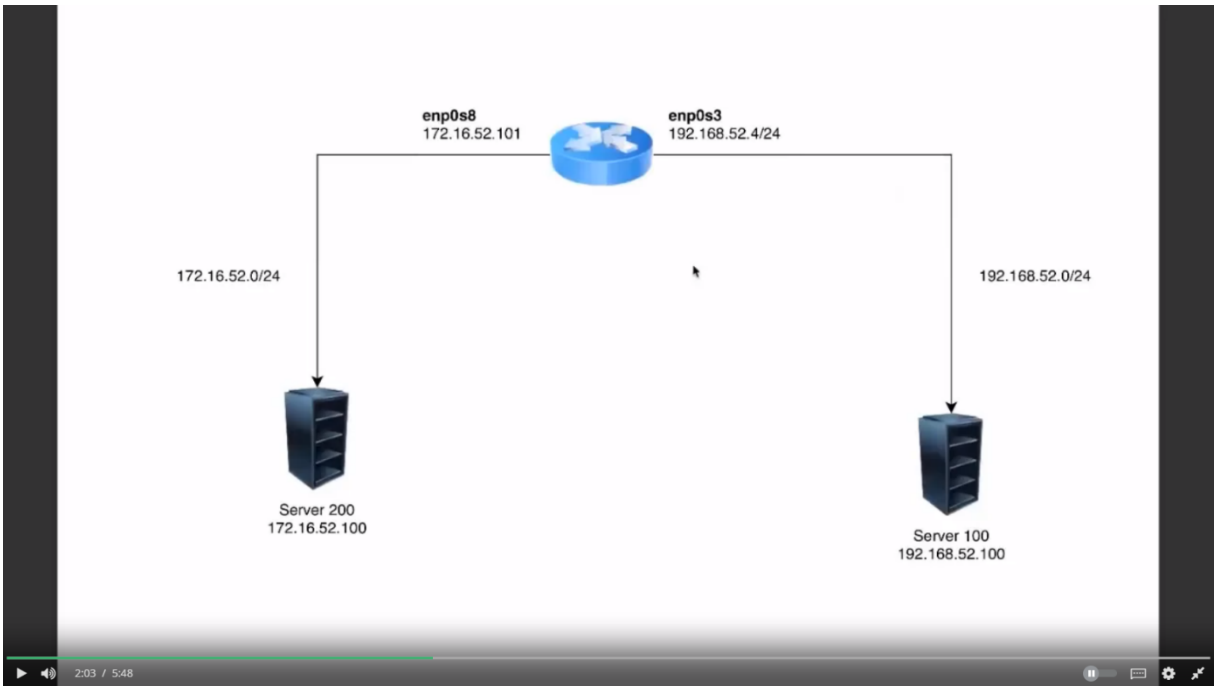
Routing in Action

PC "1.2" wants to send data to PC "3.2"



Source: https://learningportal.juniper.net/

1:53 / 5:48



Research Network Vendor Training

Check out a few of the online training resources available for the following network vendors.

Cisco

https://www.cisco.com/c/en/us/training-events/training-certifications/training-catalog/course-selector.html

Juniper Networks

https://www.juniper.net/us/en/training/

Palo Alto Networks

https://www.paloaltonetworks.com/services/education

Week 2

IP Addressing - The Basics of Binary

Networking Fundamentals: IP Addressing – The Basics of Binary

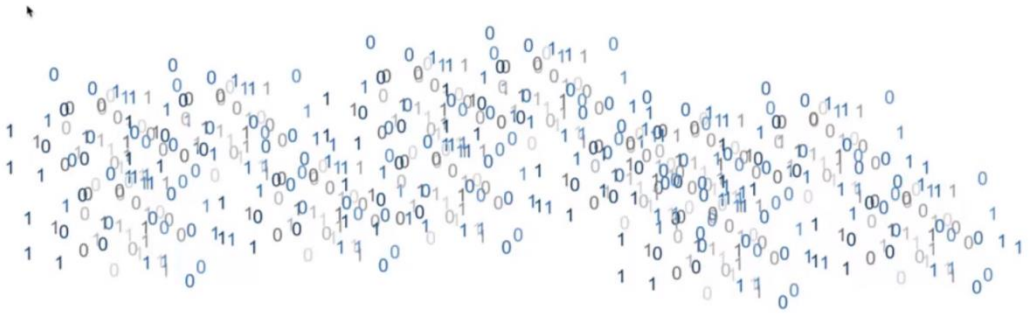
Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security

0:20 / 8:52

Binary System

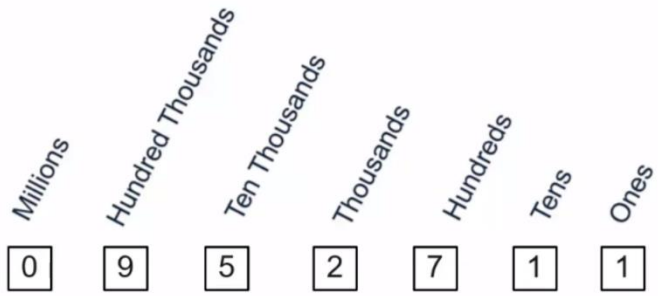
- Human beings think in terms of 10 based (decimal) numbering because we have 10 fingers/toes.
- Computers only know if the power is on (1) or off (0).
- Computers they don't know any other state.



Source: https://learningportal.ibmcpe.net/

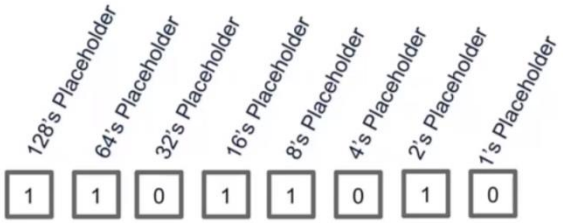
0:37 / 8:52

Decimal



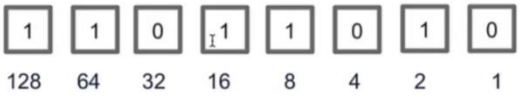
1:27 / 8:52

Binary



- Everyplace holder is twice the value of the previous placeholder.

Convert from binary to decimal

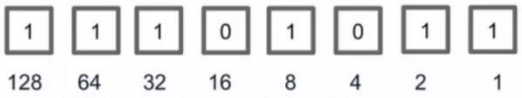


- Every placeholder can have only 2 values zero or one.
- We take the value of the placeholders, we multiple it times placeholder and then add up all the placeholders.
- 1x128 1x64 0x32 1x16 1x8 0x4 1x2 0x1
- 128 + 64 + 16 + 8 + 2 = 218

2:22 / 8:52

Convert from decimal to binary

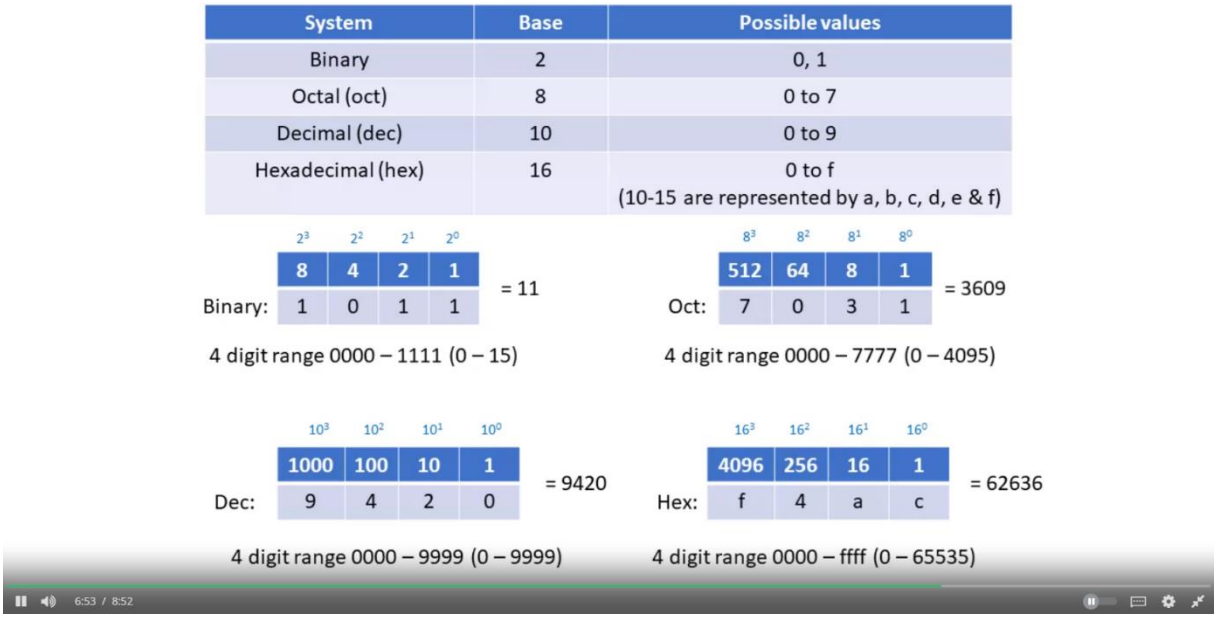
235



- Can I subtract **128** from 235? Yes 235 – 128 = **107**
- Can I subtract **64** from 107? Yes 107 – 64 = **43**
- Can I subtract **32** from 43? Yes 43 – 32 = 11
- Can I subtract **16** from 11? No
- Can I subtract **8** from 11? Yes 11 – 8 = **3**
- Can I subtract **4** from 3? No
- Can I subtract **2** from 3? Yes 3 – 2 = 1
- Can I subtract **1** from 1? Yes 1 - 1 = **0**

11101011

2:34 / 8:52



IP Address Structure and Network Classes

IP Protocol

IPv4 is a 32 bits address divided in four octets.

From 0.0.0.0 to 255.255.255.255

IPv4 has 4,294,967,296 possible addresses in its address space.

Decimal	Binary
10.195.121.10	00001010.11000011.01111001.00001010

00001010.11000011.01111001.	00001010
Network Portion	Host portion

0:26 / 5:06

Classful Addressing

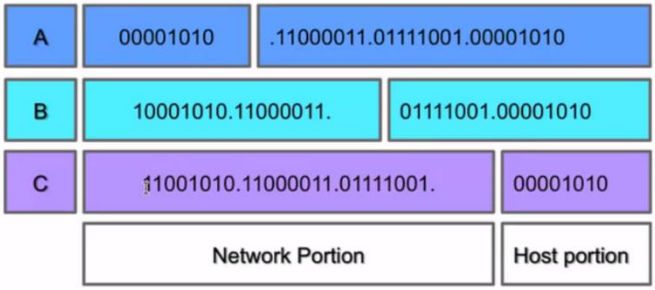
When the Internet's address structure was originally defined, every unicast IP address had a *network* portion, to identify the network on which the interface using the IP address was to be found, and a *host* portion, used to identify the particular host on the network given in the network portion.

The partitioning of the address space involved five *classes*. Each class represented a different trade-off in the number of bits of a 32-bit IPv4 address devoted to the network number versus the number of bits devoted to the host number.

Class	Address Range	Use	Default mask
A	0.0.0.0 – 127.255.255.255	Unicast/Special	255.0.0.0
B	128.0.0.0 – 191.255.255.255	Unicast/Special	255.255.0.0
C	192.0.0.0 – 223.0.0.0	Unicast/Special	255.255.255.0
D	224.0.0.0 – 239.255.255.255	Multicast	N/A
E	240.0.0.0 – 255.255.255.255	Reserved	N/A

3:45 / 5:06

Classful Addressing



IP Protocol (Internet Protocol)

- Layer 3 devices use the IP address to identify the destination of the traffic, also devices like stateful firewalls use it to identify where traffic has come from.
- IP addresses are represented in quad dotted notation, for example, 10.195.121.10.
- Each of the numbers is a nonnegative integer from 0 to 255 and represents one-quarter of the whole IP address.
- A routable protocol is a protocol whose packets may leave your network, pass through your router, and be delivered to a remote network.

0 - 255 base 10

00000000 - 11111111 base 2

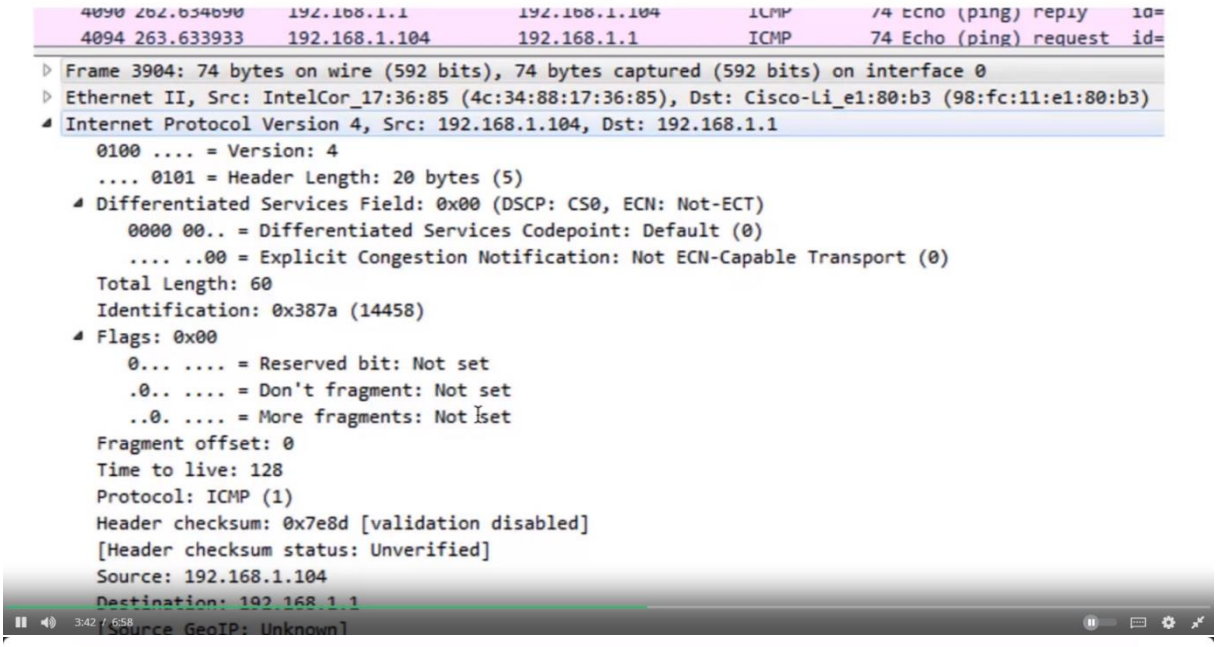
Be familiar with IP addresses, subnet masks and default gateways !!!

1:23 / 6:58

IP Protocol

Version	IHL	Service Type	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding
Payload				

1:58 / 6:58



Network Mask

- The *subnet mask* is an assignment of bits used by a host or router to determine how the network and subnetwork information is partitioned from the host information in a corresponding IP address.
- It is possible to use a shorthand format for expressing masks that simply gives the number of contiguous 1 bits in the mask (starting from the left). This format is now the most common format and is sometimes called the prefix length.
- The number of bits occupied by the network portion.
- Masks are used by routers and hosts to determine where the network/subnetwork portion of an IP address ends and the host part begins.

4:16 / 6:58

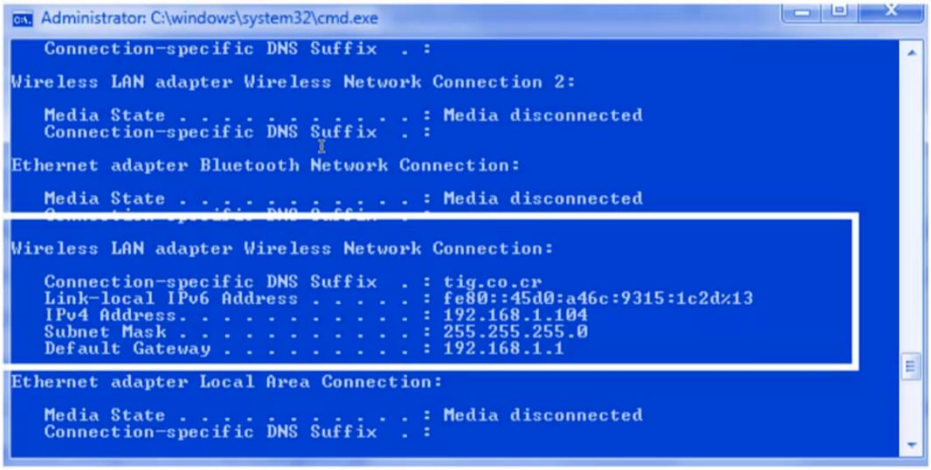
Network Mask

- The *subnet mask* is an assignment of bits used by a host or router to determine how the network and subnetwork information is partitioned from the host information in a corresponding IP address.
- It is possible to use a shorthand format for expressing masks that simply gives the number of contiguous 1 bits in the mask (starting from the left). This format is now the most common format and is sometimes called the prefix length.
- The number of bits occupied by the network portion.
- Masks are used by routers and hosts to determine where the network/subnetwork portion of an IP address ends and the host part begins.

192.168.52.3/24

4:47 / 6:58

Default Gateway



5:57 / 6:58

Broadcast Addresses

In each IPv4 subnet, a special address is reserved to be the subnet broadcast address. The subnet broadcast address is formed by setting the network/subnet portion of an IPv4 address to the appropriate value and all the bits in the Host portion to 1.

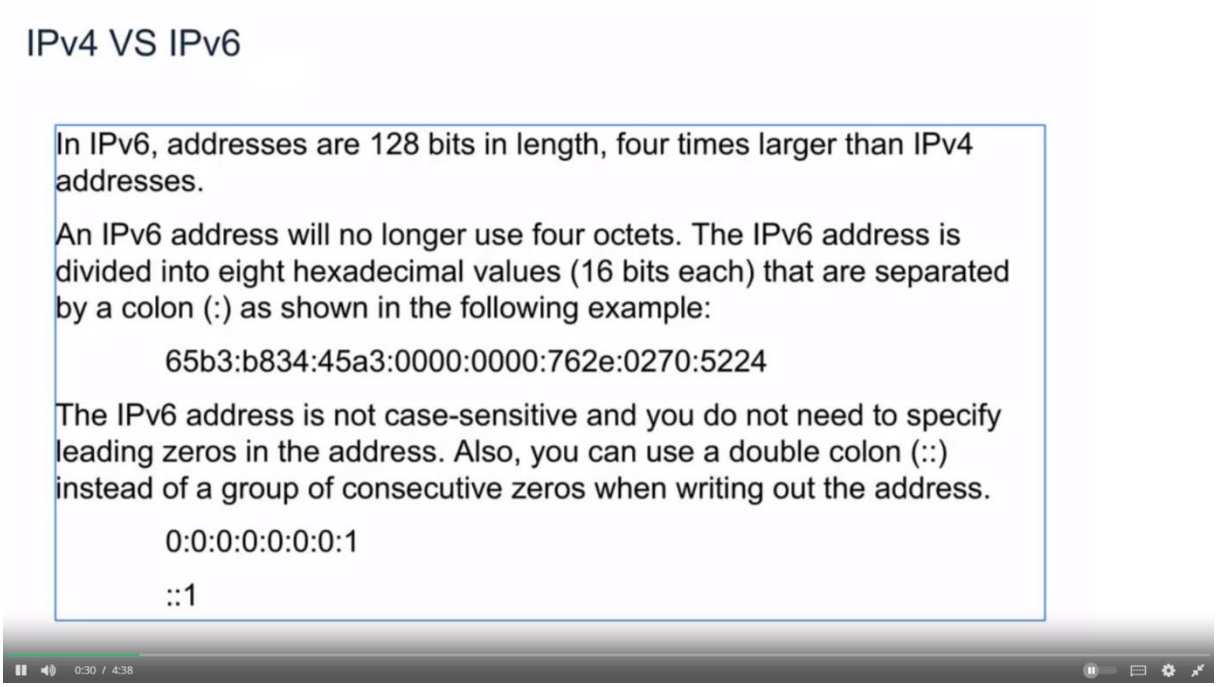
IP Address	00001010.11000011.01111001.	00001010
Broadcast Address	00001010.11000011.01111001.	11111111
	Network Portion	Host portion

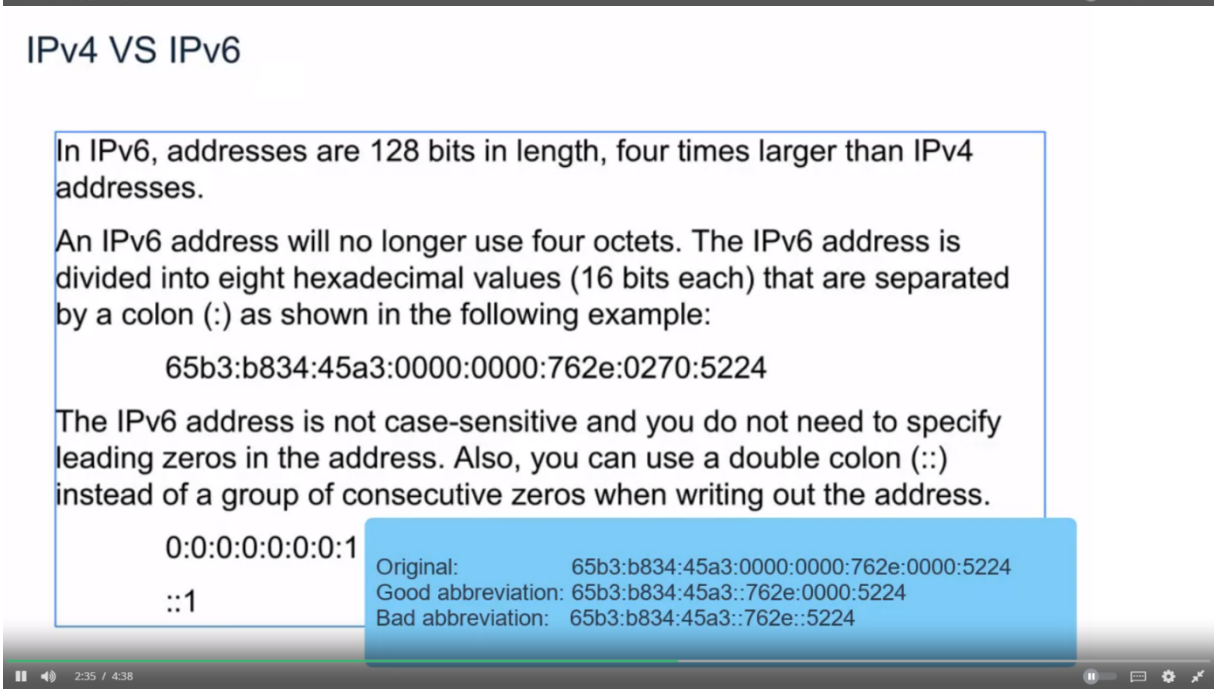
6:21 / 6:58

```
[root@server100 ~]# ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:30:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.52.3/24 brd 192.168.52.255 scope global noprefixroute dynamic enp0s3
       valid_lft 1140sec preferred_lft 1140sec
    inet 192.168.52.100/24 brd 192.168.52.255 scope global secondary enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::7f98:fcca:54d3:b511/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@server100 ~]# ip route show
default via 192.168.52.4 dev enp0s3
169.254.0.0/16 dev enp0s3 scope link metric 1002
192.168.52.0/24 dev enp0s3 proto kernel scope link src 192.168.52.3 metric 100
192.168.52.0/24 dev enp0s3 proto kernel scope link src 192.168.52.100 metric 100
[root@server100 ~]#
```

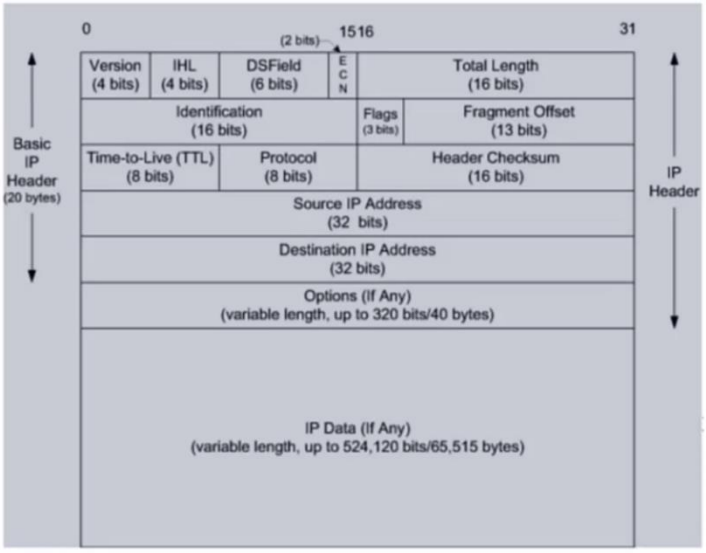
6:44 / 6:58

Introduction to the IPv6 Address Schema

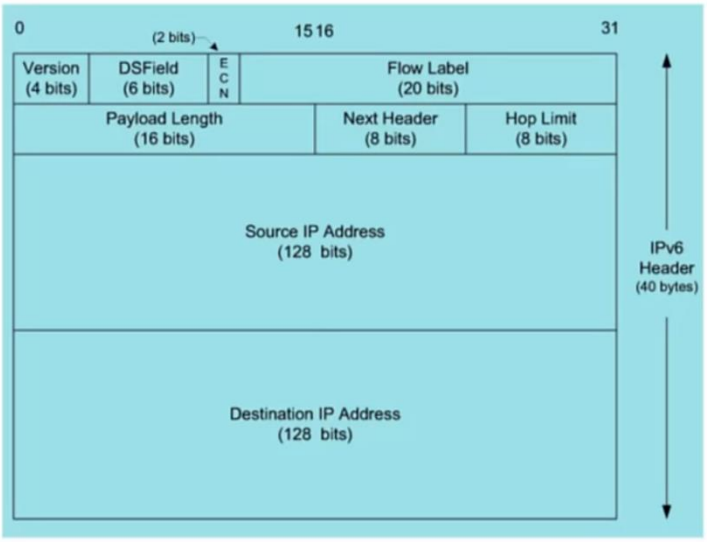


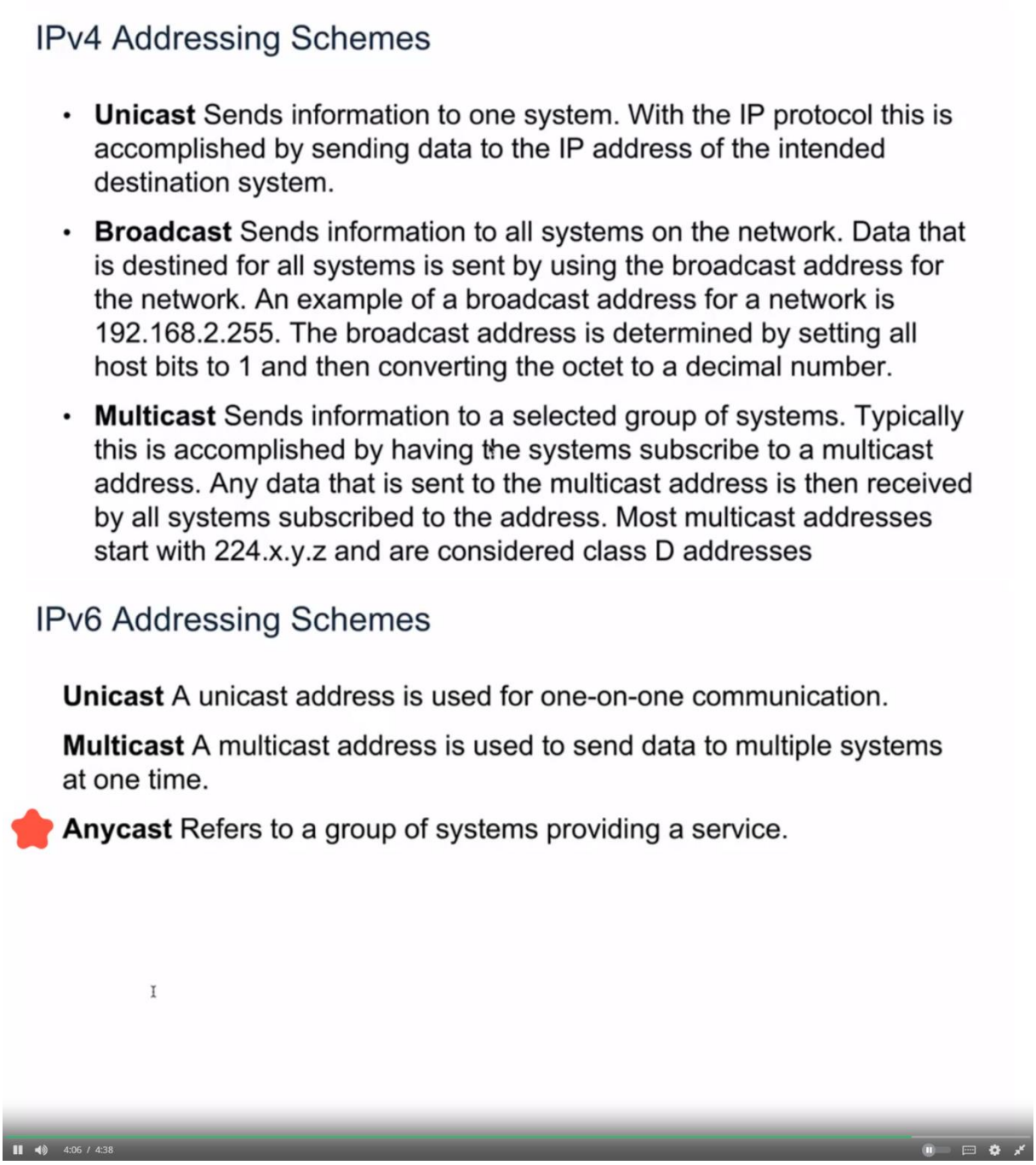


IPv4 Header



IPv6 header





Application and Transport Protocols UDP and TCP, Part 1

Networking Fundamentals Application and Transport Protocols

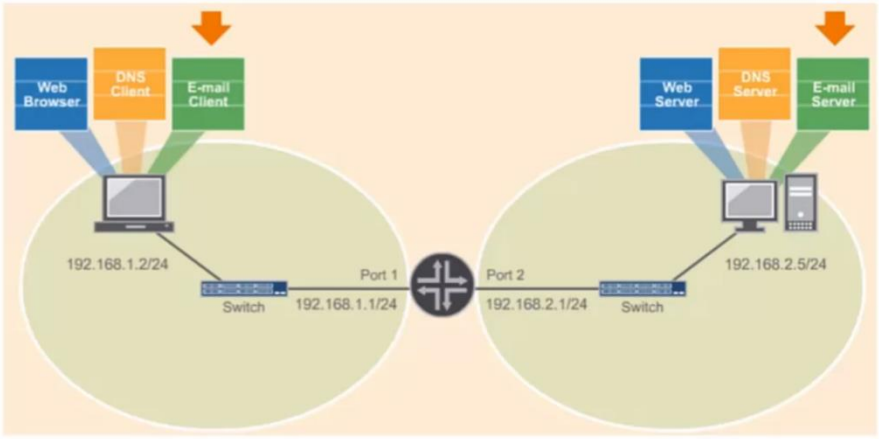
Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security

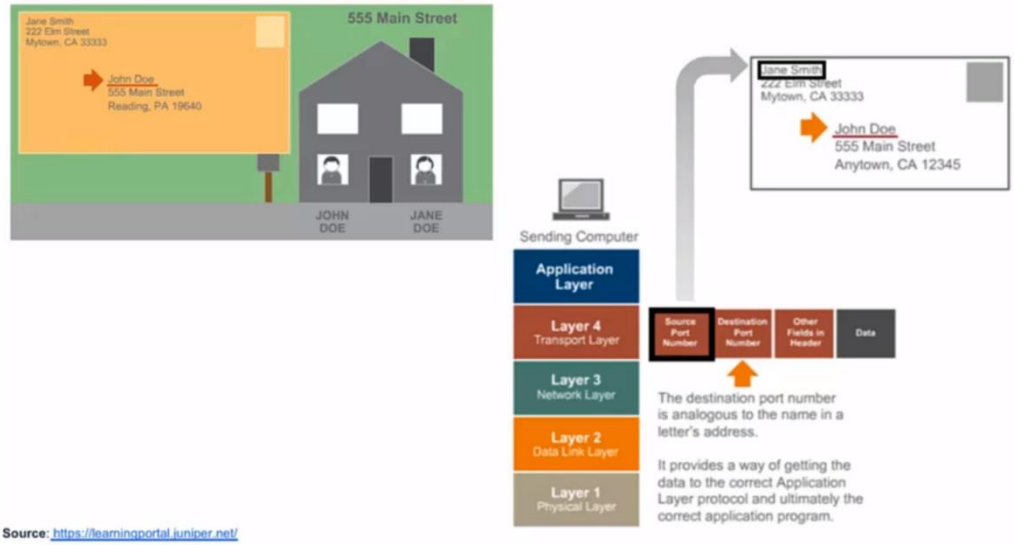
0:21 / 5:03

Objectives

- Understand the differences between TCP and UDP.

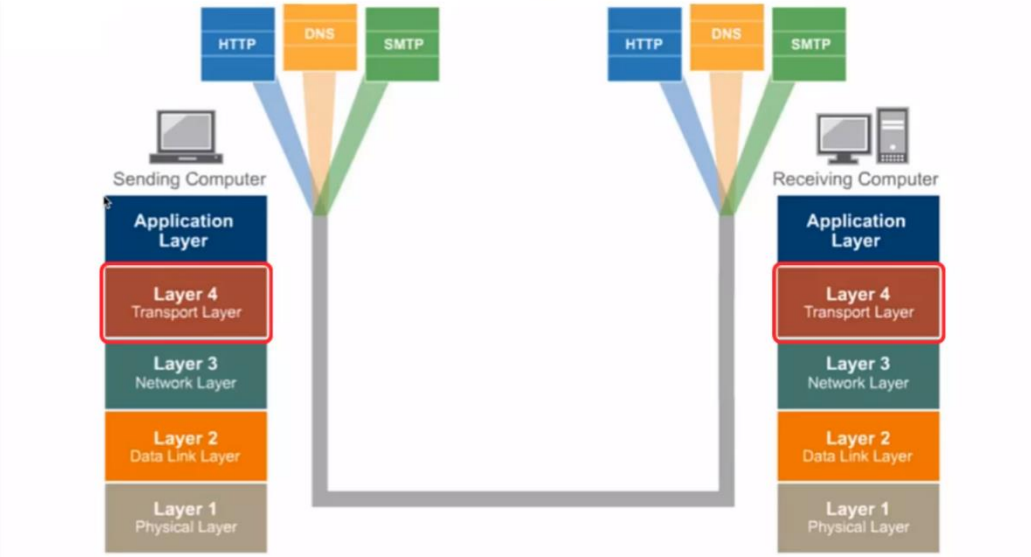


Overview of the Transport Layer Protocols

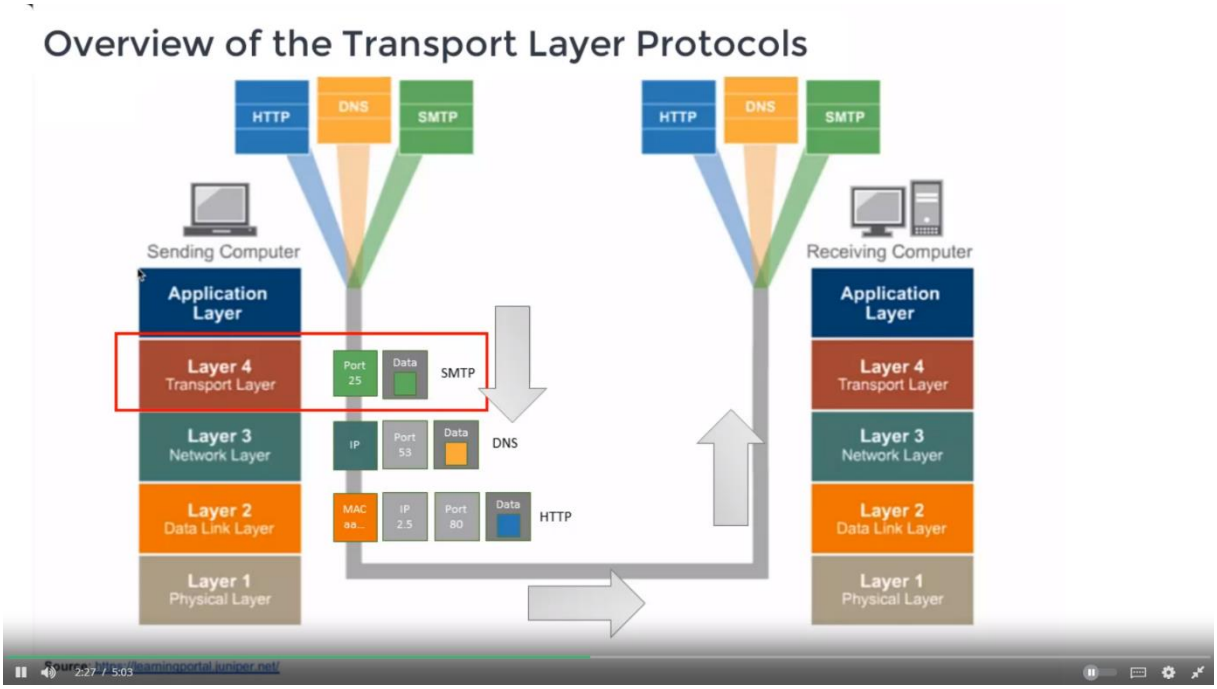


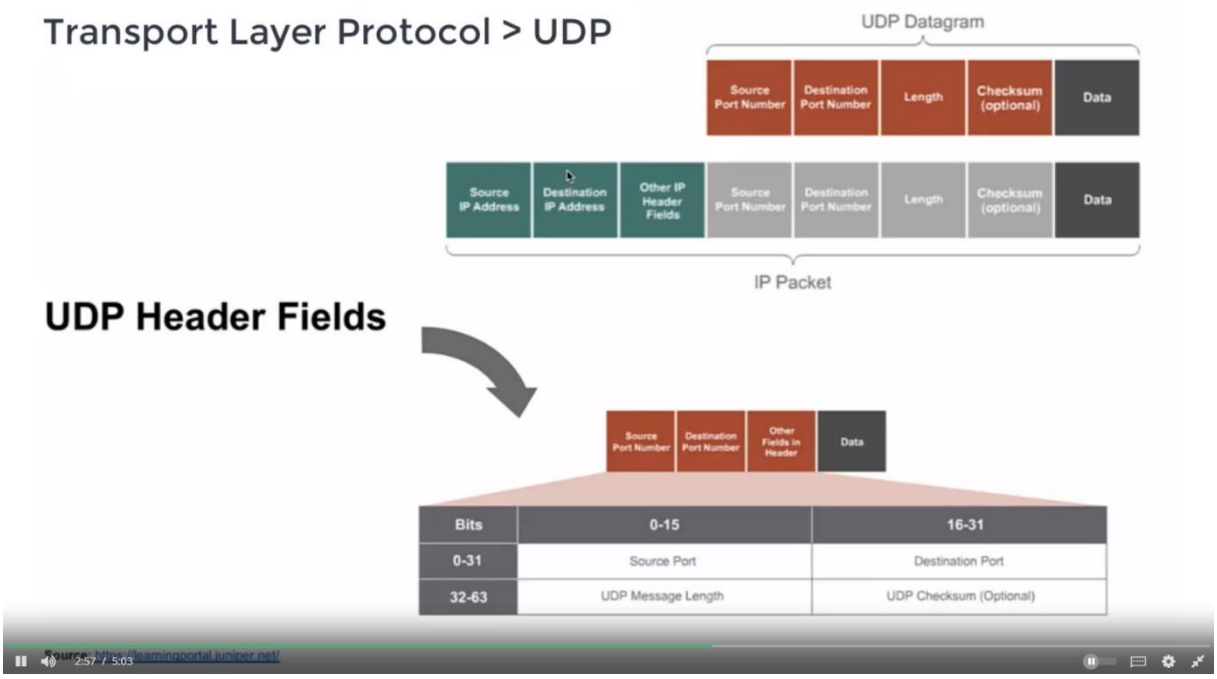
Source: https://learningportal.juniper.net/

Overview of the Transport Layer Protocols

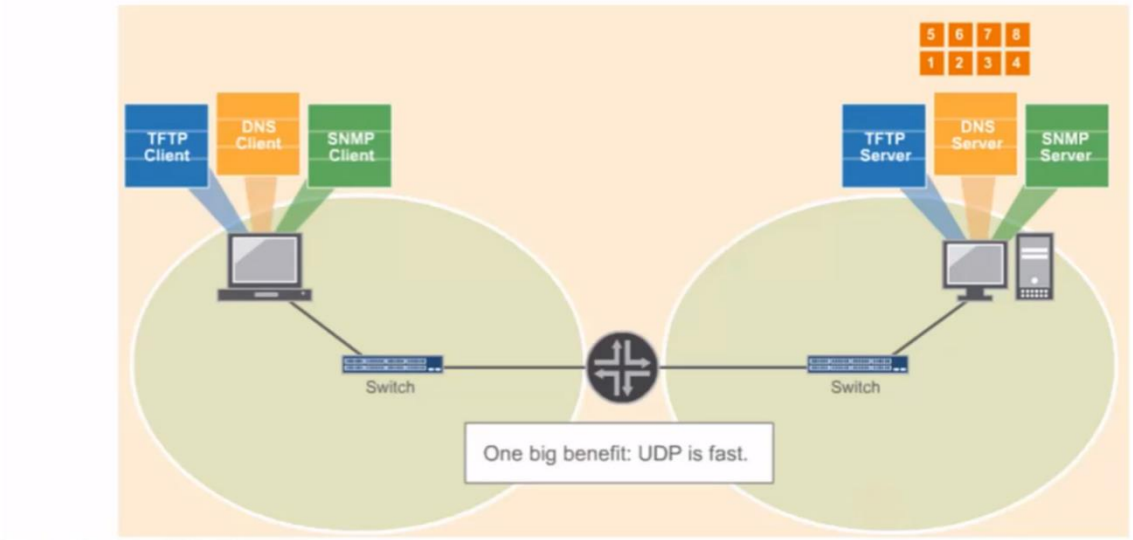


Source: https://learningportal.juniper.net/


Overview of the Transport Layer Protocols
HTTP
DNS
SMTP
Sending Computer
Application Layer
Layer 4 Transport Layer
Layer 3 Network Layer
Layer 2 Data Link Layer
Layer 1 Physical Layer
Port 25
Data
SMTP
IP
Port 53
Data
DNS
MAC aa...
IP 2.5
Port 80
Data
HTTP
Receiving Computer
Application Layer
Layer 4 Transport Layer
Layer 3 Network Layer
Layer 2 Data Link Layer
Layer 1 Physical Layer
2:27 / 5:03

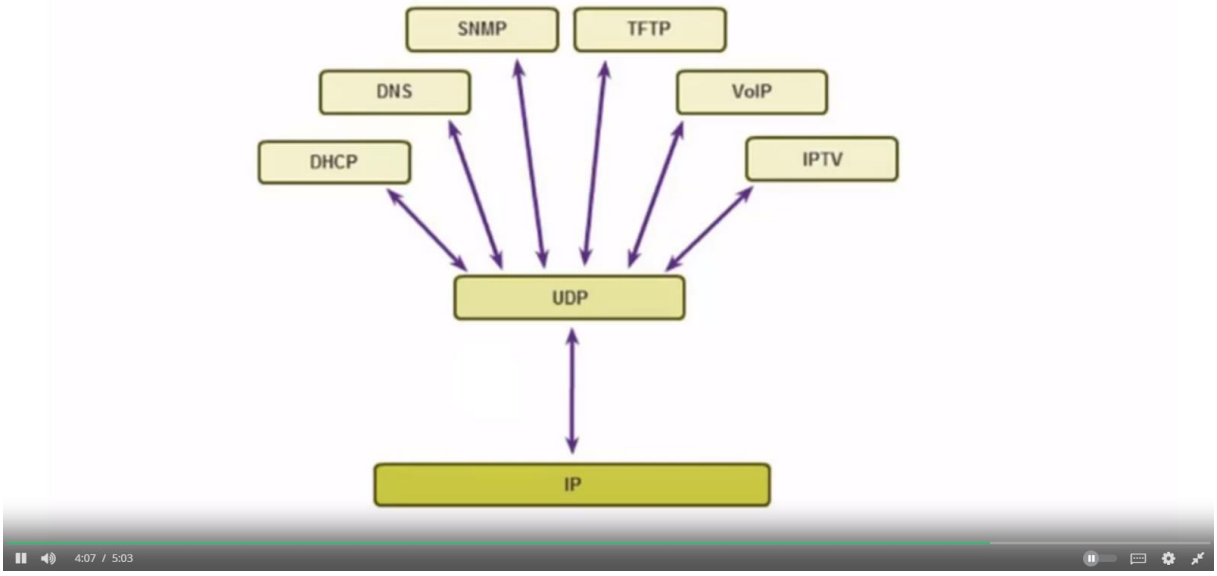

Transport Layer Protocol > UDP
UDP Datagram
Source Port Number
Destination Port Number
Length
Checksum (optional)
Data
Source IP Address
Destination IP Address
Other IP Header Fields
Source Port Number
Destination Port Number
Length
Checksum (optional)
Data
IP Packet
UDP Header Fields
Source Port Number
Destination Port Number
Other Fields in Header
Data
Bits
0-15
16-31
0-31
Source Port
Destination Port
32-63
UDP Message Length
UDP Checksum (Optional)
2:57 / 5:03

Transport Layer Protocol > UDP



Source: https://learningportal.juniper.net/

Transport Layer Protocol > UDP



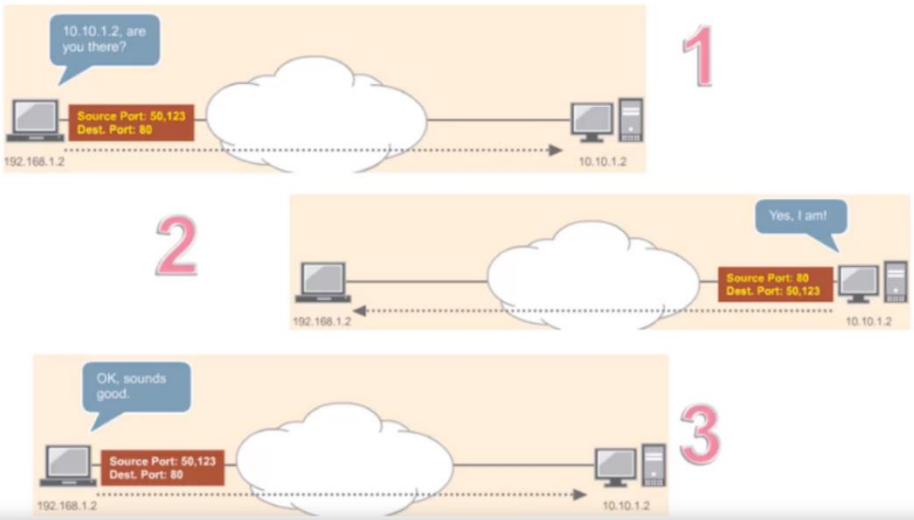
Application and Transport Protocols UDP and TCP, Part 2

Transport Layer Protocol > Overview of TCP

Source: https://learningportal.juniper.net/

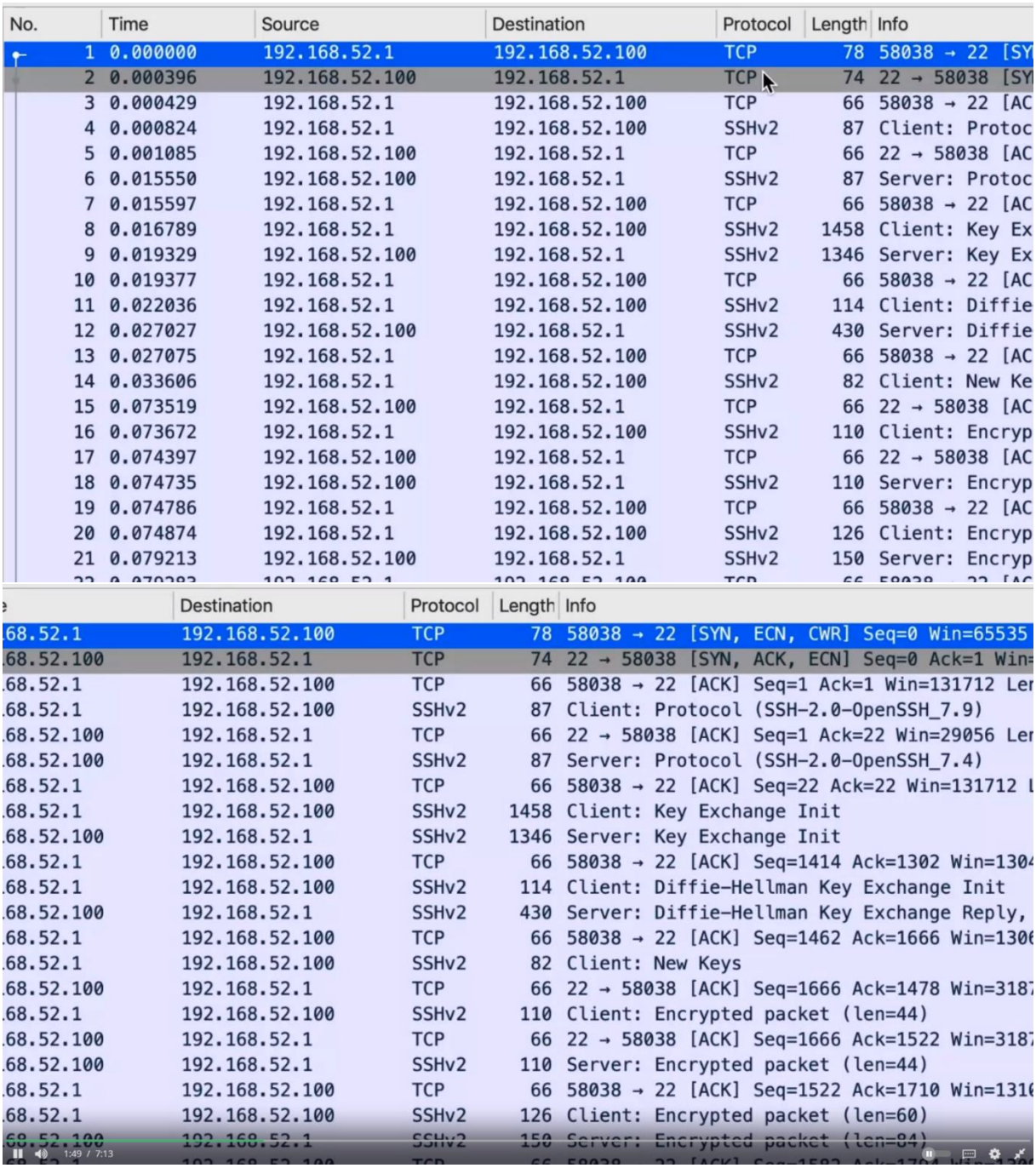
0:34 / 7:13

Transport Layer Protocol > Overview of TCP



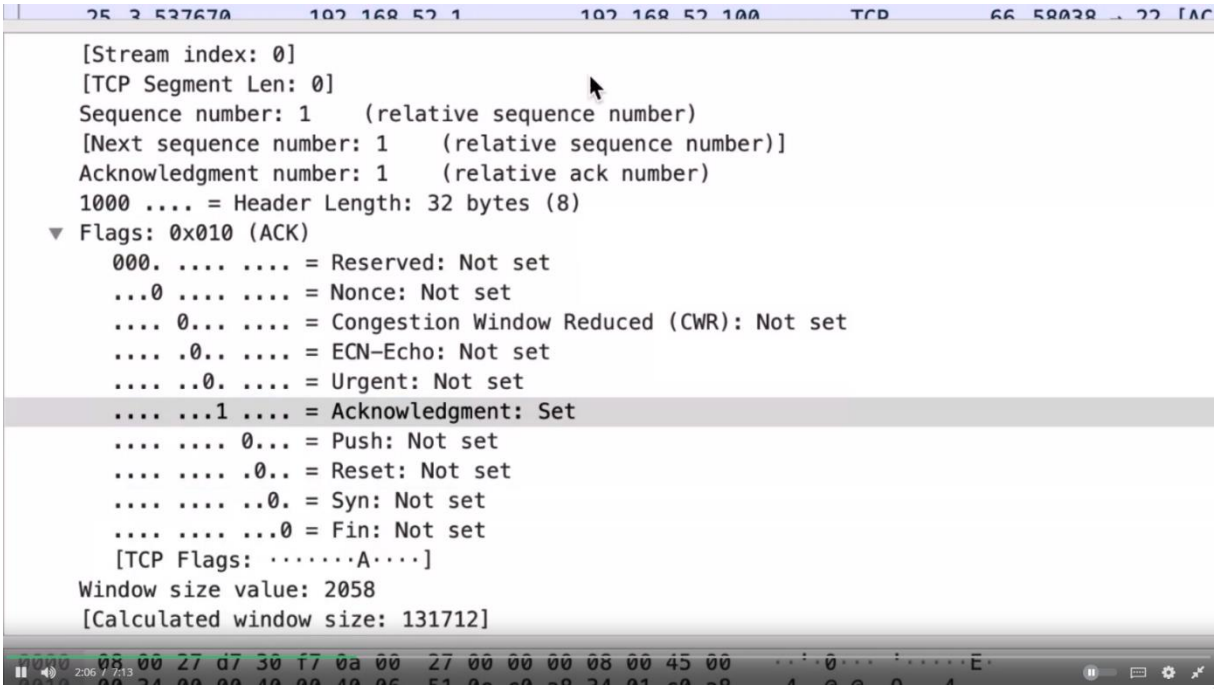
Source: https://learningportal.juniper.net/

1:05 / 7:13



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.52.1	192.168.52.100	TCP	78	58038 → 22 [SY
2	0.000396	192.168.52.100	192.168.52.1	TCP	74	22 → 58038 [SY
3	0.000429	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [AC
4	0.000824	192.168.52.1	192.168.52.100	SSHv2	87	Client: Protoc
5	0.001085	192.168.52.100	192.168.52.1	TCP	66	22 → 58038 [AC
6	0.015550	192.168.52.100	192.168.52.1	SSHv2	87	Server: Protoc
7	0.015597	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [AC
8	0.016789	192.168.52.1	192.168.52.100	SSHv2	1458	Client: Key Ex
9	0.019329	192.168.52.100	192.168.52.1	SSHv2	1346	Server: Key Ex
10	0.019377	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [AC
11	0.022036	192.168.52.1	192.168.52.100	SSHv2	114	Client: Diffie
12	0.027027	192.168.52.100	192.168.52.1	SSHv2	430	Server: Diffie
13	0.027075	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [AC
14	0.033606	192.168.52.1	192.168.52.100	SSHv2	82	Client: New Ke
15	0.073519	192.168.52.100	192.168.52.1	TCP	66	22 → 58038 [AC
16	0.073672	192.168.52.1	192.168.52.100	SSHv2	110	Client: Encryp
17	0.074397	192.168.52.100	192.168.52.1	TCP	66	22 → 58038 [AC
18	0.074735	192.168.52.100	192.168.52.1	SSHv2	110	Server: Encryp
19	0.074786	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [AC
20	0.074874	192.168.52.1	192.168.52.100	SSHv2	126	Client: Encryp
21	0.079213	192.168.52.100	192.168.52.1	SSHv2	150	Server: Encryp

e	Destination	Protocol	Length	Info
68.52.1	192.168.52.100	TCP	78	58038 → 22 [SYN, ECN, CWR] Seq=0 Win=65535
68.52.100	192.168.52.1	TCP	74	22 → 58038 [SYN, ACK, ECN] Seq=0 Ack=1 Win=
68.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK] Seq=1 Ack=1 Win=131712 Len
68.52.1	192.168.52.100	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_7.9)
68.52.100	192.168.52.1	TCP	66	22 → 58038 [ACK] Seq=1 Ack=22 Win=29056 Len
68.52.100	192.168.52.1	SSHv2	87	Server: Protocol (SSH-2.0-OpenSSH_7.4)
68.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK] Seq=22 Ack=22 Win=131712 L
68.52.1	192.168.52.100	SSHv2	1458	Client: Key Exchange Init
68.52.100	192.168.52.1	SSHv2	1346	Server: Key Exchange Init
68.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK] Seq=1414 Ack=1302 Win=1304
68.52.1	192.168.52.100	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
68.52.100	192.168.52.1	SSHv2	430	Server: Diffie-Hellman Key Exchange Reply,
68.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK] Seq=1462 Ack=1666 Win=1306
68.52.1	192.168.52.100	SSHv2	82	Client: New Keys
68.52.100	192.168.52.1	TCP	66	22 → 58038 [ACK] Seq=1666 Ack=1478 Win=3187
68.52.1	192.168.52.100	SSHv2	110	Client: Encrypted packet (len=44)
68.52.100	192.168.52.1	TCP	66	22 → 58038 [ACK] Seq=1666 Ack=1522 Win=3187
68.52.100	192.168.52.1	SSHv2	110	Server: Encrypted packet (len=44)
68.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK] Seq=1522 Ack=1710 Win=1310
68.52.1	192.168.52.100	SSHv2	126	Client: Encrypted packet (len=60)
68.52.100	192.168.52.1	SSHv2	150	Server: Encrypted packet (len=84)

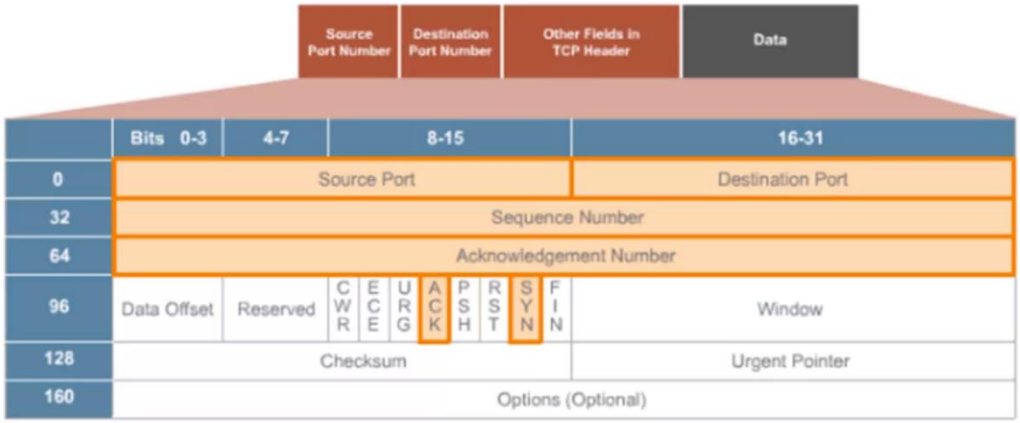


Transport Layer Protocol > Overview of TCP

UDP	TCP
Multiplexes data using ports	Multiplexes data using ports
Connectionless	Connection-oriented
Unreliable	Reliable
Unordered data; duplicates possible	Ordered data; duplicate detection
Datagrams	Segments
No flow control	Flow control

Source: https://learningportal.juniper.net/

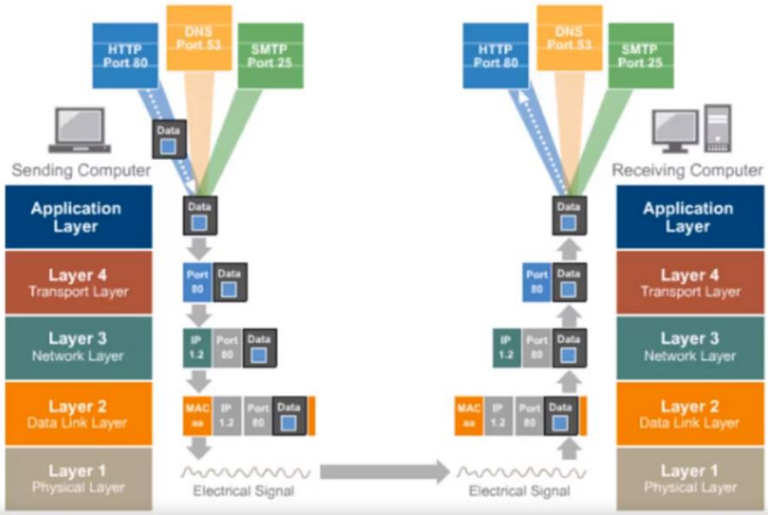
Transport Layer Protocol > TCP In Action



Source: https://learningportal.juniper.net/

4:23 / 7:13

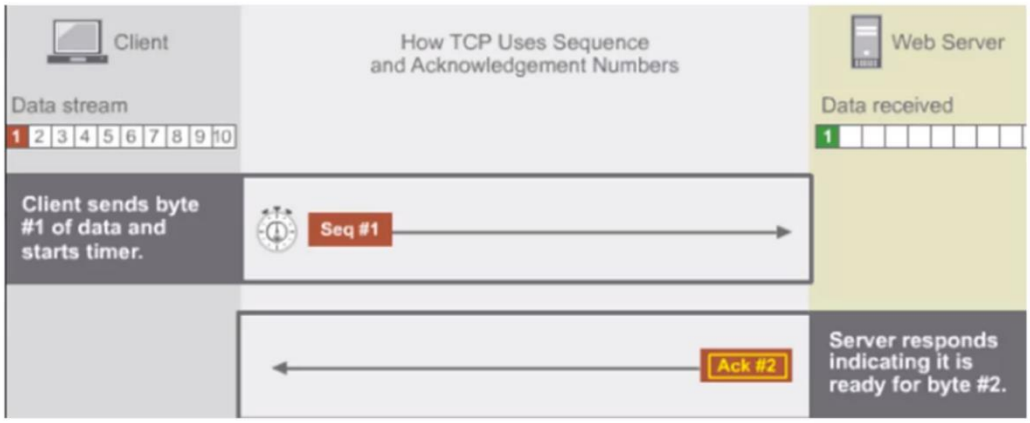
Transport Layer Protocol > TCP In Action



Source: https://learningportal.juniper.net/

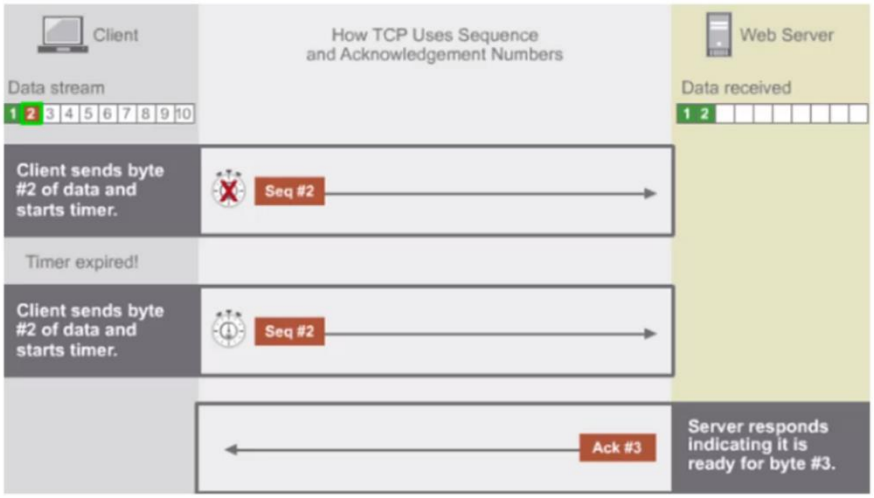
5:21 / 7:13

Transport Layer Protocol > TCP In Action

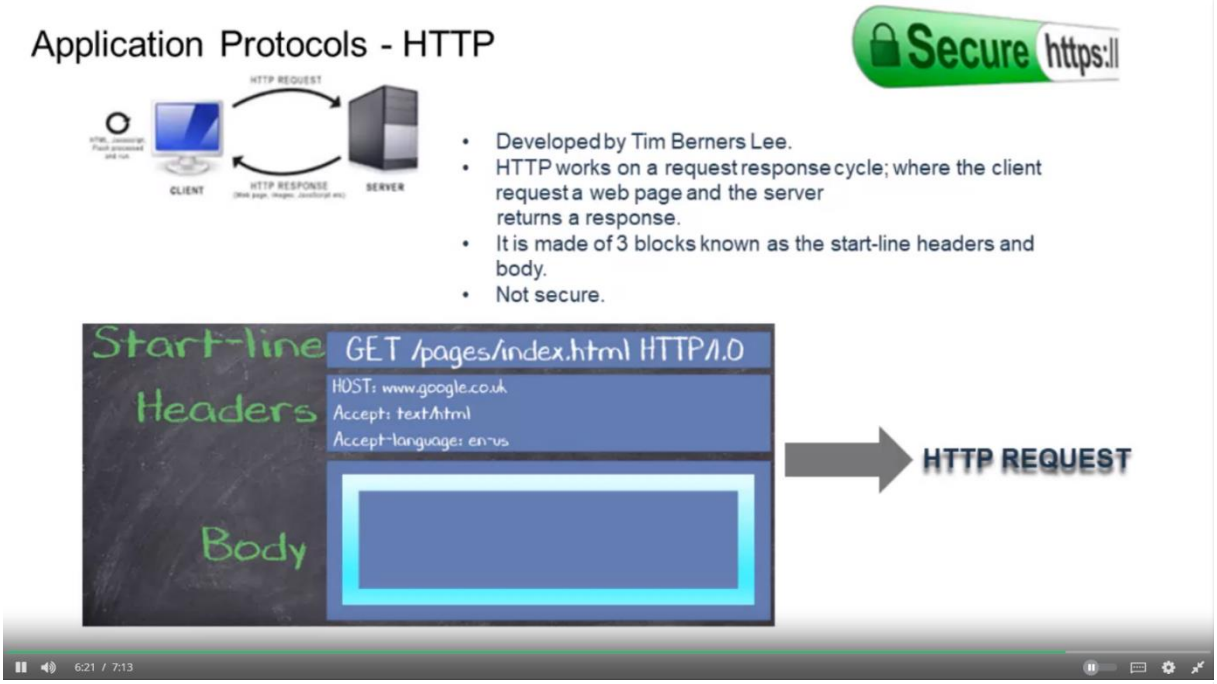


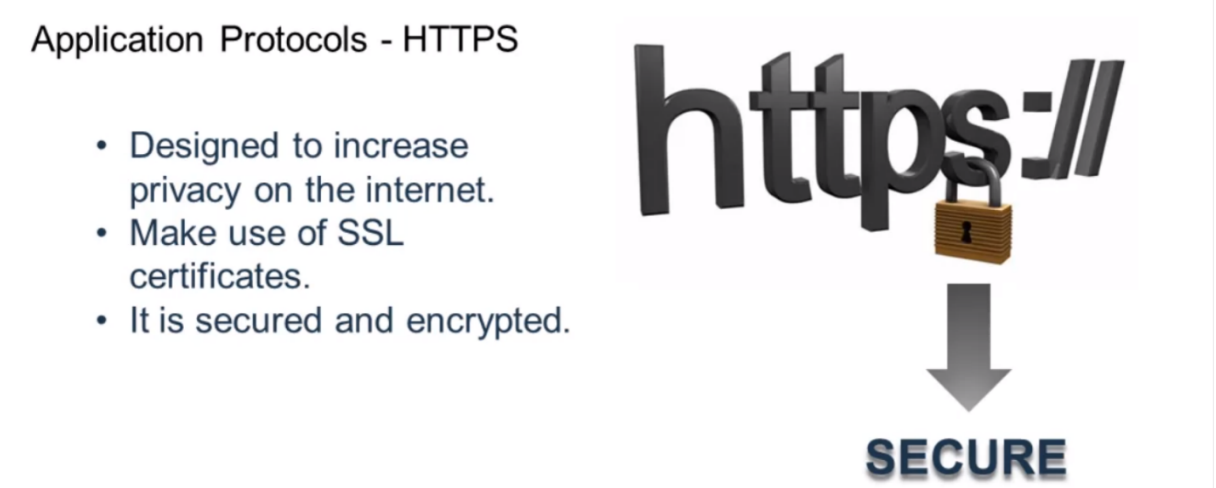
Source: https://learningportal.juniper.net/

Transport Layer Protocol > TCP In Action

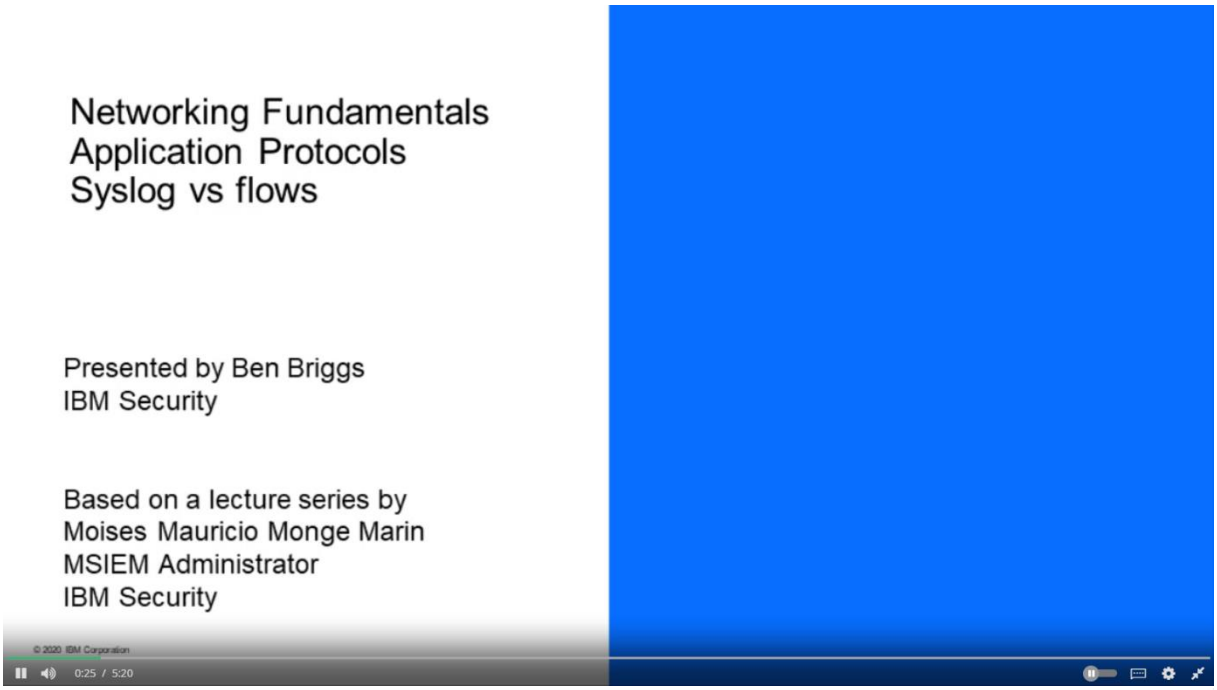


Source: https://learningportal.juniper.net/


Application Protocols - HTTP
Secure https://
HTTP REQUEST
HTTP RESPONSE
CLIENT
SERVER
Developed by Tim Berners Lee.
HTTP works on a request response cycle; where the client request a web page and the server returns a response.
It is made of 3 blocks known as the start-line headers and body.
Not secure.
Start-line
GET /pages/index.html HTTP/1.0
Headers
HOST: www.google.co.uk
Accept: text/html
Accept-language: en-us
Body
HTTP REQUEST
6:21 / 7:13


Application Protocols - HTTPS
Designed to increase privacy on the internet.
Make use of SSL certificates.
It is secured and encrypted.
https://
SECURE

DNS and DHCP



Doman Name System

```
round-trip min/avg/max/stddev = 51.109/56.688/65.404/5.211 ms
Moisess-MacBook:~ MoisesM$ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
domain hitronhub.home
nameserver 192.168.0.1
Moisess-MacBook:~ MoisesM$
```

1:26 / 5:20

Dynamic Host Configuration Protocol

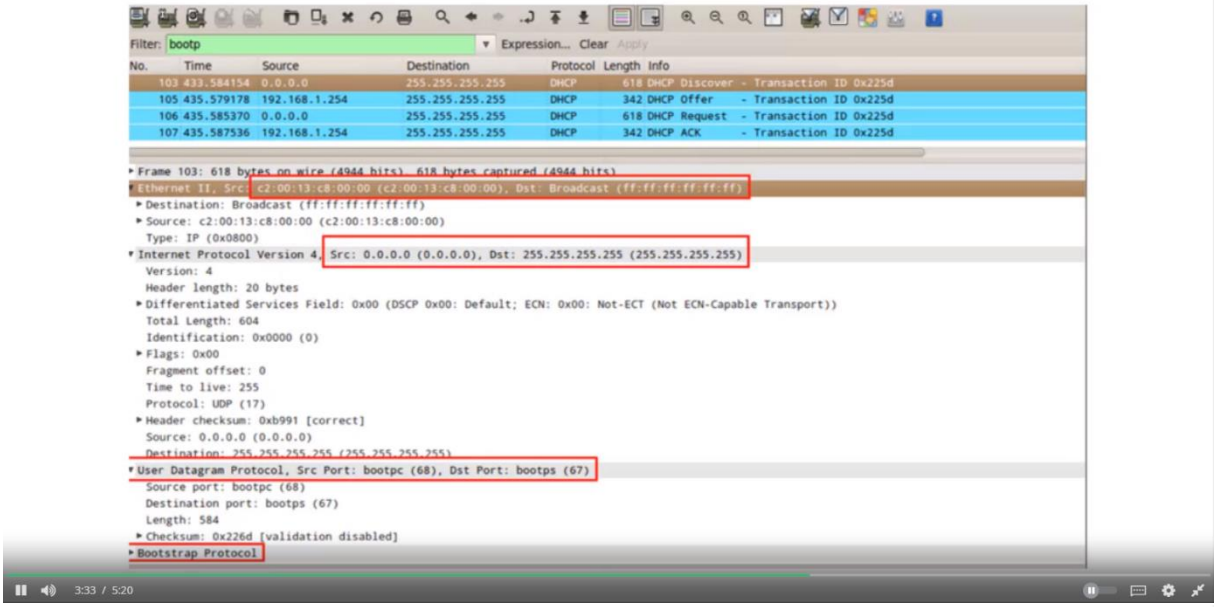
DHCP Discover (Broadcast)

DHCP Offer (Unicast/Broadcast)

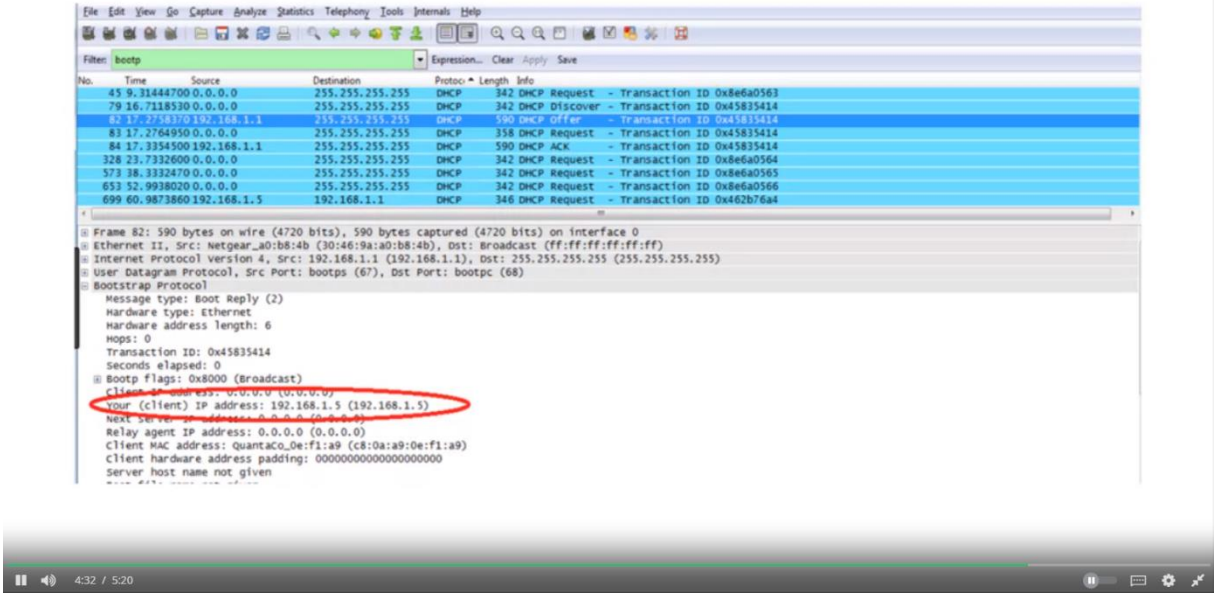
DHCP Request (Broadcast)

DHCP Ack (Unicast/Broadcast)

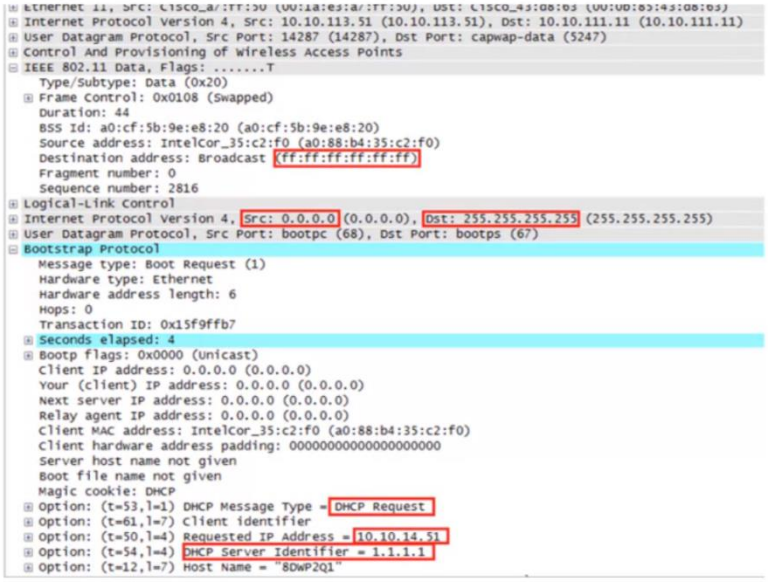
DHCP Discover



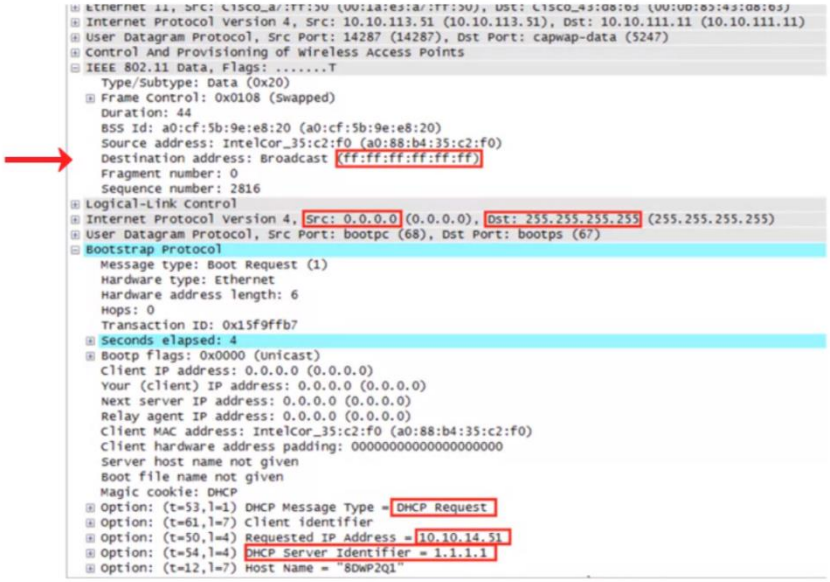
DHCP offer



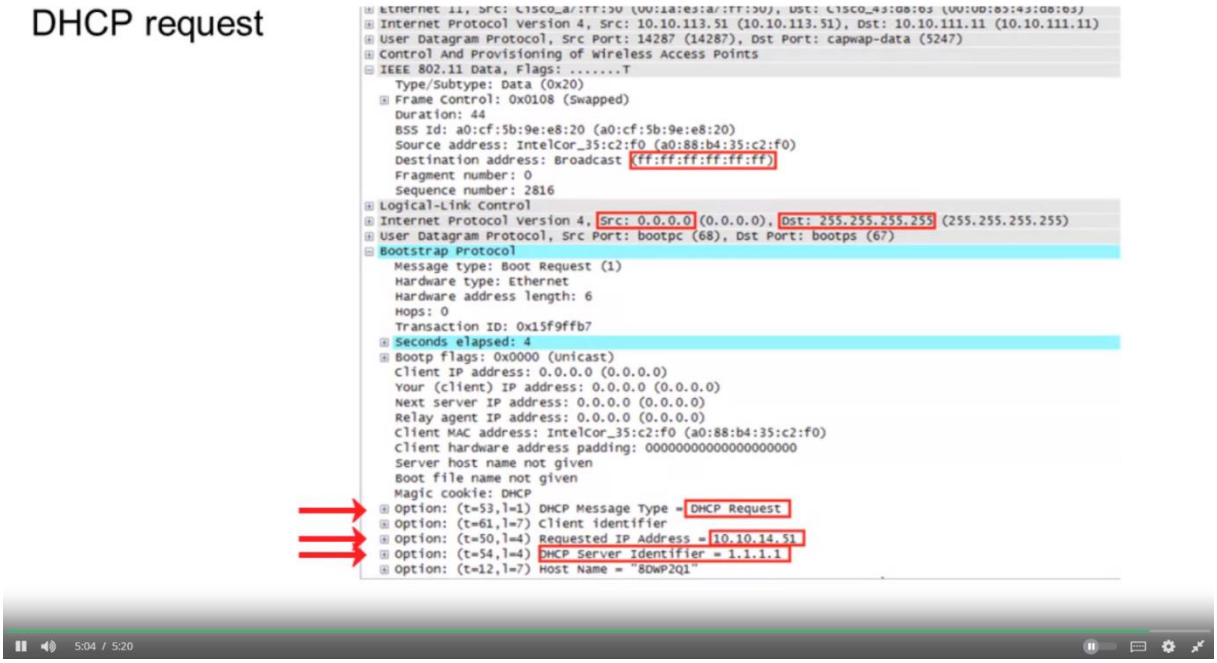
DHCP request



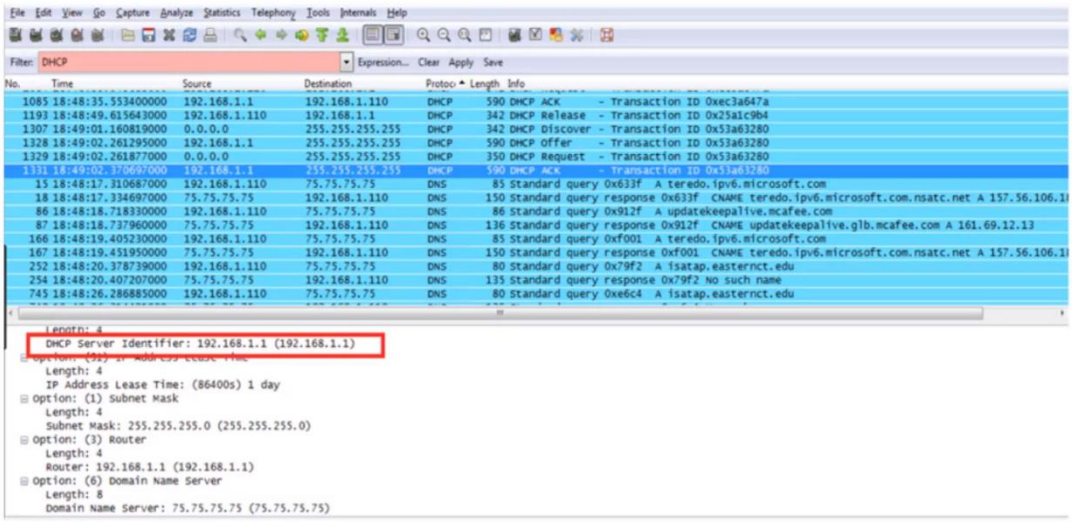
DHCP request



DHCP request



DHCP Ack



Syslog Message Logging Protocol

The syslog protocol

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

Used for:

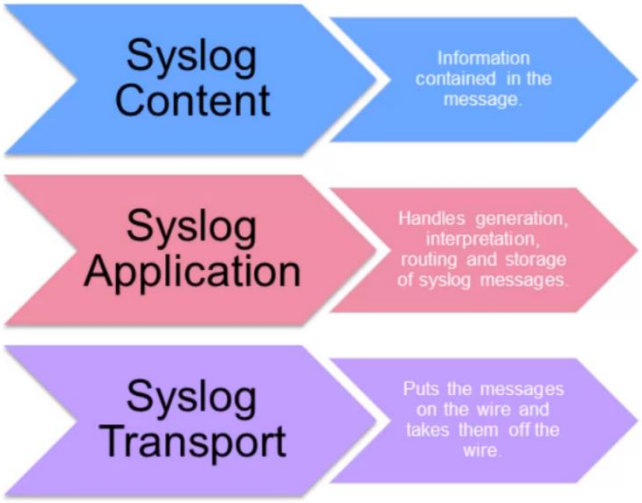
- system management
- security auditing
- general informational
- analysis, and debugging messages.

Used to convey event notification messages.

Provides a message format that allows vendor-specific extensions to be provided in a structured way.

0:24 / 4:21

Syslog utilizes three layers:



0:58 / 4:21

Functions are performed at each conceptual layer:

- An "**originator**" generates syslog content to be carried in a message. (Router, server, switch, network device, etc)
- A "**collector**" gathers syslog content for further analysis. – Syslog Server.
- A **"relay"** forwards messages, accepting messages from originators or other relays and sending them to collectors or other relays. – Syslog forwarder.
- A **"transport sender"** passes syslog messages to a specific transport protocol. – most common transport protocol is UDP, defined in the RFC5426.
- A **"transport receiver"** takes syslog messages from a specific transport protocol.

Syslog message components

- The information provided by the originator of a syslog message includes the **facility code** and the **severity level**.
- The syslog software adds information to the information header before passing the entry to the syslog receiver:
  - originator process ID
  - a timestamp
  - the hostname or IP address of the device.

Facility codes

- The facility value indicates which machine process created the message. The Syslog protocol was originally written on BSD Unix, so Facilities reflect the names of UNIX processes and daemons.

- If you are receiving messages from a UNIX system, consider using the User Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

Facility code	Keyword	Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert
15	cron	scheduling daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

Syslog Severity Levels

Value	Severity	Keyword	Description	Examples
0	Emergency	emerg	System is unusable	This level should not be used by applications.
1	Alert	alert	Should be corrected immediately	Loss of the primary ISP connection.
2	Critical	crit	Critical conditions	A failure in the system's primary application.
3	Error	err	Error conditions	An application has exceeded its file storage limit and attempts to write are failing.
4	Warning	warning	May indicate that an error will occur if action is not taken.	A non-root file system has only 2GB remaining.
5	Notice	notice	Events that are unusual, but not error conditions.	
6	Informational	info	Normal operational messages that require no action.	An application has started, paused or ended successfully.
7	Debug	debug	Information useful to developers for debugging the application.	

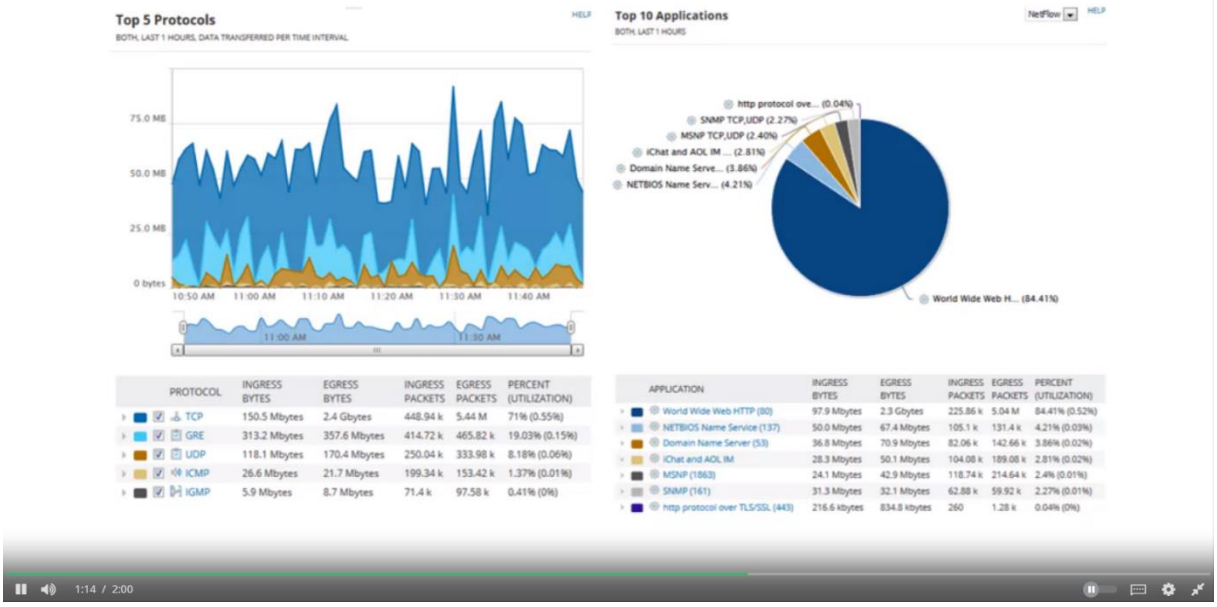
Flows and Network Analysis

What information is gathered in flows?

Usage	• Packet Count • Byte Count	• Source IP Address • Destination IP Address	To/From
Time of the day	• Start sysUpTime • End sysUpTime	• Source TCP/UDP Port • Destination TCP/UDP Port	Application
Port utilization	• Input IfIndex • Output Ifindex	• Type of service • TCP Flags • Protocol	Routing and peering
QoS	• Type of service • TCP Flags • Protocol		

0:26 / 2:00

Network Analysis



1:14 / 2:00

Port Mirroring and Promiscuous Mode

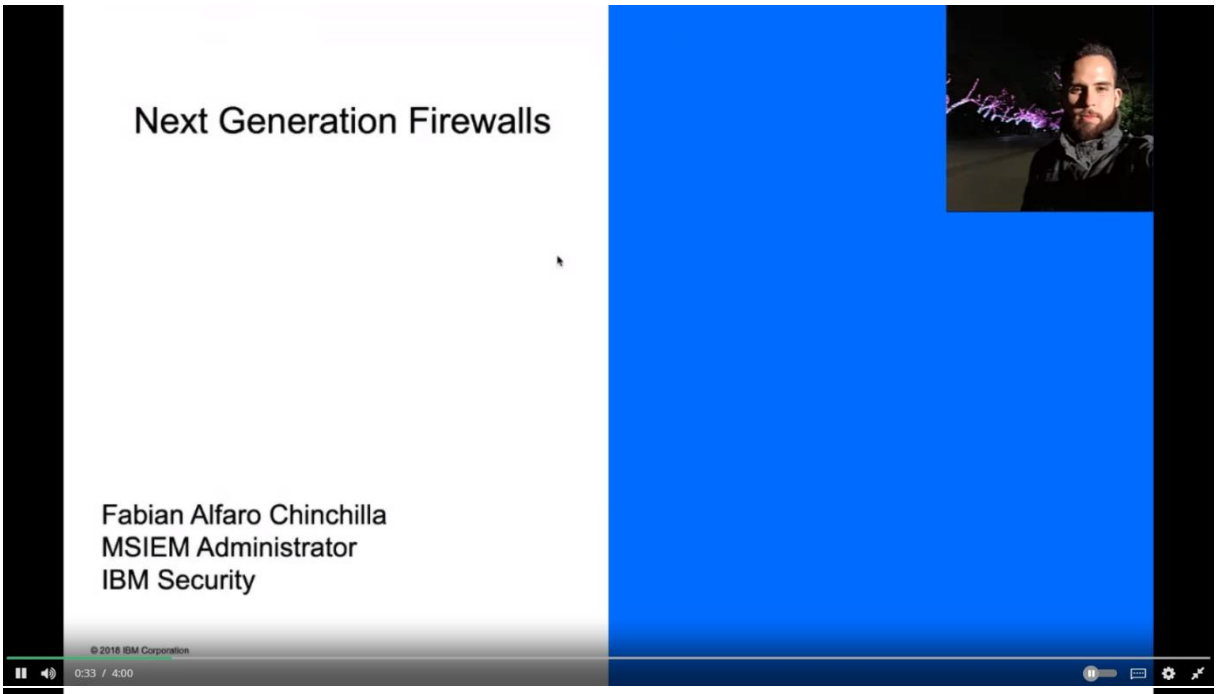
Port mirroring

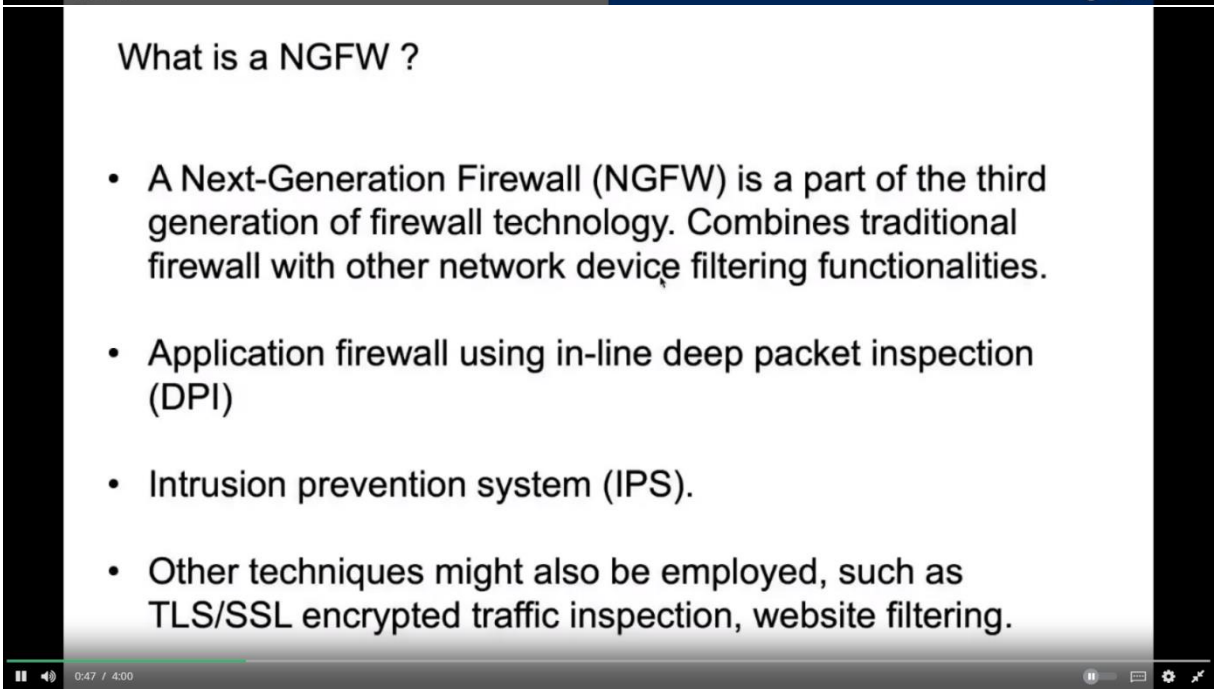
- Sends a copy of network packets traversing on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.
- Port mirroring on a Cisco Systems switch is generally referred to as Switched Port Analyzer (SPAN) or Remote Switched Port Analyzer (RSPAN).
- Other vendors have different names for it, such as Roving Analysis Port (RAP) on 3Com switches.
- This data is used to analyze and debug data or diagnose errors on a network.
- Helps administrators keep a close eye on network performance and alerts them when problems occur.
- It can be used to mirror either inbound or outbound traffic (or both) on one or various interfaces.

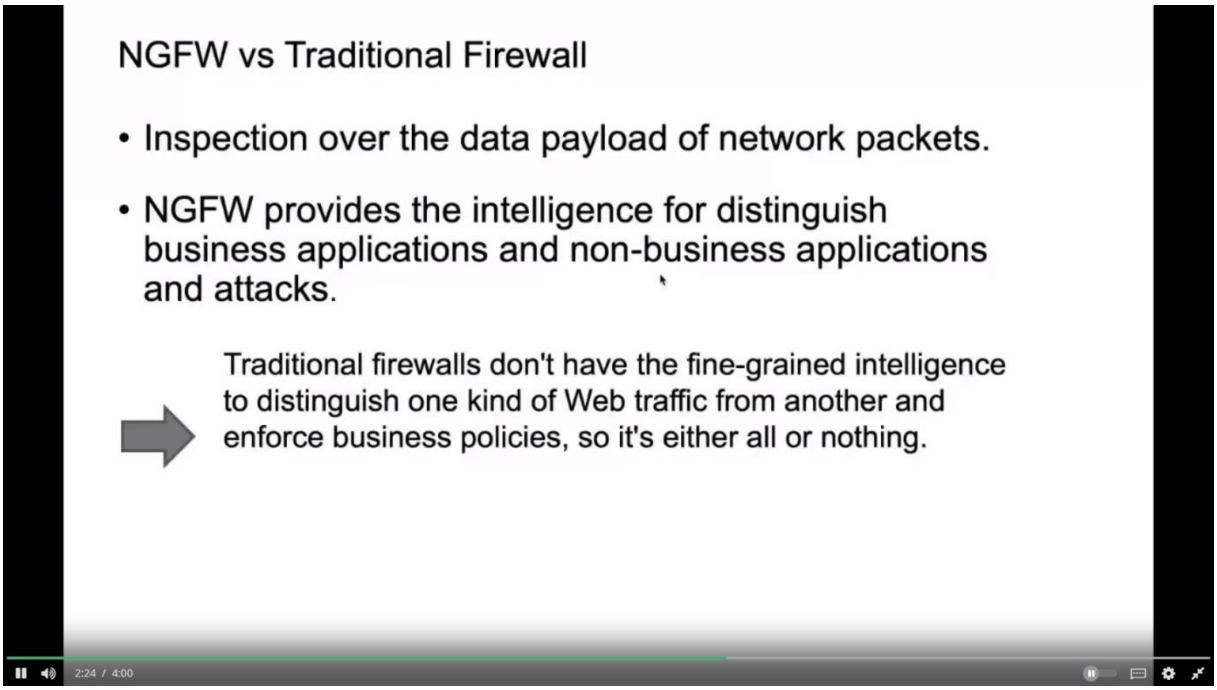
Promiscuous mode Network Interface Card (NIC)

In computer networking, promiscuous mode (often shortened to "promisc mode" or "promisc. mode") is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive.

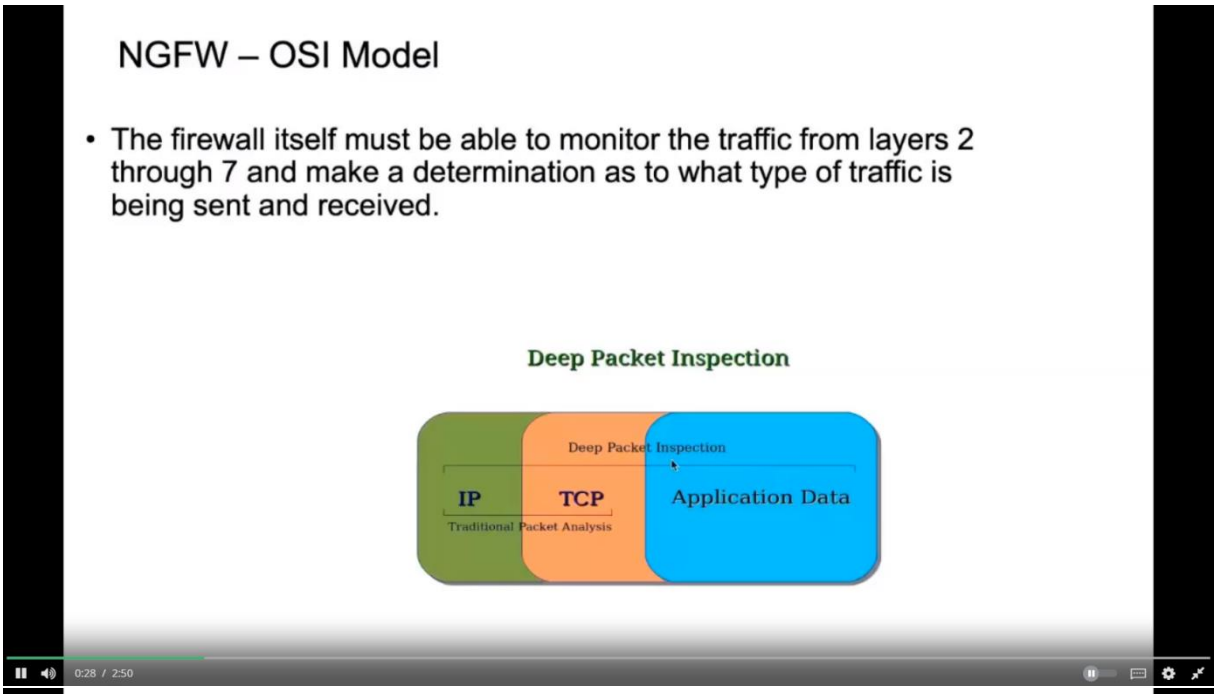
Next Generation Firewalls - Overview

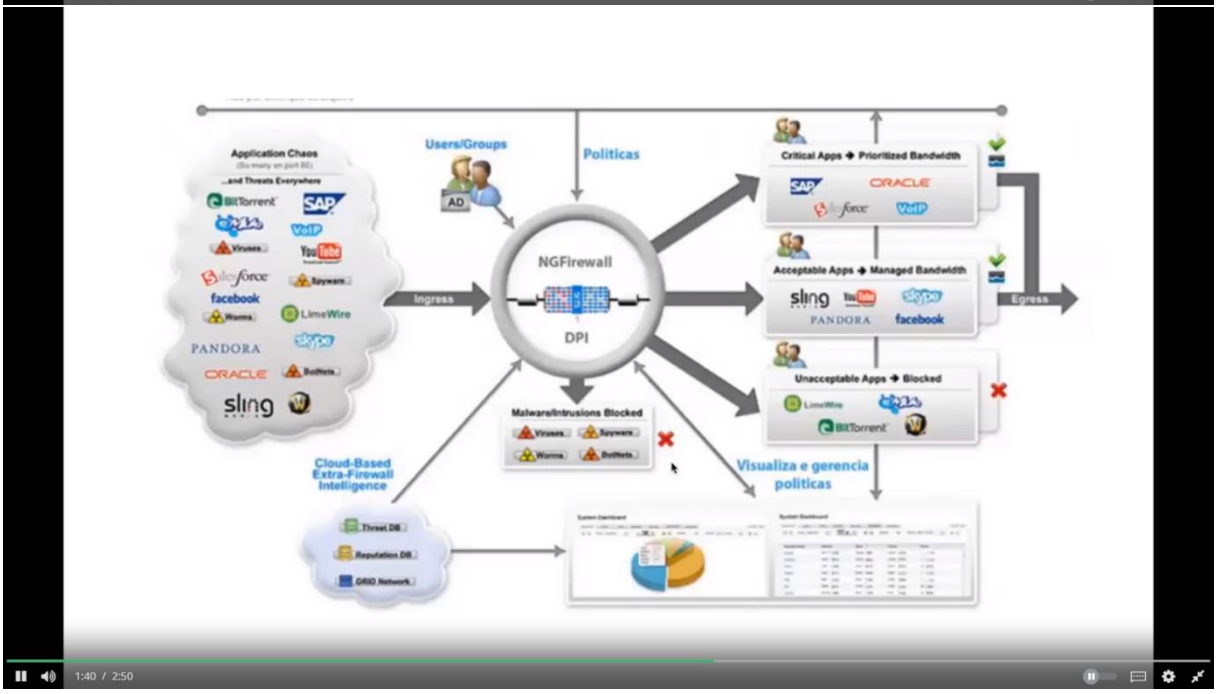

Next Generation Firewalls
Fabian Alfaro Chinchilla
MSIEM Administrator
IBM Security
© 2018 IBM Corporation
0:33 / 4:00


What is a NGFW ?
• A Next-Generation Firewall (NGFW) is a part of the third generation of firewall technology. Combines traditional firewall with other network device filtering functionalities.
• Application firewall using in-line deep packet inspection (DPI)
• Intrusion prevention system (IPS).
• Other techniques might also be employed, such as TLS/SSL encrypted traffic inspection, website filtering.
0:47 / 4:00



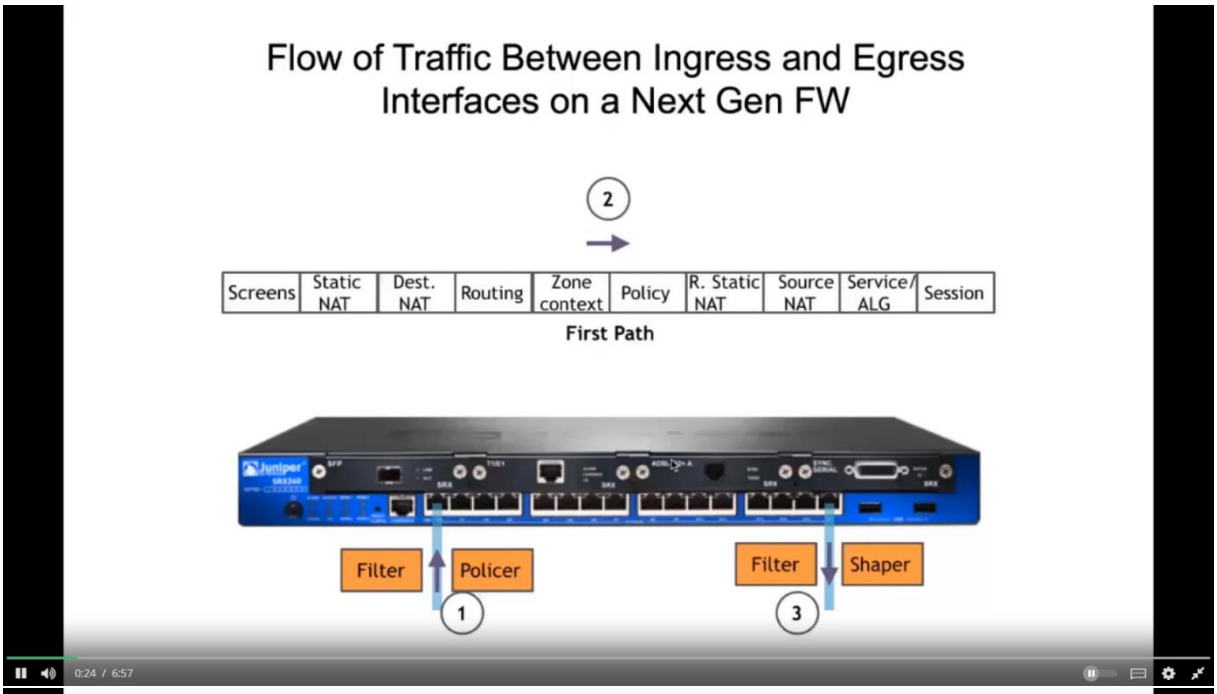
NGFW and the OSI Model



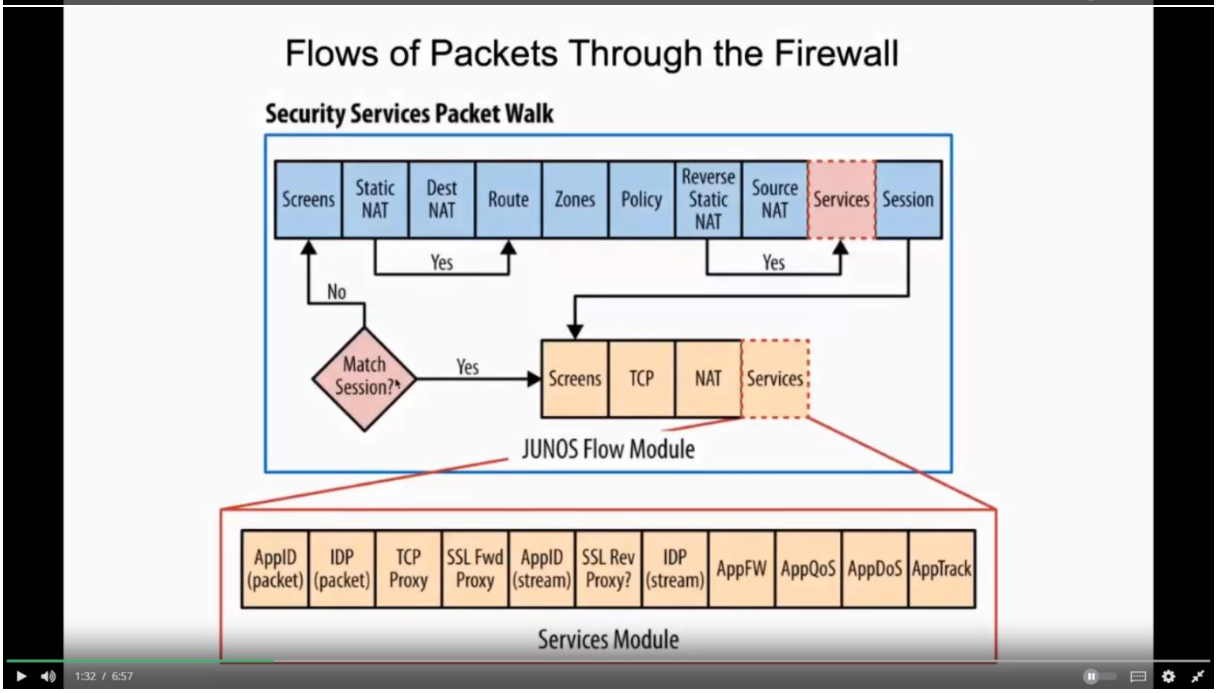


NGFW Packet Flow Example and NGFW Comparisons

Flow of Traffic Between Ingress and Egress Interfaces on a Next Gen FW



Flows of Packets Through the Firewall



NGFW Comparisons:

-Many firewall vendors offer next-generation firewalls, but they argue over whose technique is best.

-A next-generation firewall is application-aware. Unlike traditional stateful firewalls, which deal in ports and protocols, next-generation firewalls drill into traffic to identify the applications traversing the network.

-With current trends pushing applications into the public cloud or to be outsourced to Software as a Service (SaaS) providers, a higher level of granularity is needed to ensure that the proper data is coming into the enterprise network.

5:47 / 6:57

NGFW Comparisons:

- **Cisco Systems** has announced plans to add new levels of application visibility into its **Adaptive Security Appliance (ASA)**, as part of its new SecureX security architecture.
- **Palo Alto Networks** says it was the first vendor to deliver next-generation firewalls and the first to replace port-based traffic classification with application awareness. The company's products are based on a classification engine known as **App-ID.** App-ID identifies applications using several techniques, including decryption, detection, decoding, signatures and heuristics
- **Juniper Networks** uses a suite of software products, known as **AppSecure**, to deliver next-generation firewall capabilities to its SRX Services Gateway. The application-aware component, known as AppTrack, provides visibility into the network based on Juniper's signature database as well as custom application signatures created by enterprise administrators

6:16 / 6:57

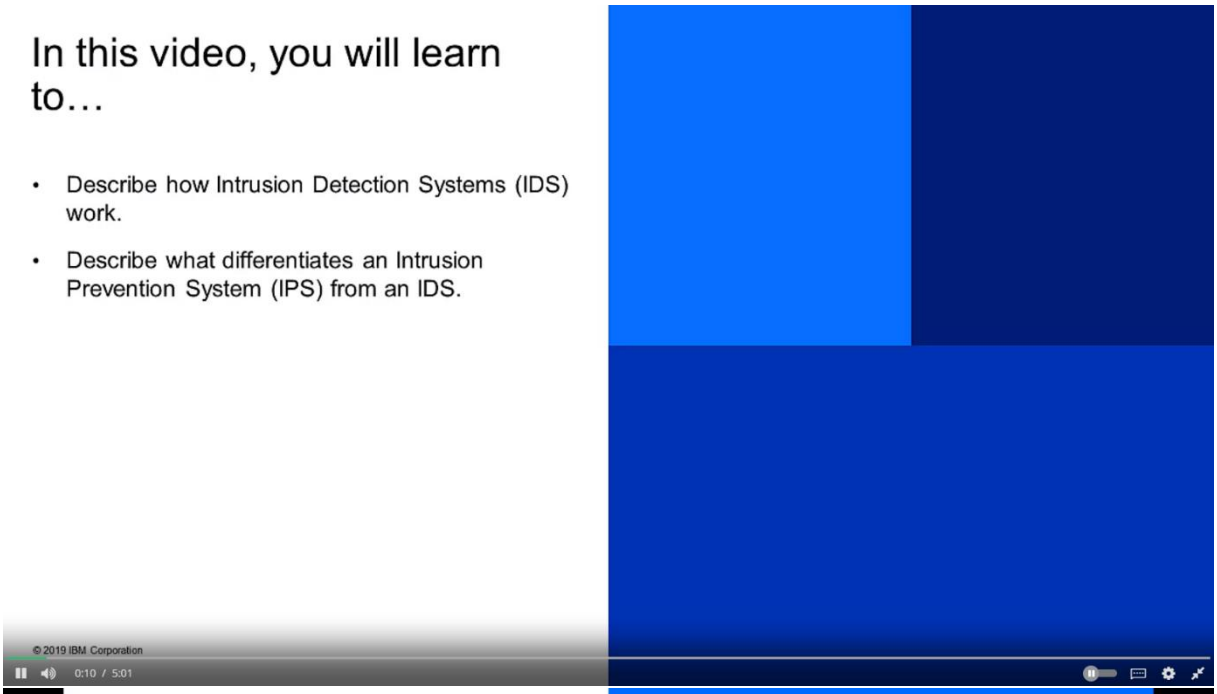
NGFW other vendors:

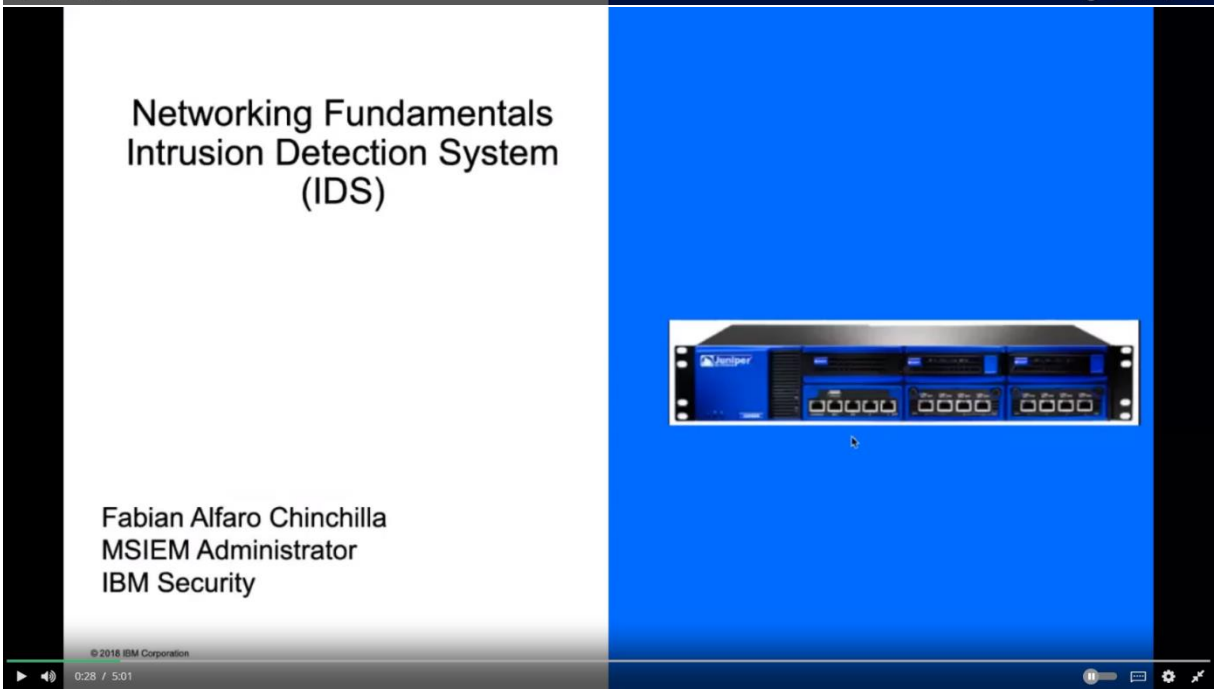
- McAfee
- Meraki MX Firewalls
- Barracuda
- Sonic Wall
- Fortinet Fortigate
- Check Point
- WatchGuard

Open Source NGFW:

- **pfSense** is a free and powerful open source firewall used mainly for FreeBSD servers. It is based on stateful packet filtering. It has a wide range of features that are normally only found in very expensive firewalls.
- **ClearOS** is a powerful firewall that provides us the tools we need to run a network, and also gives us the option to scale up as and when required. It is a modular operating system that runs in a virtual environment or on some dedicated hardware in the home, office, etc
- **VyOS** is open source and completely free, and based on Debian GNU/Linux. It can run on both physical and virtual platforms. It provides a firewall, VPN functionality and software based network routing. It also supports paravirtual drivers and integration packages for virtual platforms. Unlike OpenWRT or pfSense, VyOS provides support for advanced routing features such as dynamic routing protocols and command line interfaces.
- **IPCop** is an open source Linux firewall which is secure, user friendly, stable and easily configurable. It provides an easily understandable Web interface to manage the firewall. It is most suitable for small businesses and local PCs.

Intrusion Detection and Intrusion Prevention Systems


In this video, you will learn to…
• Describe how Intrusion Detection Systems (IDS) work.
• Describe what differentiates an Intrusion Prevention System (IPS) from an IDS.
© 2019 IBM Corporation
0:10 / 5:01


Networking Fundamentals
Intrusion Detection System (IDS)
Fabian Alfaro Chinchilla
MSIEM Administrator
IBM Security
© 2018 IBM Corporation
0:28 / 5:01

CLASSIFICATION OF IDS

- Signature based: analyses content of each packet at layer 7 with a set of predefined signatures.
- Anomaly based: monitors network traffic and compares it against an established baseline for normal use and classifying it as either normal or anomalous.

0:42 / 5:01

TYPES OF IDS

- Host based IDS (HIDS): anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside.
- Network based IDS (NIDS): anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected.

1:51 / 5:01

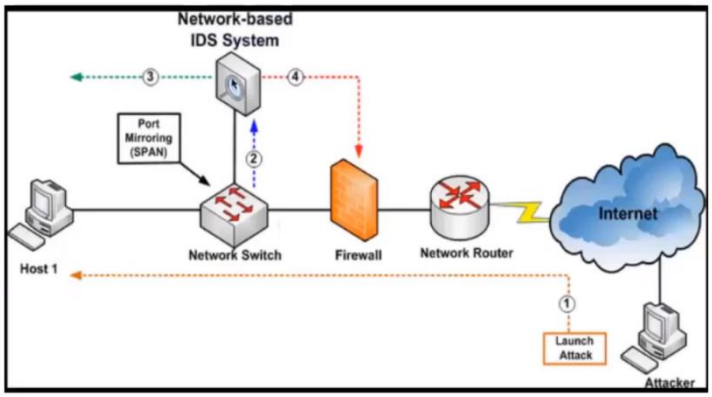
NIDS

- Appliance: IBM RealSecure Server Sensor and Cisco IDS 4200 series

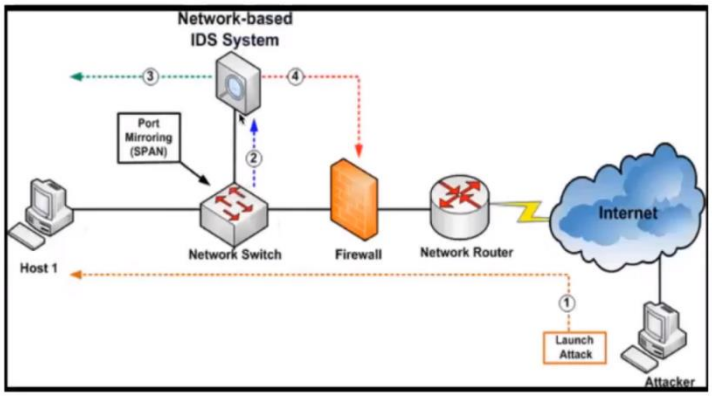
- Software: sensor software installed on server and placed in network to monitor network traffic, such as Snort.

2:07 / 5:01

IDS LOCATION ON NETWORK ???



IDS LOCATION ON NETWORK ???



2:23 / 5:01

HYBRID IDS IMPLEMENTATIONS

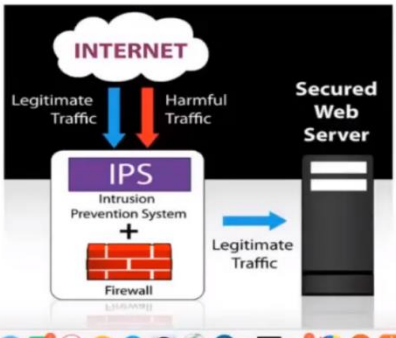
- Combines the features of HIDS and NIDS
- Gains flexibility and increases security
- Combining IDS sensors locations: put sensors on network segments and network hosts and can report attacks aimed at particular segments or the entire network.

Networking Fundamentals Intrusion Prevention System (IPS)

Fabian Alfaro Chinchilla
MSIEM Administrator
IBM Security

What is an Intrusion Protection System (IPS)?

- Network security/threat prevention technology
- Examines network traffic flows to detect and prevent vulnerability exploits
- Often sits directly behind the firewall

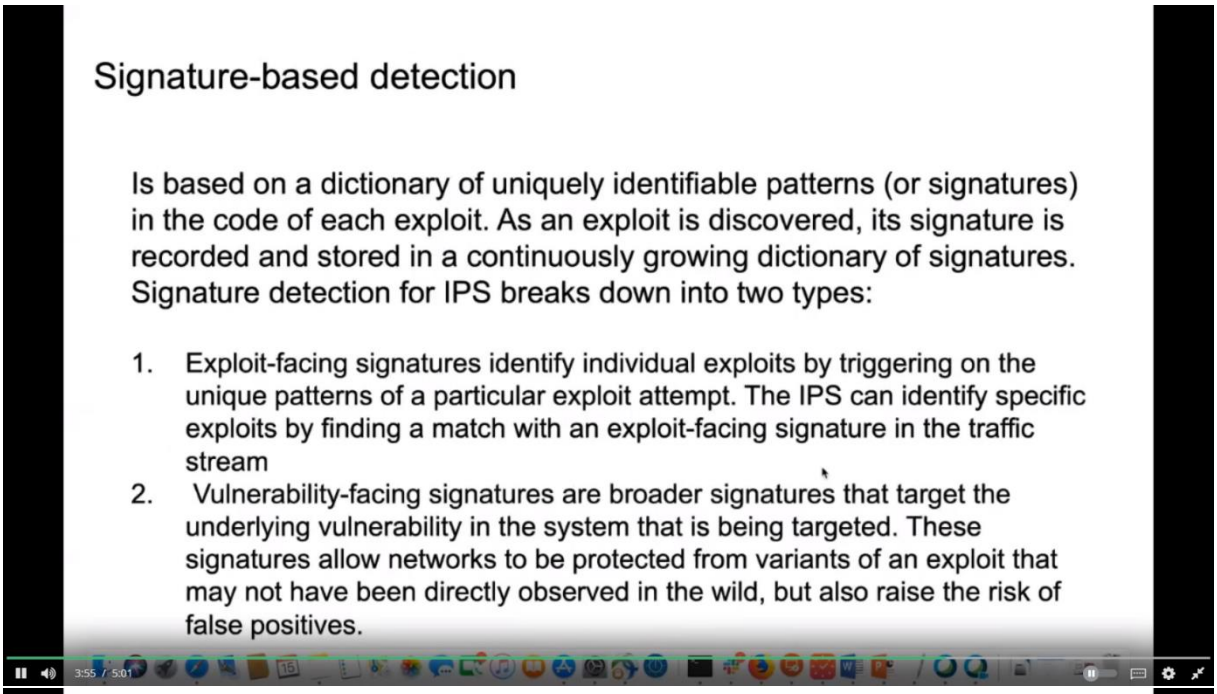


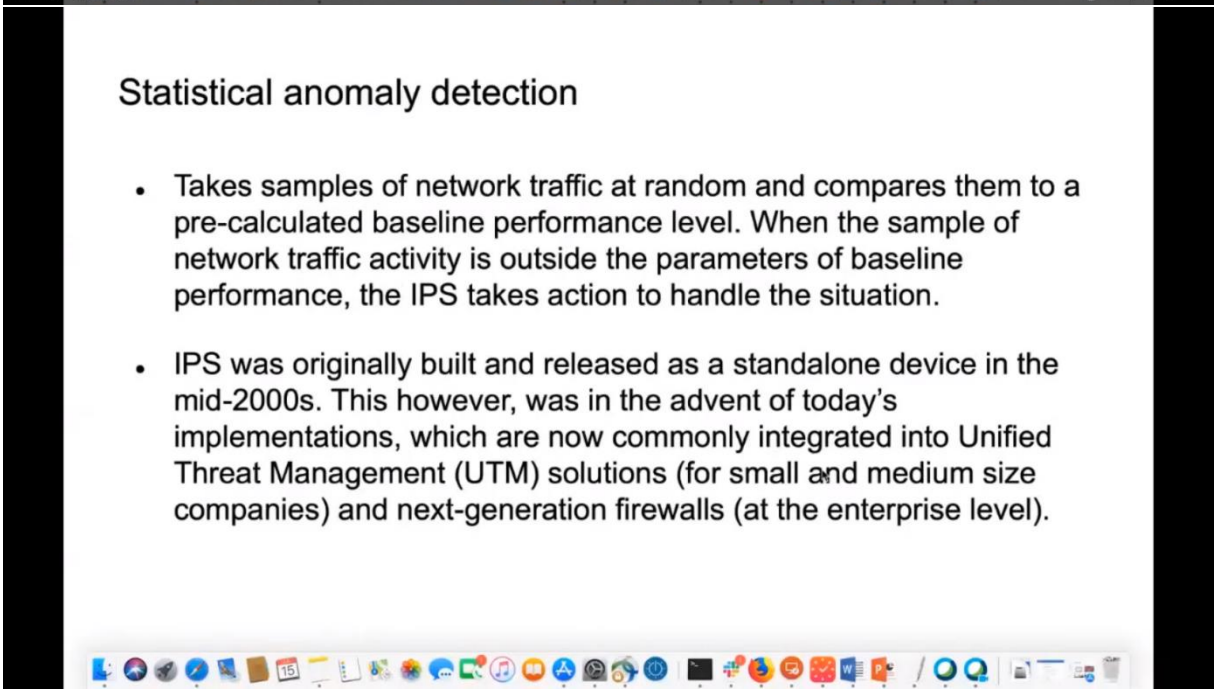
Prevention?

- The IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include
  - Sending an alarm to the administrator (as would be seen in an IDS)
  - Dropping the malicious packets
  - Blocking traffic from the source address
  - Resetting the connection

How does the attack affect me?

- Vulnerability exploits usually come in the form of malicious inputs to a target application or service
- The attackers use those exploits to interrupt and gain control of an application or machine.
- Once successful exploit, the attacker can disable the target application (DoS)
- Also can potentially access to all the rights and permissions available to the compromised application





High Availability and Clustering

Networking Fundamentals
High Availability and Clustering

Fabian Alfaro Chinchilla
SIEM Administrator
IBM Security

0:36 / 9:15

0:48 / 9:15

What is HA?

- In information technology, high availability (HA) refers to a system or component that is continuously operational for a desirably long length of time. Availability can be measured relative to "100% operational" or "never failing.“
- High availability architecture is an approach of defining the components, modules or implementation of services of a system which ensures optimal operational performance, even at times of high loads.
- Although there are no fixed rules of implementing HA systems, there are generally a few good practices that one must follow so that you gain the most out of the least resources.

What are the requirements for creating an HA cluster?

- Hosts in a virtual server cluster must have access to the same shared storage, and they must have identical network configurations.
- Domain name system (DNS) naming is important too: All hosts must resolve other hosts using DNS names, and if DNS is not set correctly, you won’t be able to configure HA settings at all.
- Same OS level.
- Connections between the primary and secondary nodes.

How High Availability Works?

To create a highly available system, three characteristics should be present:

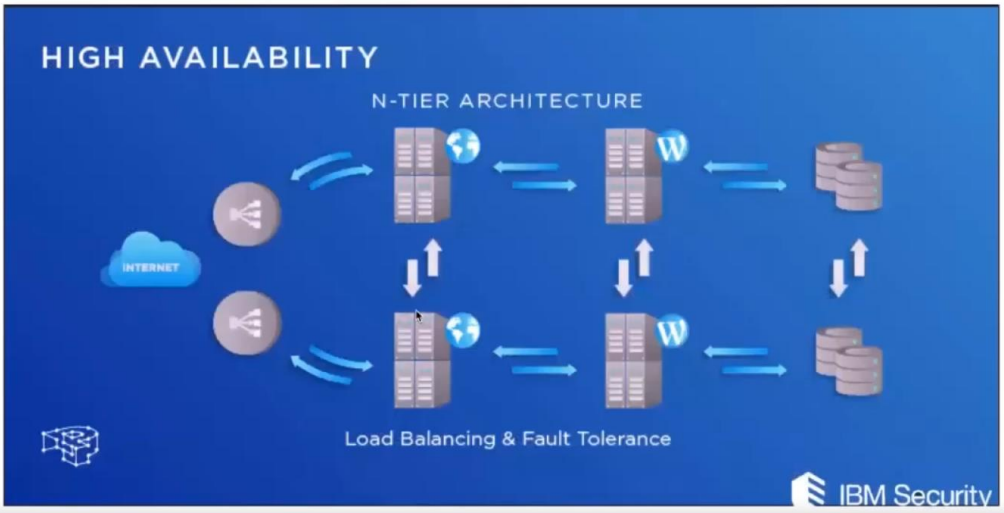
Redundancy:

– Means that there are multiple components that can perform the same task. This eliminates the single point of failure problem by allowing a second server to take over a task if the first one goes down or becomes disabled

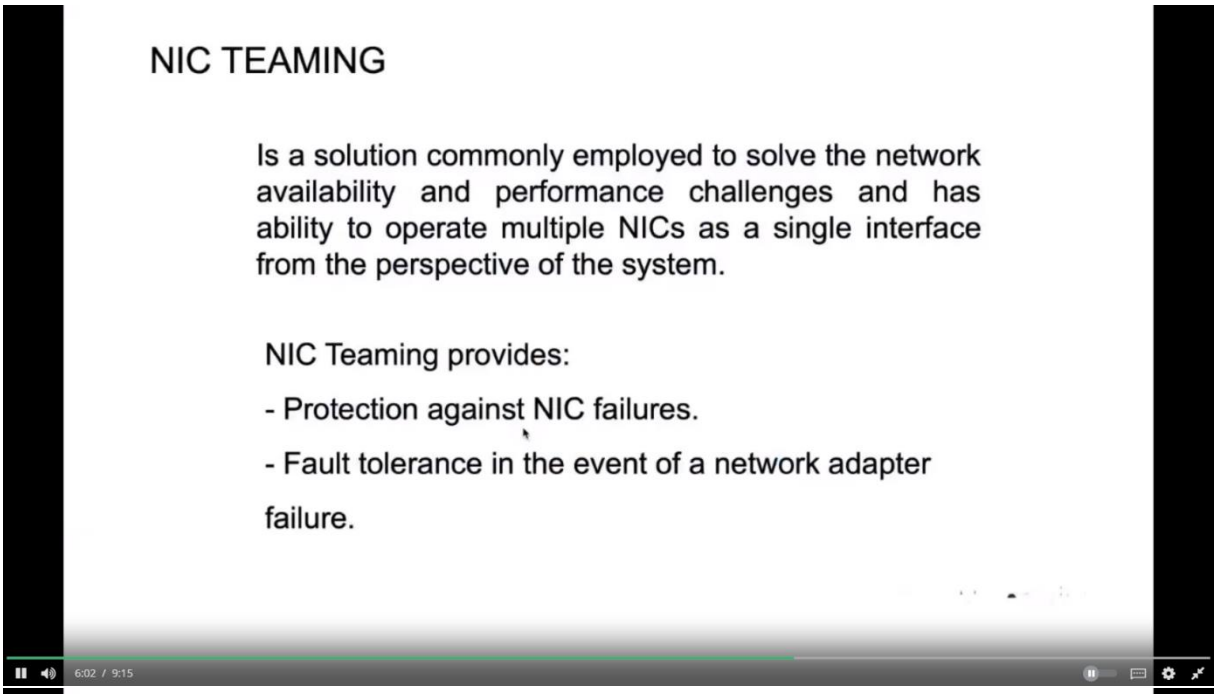
Monitoring and Failover

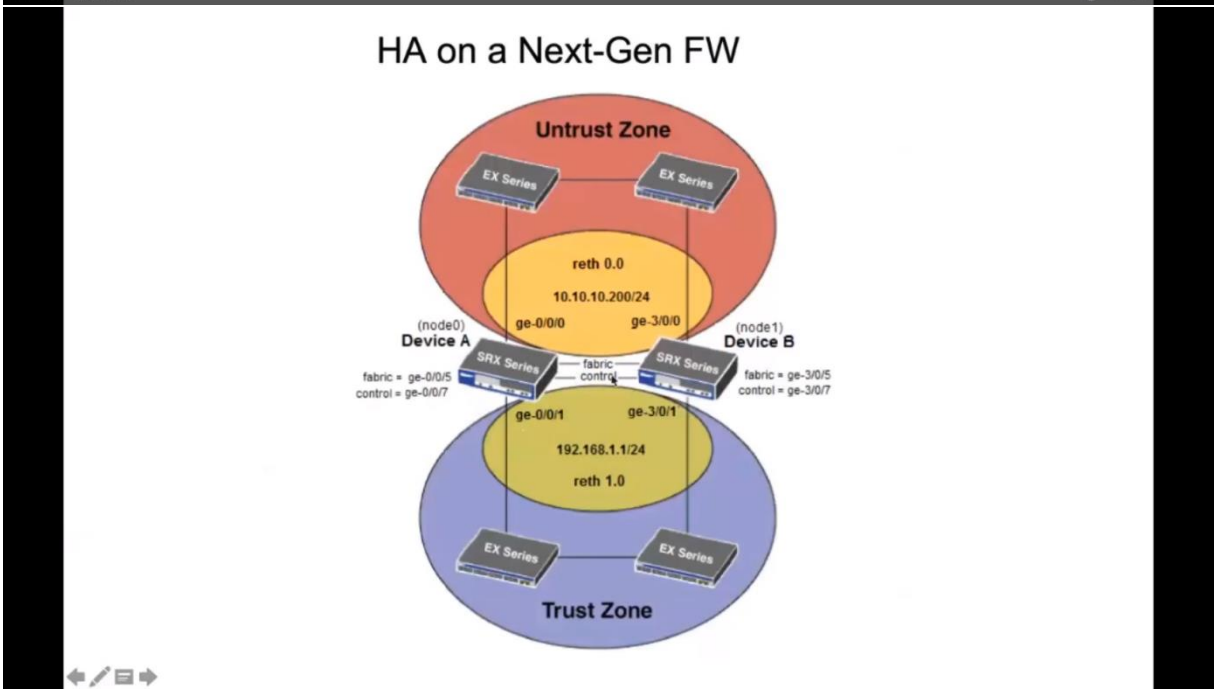
– In a highly available setup, the system needs to be able to monitor itself for failure. This means that there are regular checks to ensure that all components are working properly. Failover is the process by which a secondary component becomes primary when monitoring reveals that a primary component has failed.

4:00 / 9:15



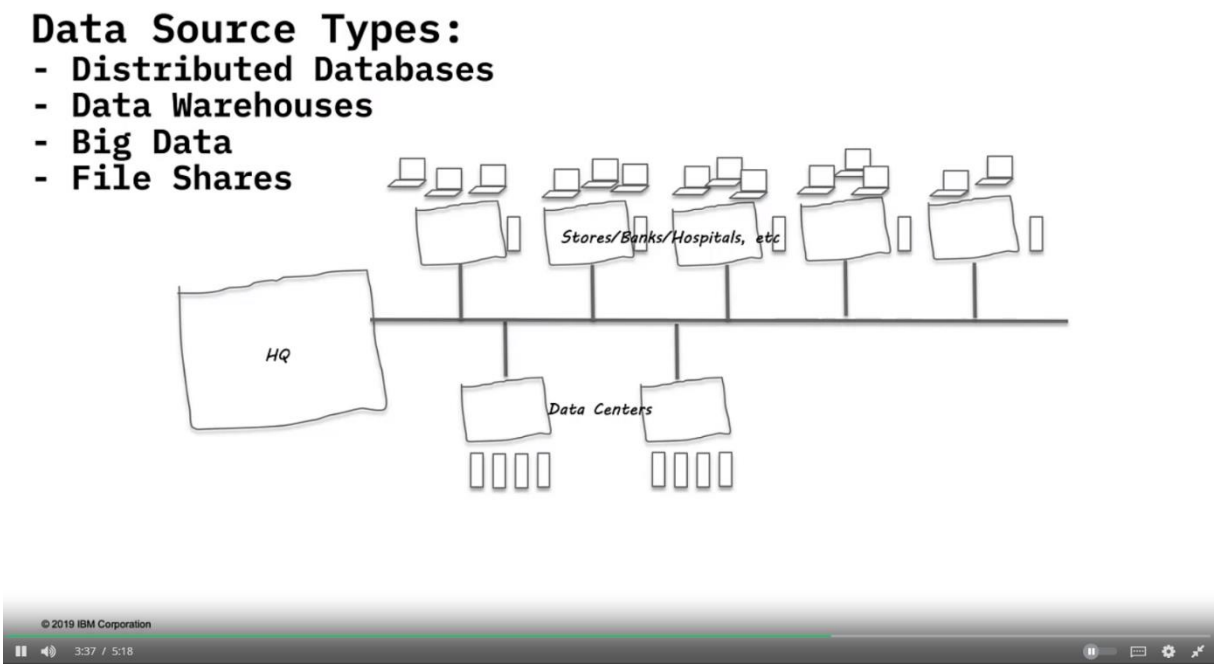
5:14 / 9:15



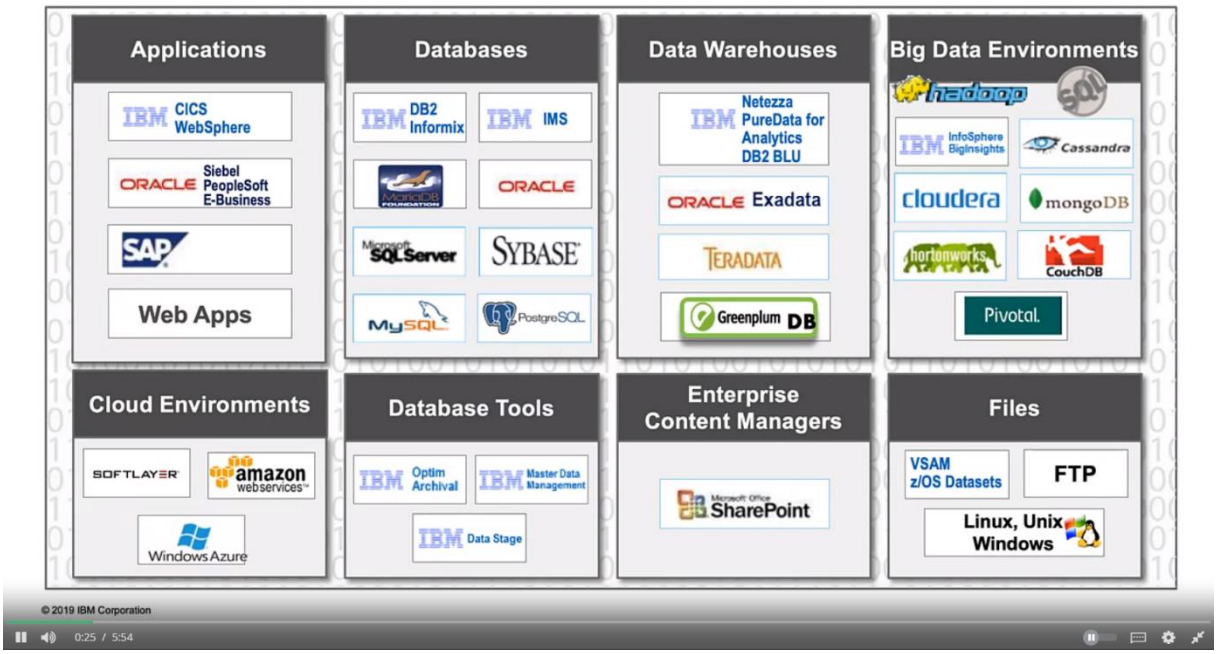


Week 3

Data Source Types Part 1



Data Source Types Part 2



Data Source Types:

- Distributed Databases
- Data Warehouses
- Big Data
- File Shares

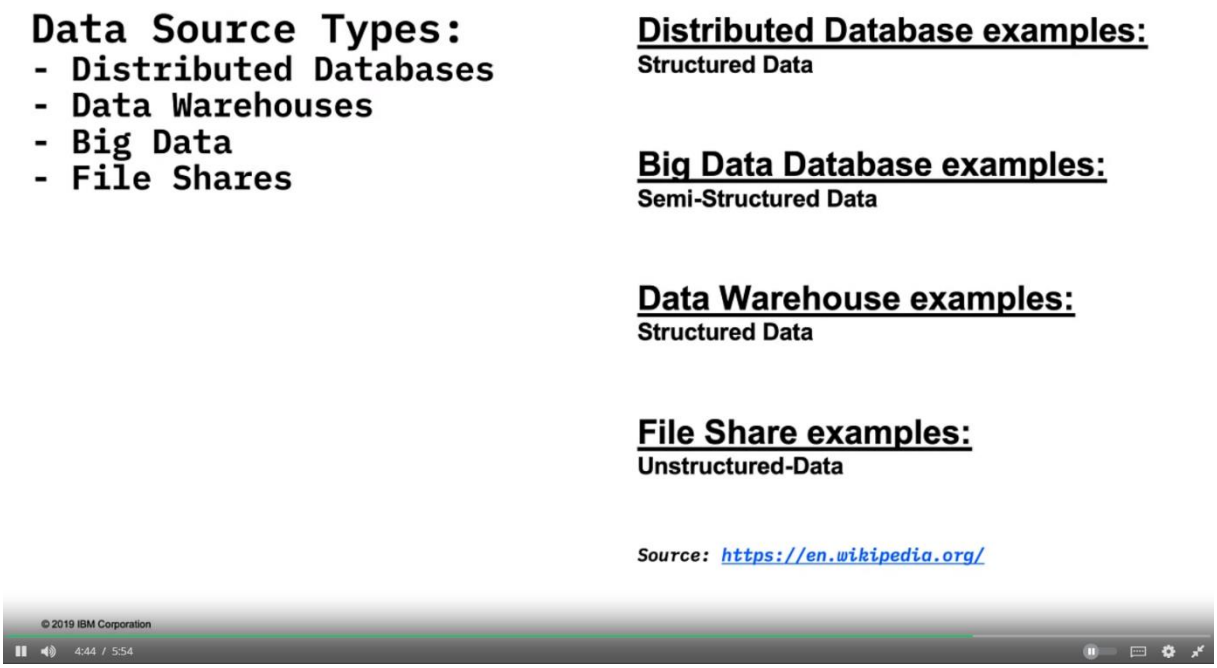
Distributed Database examples:
Oracle, DB2, Microsoft SQL Server, MySQL

Big Data Database examples:
Hadoop, MongoDB, BigTable

Data Warehouse examples:
Netezza, Exadata, Amazon Redshift, Apache Hive

Fileshare examples:
"NAS" (Network Attached Storage) Network Fileshares such as EMC or NetApp; and Cloud Shares such as Google drive, dropbox.com, box.com, and Amazon's S3 storage.

Source: https://en.wikipedia.org/



Data Model Types

Data Model Types:
- Structured Data

Structured data is data that has been organized into a formatted repository, typically a database, so that its elements can be made addressable for more effective processing and analysis.

A data structure is a kind of repository that organizes information for that purpose. In a database, for example, each field is discrete and its information can be retrieved either separately or along with data from other fields, in a variety of combinations. The power of the database is its ability to make data comprehensive, so that it yields useful information. A database query language, such as SQL (standard query language), allows a database administrator to interact with the database.

Structured data contrasts with unstructured and semi-structured data. The three can be considered to exist on a continuum, with unstructured data being the least formatted and structured data being the most formatted. Data is increasingly amenable to processing as it is increasingly structured.

Source: ***https://techtarget.com***

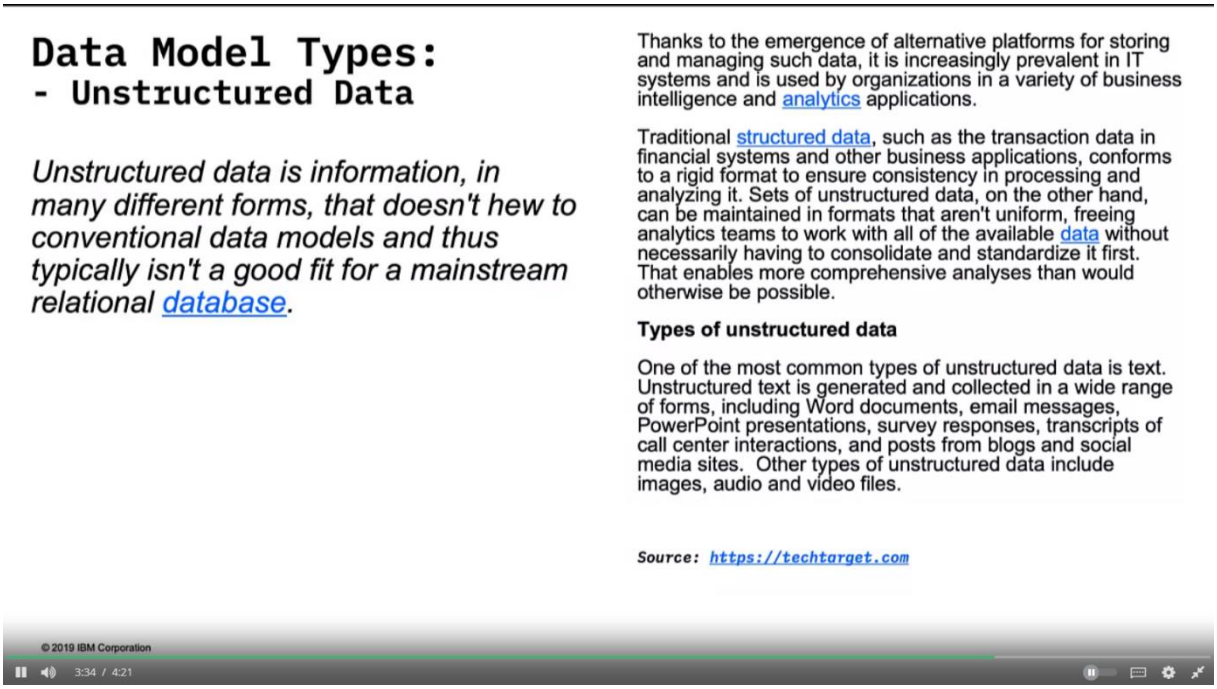
Data Model Types:
- Semi-Structured Data

Semi-structured data is data that has not been organized into a specialized repository, such as a database, but that nevertheless has associated information, such as metadata, that makes it more amenable to processing than raw data.

The difference between structured data, unstructured data and semi-structured data:
Unstructured data has not been organized into a format that makes it easier to access and process. In reality, very little data is completely unstructured. Even things that are often considered unstructured data, such as documents and images, are structured to some extent. Structured data is basically the opposite of unstructured: It has been reformatted and its elements organized into a data structure so that elements can be addressed, organized and accessed in various combinations to make better use of the information. Semi-structured data lies somewhere between the two. It is not organized in a complex manner that makes sophisticated access and analysis possible; however, it may have information associated with it, such as metadata tagging, that allows elements contained to be addressed.

Here's an example: A Word document is generally considered to be unstructured data. However, you can add metadata tags in the form of keywords and other metadata that represent the document content and make it easier for that document to be found when people search for those terms -- the data is now semi-structured. Nevertheless, the document still lacks the complex organization of the database, so falls short of being fully structured data.

Source: ***https://techtarget.com***



Structured Data

Structured Data:
Flat File Databases

Flat-file databases take all the information from all the records and store everything in one table. This works fine when you have a small number of records related to a single topic, such as a person's name and phone number, but if you have hundreds or thousands of records, each with a number of fields, the database quickly becomes difficult to use.

SID	SFName	SLName	SteleNumber	CID	Cname	TID	Trainer	TrnTeleNumber
1	Mary	Hinkle	555.123.4567	101	Data Basics	T01	Charles Hill	555.987.6543
2	Paul	Litz	555.258.8963	101	Data Basics	T01	Charles Hill	555.987.6542
1	Mary	Hinkle	555.123.4567	102	Web Design	T02	Glen Barber	555.879.4652
3	Dee	Coleman	555.357.9514	203	Relational Design	T03	Rick Dobson	555.324.2986
4	Don	Charney	555.369.8741	204	VBA Programming	T03	Rick Dobson	555.324.2986

Source: *https://en.wikipedia.org/*

Structured Data:
Relational Databases

Relational databases separate this mass of information into numerous **tables**. All the columns in each table should be about one topic, such as "student information," "class information," or "trainer information."

SID	SFName	SLName	SteleNumber
1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963
1	Mary	Hinkle	555.123.4567
3	Dee	Coleman	555.357.9514
4	Don	Charney	555.369.8741

CID	Cname
101	Data Basics
101	Data Basics
102	Web Design
203	Relational Design
204	VBA Programming

TID	Trainer	TrnTeleNumber
T01	Charles Hill	555.987.6543
T01	Charles Hill	555.987.6542
T02	Glen Barber	555.879.4652
T03	Rick Dobson	555.324.2986
T03	Rick Dobson	555.324.2986

Source: *https://en.wikipedia.org/*

Structured Data:
Relational Databases

The tables for a relational database are linked to each other through the use of **keys**. Each table may have one **primary key** and any number of **foreign keys**. A foreign key is simply a primary key from one table that has been placed in another table.

Primary Key

SID	SFName	SLName	SteleNumber
1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963
1	Mary	Hinkle	555.123.4567
3	Dee	Coleman	555.357.9514
4	Don	Charney	555.369.8741

Primary Key

SID	CID	Cname	TID
1	101	Data Basics	T01
2	101	Data Basics	T01
1	102	Web Design	T02
3	203	Relational Design	T03
4	204	VBA Programming	T03

Primary Key

TID	Trainer	TrnTeleNumber
T01	Charles Hill	555.987.6543
T01	Charles Hill	555.987.6542
T02	Glen Barber	555.879.4652
T03	Rick Dobson	555.324.2986
T03	Rick Dobson	555.324.2986

Foreign Key

Foreign Key

The most important rules for designing relational databases are called **Normal Forms**. When databases are designed properly, huge amounts of information can be kept under control. This lets you **query** the database (search for information) and quickly get the answer you need.

Query: "What students are taking classes from trainer CHARLES HILL?"

Answer:

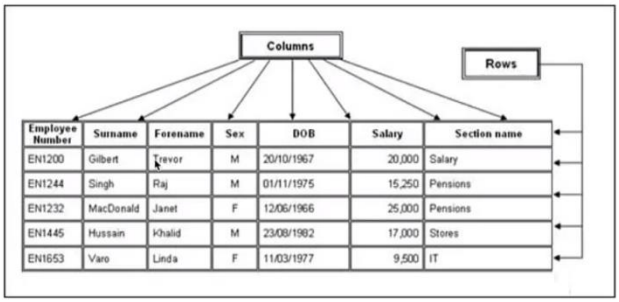
1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963

Compiled by Rick Dobson
Graphics & Design by Fred Schneider

3:33 / 7:15

Structured Data:
SQL; "Structured Query Language", the language used to interact with data inside a database.

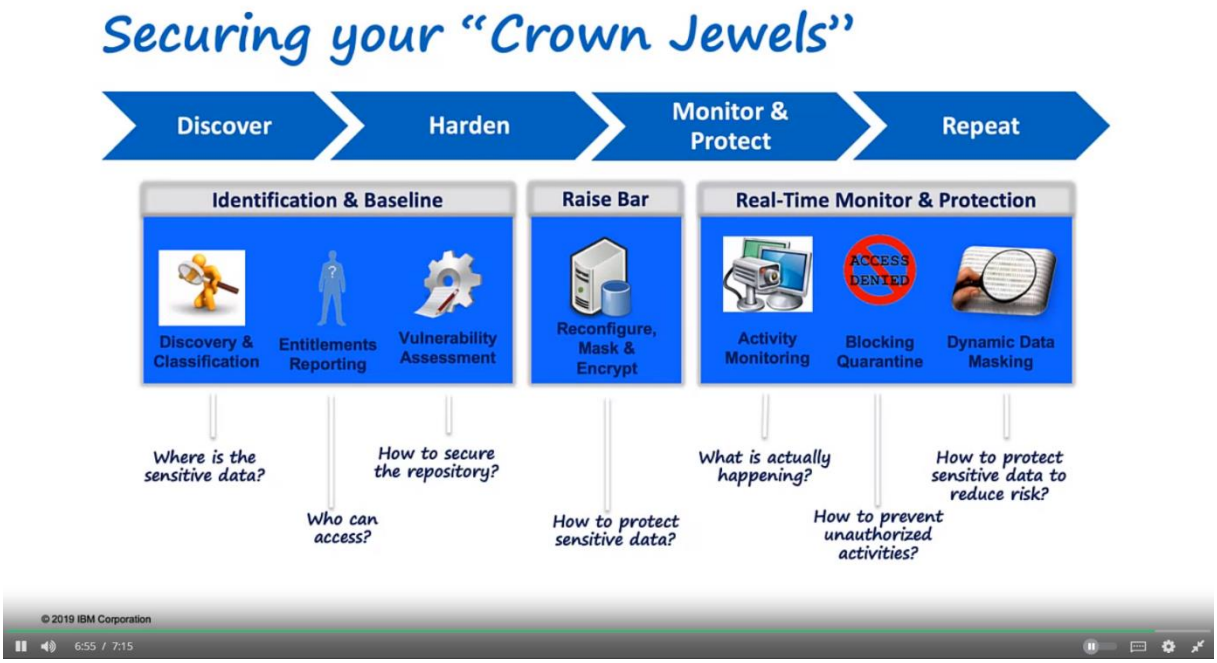
SQL (*S-Q-L*, /ˈsiːkwəl/ "sequel"; **Structured Query Language**) is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS). It is particularly useful in handling structured datawhere there are relations between different entities/variables of the data.



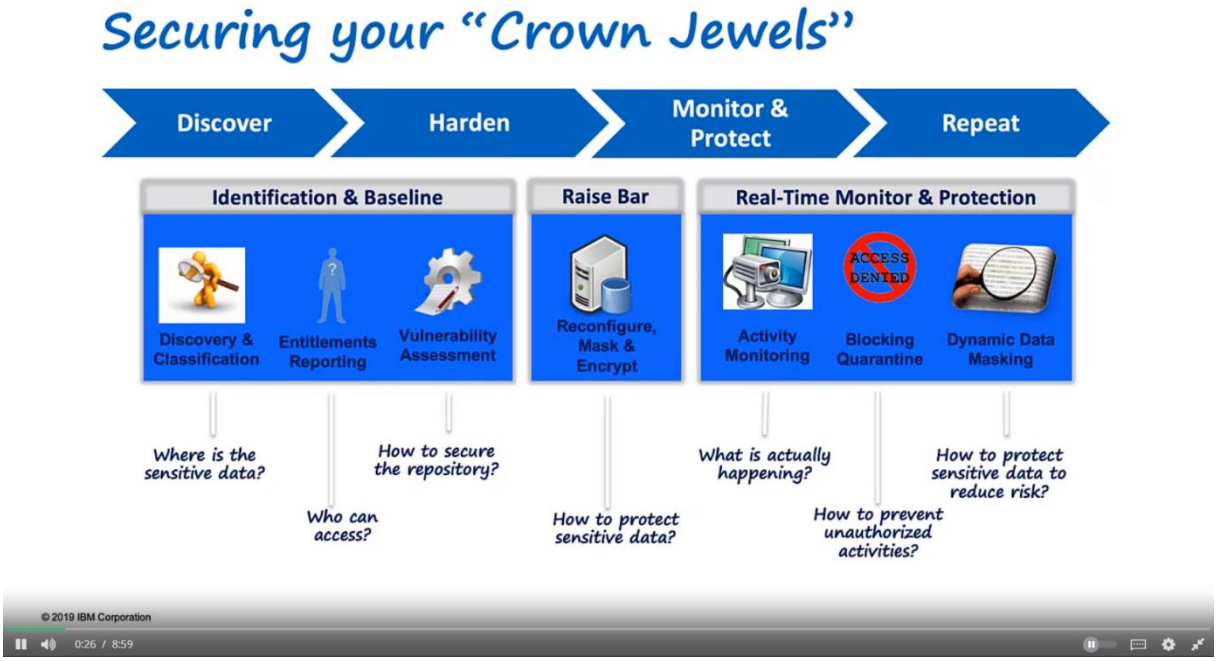

```
dvdrental=# select title, release_year, length, replacement_cost from film
dvdrental-#   where length > 120 and replacement_cost > 29.50
dvdrental-#   order by title desc;
          title          | release_year | length | replacement_cost
-------------------------+--------------+--------+------------------
 West Lion               |         2006 |    159 |            29.99
 Virgin Daisy            |         2006 |    179 |            29.99
 Uncut Suicides          |         2006 |    172 |            29.99
 Tracy Cider             |         2006 |    142 |            29.99
 Song Hedwig             |         2006 |    165 |            29.99
 Slacker Liaisons        |         2006 |    179 |            29.99
 Sassy Packer            |         2006 |    154 |            29.99
 River Outlaw            |         2006 |    149 |            29.99
 Right Cranes            |         2006 |    153 |            29.99
 Quest Mussolini         |         2006 |    177 |            29.99
 Poseidon Forever        |         2006 |    159 |            29.99
 Loathing Legally        |         2006 |    140 |            29.99
 Lawless Vision          |         2006 |    181 |            29.99
 Jingle Sagebrush        |         2006 |    124 |            29.99
 Jericho Mulan           |         2006 |    171 |            29.99
 Japanese Run            |         2006 |    135 |            29.99
 Gilmore Boiled          |         2006 |    163 |            29.99
 Floats Garden           |         2006 |    145 |            29.99
 Fantasia Park           |         2006 |    131 |            29.99
 Extraordinary Conquerer |         2006 |    122 |            29.99
 Everyone Craft          |         2006 |    163 |            29.99
 Dirty Ace               |         2006 |    147 |            29.99
 Clyde Theory            |         2006 |    139 |            29.99
 Clockwork Paradise      |         2006 |    143 |            29.99
 Ballroom Mockingbird    |         2006 |    173 |            29.99
(25 rows)
```

Source: *https://en.wikipedia.org/*

5:09 / 7:15



Securing the Crown Jewels

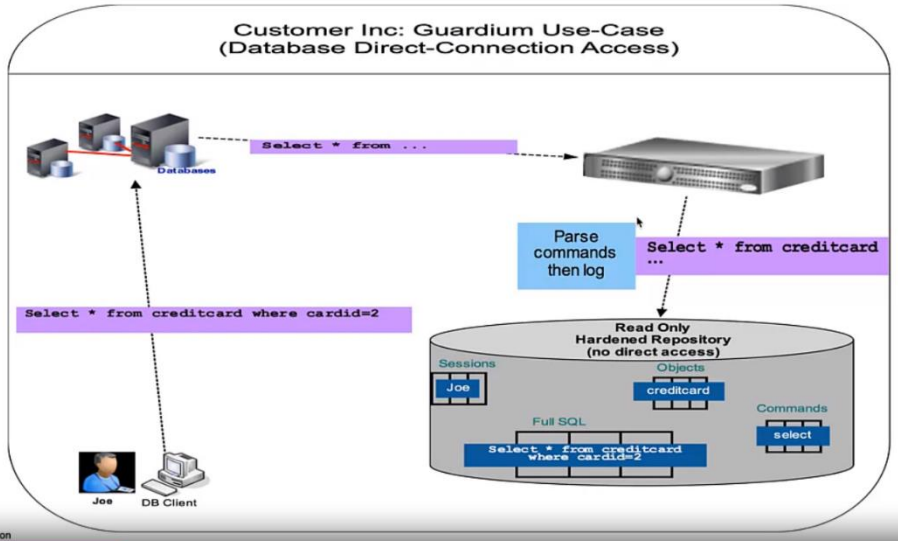


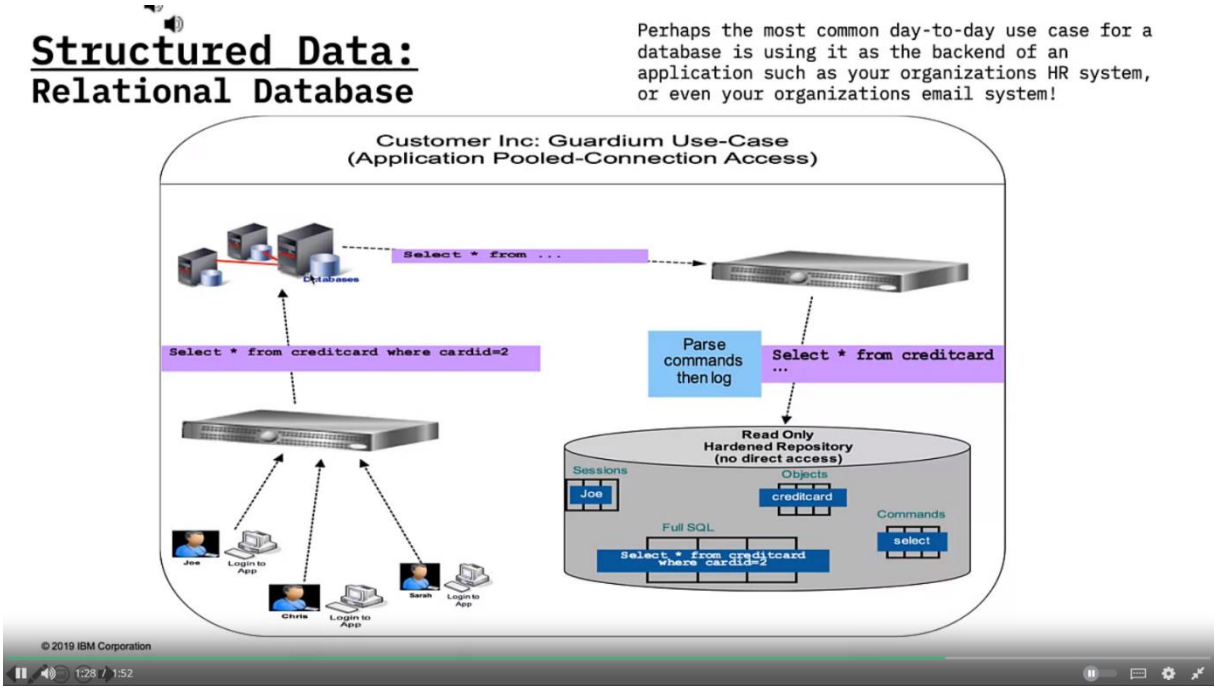
Leveraging Security Industry Best Practices

Structured Data and Relational Databases

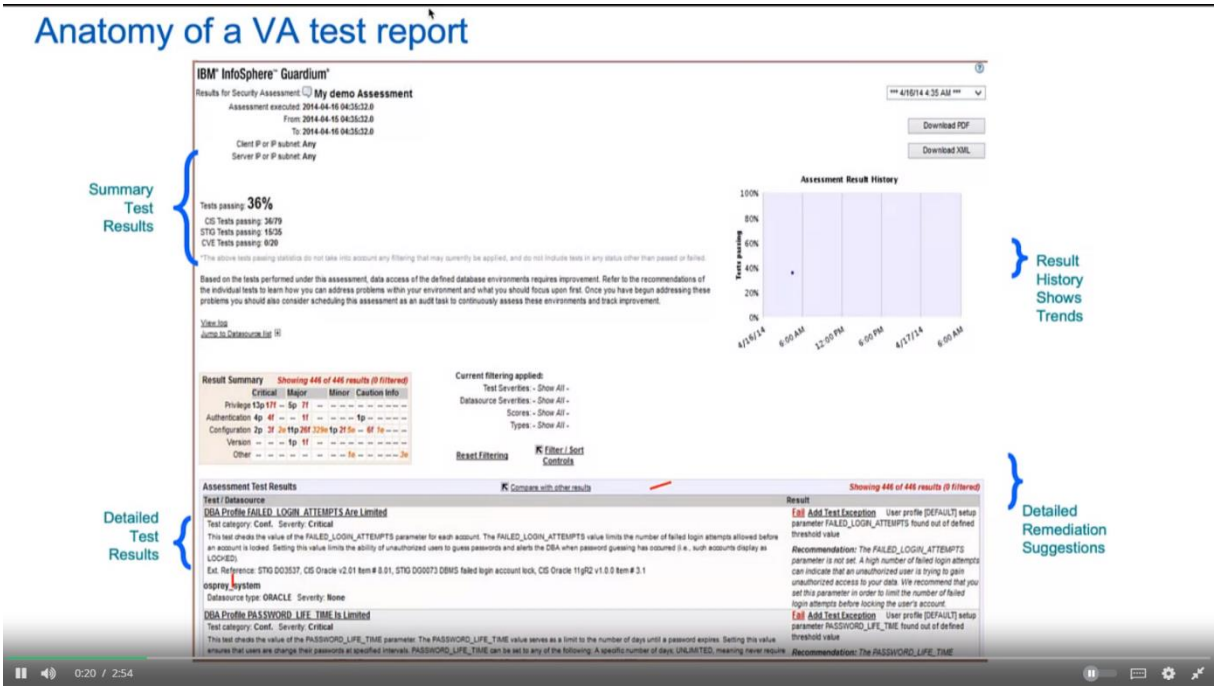
Structured Data:
Relational Database

A database administrators will login through a db client to make big changes to a database.





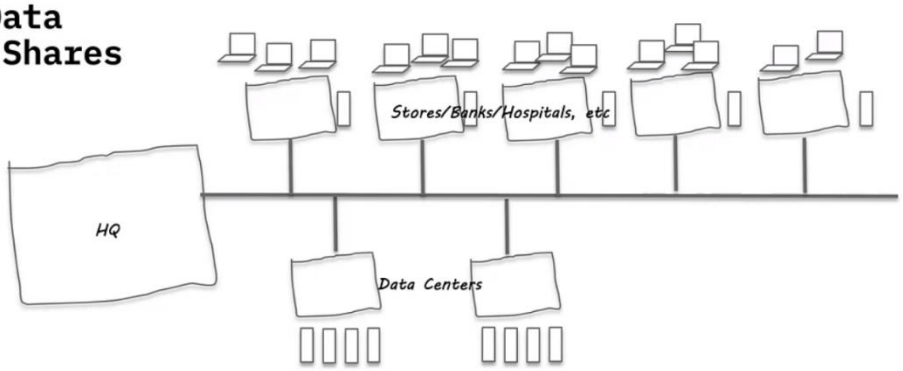
Anatomy of a Vulnerability Assessment Test Report



Securing Data Sources by Type

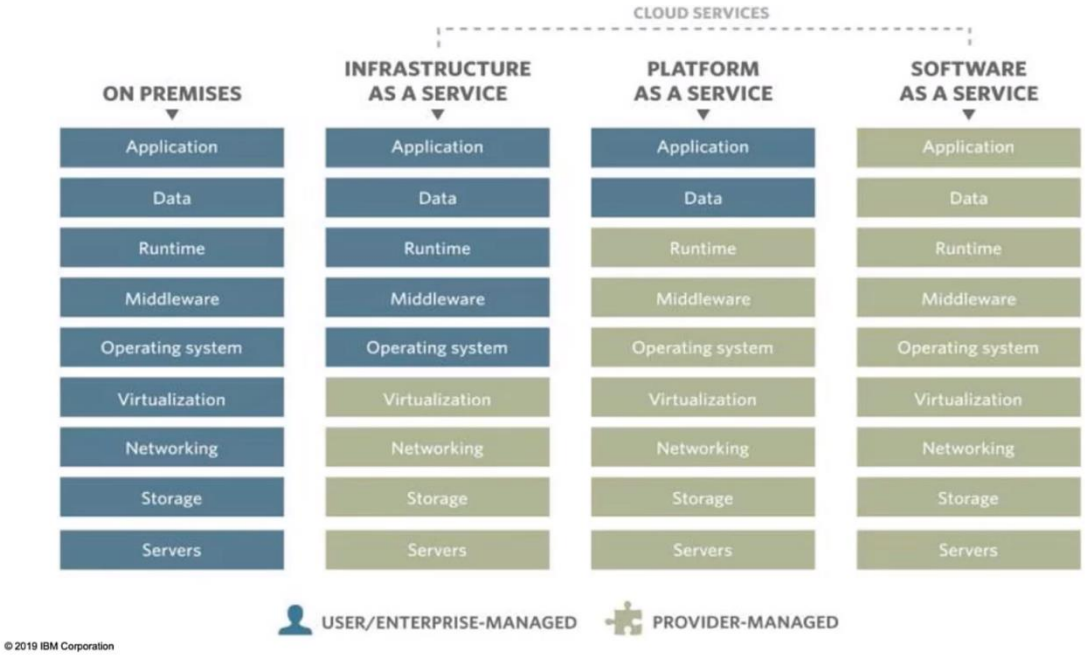
Data Source Types:

- Distributed Databases
- Data Warehouses
- Big Data
- File Shares

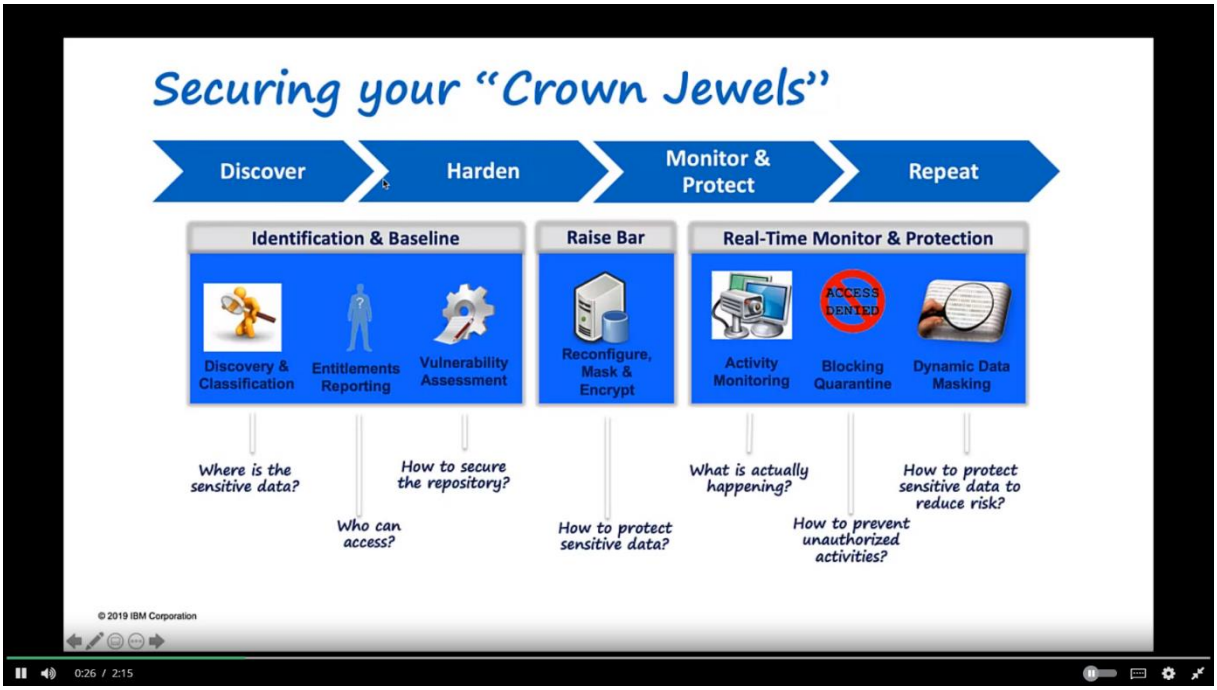


0:37 / 8:55

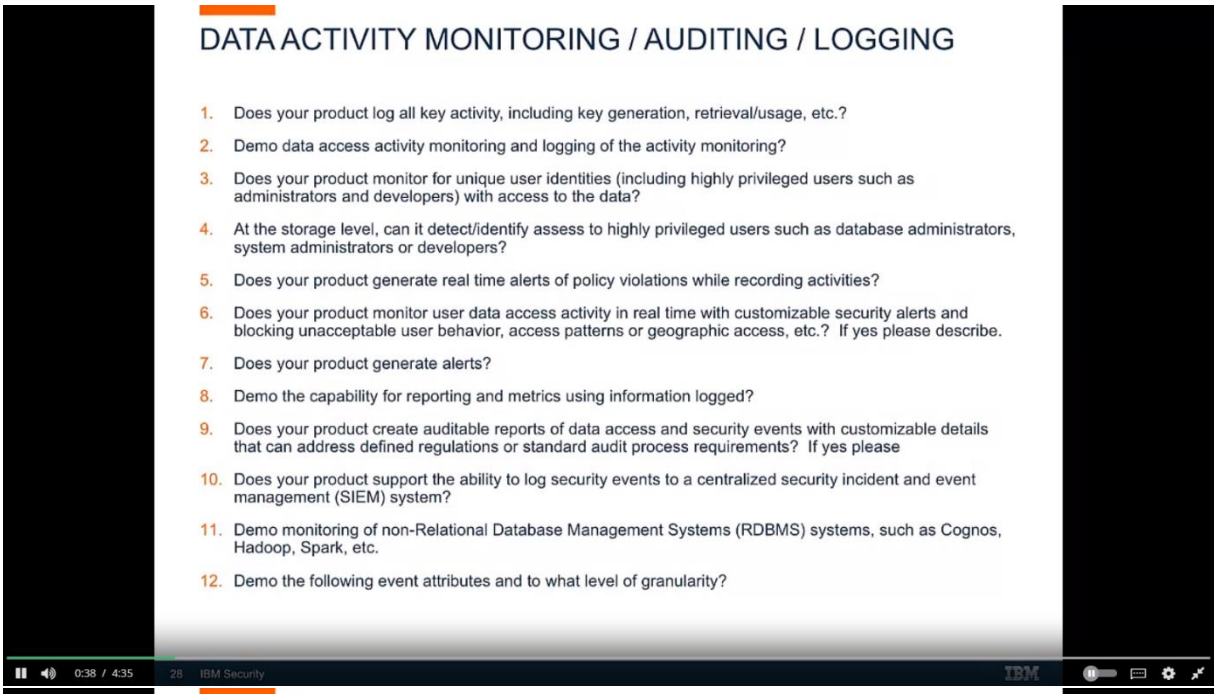
1:59 / 8:55

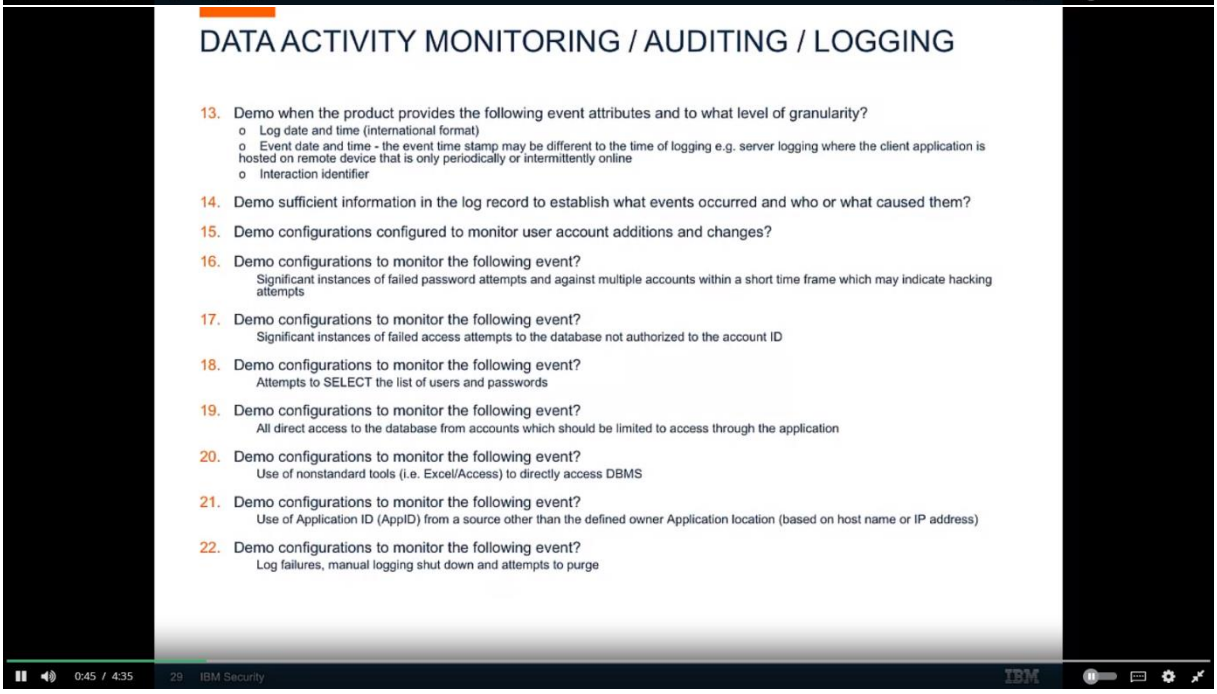


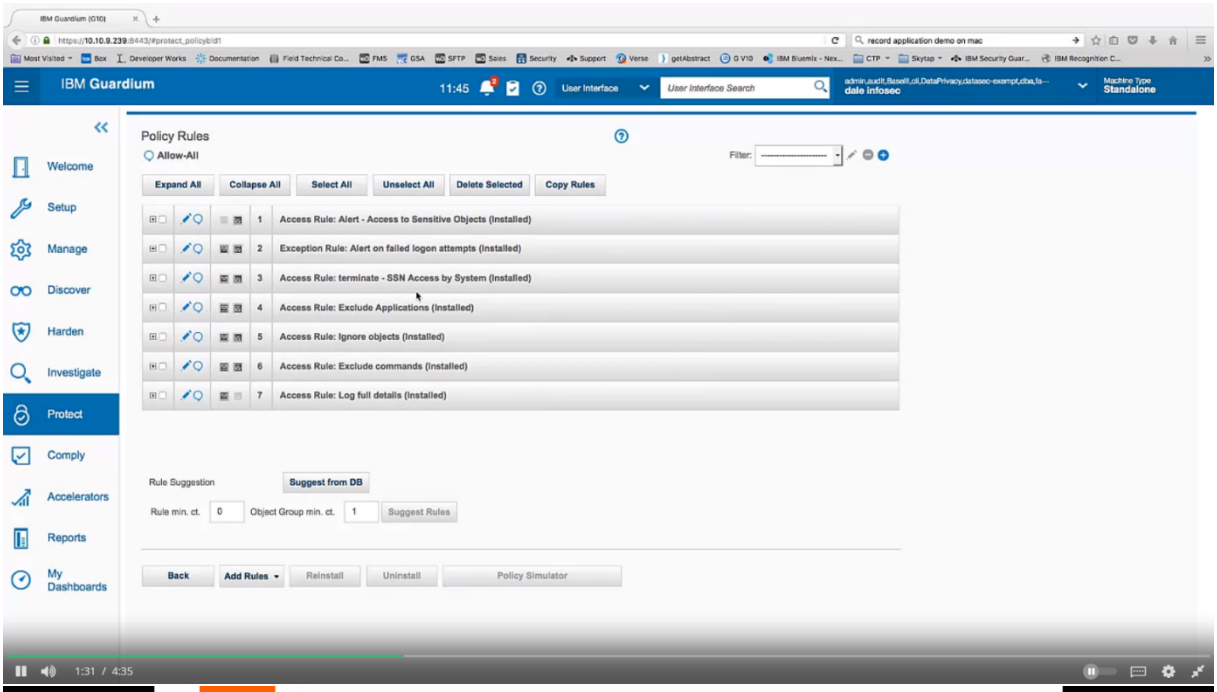
Securing Databases Wrap Up

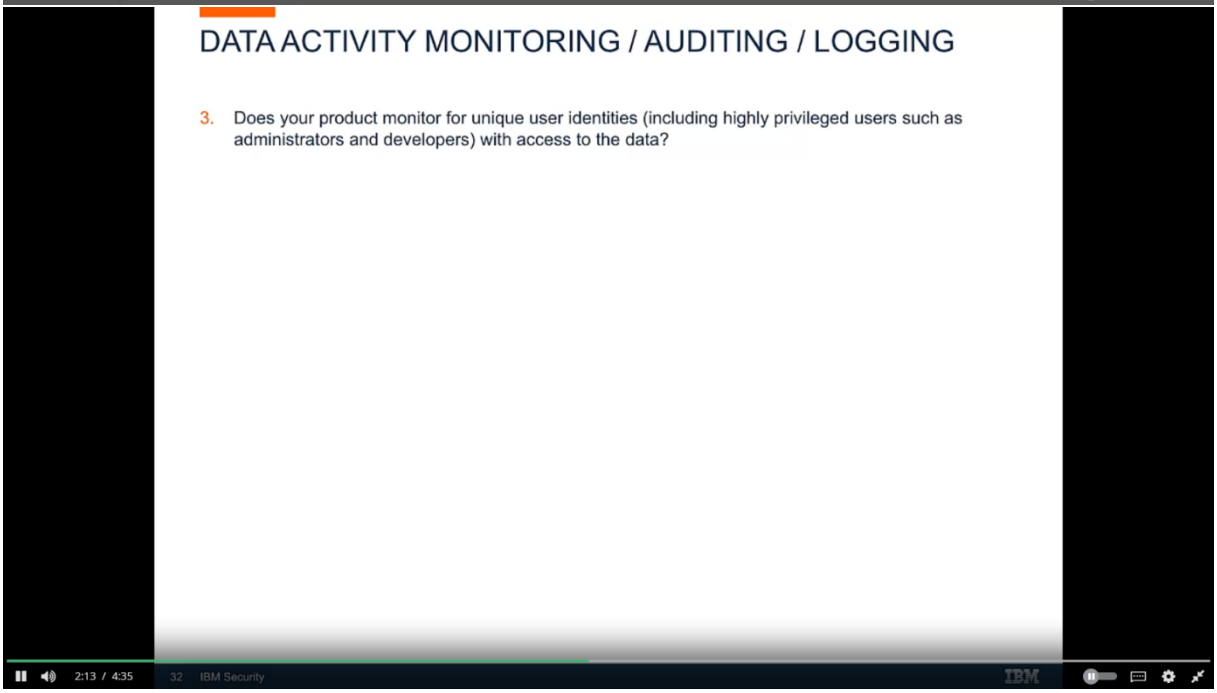


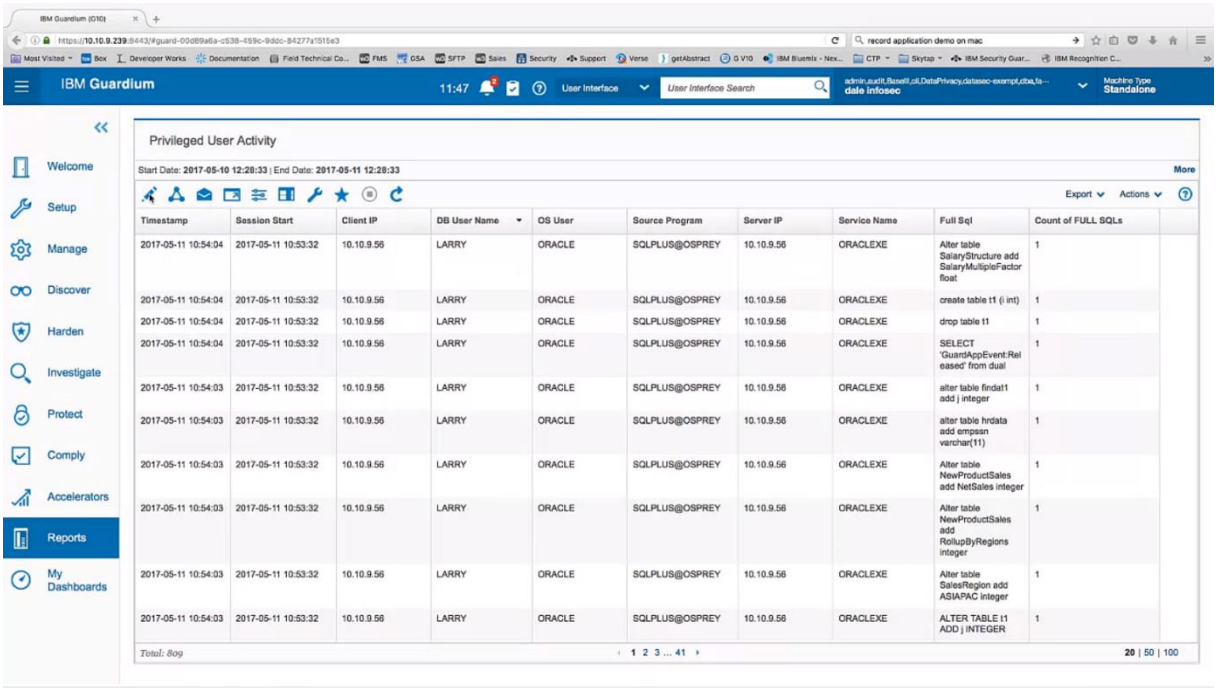
Data Monitoring


DATA ACTIVITY MONITORING / AUDITING / LOGGING
1. Does your product log all key activity, including key generation, retrieval/usage, etc.?
2. Demo data access activity monitoring and logging of the activity monitoring?
3. Does your product monitor for unique user identities (including highly privileged users such as administrators and developers) with access to the data?
4. At the storage level, can it detect/identify assess to highly privileged users such as database administrators, system administrators or developers?
5. Does your product generate real time alerts of policy violations while recording activities?
6. Does your product monitor user data access activity in real time with customizable security alerts and blocking unacceptable user behavior, access patterns or geographic access, etc.? If yes please describe.
7. Does your product generate alerts?
8. Demo the capability for reporting and metrics using information logged?
9. Does your product create auditable reports of data access and security events with customizable details that can address defined regulations or standard audit process requirements? If yes please
10. Does your product support the ability to log security events to a centralized security incident and event management (SIEM) system?
11. Demo monitoring of non-Relational Database Management Systems (RDBMS) systems, such as Cognos, Hadoop, Spark, etc.
12. Demo the following event attributes and to what level of granularity?
0:38 / 4:35
28 IBM Security
IBM


DATA ACTIVITY MONITORING / AUDITING / LOGGING
13. Demo when the product provides the following event attributes and to what level of granularity?
o Log date and time (international format)
o Event date and time - the event time stamp may be different to the time of logging e.g. server logging where the client application is hosted on remote device that is only periodically or intermittently online
o Interaction identifier
14. Demo sufficient information in the log record to establish what events occurred and who or what caused them?
15. Demo configurations configured to monitor user account additions and changes?
16. Demo configurations to monitor the following event?
Significant instances of failed password attempts and against multiple accounts within a short time frame which may indicate hacking attempts
17. Demo configurations to monitor the following event?
Significant instances of failed access attempts to the database not authorized to the account ID
18. Demo configurations to monitor the following event?
Attempts to SELECT the list of users and passwords
19. Demo configurations to monitor the following event?
All direct access to the database from accounts which should be limited to access through the application
20. Demo configurations to monitor the following event?
Use of nonstandard tools (i.e. Excel/Access) to directly access DBMS
21. Demo configurations to monitor the following event?
Use of Application ID (AppID) from a source other than the defined owner Application location (based on host name or IP address)
22. Demo configurations to monitor the following event?
Log failures, manual logging shut down and attempts to purge
0:45 / 4:35
29 IBM Security
IBM

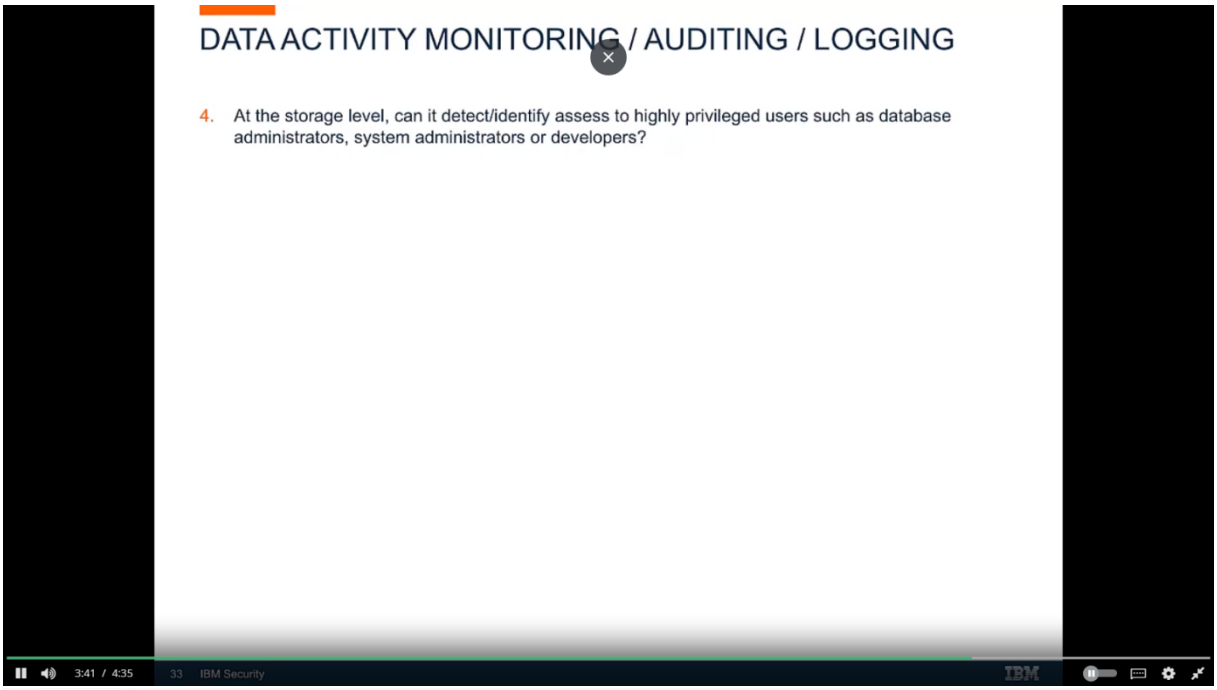

IBM Guardium
11:45
User Interface
User Interface Search
admin,audit,Base#,cli,DataPrivacy,dataec-exempt,cba,fa--
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Policy Rules
Allow-All
Filter:
Expand All
Collapse All
Select All
Unselect All
Delete Selected
Copy Rules
1 Access Rule: Alert - Access to Sensitive Objects (Installed)
2 Exception Rule: Alert on failed logon attempts (Installed)
3 Access Rule: terminate - SSN Access by System (Installed)
4 Access Rule: Exclude Applications (Installed)
5 Access Rule: Ignore objects (Installed)
6 Access Rule: Exclude commands (Installed)
7 Access Rule: Log full details (Installed)
Rule Suggestion
Suggest from DB
Rule min. ct.
0
Object Group min. ct.
1
Suggest Rules
Back
Add Rules
Reinstall
Uninstall
Policy Simulator
1:31 / 4:35

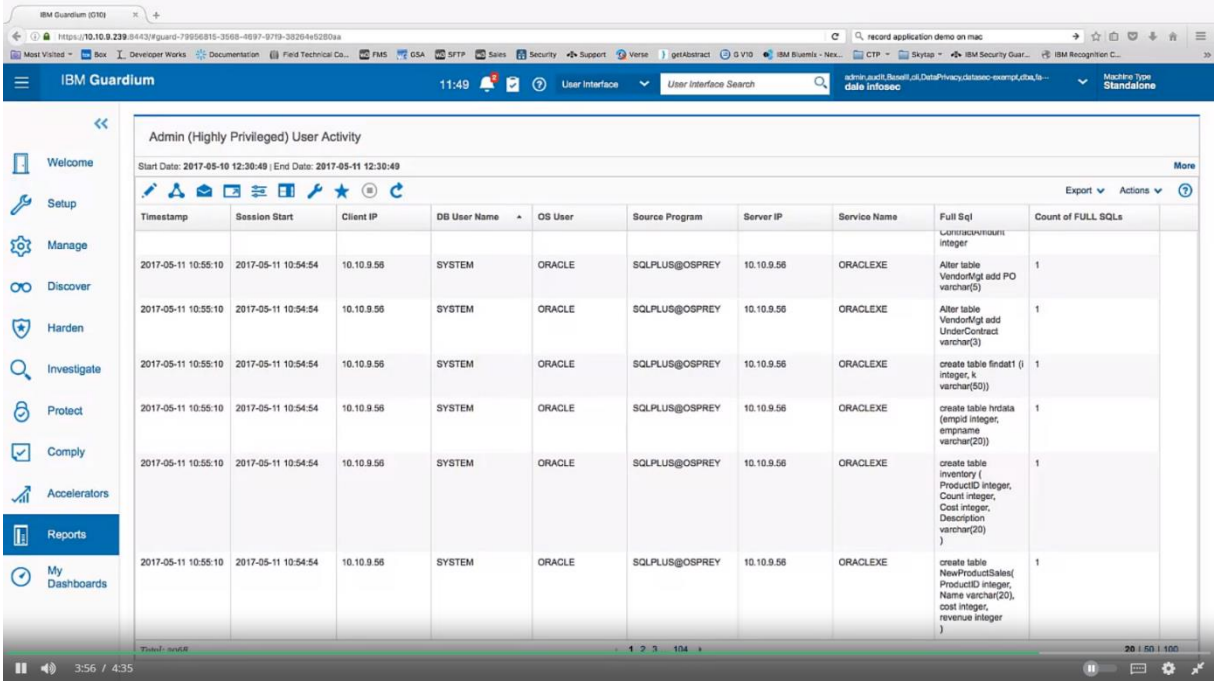

DATA ACTIVITY MONITORING / AUDITING / LOGGING
3. Does your product monitor for unique user identities (including highly privileged users such as administrators and developers) with access to the data?
2:13 / 4:35
32 IBM Security



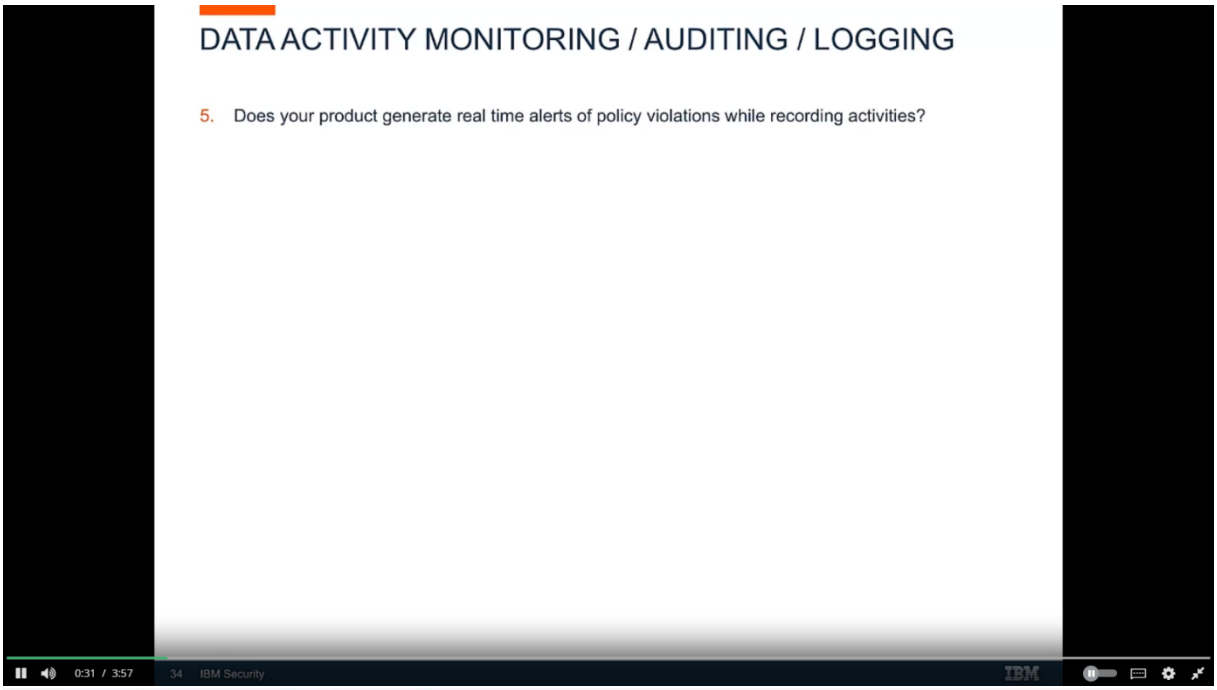
Privileged User Activity
Generated by user: dale
On: 2017-05-11 12:29:04
REMOTE_SOURCE:
From: NOW -1 DAY
To: NOW
Alias: Off

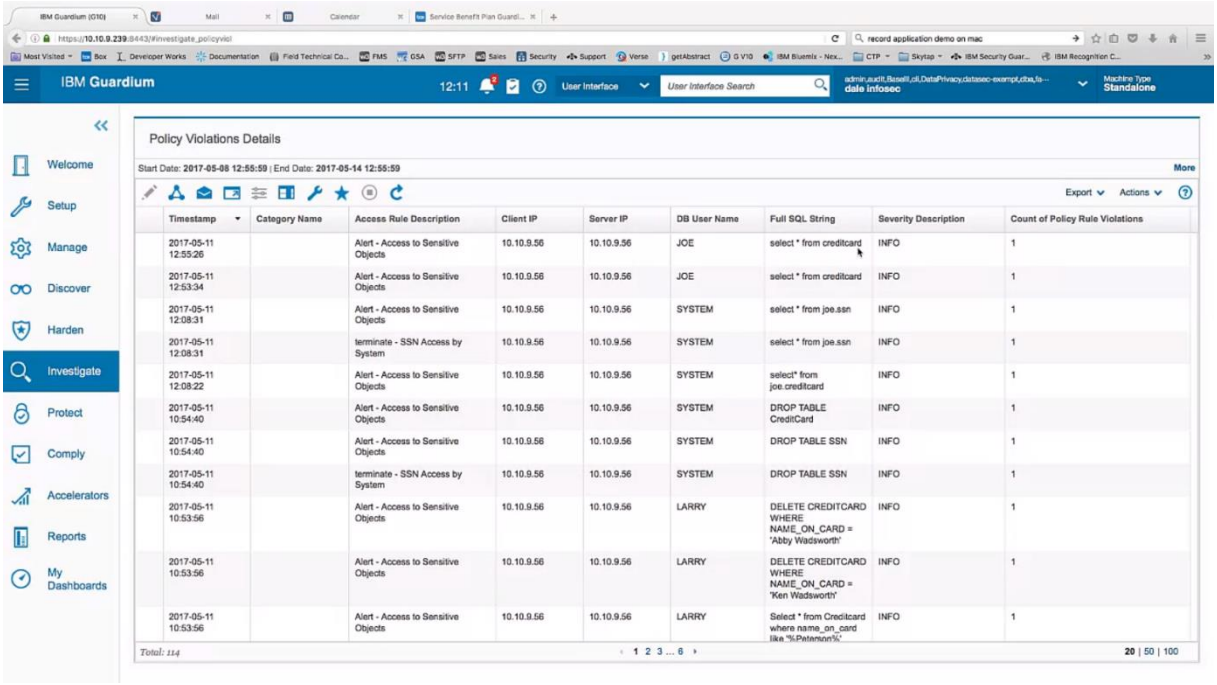
Timestamp	Session Start	Client IP	DB User Name	OS User	Source Program	Server IP	Service Name	Full Sql	Count of FULL SQLs
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalaryStructure add SalaryMultipleFactor float	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table t1 (i int)	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	drop table t1	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	SELECT 'GuardAppEvent:Released' from dual	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table findat1 add j integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table hrdata add empssn varchar(11)	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add RollupByRegions integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalesRegion add ASIAPAC integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	ALTER TABLE t1 ADD j INTEGER	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table test1 add j integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add Amount integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add ContractAmount integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add PO varchar(5)	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add UnderContract varchar(3)	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table findat1 (i integer, k varchar(50))	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table hrdata (empid integer, empname varchar(20))	1

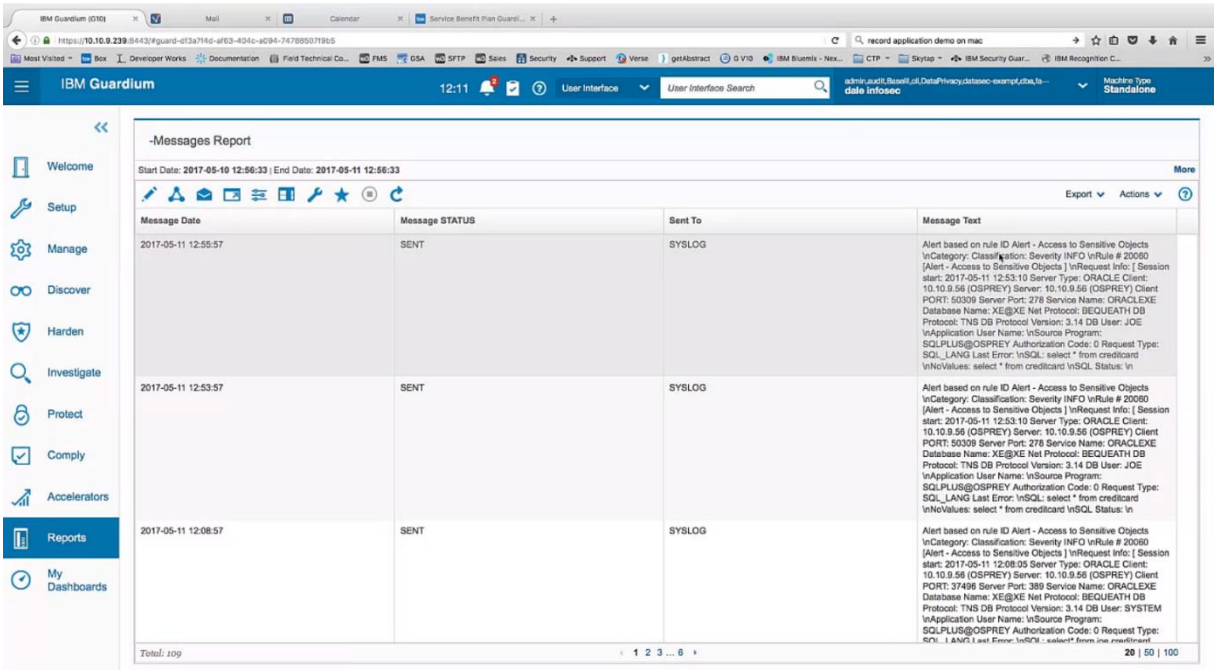

DATA ACTIVITY MONITORING / AUDITING / LOGGING
4. At the storage level, can it detect/identify assess to highly privileged users such as database administrators, system administrators or developers?
3:41 / 4:35
33 IBM Security
IBM

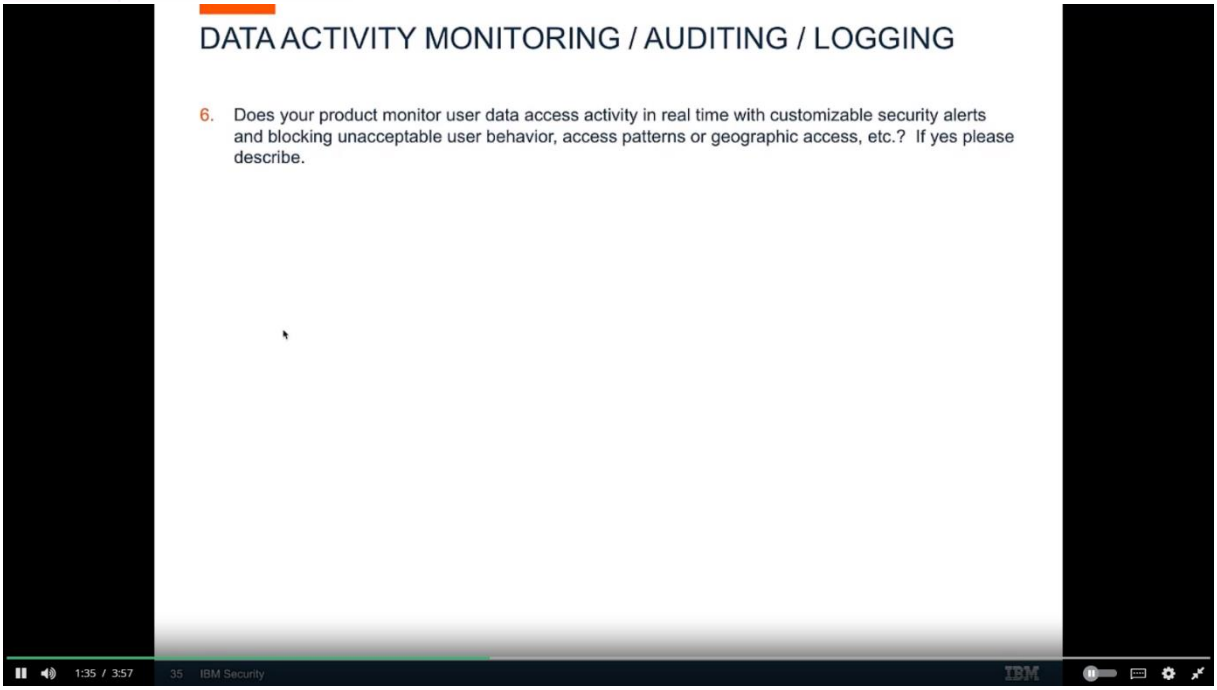

IBM Guardium
11:49
User Interface
User Interface Search
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Admin (Highly Privileged) User Activity
Start Date: 2017-05-10 12:30:49 | End Date: 2017-05-11 12:30:49
More
Export
Actions
Timestamp
Session Start
Client IP
DB User Name
OS User
Source Program
Server IP
Service Name
Full Sql
Count of FULL SQLs
2017-05-11 10:55:10
2017-05-11 10:54:54
10.10.9.56
SYSTEM
ORACLE
SQLPLUS@OSPREY
10.10.9.56
ORACLEXE
Alter table VendorMgt add PO varchar(5)
Alter table VendorMgt add UnderContract varchar(3)
create table findat1 (i integer, k varchar(50))
create table hrdata (empid integer, empname varchar(20))
create table inventory (ProductID integer, Count integer, Cost integer, Description varchar(20))
create table NewProductSales(ProductID integer, Name varchar(20), cost integer, revenue integer)
1
3:56 / 4:35

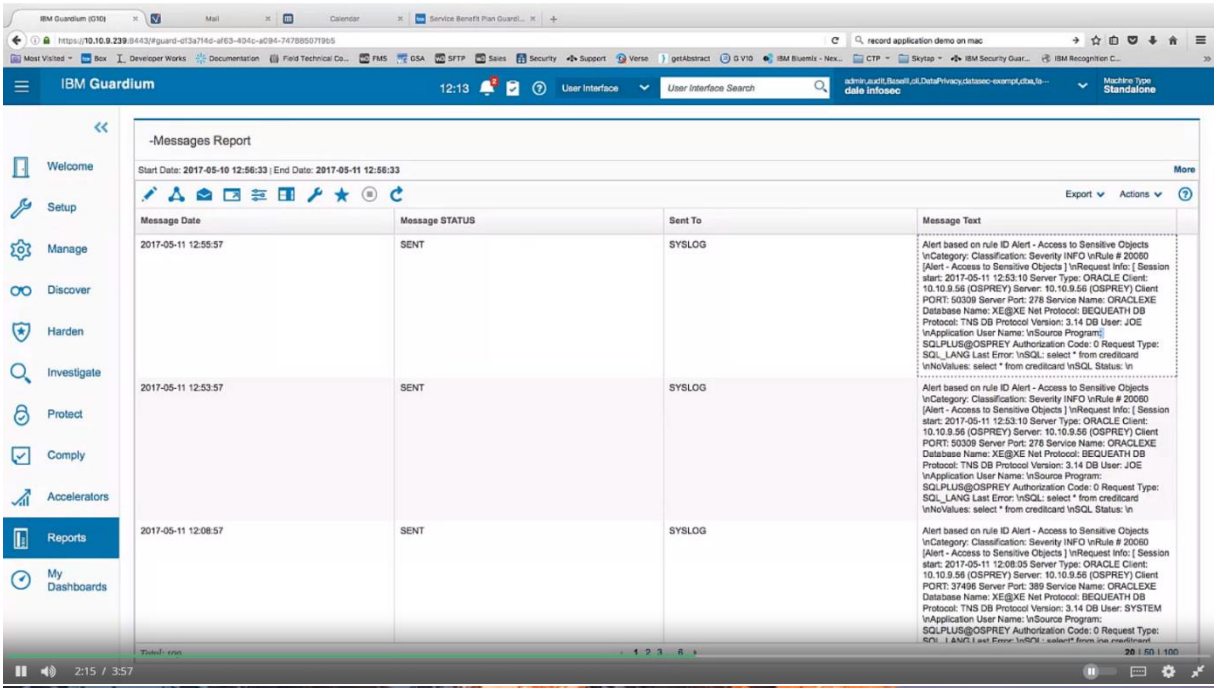
Data Alerts

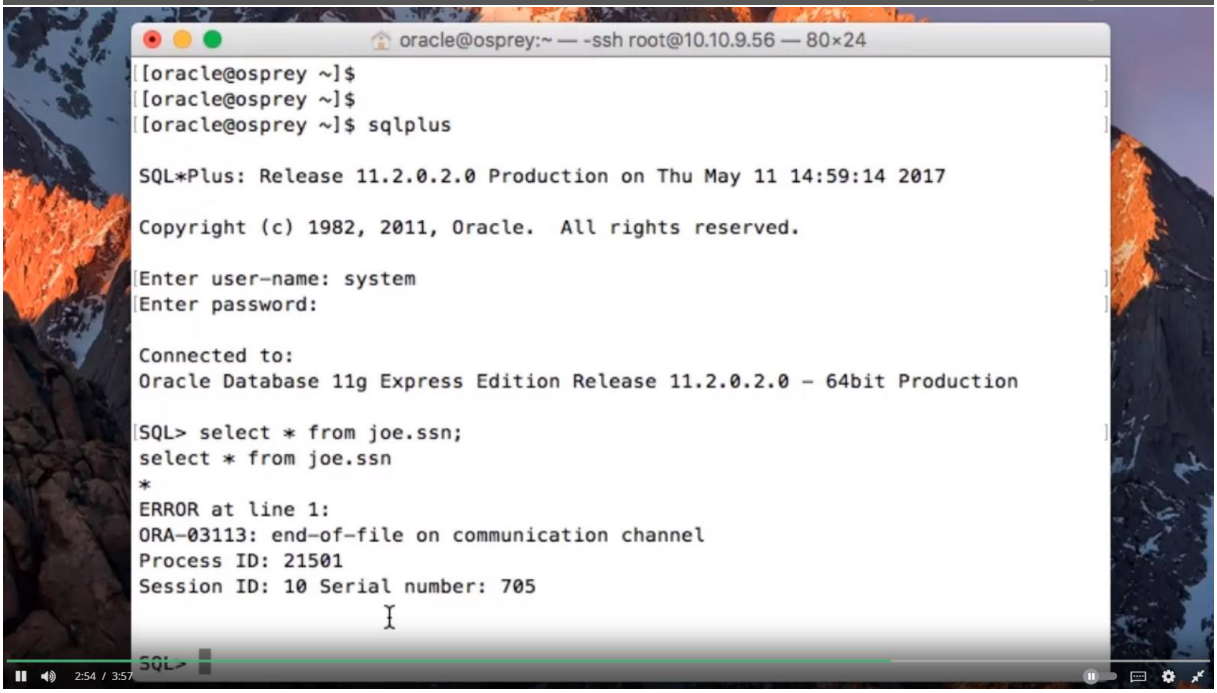

DATA ACTIVITY MONITORING / AUDITING / LOGGING
5. Does your product generate real time alerts of policy violations while recording activities?
0:31 / 3:57
34 IBM Security
IBM

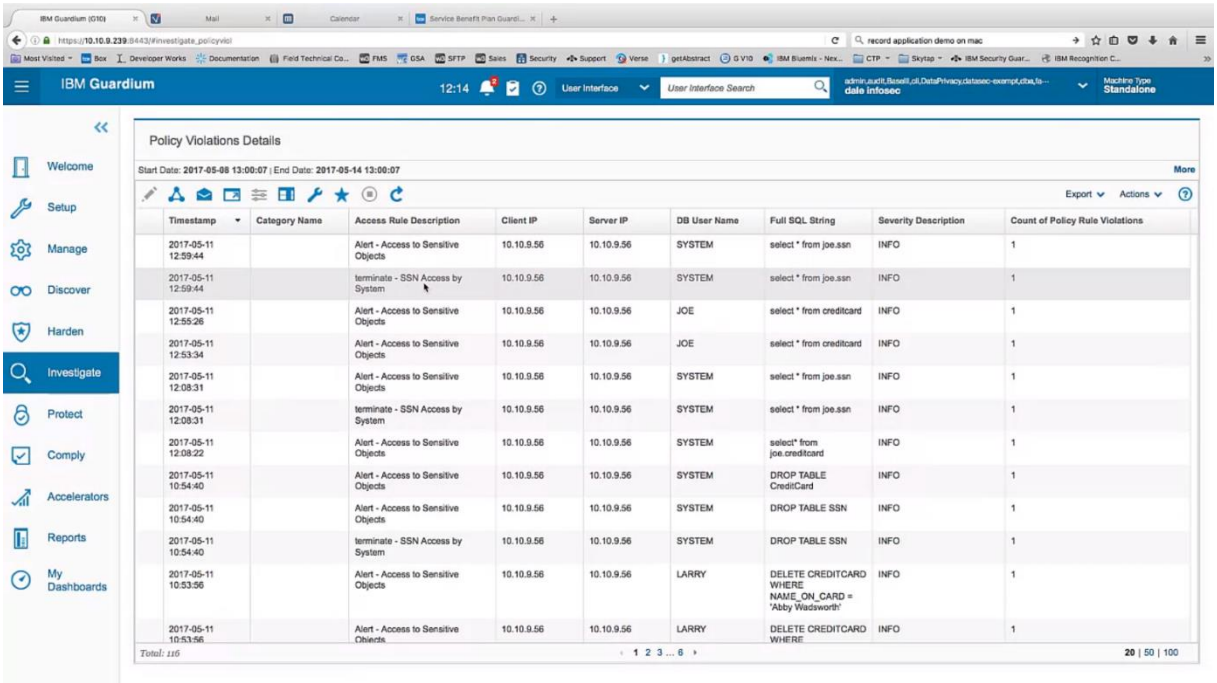

IBM Guardium
12:11
User Interface
User Interface Search
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Policy Violations Details
Start Date: 2017-05-08 12:55:59 | End Date: 2017-05-14 12:55:59
More
Export
Actions
Timestamp
Category Name
Access Rule Description
Client IP
Server IP
DB User Name
Full SQL String
Severity Description
Count of Policy Rule Violations
2017-05-11 12:55:26 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 JOE select * from creditcard INFO 1
2017-05-11 12:53:34 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 JOE select * from creditcard INFO 1
2017-05-11 12:08:31 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 SYSTEM select * from joe.ssn INFO 1
2017-05-11 12:08:31 terminate - SSN Access by System 10.10.9.56 10.10.9.56 SYSTEM select * from joe.ssn INFO 1
2017-05-11 12:08:22 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 SYSTEM select* from joe.creditcard INFO 1
2017-05-11 10:54:40 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 SYSTEM DROP TABLE CreditCard INFO 1
2017-05-11 10:54:40 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 SYSTEM DROP TABLE SSN INFO 1
2017-05-11 10:54:40 terminate - SSN Access by System 10.10.9.56 10.10.9.56 SYSTEM DROP TABLE SSN INFO 1
2017-05-11 10:53:56 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 LARRY DELETE CREDITCARD WHERE NAME_ON_CARD = 'Abby Wadsworth' INFO 1
2017-05-11 10:53:56 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 LARRY DELETE CREDITCARD WHERE NAME_ON_CARD = 'Ken Wadsworth' INFO 1
2017-05-11 10:53:56 Alert - Access to Sensitive Objects 10.10.9.56 10.10.9.56 LARRY Select * from Creditcard where name_on_card like '%Peterson%' INFO 1
Total: 114
1 2 3 ... 6
20 | 50 | 100


IBM Guardium
12:11
User Interface
User Interface Search
admin,audit,Baselil,cli,DataPrivacy,datasec-exampt,cba,ta--
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
-Messages Report
Start Date: 2017-05-10 12:56:33 | End Date: 2017-05-11 12:56:33
More
Export
Actions
Message Date
Message STATUS
Sent To
Message Text
2017-05-11 12:55:57
SENT
SYSLOG
Alert based on rule ID Alert - Access to Sensitive Objects \nCategory: Classification: Severity INFO \nRule # 20060 [Alert - Access to Sensitive Objects] \nRequest Info: [Session start: 2017-05-11 12:53:10 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 50309 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE \nApplication User Name: \nSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: \nSQL: select * from creditcard \nNoValues: select * from creditcard \nSQL Status: \n
2017-05-11 12:53:57
SENT
SYSLOG
Alert based on rule ID Alert - Access to Sensitive Objects \nCategory: Classification: Severity INFO \nRule # 20060 [Alert - Access to Sensitive Objects] \nRequest Info: [Session start: 2017-05-11 12:53:10 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 50309 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE \nApplication User Name: \nSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: \nSQL: select * from creditcard \nNoValues: select * from creditcard \nSQL Status: \n
2017-05-11 12:08:57
SENT
SYSLOG
Alert based on rule ID Alert - Access to Sensitive Objects \nCategory: Classification: Severity INFO \nRule # 20060 [Alert - Access to Sensitive Objects] \nRequest Info: [Session start: 2017-05-11 12:08:05 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 37496 Server Port: 389 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: SYSTEM \nApplication User Name: \nSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type:
Total: 109
1 2 3 ... 8
20 | 50 | 100


DATA ACTIVITY MONITORING / AUDITING / LOGGING
6. Does your product monitor user data access activity in real time with customizable security alerts and blocking unacceptable user behavior, access patterns or geographic access, etc.? If yes please describe.
1:35 / 3:57
35 IBM Security

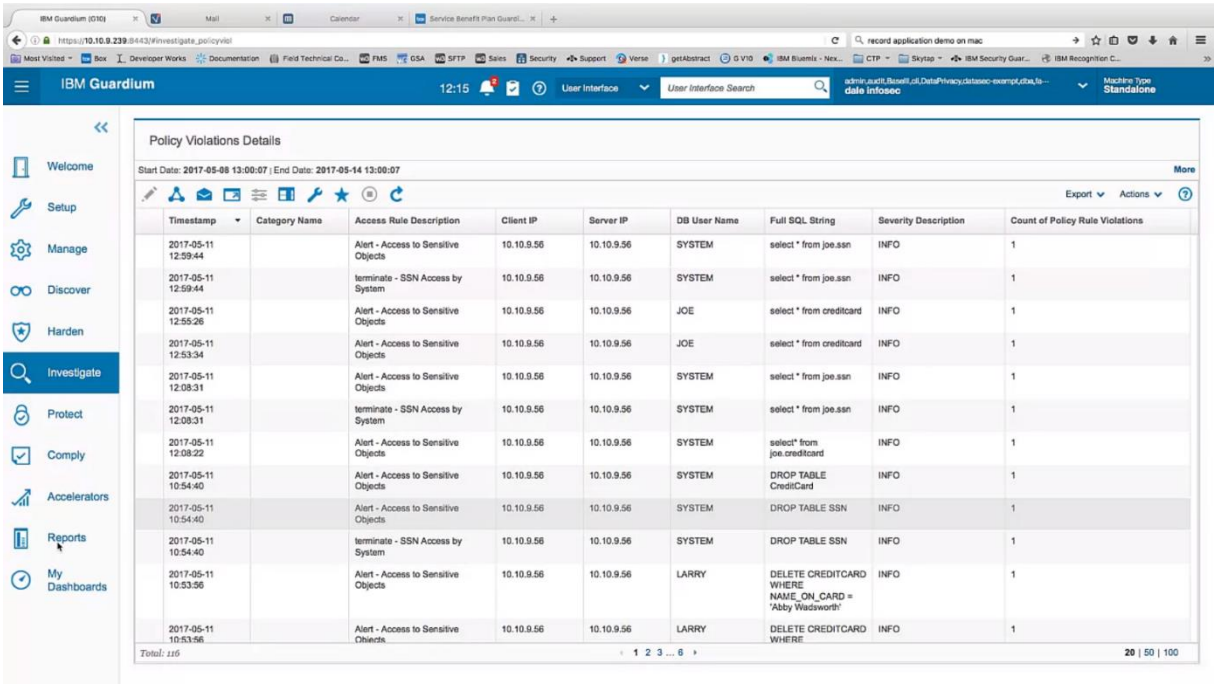

IBM Guardium
-Messages Report
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Message Date
Message STATUS
Sent To
Message Text
2017-05-11 12:55:57
SENT
SYSLOG
2017-05-11 12:53:57
SENT
SYSLOG
2017-05-11 12:08:57
SENT
SYSLOG
2:15 / 3:57


oracle@osprey:~ — -ssh root@10.10.9.56 — 80×24
[oracle@osprey ~]$
[oracle@osprey ~]$
[oracle@osprey ~]$ sqlplus
SQL*Plus: Release 11.2.0.2.0 Production on Thu May 11 14:59:14 2017
Copyright (c) 1982, 2011, Oracle. All rights reserved.
Enter user-name: system
Enter password:
Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production
SQL> select * from joe.ssn;
select * from joe.ssn
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel
Process ID: 21501
Session ID: 10 Serial number: 705
SQL>
2:54 / 3:57



DATA ACTIVITY MONITORING / AUDITING / LOGGING

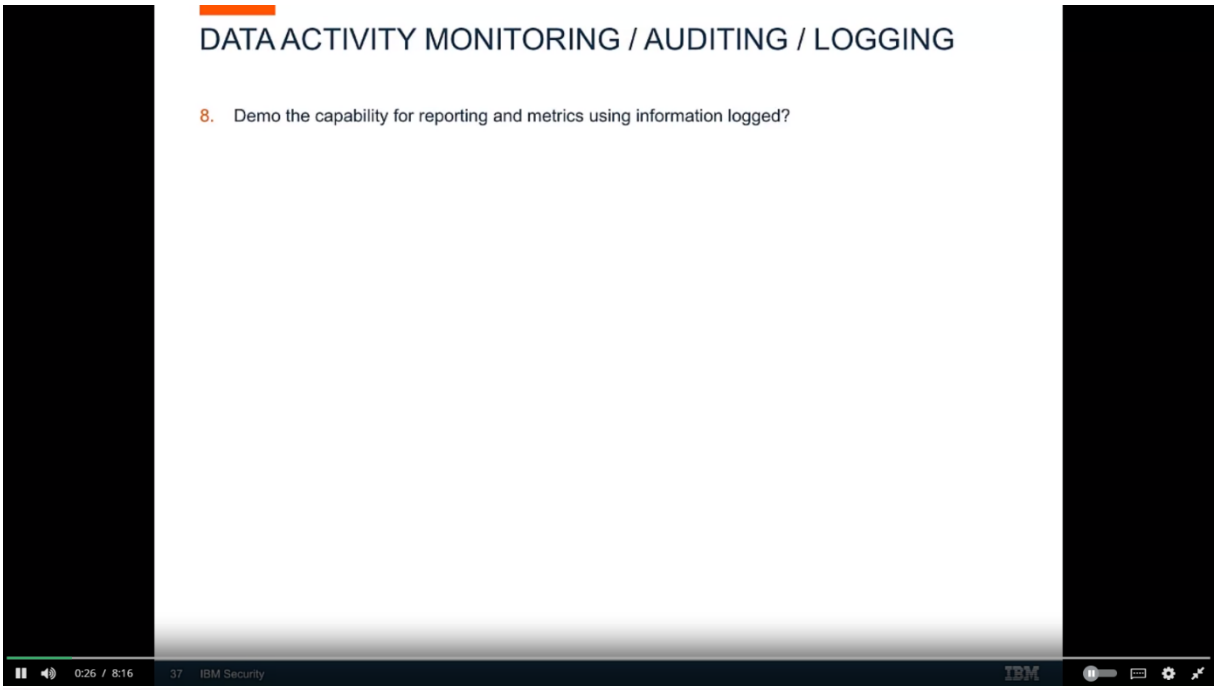
7. Does your product generate alerts?

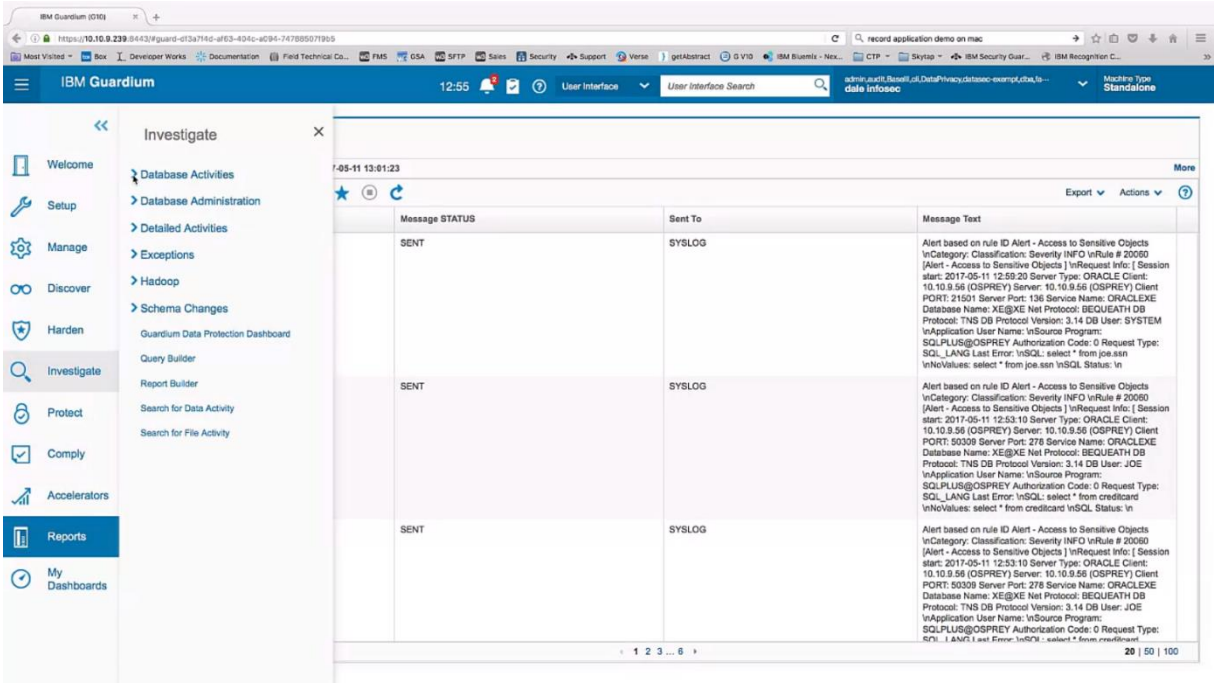


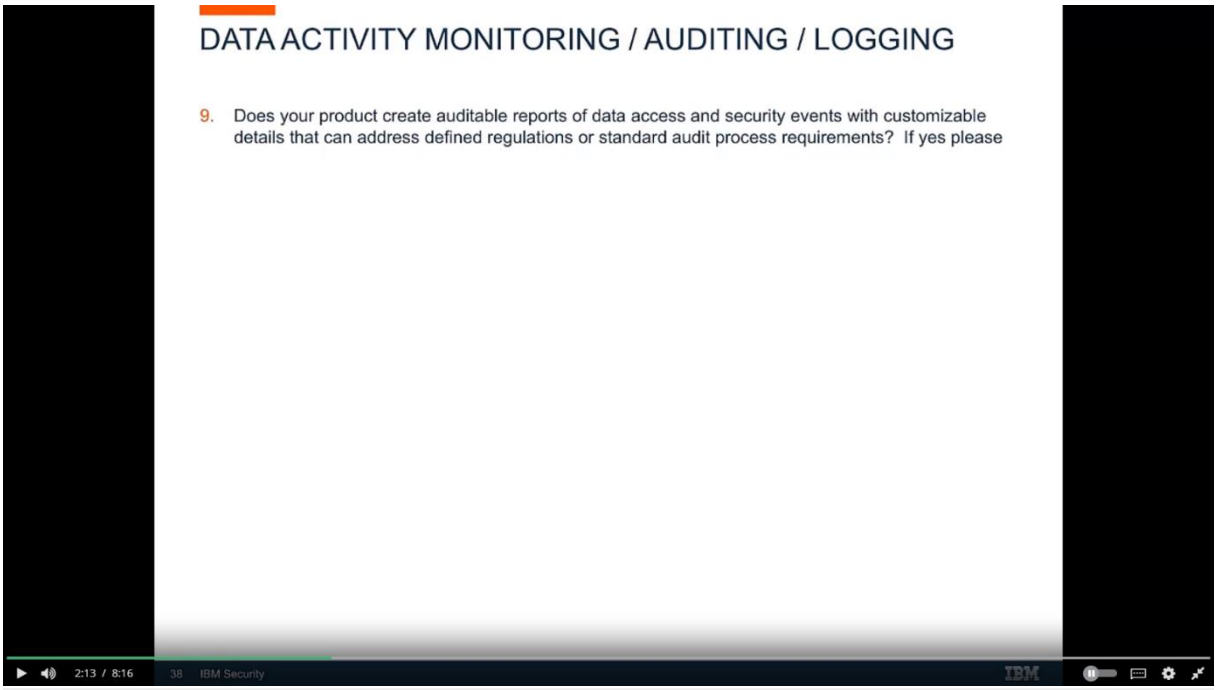
Data Activity Reporting

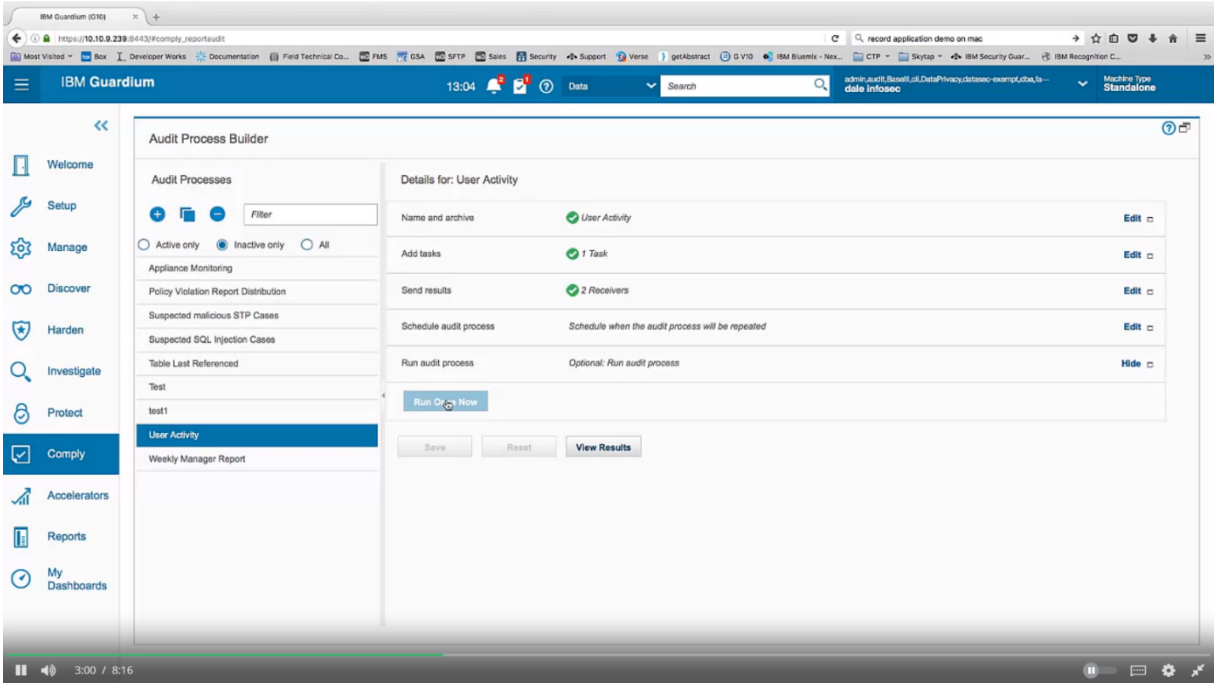
DATA ACTIVITY MONITORING / AUDITING / LOGGING

8. Demo the capability for reporting and metrics using information logged?



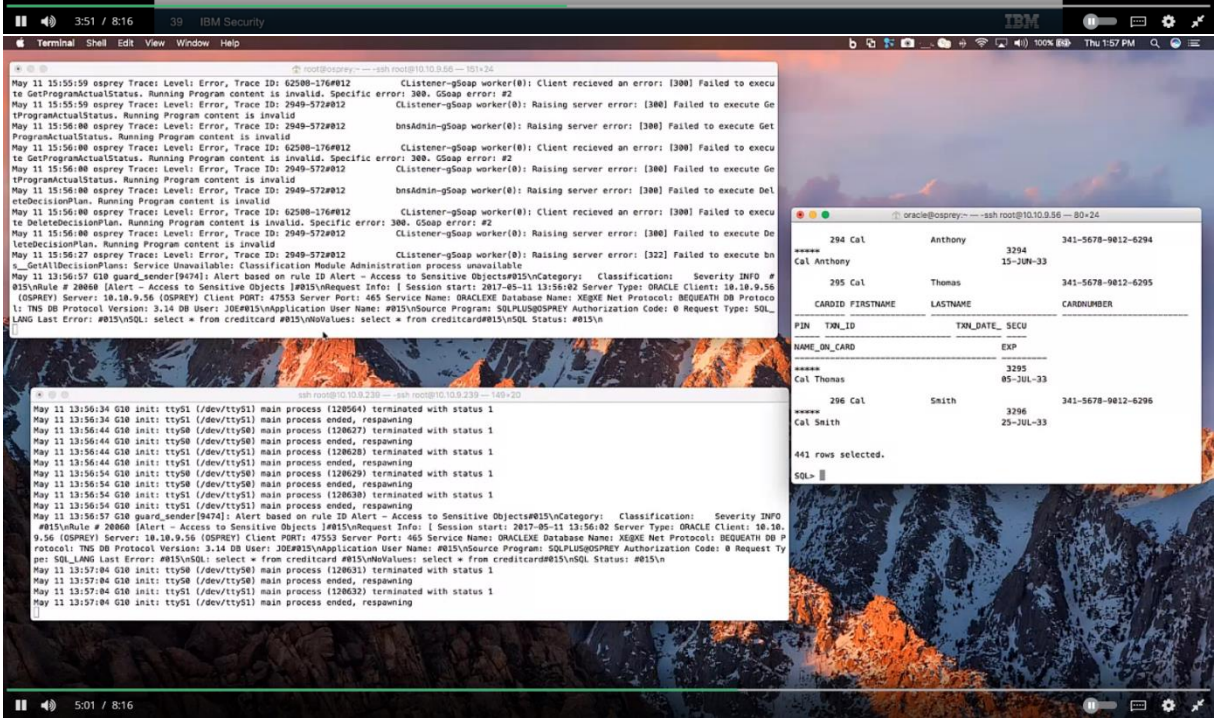


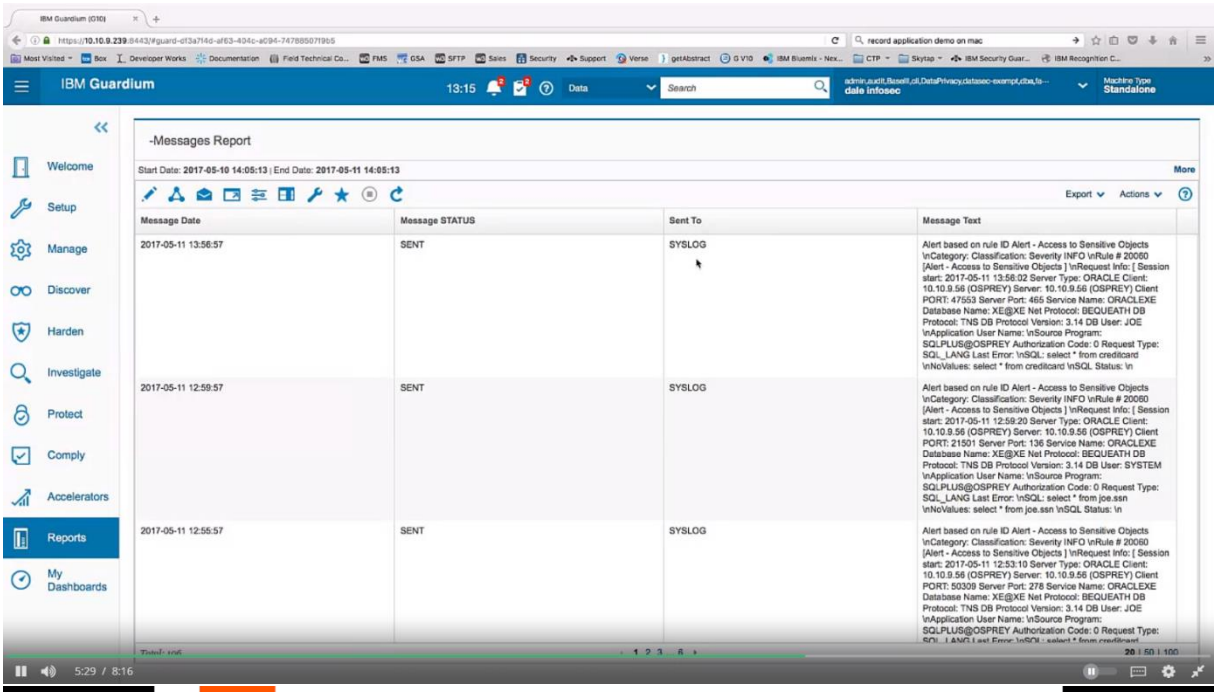

DATA ACTIVITY MONITORING / AUDITING / LOGGING
9. Does your product create auditable reports of data access and security events with customizable details that can address defined regulations or standard audit process requirements? If yes please
2:13 / 8:16
38 IBM Security

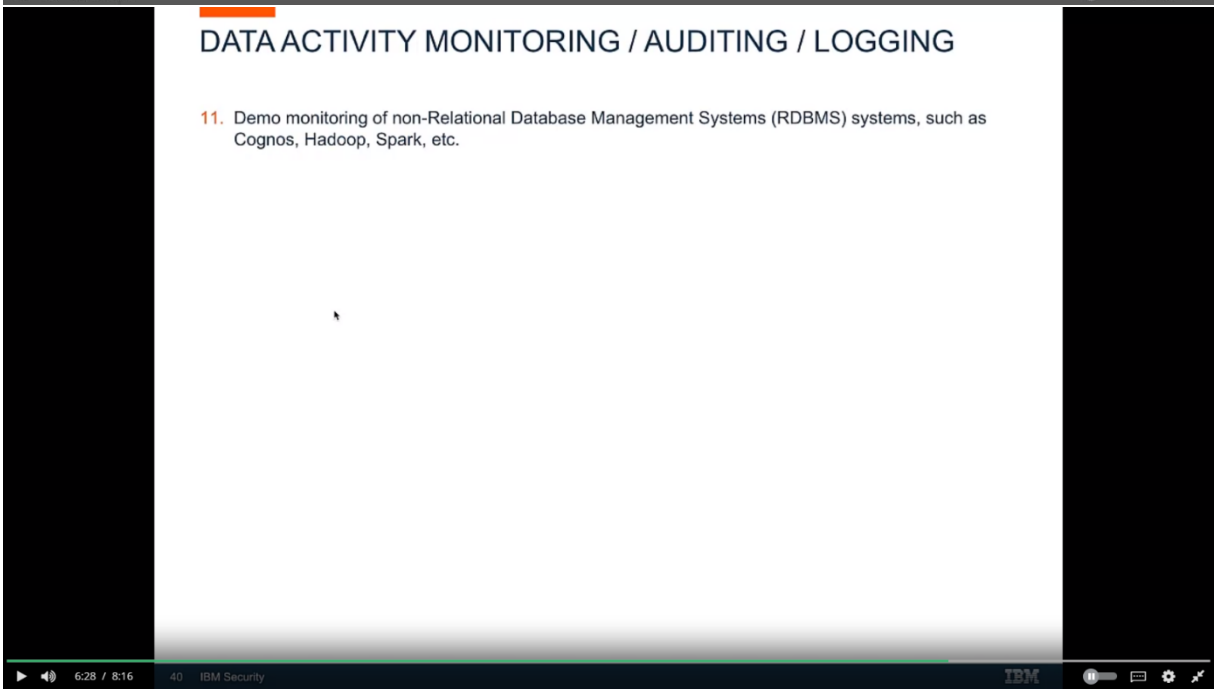

IBM Guardium
13:04
Data
Search
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Audit Process Builder
Audit Processes
Filter
Active only
Inactive only
All
Appliance Monitoring
Policy Violation Report Distribution
Suspected malicious STP Cases
Suspected SQL Injection Cases
Table Last Referenced
Test
test1
User Activity
Weekly Manager Report
Details for: User Activity
Name and archive
User Activity
Edit
Add tasks
1 Task
Edit
Send results
2 Receivers
Edit
Schedule audit process
Schedule when the audit process will be repeated
Edit
Run audit process
Optional: Run audit process
Hide
Run Once Now
Save
Reset
View Results
3:00 / 8:16

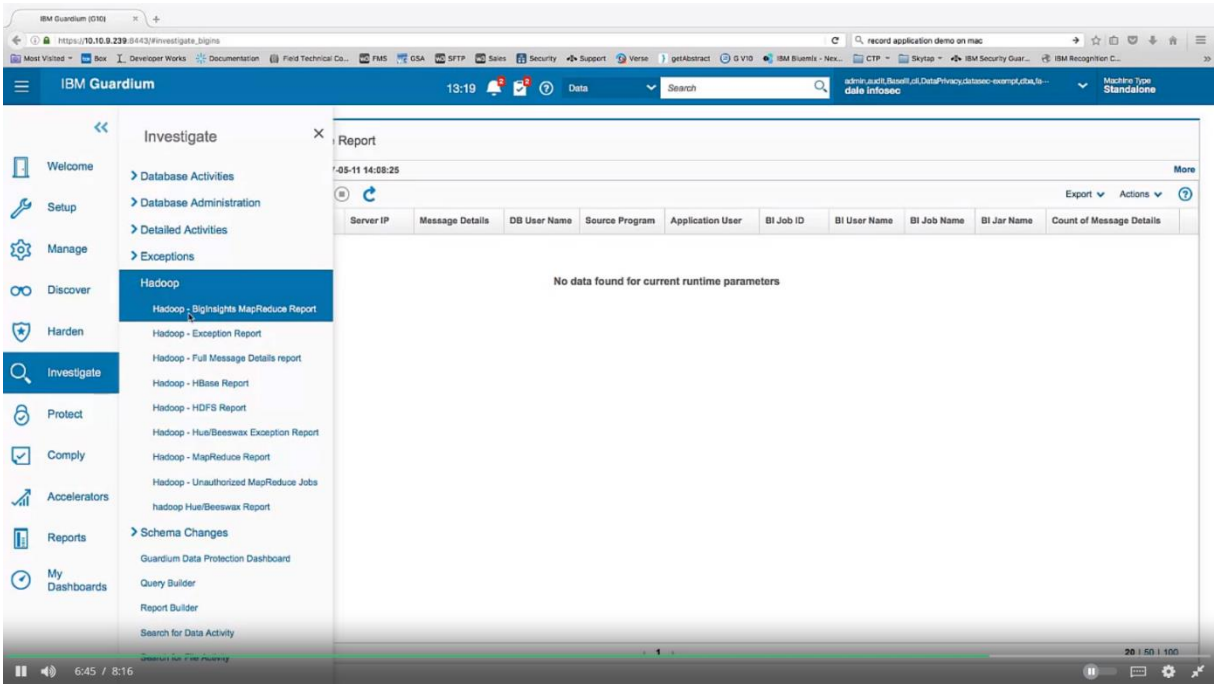
DATA ACTIVITY MONITORING / AUDITING / LOGGING

10. Does your product support the ability to log security events to a centralized security incident and event management (SIEM) system?

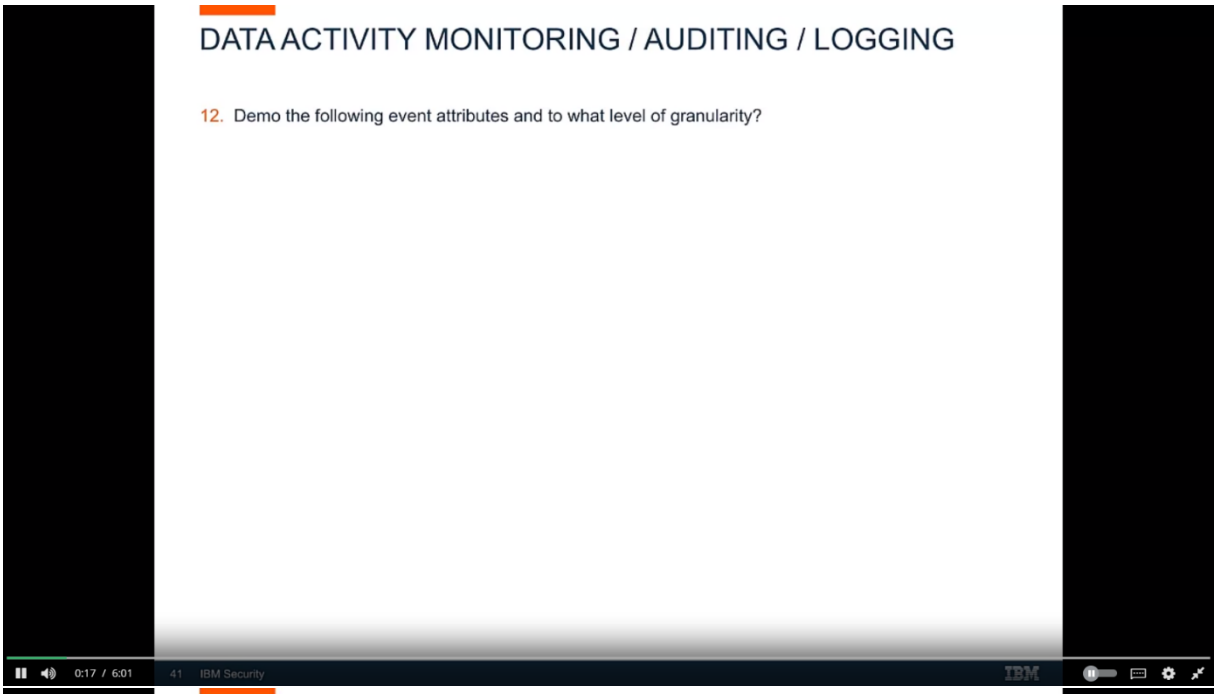


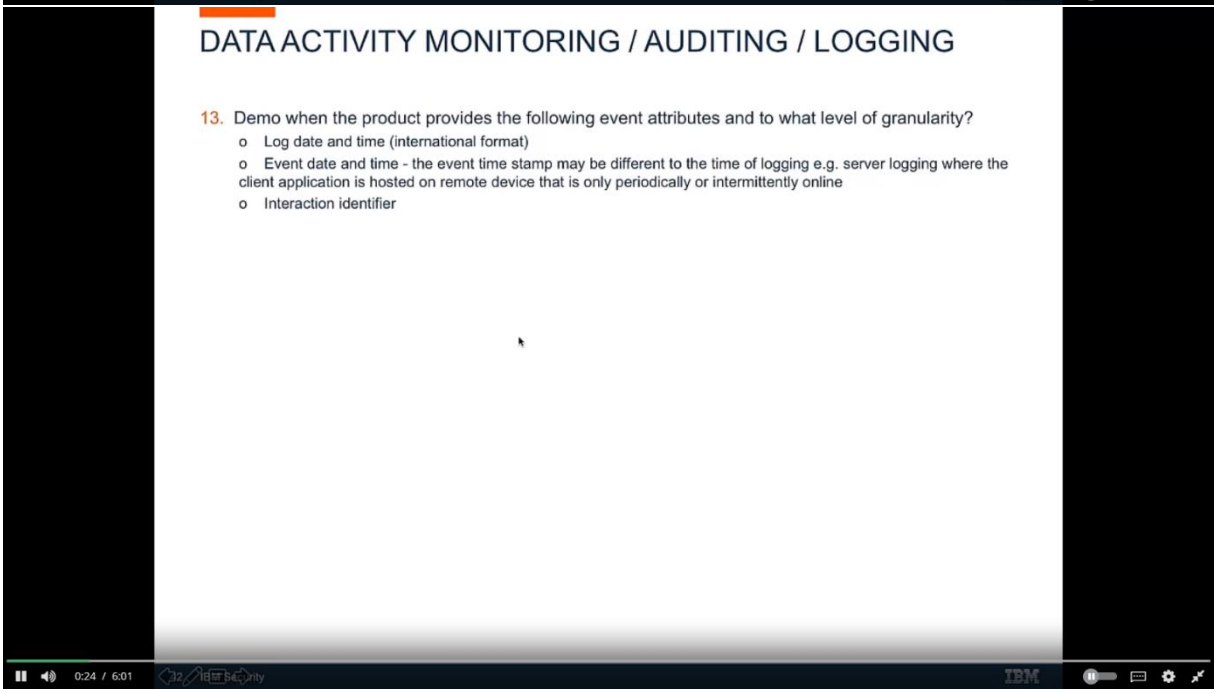

IBM Guardium
13:15
Data
Search
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
-Messages Report
Start Date: 2017-05-10 14:05:13 | End Date: 2017-05-11 14:05:13
More
Export
Actions
Message Date
Message STATUS
Sent To
Message Text
2017-05-11 13:56:57
SENT
SYSLOG
Alert based on rule ID Alert - Access to Sensitive Objects \nCategory: Classification: Severity INFO \nRule # 20060 [Alert - Access to Sensitive Objects] \nRequest Info: [Session start: 2017-05-11 13:56:02 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 47553 Server Port: 465 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE \nApplication User Name: \nSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: \nSQL: select * from creditcard \nNoValues: select * from creditcard \nSQL Status: \n
2017-05-11 12:59:57
SENT
SYSLOG
Alert based on rule ID Alert - Access to Sensitive Objects \nCategory: Classification: Severity INFO \nRule # 20060 [Alert - Access to Sensitive Objects] \nRequest Info: [Session start: 2017-05-11 12:59:20 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 21501 Server Port: 136 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: SYSTEM \nApplication User Name: \nSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: \nSQL: select * from joe.ssn \nNoValues: select * from joe.ssn \nSQL Status: \n
2017-05-11 12:55:57
SENT
SYSLOG
Alert based on rule ID Alert - Access to Sensitive Objects \nCategory: Classification: Severity INFO \nRule # 20060 [Alert - Access to Sensitive Objects] \nRequest Info: [Session start: 2017-05-11 12:53:10 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 50309 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE \nApplication User Name: \nSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type:
5:29 / 8:16

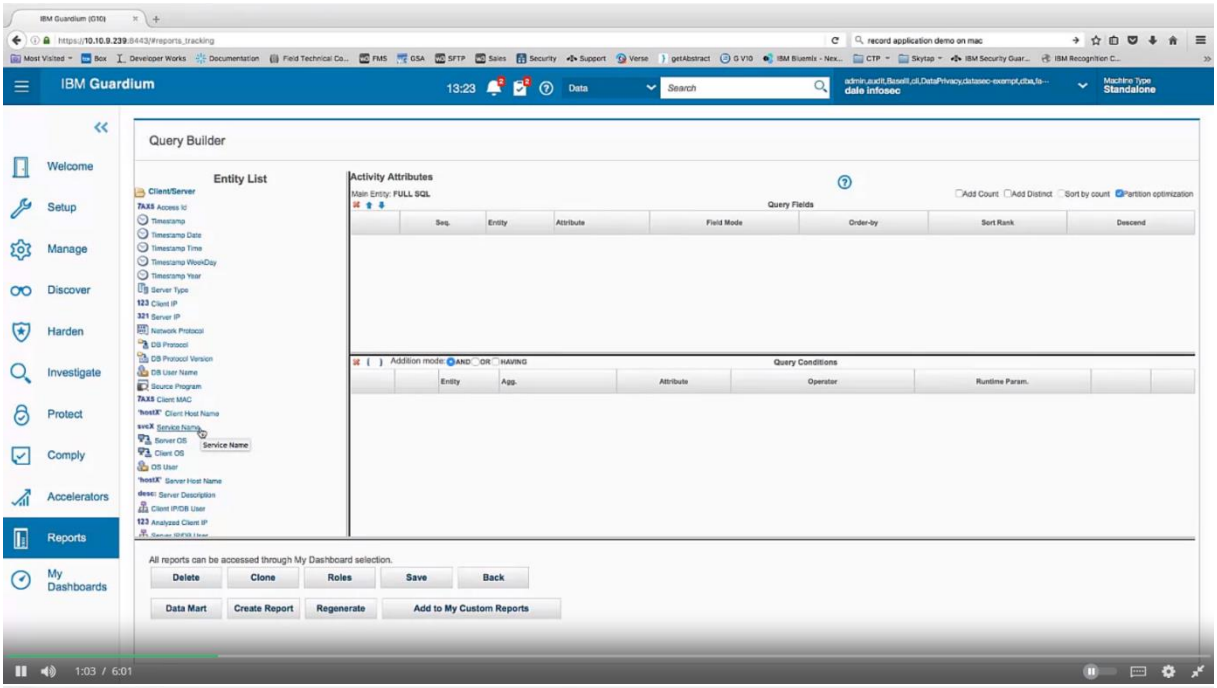

DATA ACTIVITY MONITORING / AUDITING / LOGGING
11. Demo monitoring of non-Relational Database Management Systems (RDBMS) systems, such as Cognos, Hadoop, Spark, etc.
6:28 / 8:16
40
IBM Security
IBM

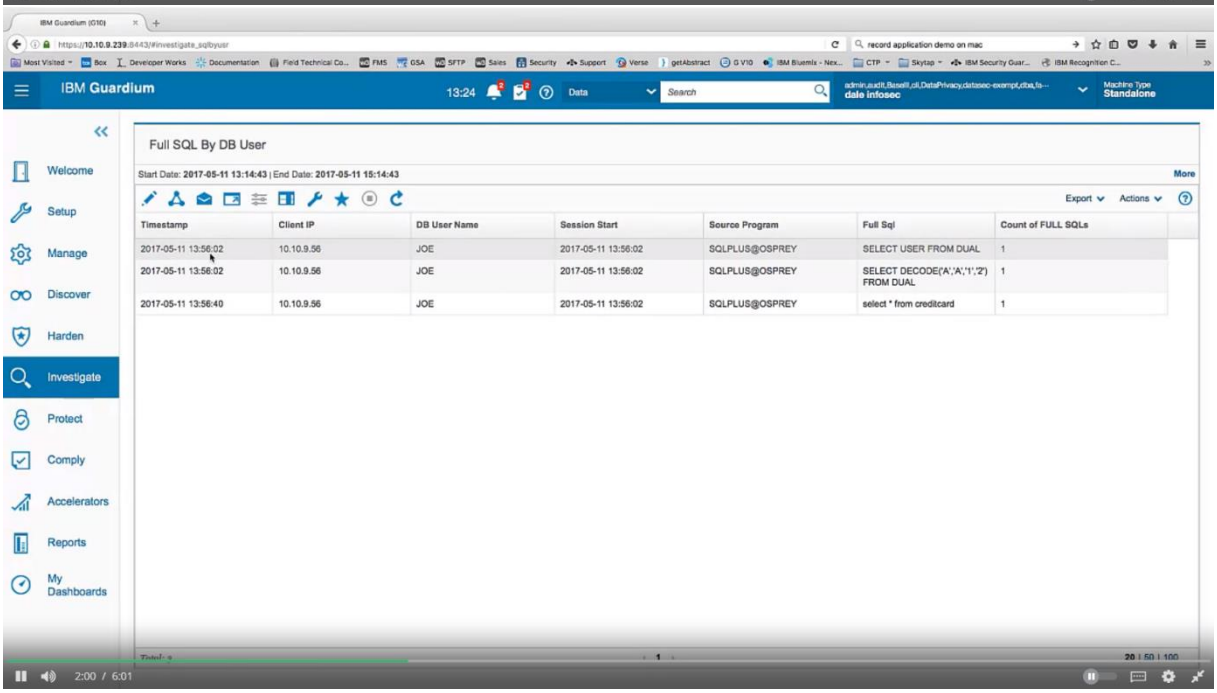


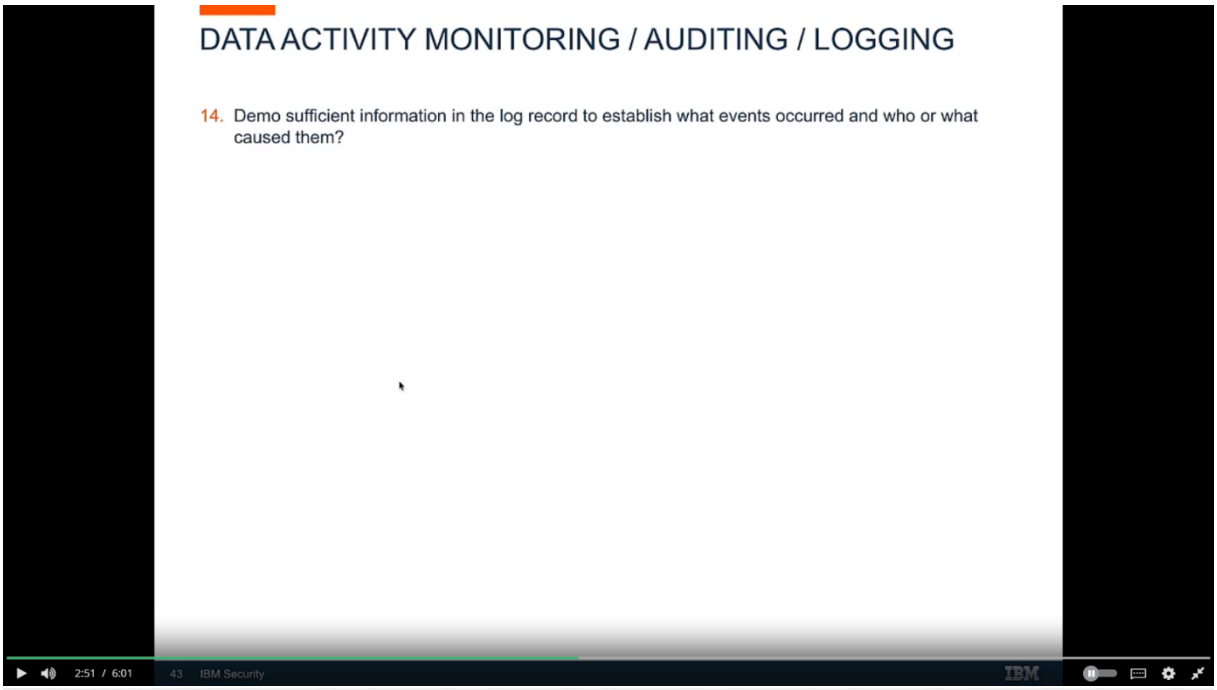
Attributes to Include in Logging

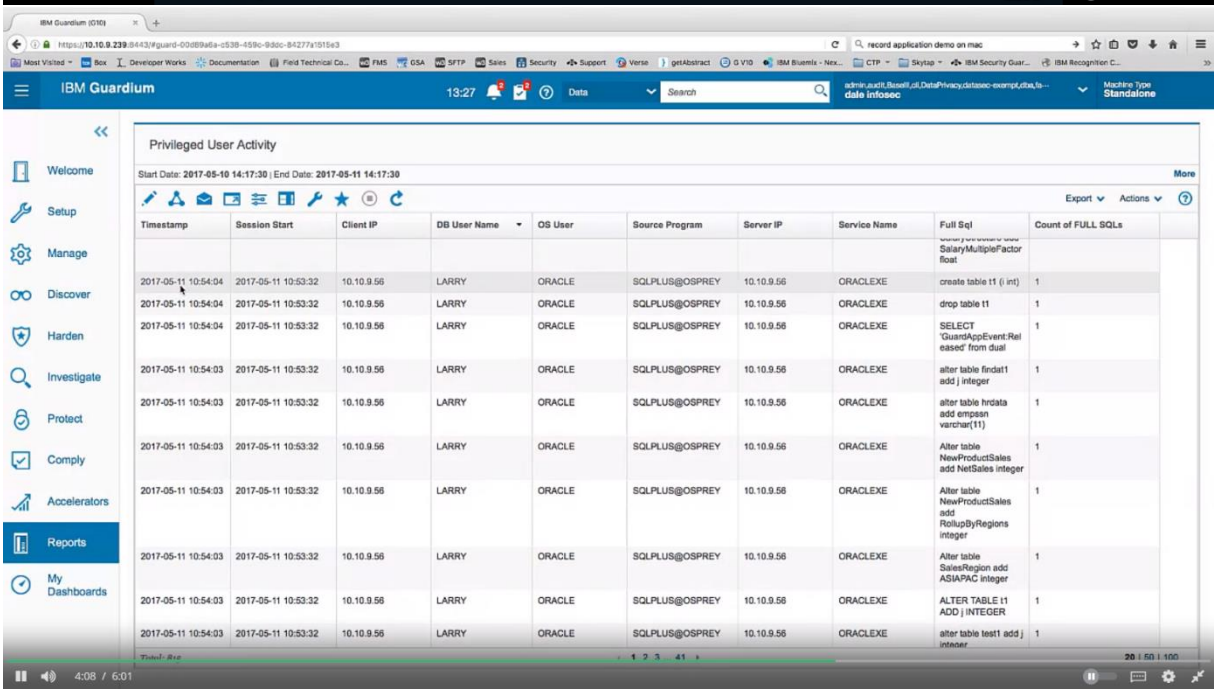

DATA ACTIVITY MONITORING / AUDITING / LOGGING
12. Demo the following event attributes and to what level of granularity?
0:17 / 6:01
41 IBM Security
IBM

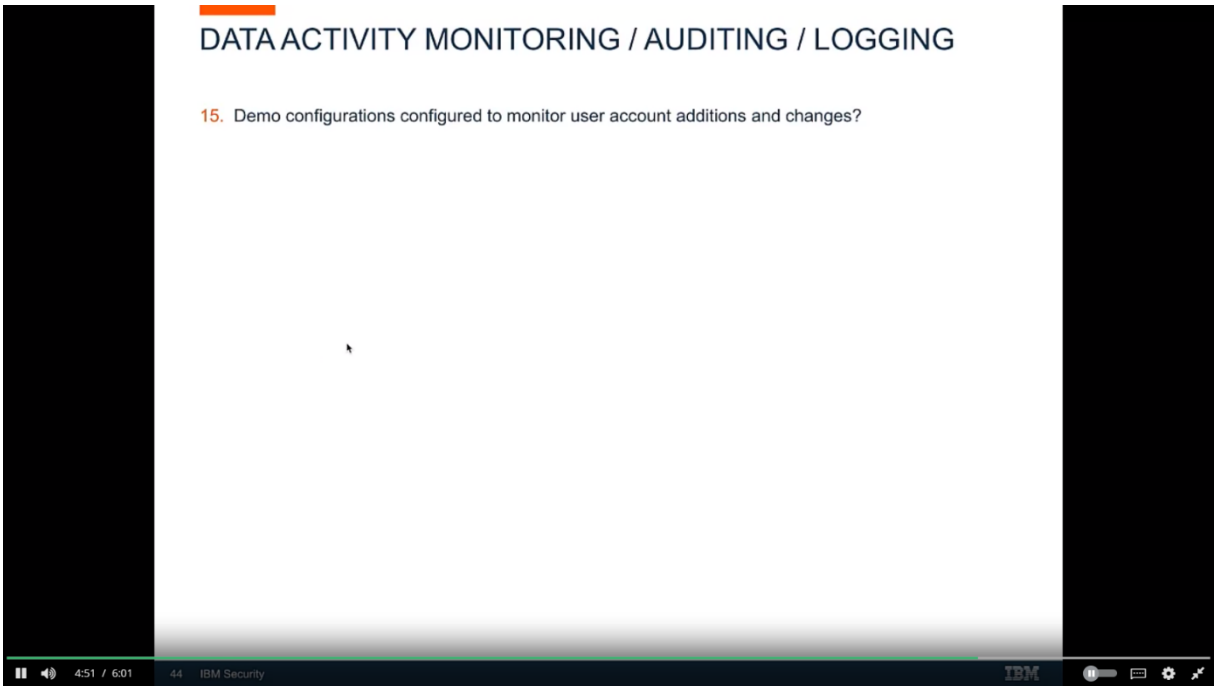

DATA ACTIVITY MONITORING / AUDITING / LOGGING
13. Demo when the product provides the following event attributes and to what level of granularity?
o Log date and time (international format)
o Event date and time - the event time stamp may be different to the time of logging e.g. server logging where the client application is hosted on remote device that is only periodically or intermittently online
o Interaction identifier
0:24 / 6:01
IBM


IBM Guardium
13:23
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Query Builder
Entity List
Activity Attributes
Query Fields
Query Conditions
All reports can be accessed through My Dashboard selection.
Delete
Clone
Roles
Save
Back
Data Mart
Create Report
Regenerate
Add to My Custom Reports
1:03 / 6:01

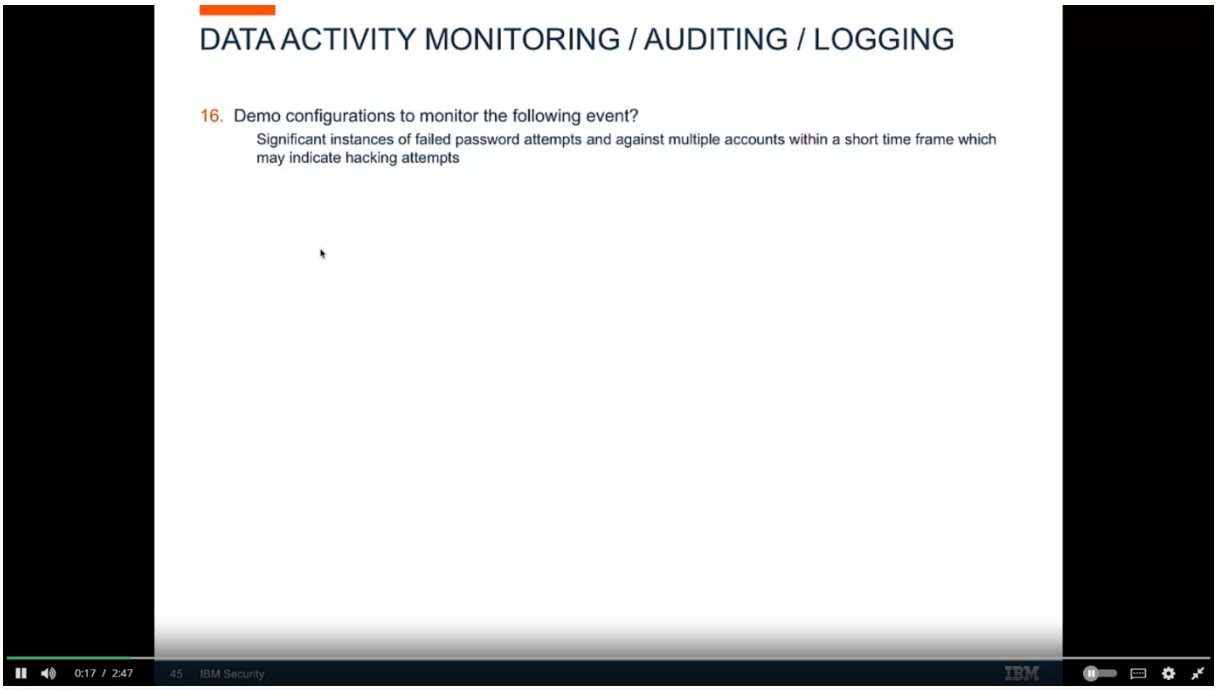

IBM Guardium
13:24
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Full SQL By DB User
Start Date: 2017-05-11 13:14:43 | End Date: 2017-05-11 15:14:43
Timestamp
Client IP
DB User Name
Session Start
Source Program
Full Sql
Count of FULL SQLs
2017-05-11 13:56:02 10.10.9.56 JOE 2017-05-11 13:56:02 SQLPLUS@OSPREY SELECT USER FROM DUAL 1
2017-05-11 13:56:02 10.10.9.56 JOE 2017-05-11 13:56:02 SQLPLUS@OSPREY SELECT DECODE('A','A','1','2') FROM DUAL 1
2017-05-11 13:56:40 10.10.9.56 JOE 2017-05-11 13:56:02 SQLPLUS@OSPREY select * from creditcard 1
2:00 / 6:01

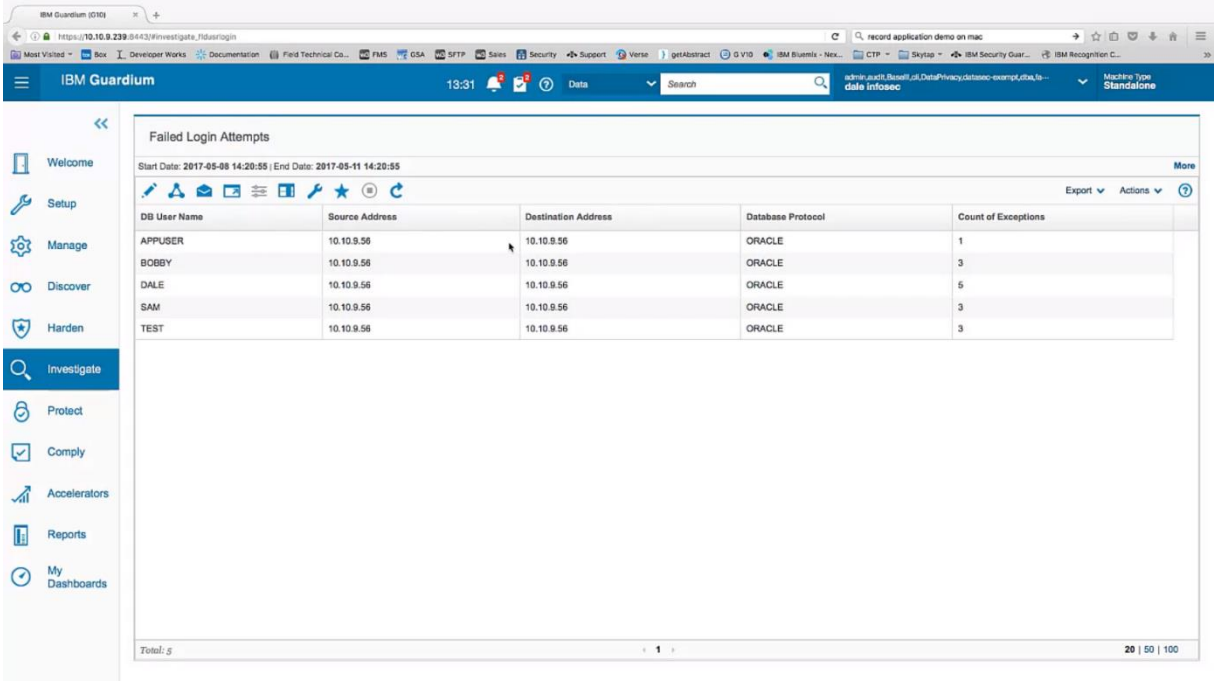

DATA ACTIVITY MONITORING / AUDITING / LOGGING
14. Demo sufficient information in the log record to establish what events occurred and who or what caused them?
2:51 / 6:01
43 IBM Security
IBM

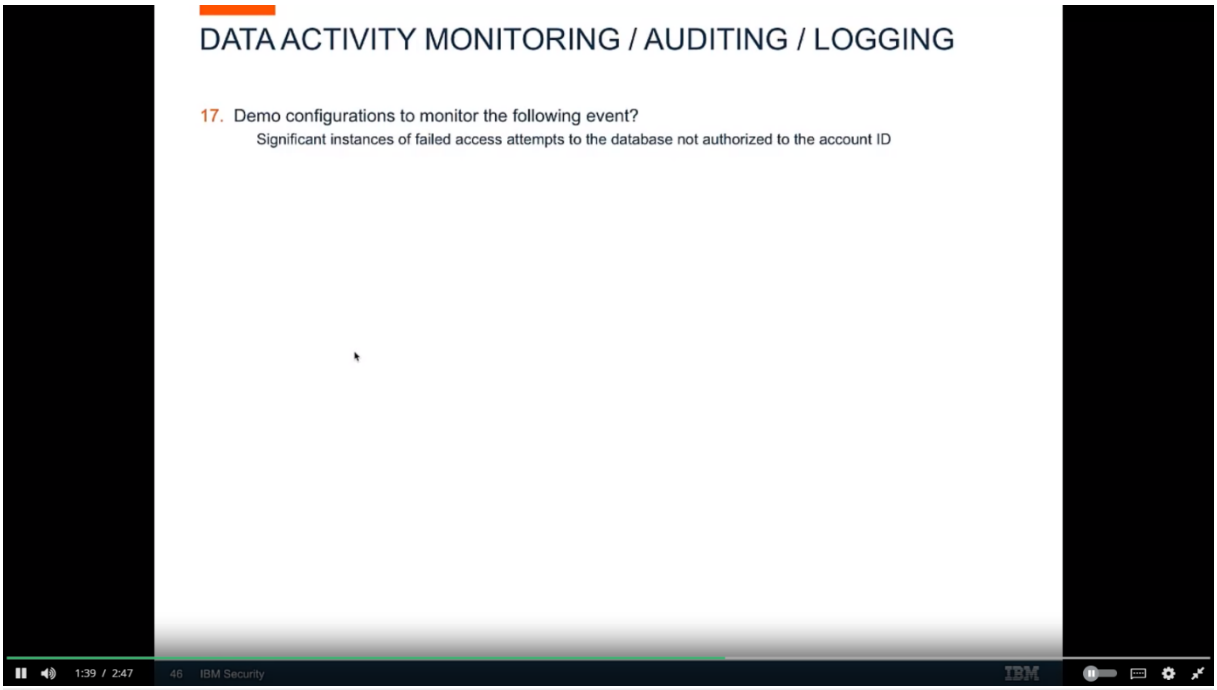

IBM Guardium
13:27
Data
Search
admin,audit,BaseII,cli,DataPrivacy,datasec-exempt,dba,fa...
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Privileged User Activity
Start Date: 2017-05-10 14:17:30 | End Date: 2017-05-11 14:17:30
More
Export
Actions
Timestamp | Session Start | Client IP | DB User Name | OS User | Source Program | Server IP | Service Name | Full Sql | Count of FULL SQLs
2017-05-11 10:54:04 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | create table t1 (i int) | 1
2017-05-11 10:54:04 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | drop table t1 | 1
2017-05-11 10:54:04 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | SELECT 'GuardAppEvent:Released' from dual | 1
2017-05-11 10:54:03 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | alter table findat1 add j integer | 1
2017-05-11 10:54:03 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | alter table hrdata add empssn varchar(11) | 1
2017-05-11 10:54:03 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | Alter table NewProductSales add NetSales integer | 1
2017-05-11 10:54:03 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | Alter table NewProductSales add RollupByRegions integer | 1
2017-05-11 10:54:03 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | Alter table SalesRegion add ASIAPAC integer | 1
2017-05-11 10:54:03 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | ALTER TABLE t1 ADD j INTEGER | 1
2017-05-11 10:54:03 | 2017-05-11 10:53:32 | 10.10.9.56 | LARRY | ORACLE | SQLPLUS@OSPREY | 10.10.9.56 | ORACLEXE | alter table test1 add j integer | 1
1 2 3 ... 41
20 | 50 | 100
4:08 / 6:01

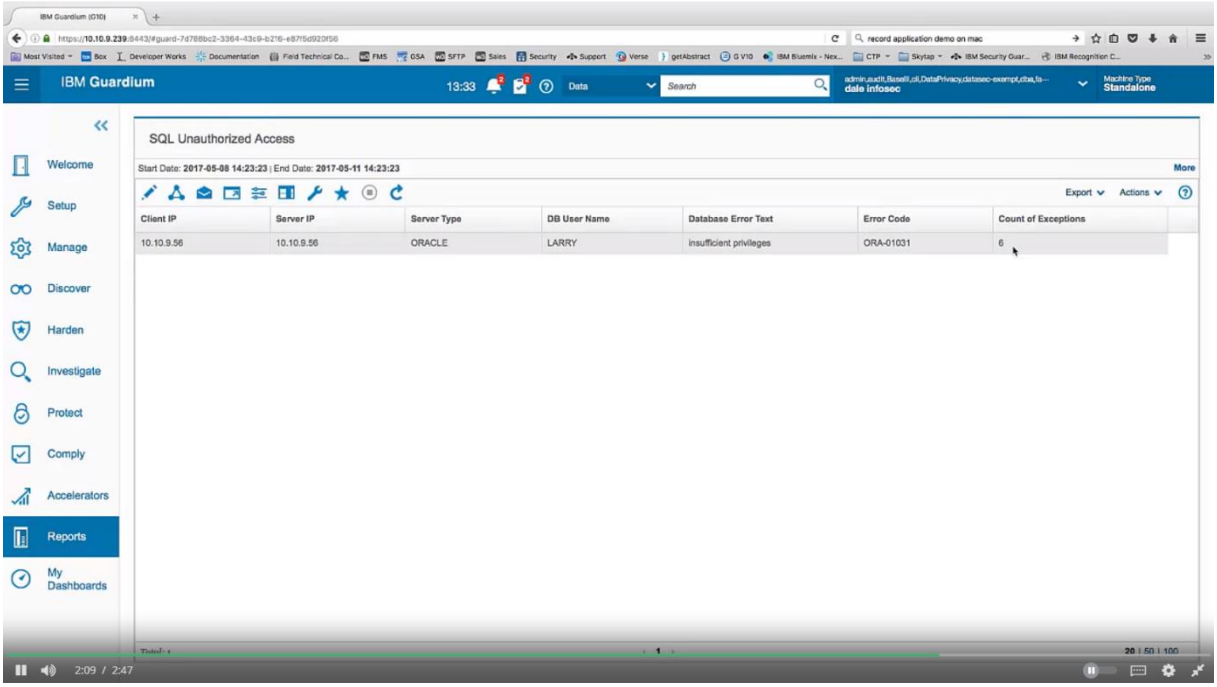


Failed Access Monitoring

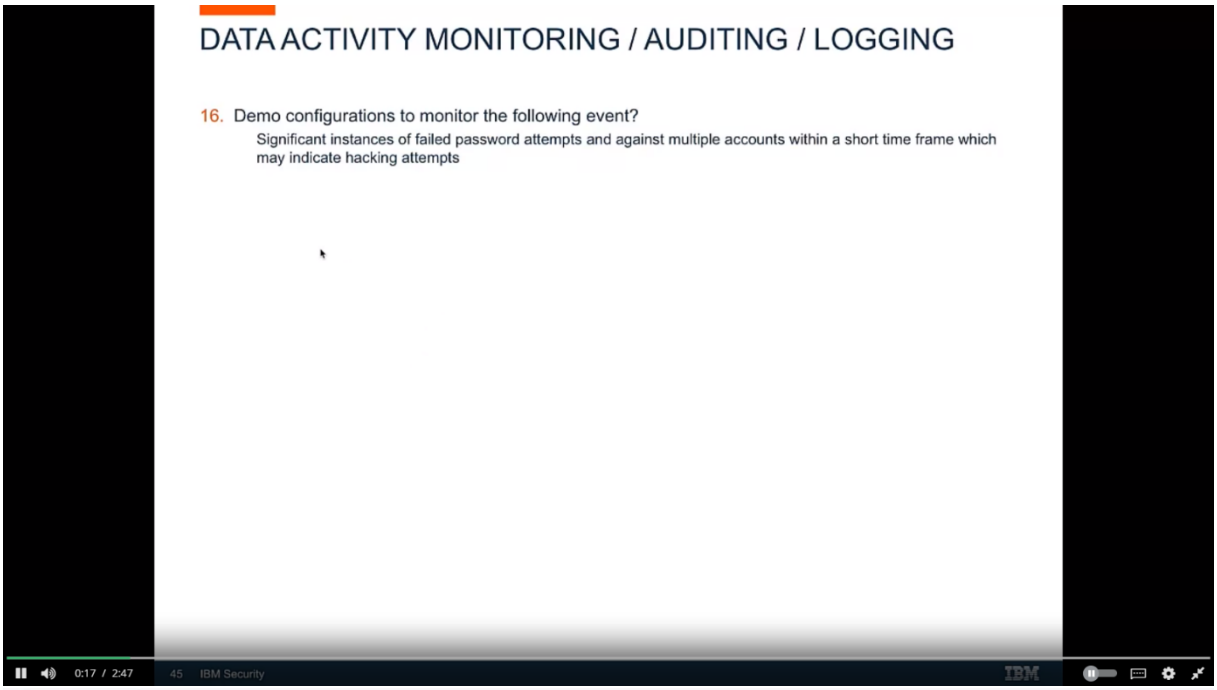

DATA ACTIVITY MONITORING / AUDITING / LOGGING
16. Demo configurations to monitor the following event?
Significant instances of failed password attempts and against multiple accounts within a short time frame which may indicate hacking attempts
0:17 / 2:47
45 IBM Security
IBM

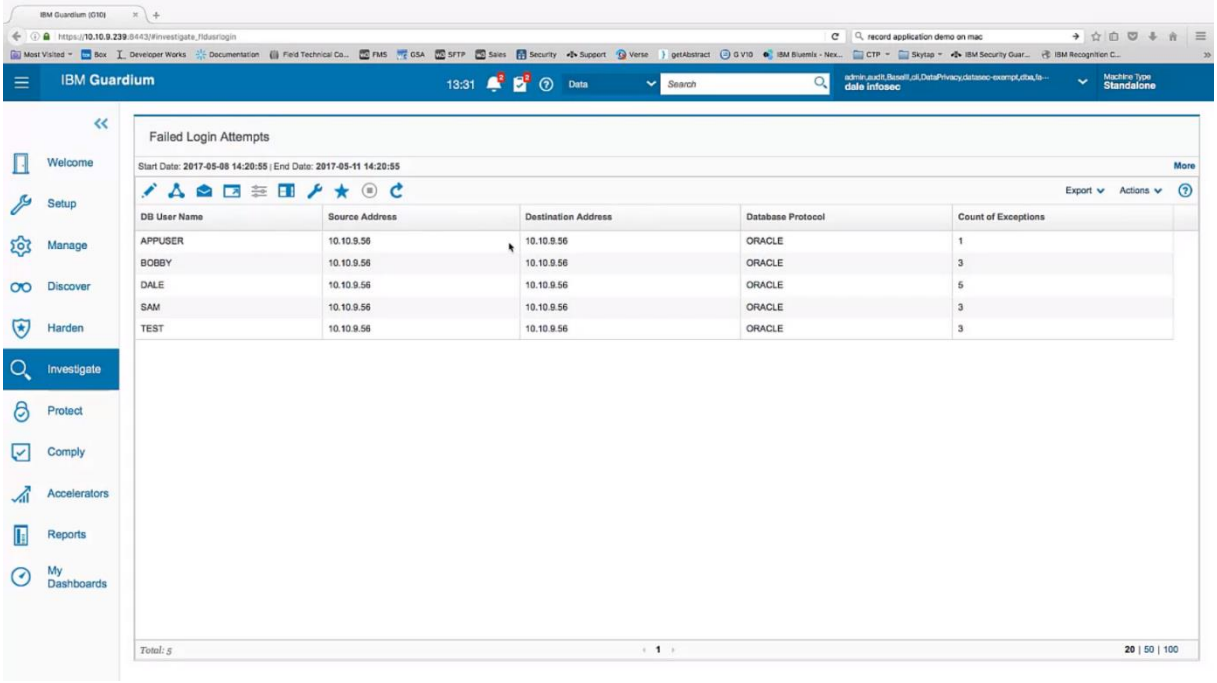

IBM Guardium
13:31
Data
Search
admin,audit,Basell,cli,DataPrivacy,datasec-exempt,dba,fa--
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Failed Login Attempts
Start Date: 2017-05-08 14:20:55 | End Date: 2017-05-11 14:20:55
More
Export
Actions
DB User Name
Source Address
Destination Address
Database Protocol
Count of Exceptions
APPUSER 10.10.9.56 10.10.9.56 ORACLE 1
BOBBY 10.10.9.56 10.10.9.56 ORACLE 3
DALE 10.10.9.56 10.10.9.56 ORACLE 5
SAM 10.10.9.56 10.10.9.56 ORACLE 3
TEST 10.10.9.56 10.10.9.56 ORACLE 3
Total: 5
1
20 | 50 | 100

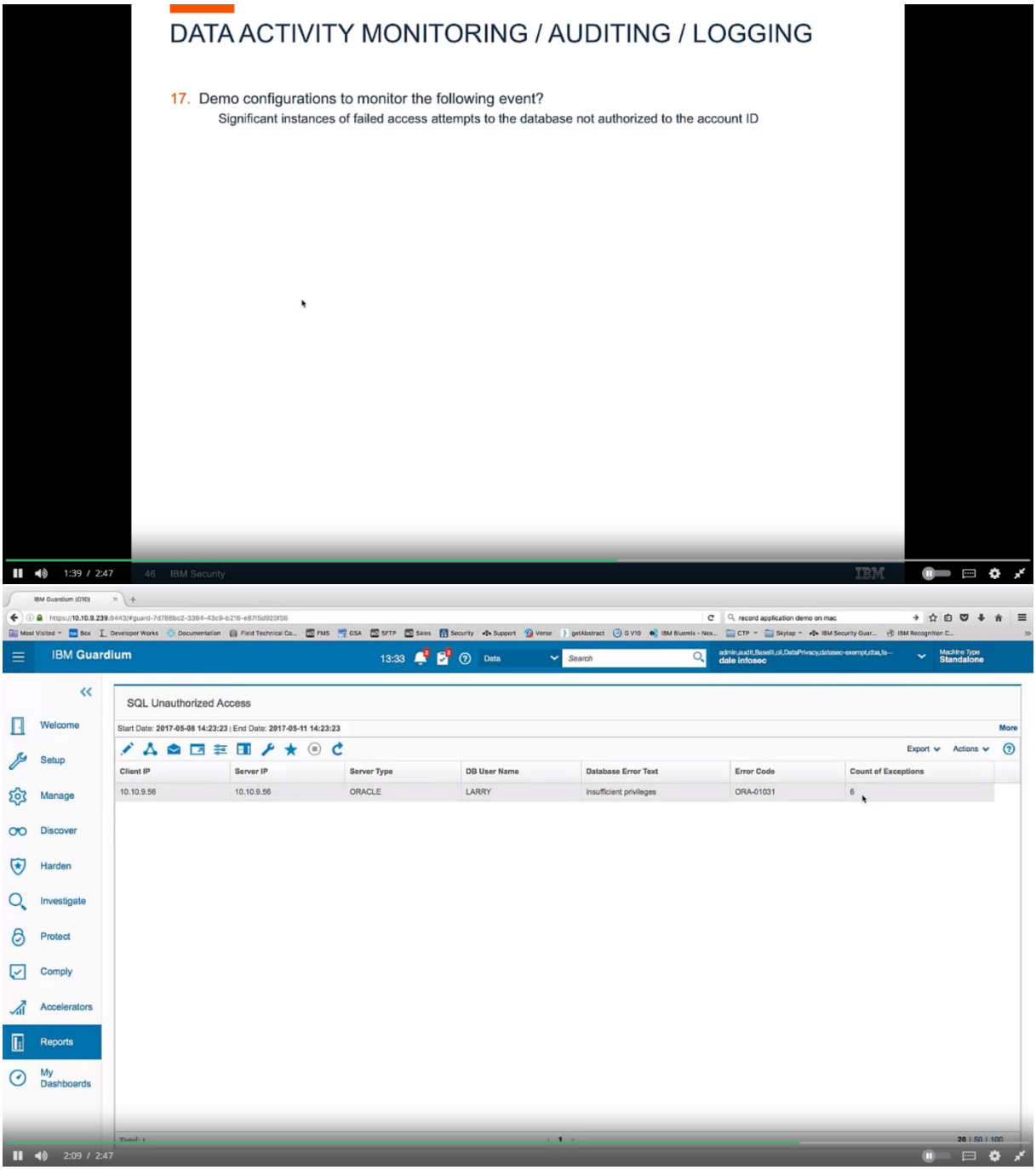




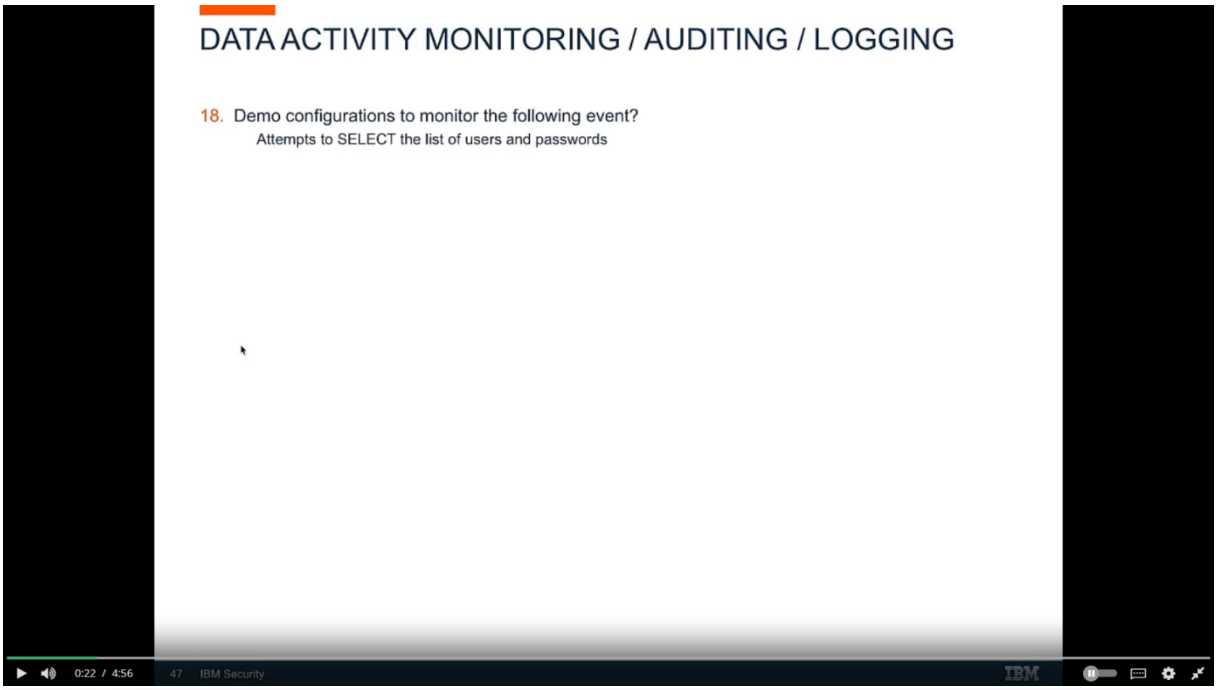
Failed Access Monitoring

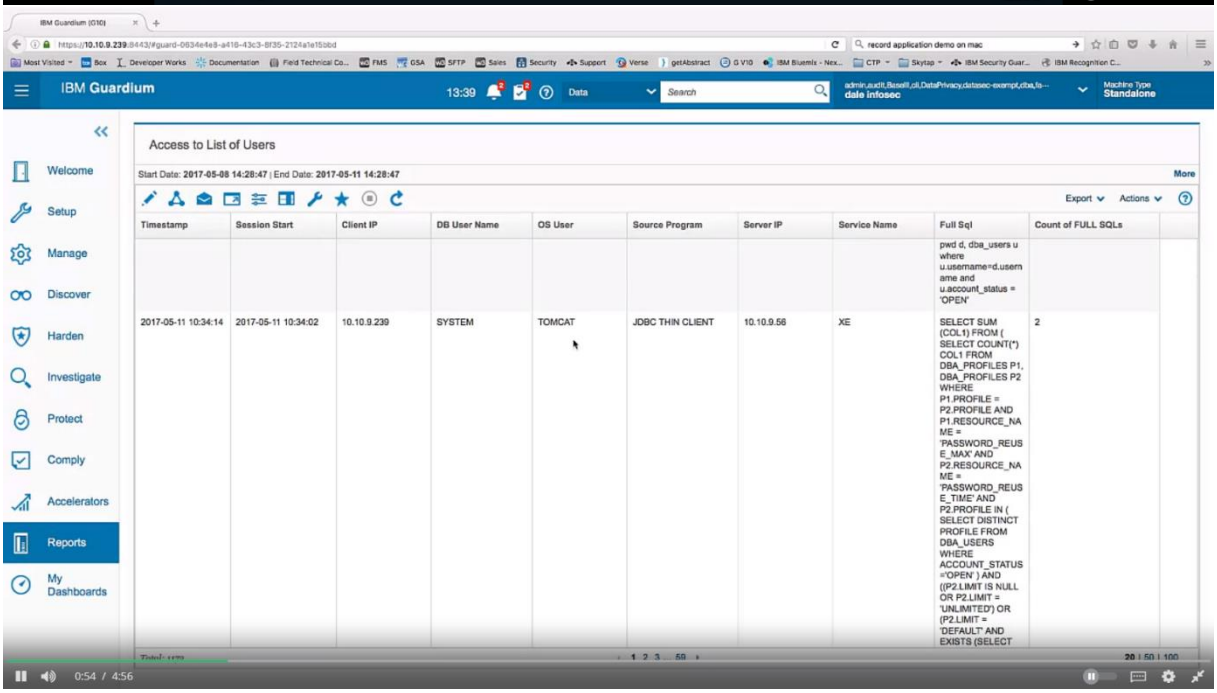

DATA ACTIVITY MONITORING / AUDITING / LOGGING
16. Demo configurations to monitor the following event?
Significant instances of failed password attempts and against multiple accounts within a short time frame which may indicate hacking attempts
0:17 / 2:47
45 IBM Security
IBM


IBM Guardium
13:31
Data
Search
admin,audit,Basell,cli,DataPrivacy,datasec-exempt,dba,fa--
dale infosec
Machine Type
Standalone
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Failed Login Attempts
Start Date: 2017-05-08 14:20:55 | End Date: 2017-05-11 14:20:55
More
Export
Actions
DB User Name
Source Address
Destination Address
Database Protocol
Count of Exceptions
APPUSER 10.10.9.56 10.10.9.56 ORACLE 1
BOBBY 10.10.9.56 10.10.9.56 ORACLE 3
DALE 10.10.9.56 10.10.9.56 ORACLE 5
SAM 10.10.9.56 10.10.9.56 ORACLE 3
TEST 10.10.9.56 10.10.9.56 ORACLE 3
Total: 5
1
20 | 50 | 100



Suspicious Access Events, Part 1

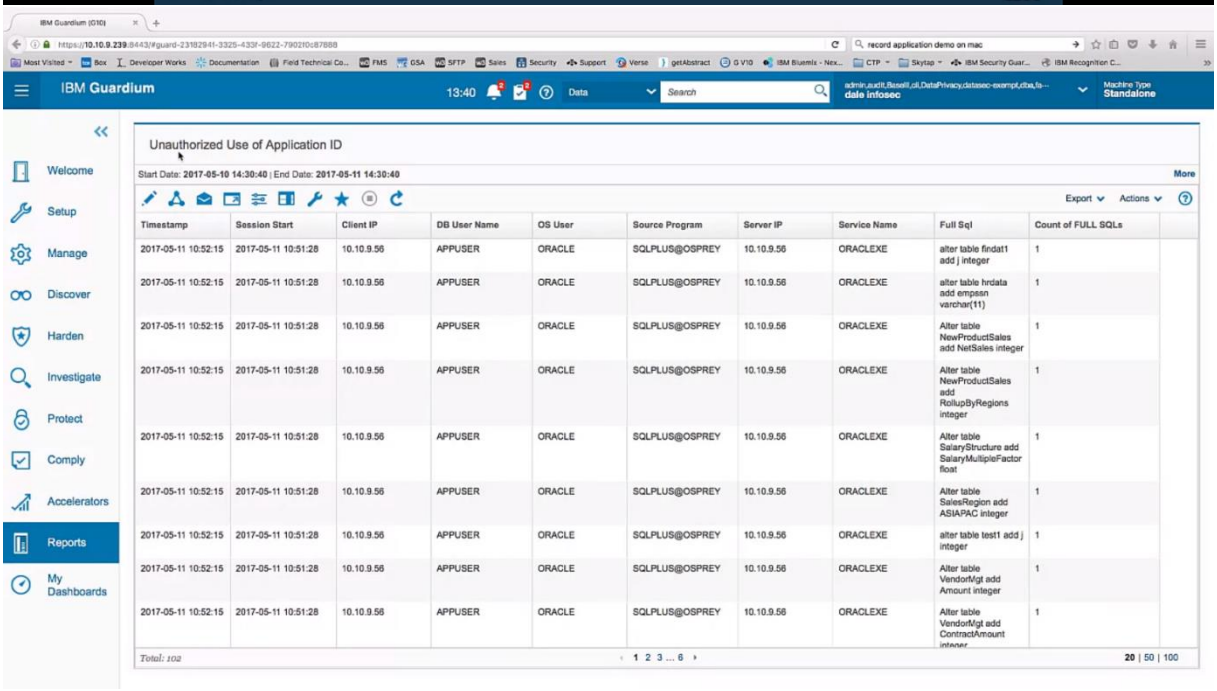

DATA ACTIVITY MONITORING / AUDITING / LOGGING
18. Demo configurations to monitor the following event?
Attempts to SELECT the list of users and passwords
0:22 / 4:56
47 IBM Security

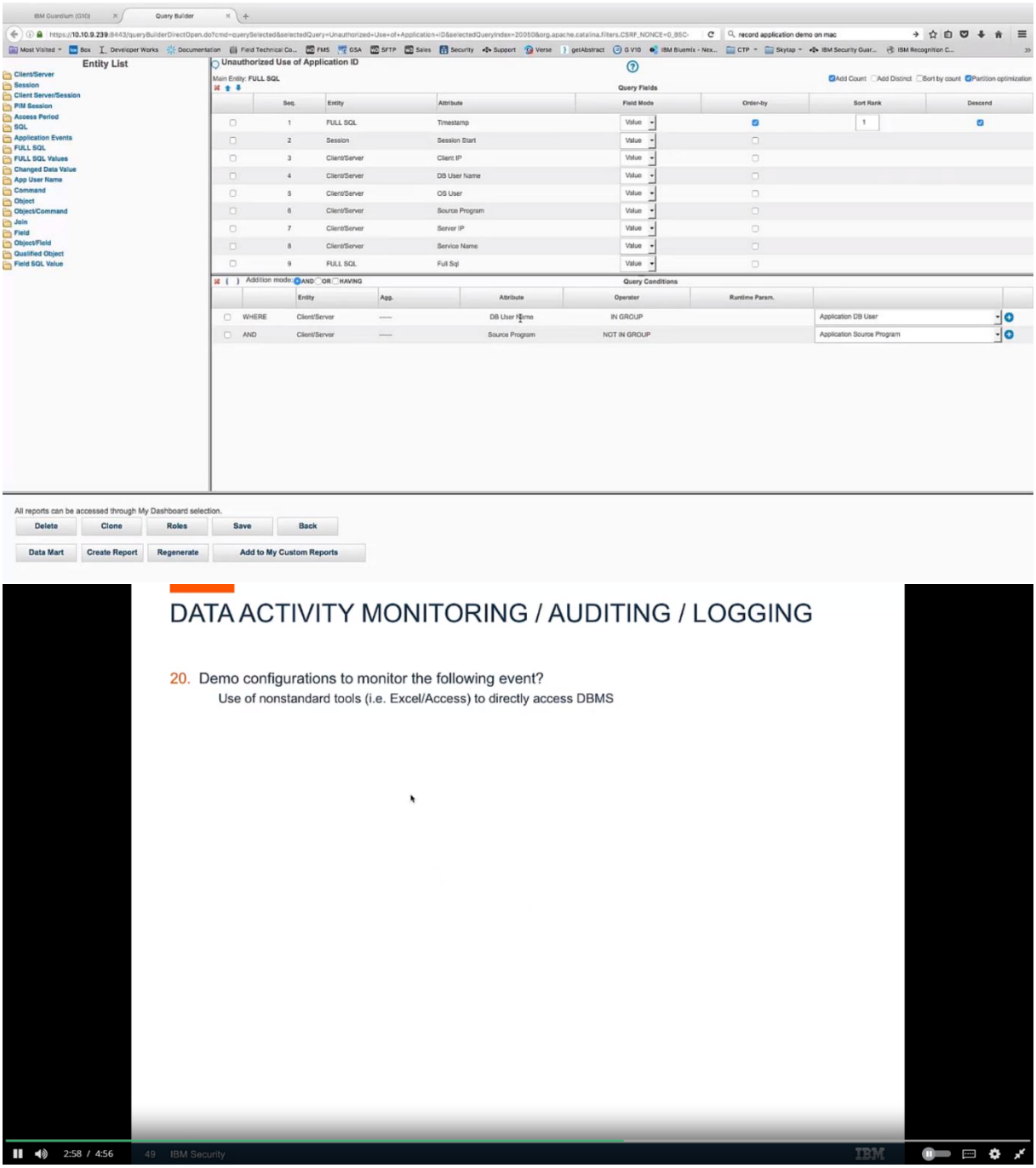

IBM Guardium
13:39
Welcome
Setup
Manage
Discover
Harden
Investigate
Protect
Comply
Accelerators
Reports
My Dashboards
Access to List of Users
Start Date: 2017-05-08 14:28:47 | End Date: 2017-05-11 14:28:47
Export
Actions
Timestamp
Session Start
Client IP
DB User Name
OS User
Source Program
Server IP
Service Name
Full Sql
Count of FULL SQLs
2017-05-11 10:34:14
2017-05-11 10:34:02
10.10.9.239
SYSTEM
TOMCAT
JDBC THIN CLIENT
10.10.9.56
XE
2
0:54 / 4:56

DATA ACTIVITY MONITORING / AUDITING / LOGGING

19. Demo configurations to monitor the following event?

All direct access to the database from accounts which should be limited to access through the application





Data Breach Feeds

Data Breach Feeds

In today's environment there are multiple data breaches that occur every day. As an analyst you will want to keep track of what is going on in the world every day.

Data Breaches reports on current breaches from Malware to Data exposures

DataBreaches.net

Read the very latest data breach news: https://www.databreaches.net/news/

Search among many thousands of data breach cases by breach type, industry, etc.: https://www.databreaches.net/?s=case+studies

Learn about data breach notification laws: https://www.databreaches.net/state-breach-notification-laws/

Bleeping Computer reports news on current breaches and threats

BleepingComputer.com

Think using a VPN will guaranty your security? This article from 2021 might have you thinking again.

https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/

IBM X-Force Exchange current, real-time world threat map

https://exchange.xforce.ibmcloud.com/activity/map

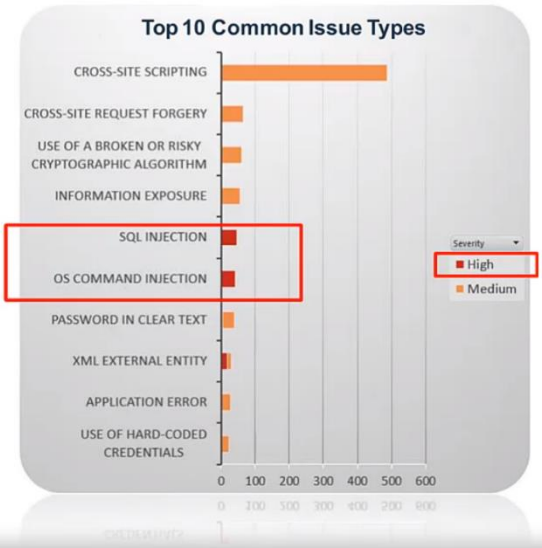
Click on any IP address at the top of the map and you will see details of the threat.

Week 4

Introduction to Injection Flaws

What are injection flaws?

- ***Injection flaws*** allow attackers to relay malicious code through the vulnerable application to another system (OS, Database server, LDAP server, etc.)
- They are extremely dangerous, and may allow full takeover of the vulnerable system
- Injection flaws appear internally & externally as a Top Issue



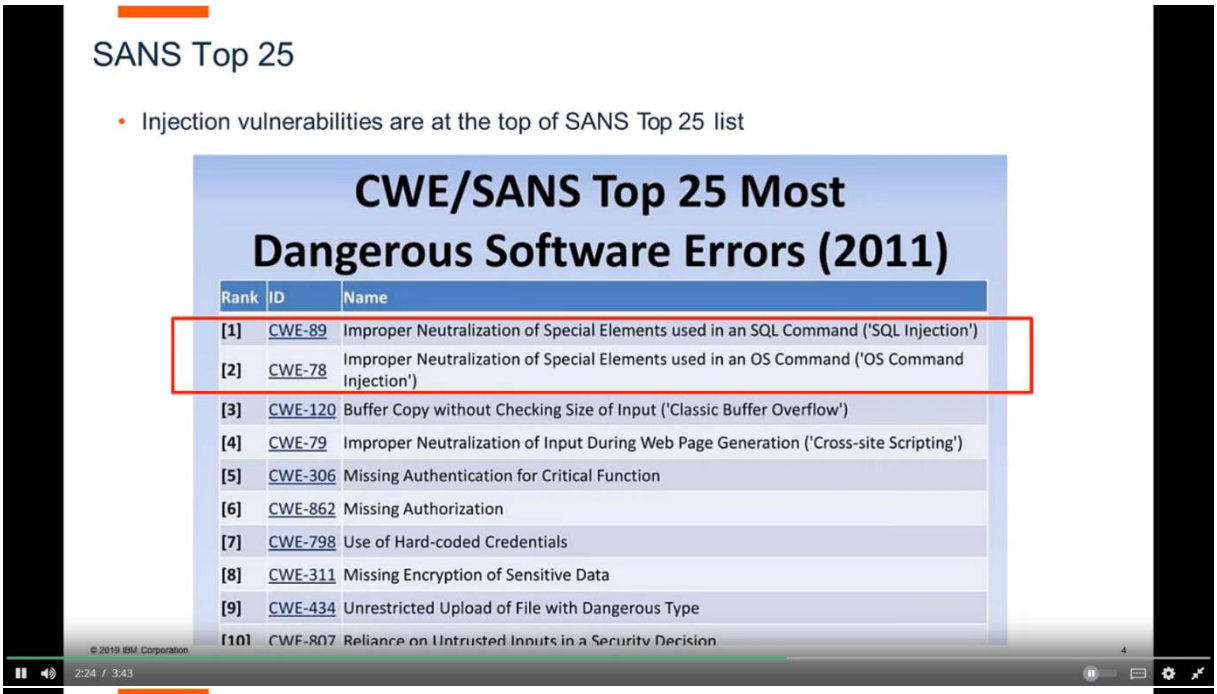
1:24 / 3:43

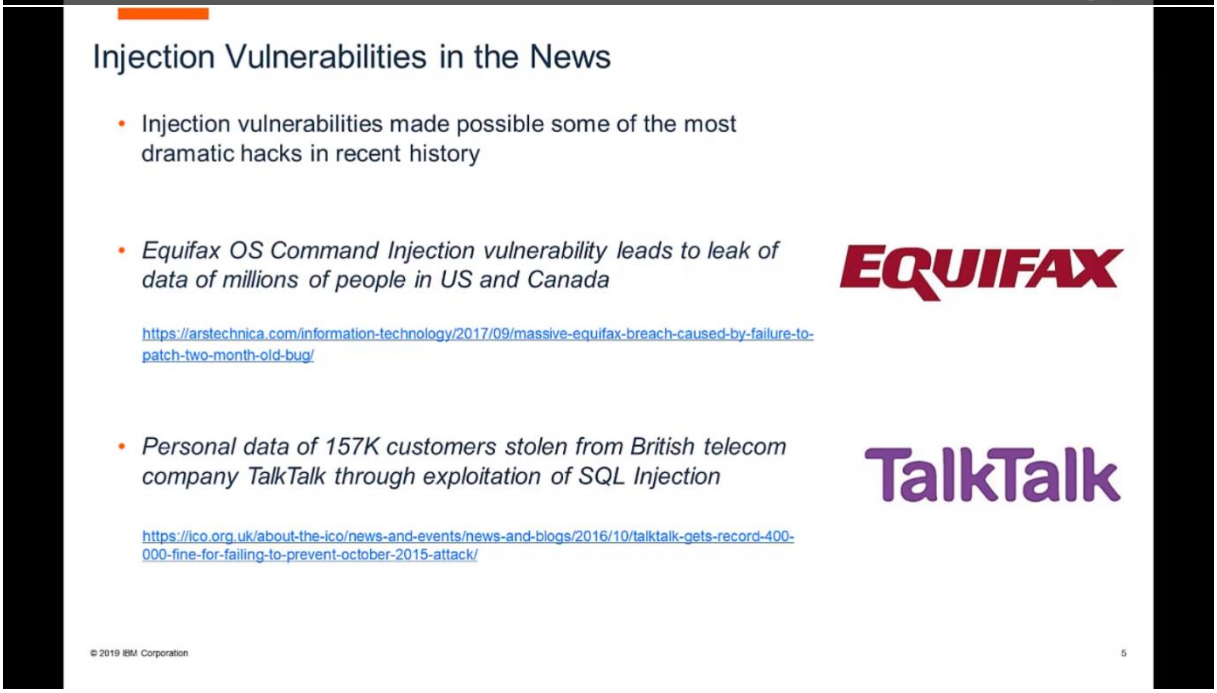
OWASP Top 10

- Injection vulnerabilities are consistently considered to be #1 on OWASP Top 10 list

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

1:52 / 3:43





OS Command Injection Part 1

What is OS Command Injection?

- Abuse of vulnerable application functionality that causes execution of attacker-specified OS commands
- Applies to all operating systems – Linux, Windows, MacOS
- Made possible by lack of sufficient input sanitization, and by unsafe execution of OS commands

Example

- Consider a usecase where application allows user to delete log files:

- The deletion command sent as a POST request that may look like this:

```
action=delete&file=auditlog9.log
```

- On the server the following code is executed (assume Java is the implementation language):

```
Runtime.getRuntime().exec("/bin/sh -c \"/bin/rm
/var/app/logs/"+logFile+"\"");
```

- Which translates to the following command:

```
/bin/sh -c "/bin/rm /var/app/logs/auditlog9.log"
```

Example

- Consider a usecase where application allows user to delete log files:

- The deletion command sent as a POST request that may look like this:

```
action=delete&file=auditlog9.log
```

- On the server the following code is executed (assume Java is the implementation language):

```
Runtime.getRuntime().exec("/bin/sh -c \"/bin/rm
/var/app/logs/"+logFile+"\"");
```

- Which translates to the following command:

```
/bin/sh -c "/bin/rm /var/app/logs/auditlog9.log"
```


What is the Worst That Could Happen?

- Attacker can replace file to be deleted - BAD:

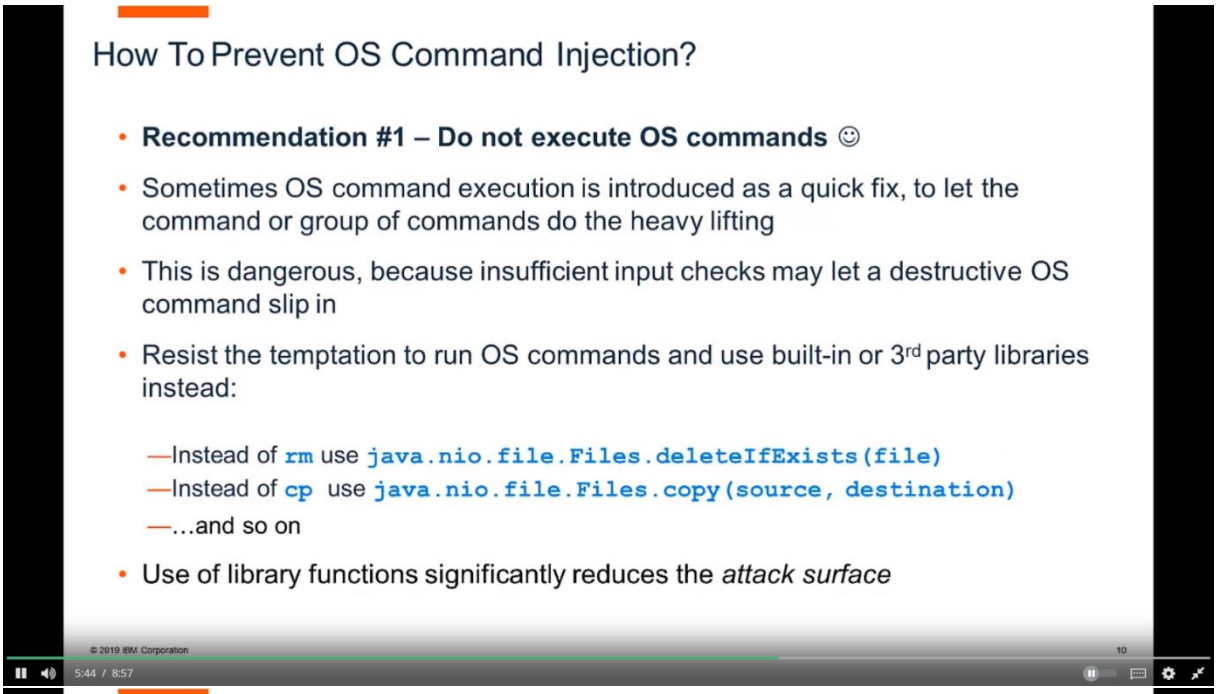
```
/bin/sh -c "/bin/rm /var/app/logs/../../../lib/libc.so.6"
```

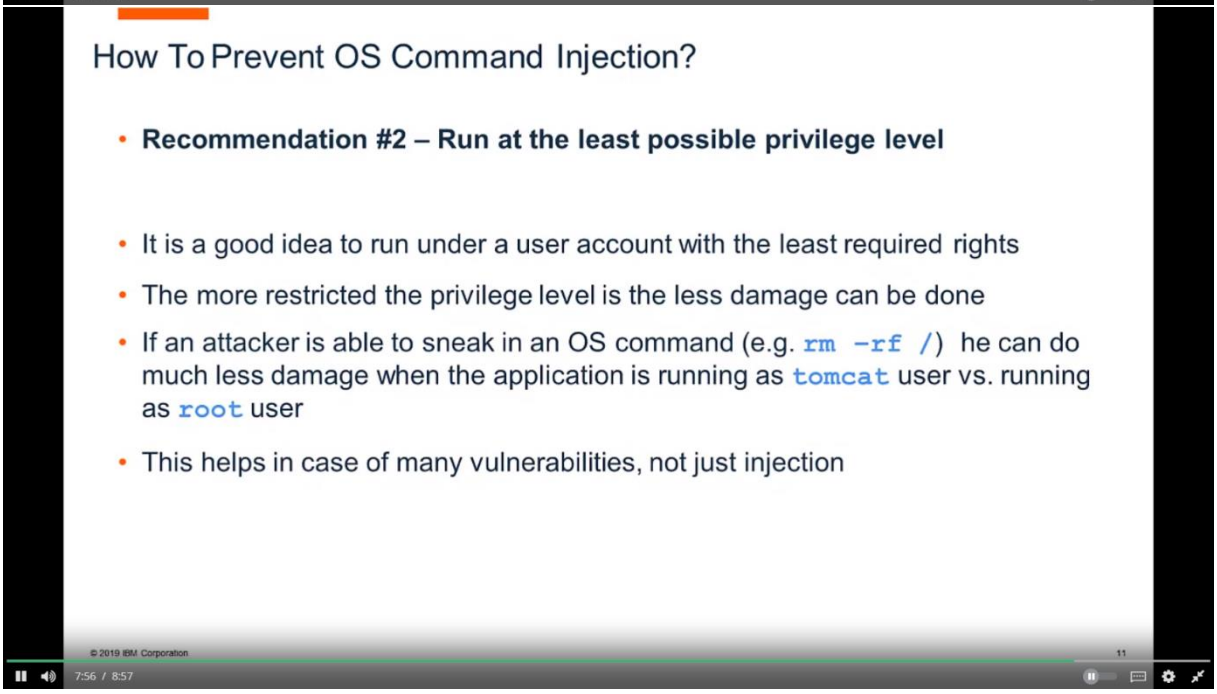
- Attacker can inject ***arbitrary malicious OS command*** – MUCHWORSE:

```
/bin/sh -c "/bin/rm /var/app/logs/x;rm -rf /"
```

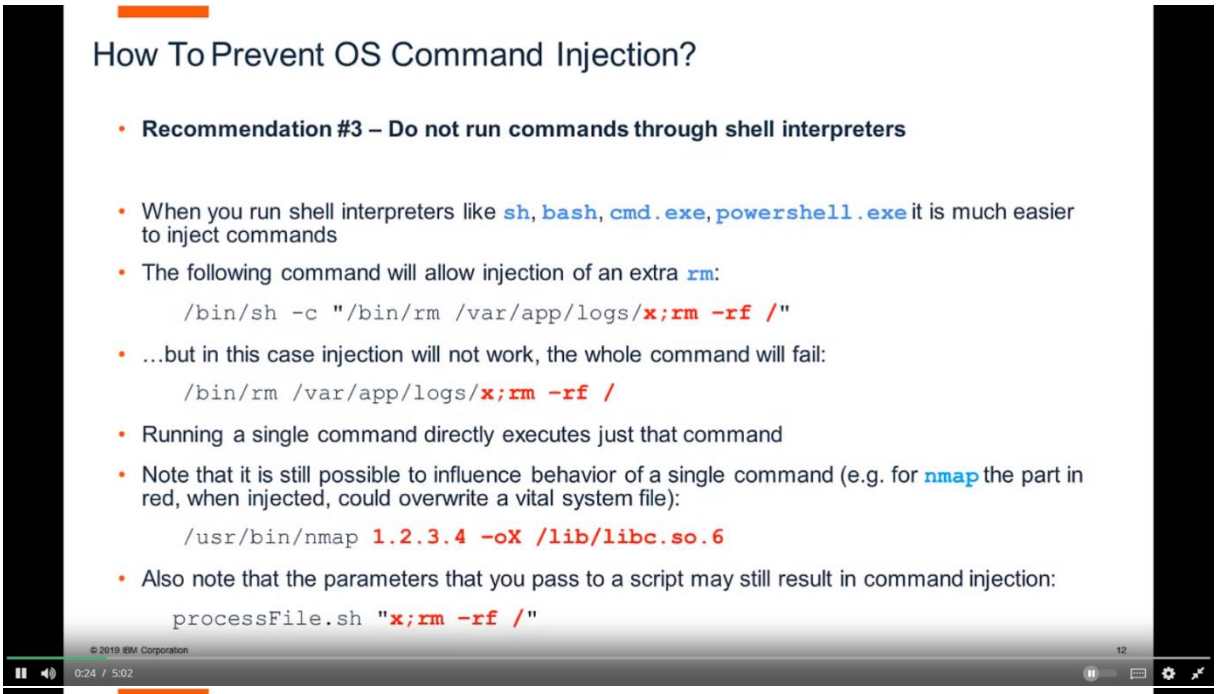
- OS Command Injection can lead to:
  - Full system takeover
  - Denial of service
  - Stolen sensitive information (passwords, crypto keys, sensitive personal info, business confidential data)
  - Lateral movement on the network, launching pad for attacks on other systems
  - Use of system for botnets or cryptomining

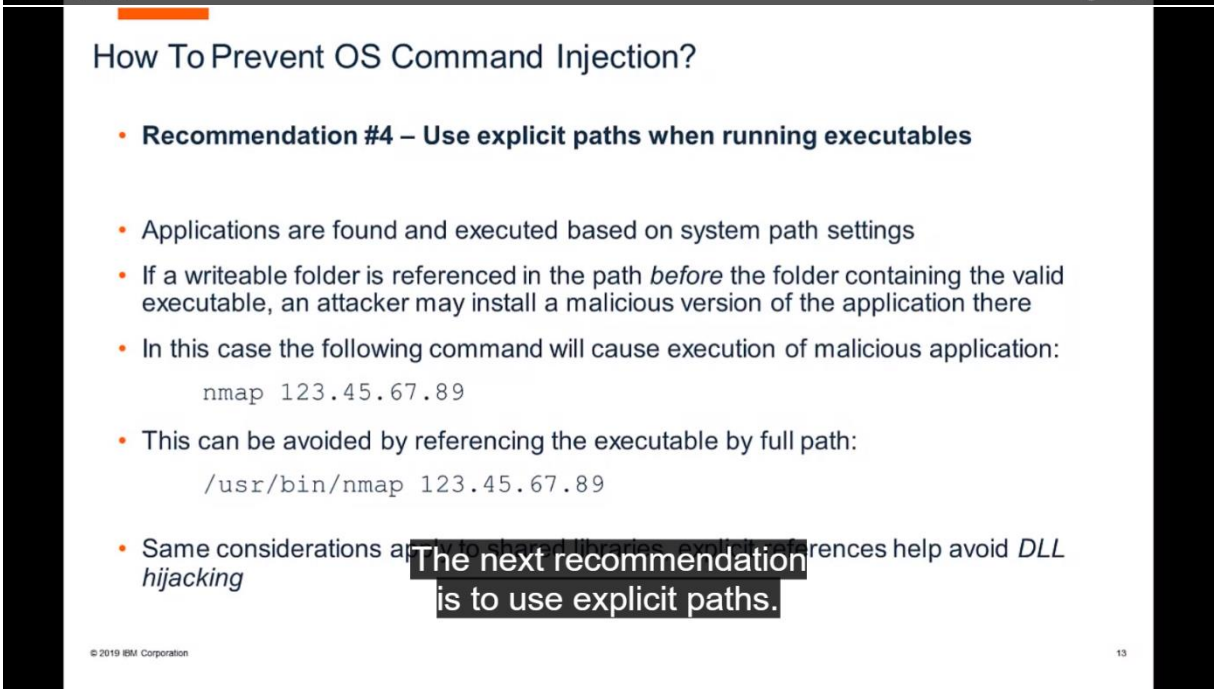
- This is as bad as it gets, a “GAME OVER” event





OS Command Injection Part 2





OS Command Injection Part 3

How To Prevent OS Command Injection?

- **Recommendation #5 – Use safer functions when running system commands**

- If available, use functionality that helps prevent command injection
- For example, the following function call is vulnerable to new parameter injection (one could include more parameters, separated by spaces, in `ipAddress`):

```
Runtime.getRuntime().exec("/usr/bin/nmap " + ipAddress);
```

- … but this call is not vulnerable:

```
Runtime.getRuntime().exec(new String[]
{"/usr/bin/nmap",ipAddress});
```


0:44 / 7:32

How To Prevent OS Command Injection?

- **Recommendation #6 – If possible, do not let user input reach command execution unchanged**

- Modifying user input, or replacing user-specified values with others (e.g. using translation tables) helps protect against injection
- For example, instead of allowing user to specify file to delete, let her select a unique file ID:

```
action=delete&file=457
```

- When submitted, translate that ID into a real file name:

```
realName = getRealFileName(fileID);
Runtime.getRuntime().exec(new
String[]{"/bin/rm","/var/app/logs/"+realName});
```


2:03 / 7:32

How To Prevent OS Command Injection?

- **Recommendation #7 – Sanitize user input with strict whitelists (not blacklists!)**
- In our products we often see blacklists used for parameter sanitization; some of them are incorrect
- It is ***hard*** to build a successful blacklist – hackers are very inventive (some examples)!
- Suppose we want to blacklist characters used in a file name for command `rm /var/app/logs/file`

Mitigation	Evasion
Blacklist ; & |	`/bin/rm /var/app/logs/x`rm -rf /``
Blacklist ; & | `	`/bin/rm /var/app/logs/x$(rm -rf /)`
Blacklist spaces	`/bin/rm /var/app/logs/x;rm${IFS:0:1}-rf${IFS:0:1}/`
Enclose value in double quotes, escape them in value	`/bin/rm "/var/app/logs/x\";rm -rf /;echo \"`

- A more robust and simpler solution is to whitelist file name as **[A-Za-z0-9.]+**

Key Takeaways

- DO NOT use OS commands
  - —If possible, use built in or secure/approved 3rd party libraries instead
- DO run your code with least possible privilege
- DO NOT run commands with shell interpreters
  - —Instead, run commands directly
- DO use explicit paths when running applications and using shared libraries
- DO use safe library functions when running OS commands
- DO NOT let user input reach OS command unchanged
  - —If possible, replace user input with generated IDs
- DO sanitize all user input
  - —ONLY use whitelists for sanitization; blacklists are unsafe

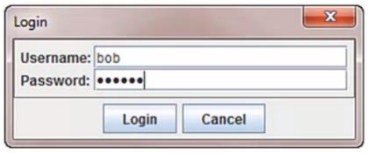
SQL Injection Part 1

What is SQL Injection?

- Abuse of vulnerable application functionality that causes execution of attacker-specified SQL queries
- Is possible in any SQL database
- Made possible by lack of sufficient input sanitization

Example

- Suppose our application has a login dialog:



- On the back end the code may be as follows:

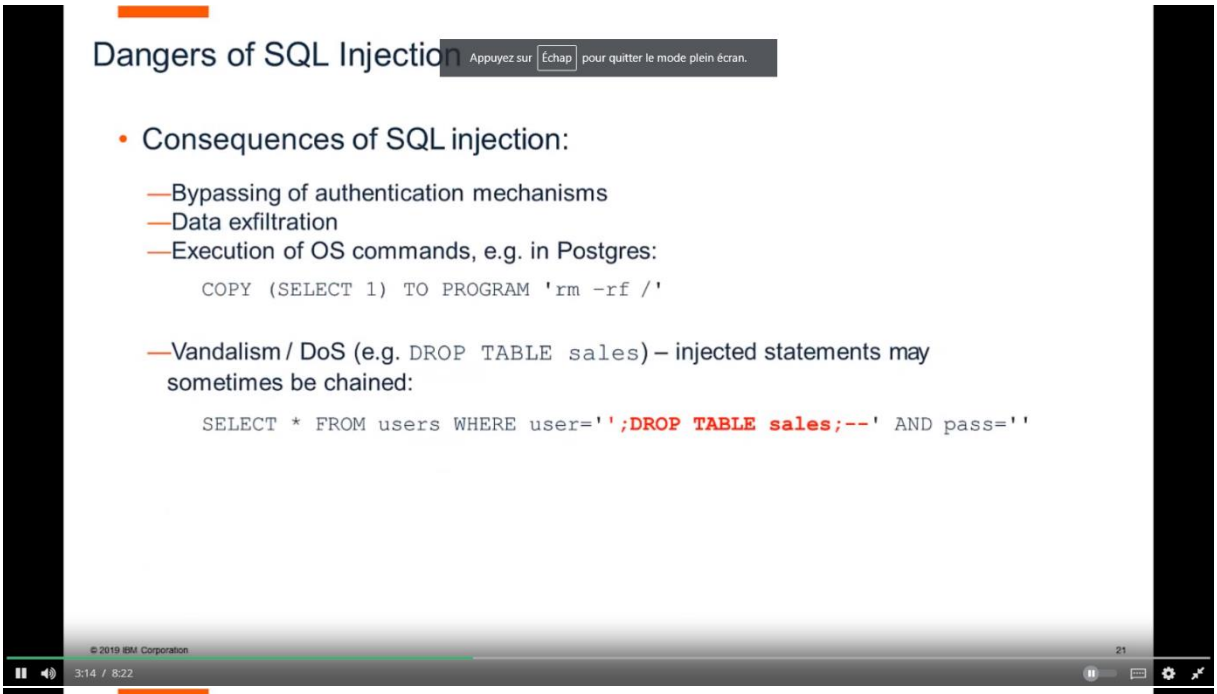
```
stmt.executeQuery("SELECT * FROM users WHERE user='"+user+"' AND
pass='"+pass+"'")
```

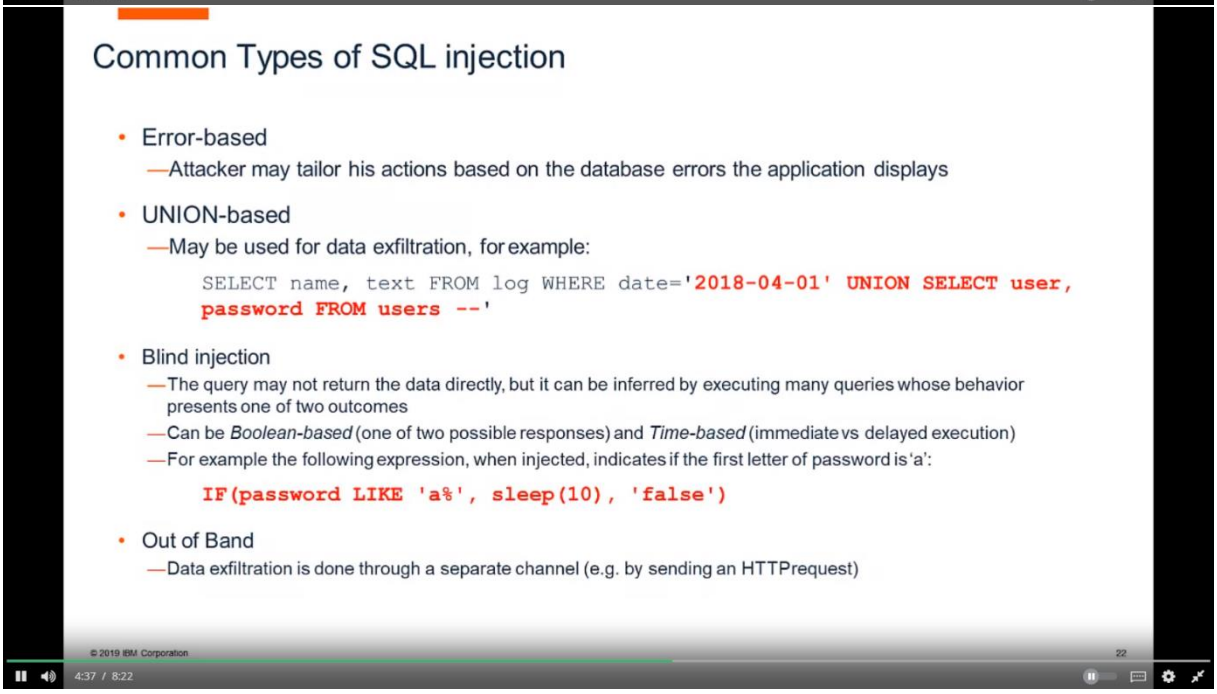
- With regular input the query would be as follows, selecting a record only if the match is found:

```
SELECT * FROM users WHERE user='bob' AND pass='secret'
```

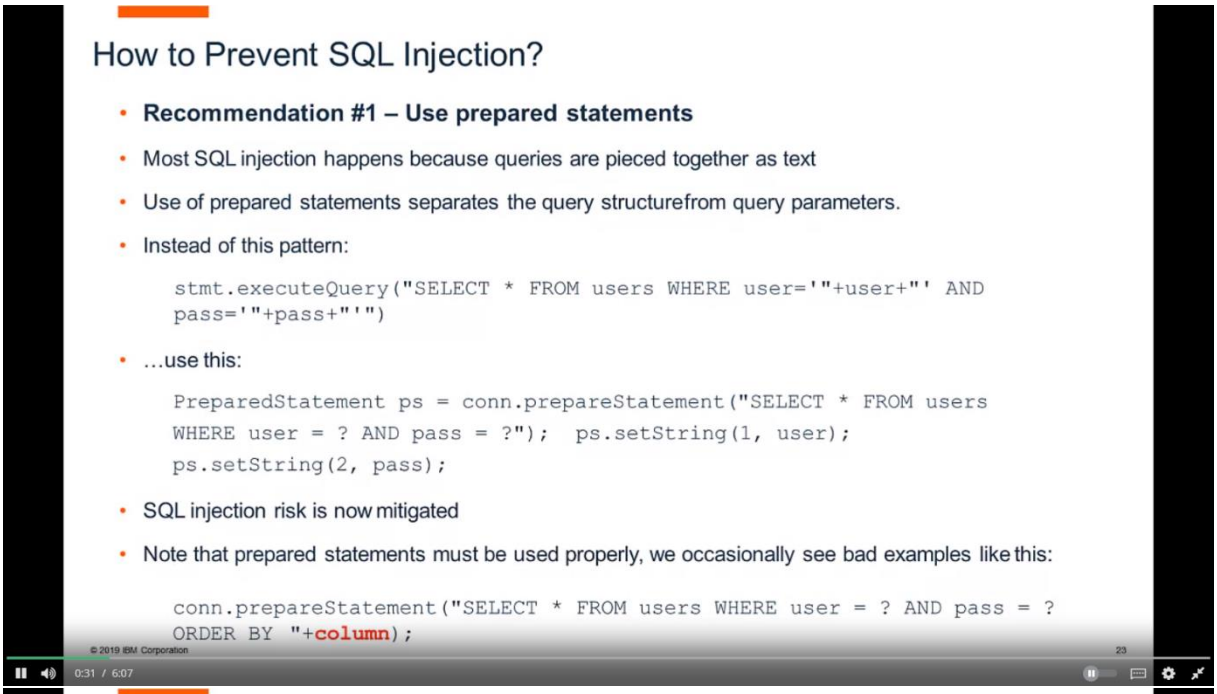
- In case of malicious input hacker can login without valid credentials:

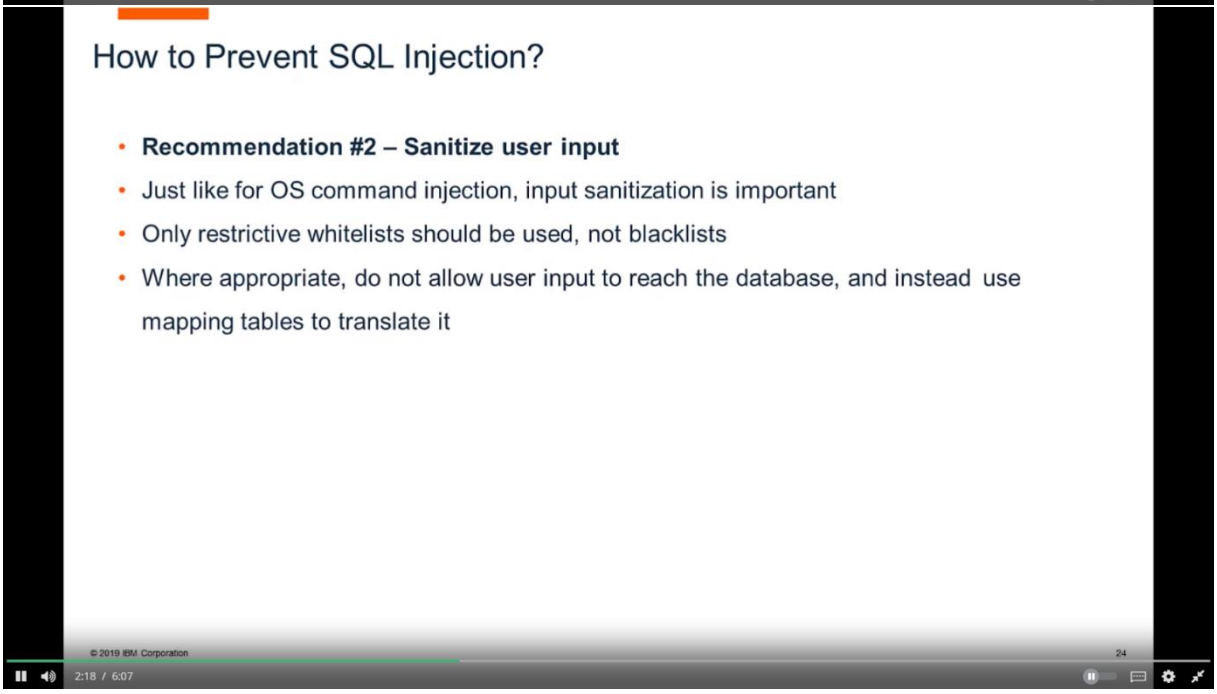
```
SELECT * FROM users WHERE user='' OR 1=1;--' AND pass=''
```





SQL Injection Part 2


How to Prevent SQL Injection?
• Recommendation #1 – Use prepared statements
• Most SQL injection happens because queries are pieced together as text
• Use of prepared statements separates the query structurefrom query parameters.
• Instead of this pattern:
stmt.executeQuery("SELECT * FROM users WHERE user='"+user+"' AND pass='"+pass+"'")
• …use this:
PreparedStatement ps = conn.prepareStatement("SELECT * FROM users WHERE user = ? AND pass = ?"); ps.setString(1, user); ps.setString(2, pass);
• SQL injection risk is now mitigated
• Note that prepared statements must be used properly, we occasionally see bad examples like this:
conn.prepareStatement("SELECT * FROM users WHERE user = ? AND pass = ? ORDER BY "+column);
© 2019 IBM Corporation
23
0:31 / 6:07


How to Prevent SQL Injection?
• Recommendation #2 – Sanitize user input
• Just like for OS command injection, input sanitization is important
• Only restrictive whitelists should be used, not blacklists
• Where appropriate, do not allow user input to reach the database, and instead use mapping tables to translate it
© 2019 IBM Corporation
24
2:18 / 6:07

How to Prevent SQL Injection?

- **Recommendation #3 – Do not expose native database errors to the user**
- Application errors should not expose internal information to the user
- Details belong in an internal log file
- Exposed details can be abused for tailoring SQL injection commands
- For example, the following error message exposes both the internal query structure and the database type, helping attackers in their efforts:

> If you have an error in your SQL syntax, check the manual that corresponds to your MySQL server version for the right syntax to use near `"x" GROUP BY username ORDER BY username ASC' at line 1`

How to Prevent SQL Injection?

- **Recommendation #4 – Limit database user permissions**
- When user queries are executed under a restricted user less damage is possible if SQL injection happens
- Consider using user with read-only permissions when database updates are not required, or use different users for different operations

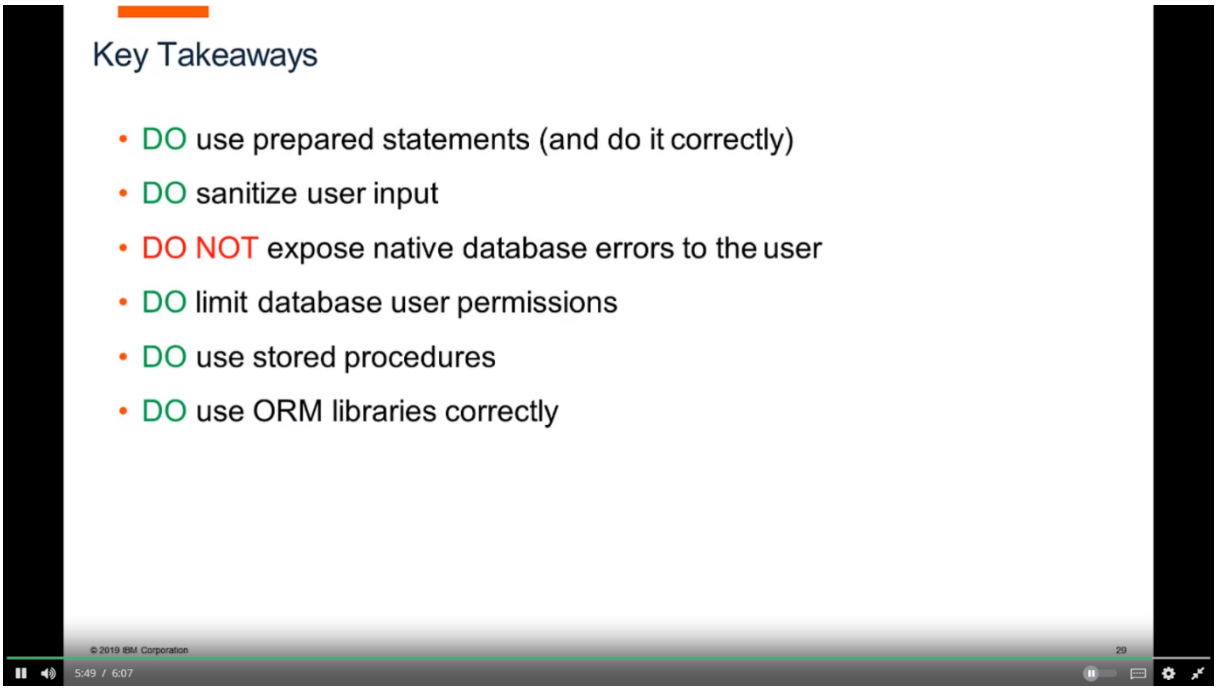
How to Prevent SQL Injection?

- **Recommendation #5 – Use stored procedures**
- Use of stored procedures mitigates the risk by moving SQL queries into the database engine
- Fewer SQL queries will be under direct control of the application, reducing likelihood of abuse

How to Prevent SQL Injection?

- **Recommendation #6 – Use ORM libraries**
- Object-relational mapping (ORM) libraries help mitigate SQL injection
  - Example: Java Persistence API (JPA) implementations like Hibernate
- ORM helps reduce or eliminate the need for direct SQL composition
- However, if ORM is used improperly SQL Injection may still be possible:

```
Query hqlQuery = session.createQuery("SELECT * FROM users WHERE
                 user='"+user+"'AND pass='"+pass+"'")
```



Other Types of Injection

Other Types of Injection

Other types of Injection

- Injection flaws exist in many other technologies"

NoSQL Injection

- In MongoDB `$where` query parameter is interpreted as JavaScript
- Suppose we take an expression parameter as input:

```
$where: "$expression"
```

- In simple cases it is harmless:

```
$where: "this.userType==3"
```

- However an attacker can perform a DoS attack:

```
$where: "d = new Date; do {c = new Date;} while (c - d < 100000;"
```

Other types of Injection

XPath Injection

- Suppose we use XPath expressions to select user on login:

```
"//Employee[UserName/text()='" + Request ("Username") + "' AND
Password/text()='" + Request ("Password") + "']"
```

- In the benign case it will select only the user whose name and password match:

```
//Employee[UserName/text()='bob' AND Password/text()='secret']
```

- In the malicious case it will select any user:

```
//Employee[UserName/text()='' or 1=1 or '1'='1' And Password/text()='']
```


Other types of Injection

LDAP Injection

- LDAP is a common mechanism for managing user identity information. The following expression will find the user with the specified username and password.

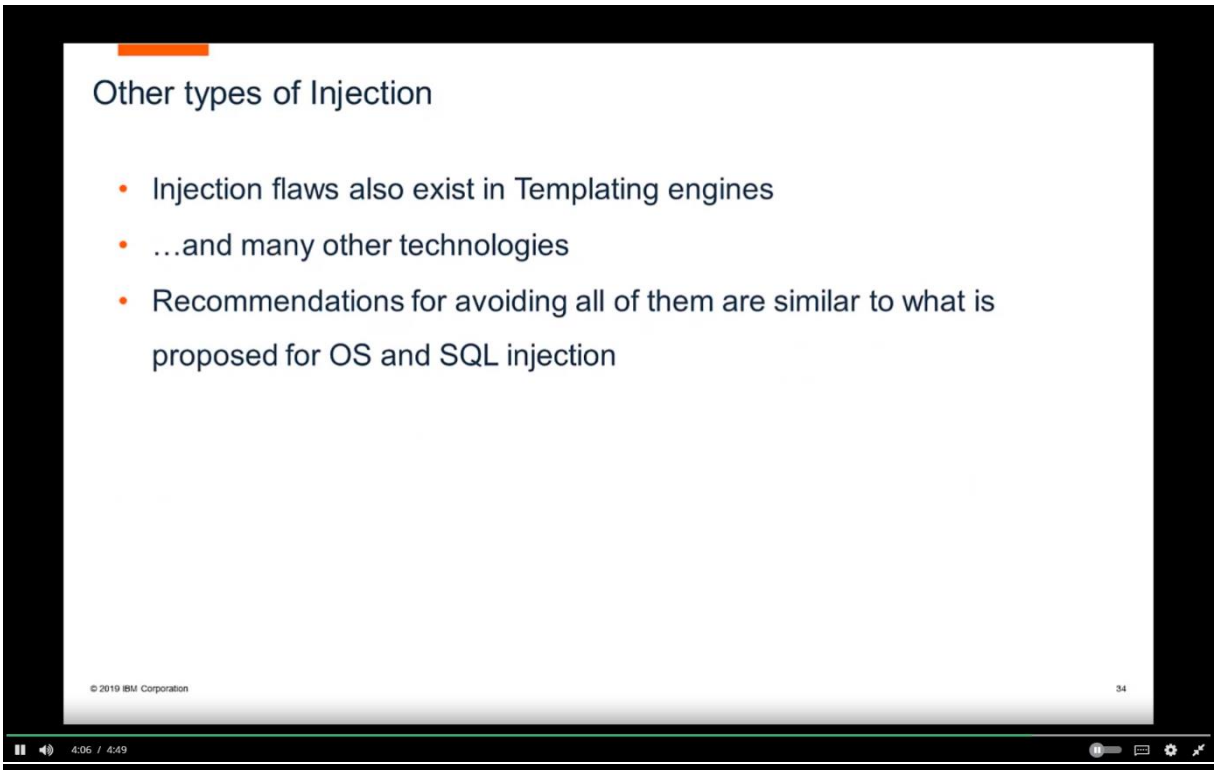
```
find("(&(cn=" + user +")(password=" + pass +"))")
```

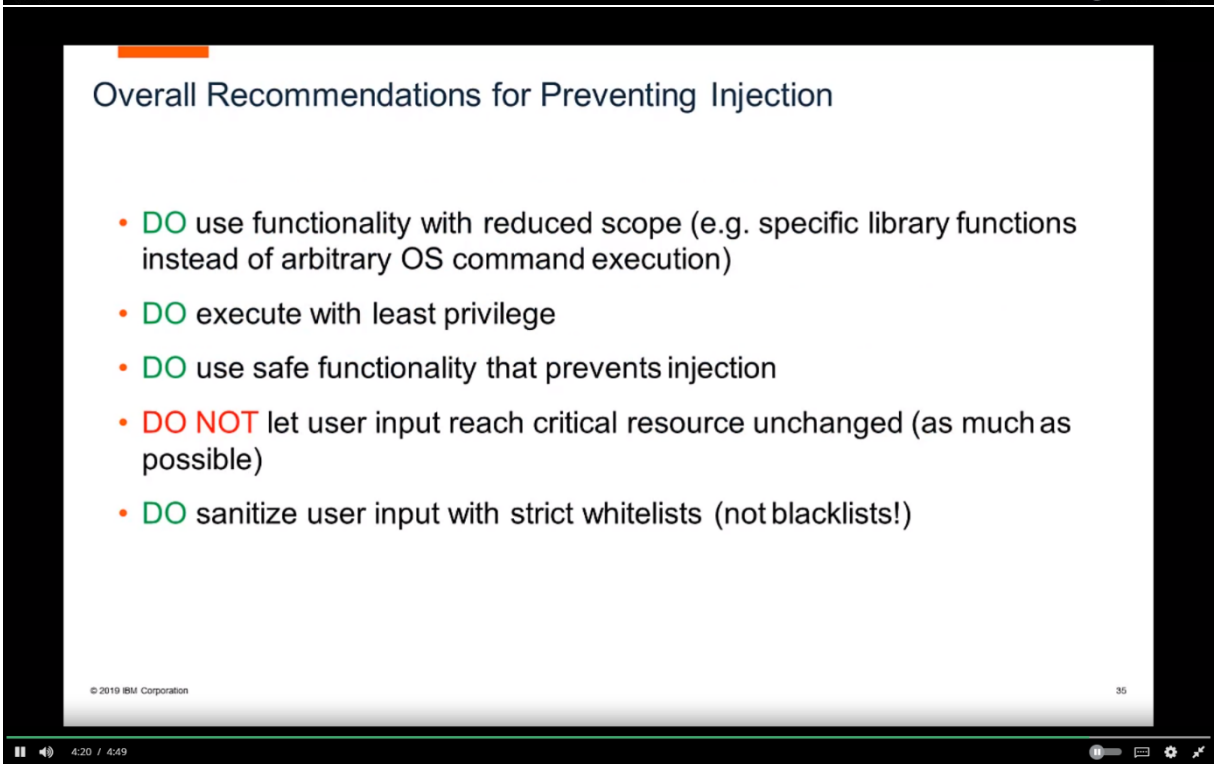
- In the regular case the LDAP expression will work only if the username and password match:

```
find("(&(cn=bob)(password=secret))")
```

- Malicious users may tweak the username to foce expression to find any user:

```
find("(&(cn=*)(cn=*))(|cn=*)(password=any))")
```





Additional Resources

Additional Resources

This course is the beginning of your journey. In Cybersecurity there is no way to know everything about Databases or Networking and their vulnerabilities. You need to know where to find additional information and detailed steps to safeguard data. Here are some additional resources that are important to be aware of and explore as you are developing your Cybersecurity skills.

OWASP Cheat Sheets

Injection Flaws https://owasp.org/www-community/Injection_Flaws

OS Command Injection https://owasp.org/www-community/attacks/Command_Injection

SQL Injection https://owasp.org/www-community/attacks/SQL_Injection

LDAP Injection
https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html

pentestmonkey

MSSQL injection cheat sheet: http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet

Oracle injection cheat sheet: http://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet

DB2 injection cheat sheet: http://pentestmonkey.net/cheat-sheet/sql-injection/db2-sql-injection-cheat-sheet

Postgres injection cheat sheet: http://pentestmonkey.net/cheat-sheet/sql-injection/postgres-sql-injection-cheat-sheet

MySQL injection cheat sheet: http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet The

Database Hacker's Handbook: Defending Database Servers

You can find this book at different retailers such as Amazon.com.

Software Vulnerabilities

A *vulnerability* is a potential weakness that someone can exploit in a system, network, or application. When targeting applications, attackers commonly exploit the following vulnerabilities:

- Broken access control or authentication
- Unencrypted data
- Use of default passwords or configurations
- Unpatched flaws
- Unused pages

By exploiting these vulnerabilities, attackers can circumvent an application's security to steal protected information, damage systems, or disable services.

Common Attacks

The following list describes some of the most common attacks on applications:

- *SQL injection* involves placing malicious code into a Structured Query Language (SQL) statement through a web page. The attacker typically uses a user input request, such as a username, to enter an SQL statement that will run on your database.
- *Cross-site scripting (XSS)* is an injection in which the attacker uses a web application to send a browser-side script to another user. Because the user's browser recognizes the script as coming from a trusted site, the script runs.

- *File inclusion* targets poorly written web applications that allow users to upload files without appropriate validation. The attacker tricks the web application into showing or running files that should not be publicly visible or available.
- *Buffer overflow* occurs when the amount of data sent exceeds what the memory buffer can handle. If the application is not properly secured, a knowledgeable attacker can use a buffer overflow attack to crash the system. The attacker could even overwrite existing executable code with their own to take control of the system.

Prevention Measures

To defend against common attacks, developers should build security into each step of the *software development life cycle (SDLC)*. They should consider and plan for potential security threats early on and test, scan, audit, and review code throughout development. Plus, various tools can automate security checks through nearly every stage of development, freeing developers to focus on other tasks.

Developers should also limit the number of applications and pages the product has. Extra pages, documentation, and features can increase the attack surface for attackers to target.

Security monitoring and logging practices help teams identify login, validation, and access control errors before a potential attacker can do damage. Personnel can respond quickly to patch the application if needed.

Another critical defense against common attacks is vulnerability scans. These scans identify vulnerabilities in the application and from libraries (collections of reusable code) on which the application depends. A standard type of vulnerability scan is a penetration test. A *penetration test (pentest)* simulates real hacking techniques to find application or system vulnerabilities that attackers can exploit. Organizations should perform pentesting regularly. Some useful pentesting tools for identifying web applications include OWASP ZAP, Comodo, and Vega.