



Mississippi State
UNIVERSITY

CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762



Mississippi State University Center for Cyber Innovation



CySA+

Part 1 Threat Management



Analyzing the Results of Reconnaissance

Chapter 2



Outline

- Sources of data to consider in your analysis
- Point-in-time data analysis
- Data correlation and analysis
- Common tools used in security analytics



Data Sources

- **Firewall Logs**
 - Rules are put in place to restrict the flow of network traffic through a firewall
 - Inbound and outbound traffic will have their own set of firewall rules
 - Every packet that is denied, accepted, or dropped creates a firewall log
- **Some Firewall Log Parameters**

Field	Description
Timestamp	Date and time at which the packet was logged
Source Address	IP address of the source of the packet
Source Port	Port number at the source
Destination Address	IP address of the destination of the packet
Destination Port	Port number at the destination
Protocol	IP protocol of the packet (for example, TCP, UDP, or ICMP)
IN Interface	Firewall interface that received the packet
OUT Interface	Firewall interface on which the packet was forwarded (unless denied or dropped)
Rule Name	Firewall rule that was applied to the packet resulting in whatever action was taken
Action	Action taken by the firewall (for example, accept, deny, or drop)

[1]



Data Sources

- **Intrusion Detection/ Prevention Systems**
 - **IDS/IPS set of rules are more complex than a firewall set of rules**
 - **IDS/IPS can be set up to detect specific signatures and behaviors**
- **Example IDS Alert**
 - **An alert triggered in Snort by a port scan**

```
[**] [1:469:3] ICMP PING NMAP [**]  
[Classification: Attempted Information Leak] [Priority: 2]  
01/20-17:30:12.439889 192.168.192.7 -> 192.168.192.8  
ICMP TTL:48 TOS:0x0 ID:63971 IpLen:20 DgmLen:28  
Type:8 Code:0 ID:56127 Seq:45129 ECHO  
[Xref -> http://www.whitehats.com/info/IDS162]  
  
[**] [122:1:0] (portscan) TCP Portscan [**]  
01/20-17:30:12.724540 192.168.192.7 -> 192.168.192.8  
PROTO255 TTL:0 TOS:0x0 ID:0 IpLen:20 DgmLen:162 DF
```

[1]



Data Sources

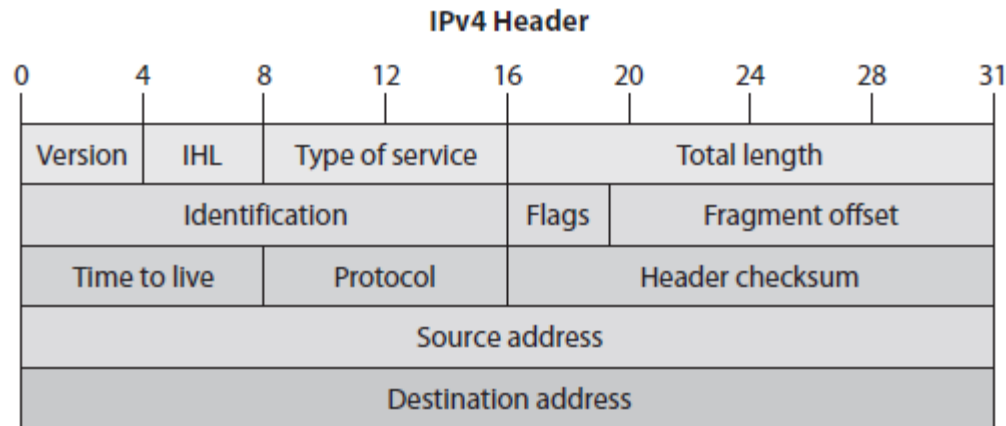
- **Packet Capture**
 - **Header Packet Capture**
 - Capturing only the header information from each packet
 - **Full Capture**
 - Captures the whole packages, including the packet header and the packet payload
- IPv4 and IPv6 packet headers have different fields of information
- The Comp TIA CySA+ exam will focus on IPv4 packets

[1]



Data Sources

- **Some fields to highlight in an IPv4 packet header**
 - **IP Header Length (IHL)**
 - The length of the header in 32-bit words
 - **Total Length:**
 - In the bits total length of the packet, including the payload
 - **Time To Live (TTL):**
 - The value decremented each time it's received by an interface, and the interface will drop the packet is that value reaches zero



[1]



Data Sources

- **System Logs**
 - **Two formats**
 - **Windows Event Logs format**
 - **Syslog format**
 - **Both formats are used by available products to aggregate the logs into one event log**
- **Nmap Scan Results**
 - **Nmap**
 - **Can be used to identify changes to a target host**
 - **Is used by some organizations to inventory assets on a network**
 - **A significant defensive measure is maintaining an accurate inventory of all hardware and software on your network**



Point-in-Time Analysis

- **Point-in-time Analysis**
 - Analyzing data around an event or an alert from a specific point or window of time
- **Packet Analysis**
 - Full packet capture challenges
 - Need lots of storage space
 - Can be quite difficult to find useful data
- **Filters**
 - Capture filters
 - Limit the number of packets captured with a set of criteria
 - Display filters
 - Capture all the packets
 - Use filters to only see parts of the data

[1]



Point-in-Time Analysis

- **Transport Control Protocol (TCP) Streams**
 - It is a stream of data
 - Packets do not normally arrive at their destination in order or at the same time TCP and UDP manages this
 - Wireshark can reconstruct TCP data streams
 - Can recover files or see the content of web pages visited
- **Encryption**
 - Encrypted packets can be of limited use in packets analysis
 - HTTPS proxies
 - Terminates Transport Layer Security (TLS) or Secure Socket Layer (SSL) connections
 - Allows capture of content that would have been encrypted
 - Can have privacy legal consequence, ensure to talk to your legal counsel before using HTTPS proxies

[1]



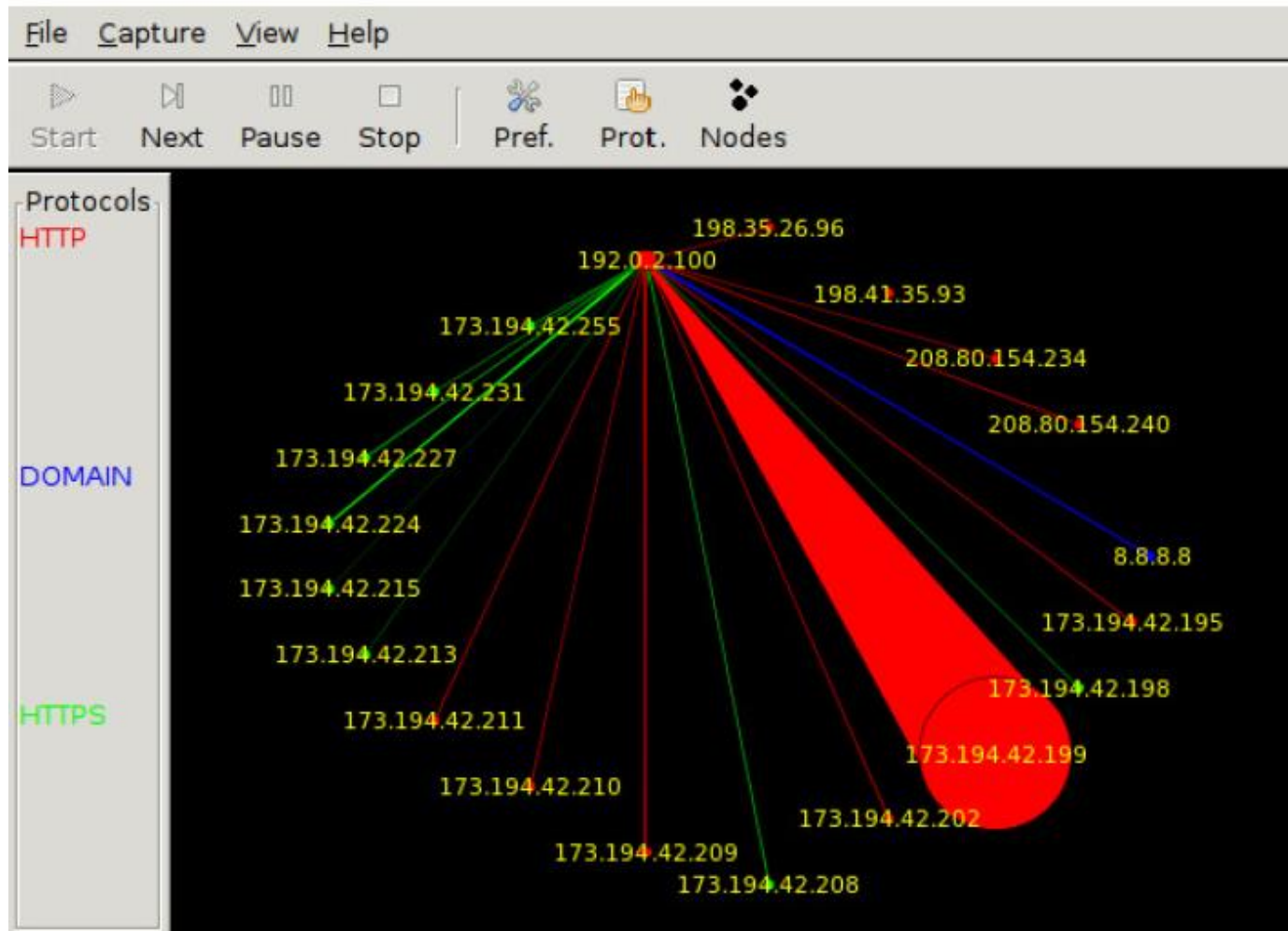
Point-in-Time Analysis

- **Protocol Analysis**
 - Analysis of how a packet conforms to the protocol it is thought to be implementing
 - For example:
 - Internet Control Message Protocol (ICMP) echo requests/replies can have a payload if the total packet length is no larger than the network's Maximum Transmission Unit (MTU)
 - ICMP tunnel can be created by attackers by exploiting the ICMP echo requests/replies
 - Analysis of this protocol would unveil any ICMP tunnels
- **Traffic Analysis**
 - Users may accidentally click on the wrong URL creating false positives in a traffic analysis
 - VirusTotal.com can be used to quickly check if a URL has been reported as malicious or not
 - Monitoring the volume of traffic
 - A large increase in traffic from a host could be an indicator of malicious activity
 - Traffic analysis is most useful as an early indicator, and an analyst will need to perform any further analysis

[1]



Traffic analysis example



[1]



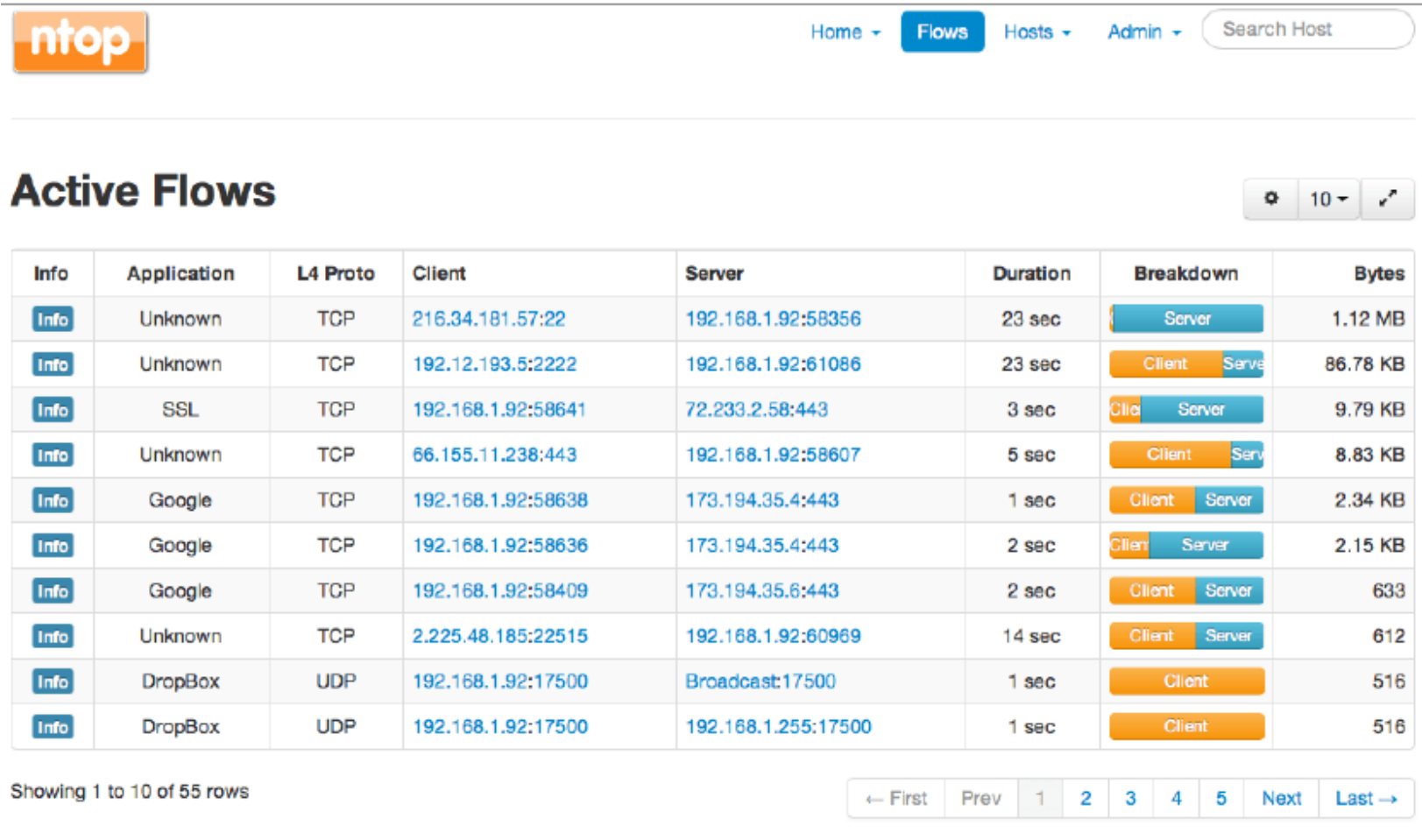
Point-in-Time Analysis

- **NetFlow Analysis**
 - **NetFlow**
 - Provides Analysts with statistics on network traffic
 - Groups packets into “flows” that share certain characteristics
 - The interface the packet arrives at such as a switch or router
 - IP addresses of the source and destination
 - Port numbers of the source and destination
 - IP protocol
 - IP type of service
 - **NetFlow-enable network device**
 - Creates a new flow for packets that arrive without any known flows and will start tracking related packets
 - Will aggregate statistics about the flow once the flow has ended
 - **Analysis**
 - More appropriate for forensic investigations
 - Captures aggregated statistics and therefore most valuable in the early stages of an investigation

[1]



NetFlow Analysis example



The screenshot shows the ntop interface for Active Flows. The top navigation bar includes 'Home', 'Flows' (selected), 'Hosts', and 'Admin', along with a 'Search Host' input field. The main section is titled 'Active Flows' and features a settings icon, a page size dropdown set to '10', and a refresh icon. Below this is a table with 11 rows of active flows. Each row includes an 'Info' button, the application name, L4 protocol, client IP, server IP, duration, a breakdown bar chart, and the total bytes transferred.

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Bytes
Info	Unknown	TCP	216.34.181.57:22	192.168.1.92:58356	23 sec	Server	1.12 MB
Info	Unknown	TCP	192.12.193.5:2222	192.168.1.92:61086	23 sec	Client Server	86.78 KB
Info	SSL	TCP	192.168.1.92:58641	72.233.2.58:443	3 sec	Client Server	9.79 KB
Info	Unknown	TCP	66.155.11.238:443	192.168.1.92:58607	5 sec	Client Server	8.83 KB
Info	Google	TCP	192.168.1.92:58638	173.194.35.4:443	1 sec	Client Server	2.34 KB
Info	Google	TCP	192.168.1.92:58636	173.194.35.4:443	2 sec	Client Server	2.15 KB
Info	Google	TCP	192.168.1.92:58409	173.194.35.6:443	2 sec	Client Server	633
Info	Unknown	TCP	2.225.48.185:22515	192.168.1.92:60969	14 sec	Client Server	612
Info	DropBox	UDP	192.168.1.92:17500	Broadcast:17500	1 sec	Client	516
Info	DropBox	UDP	192.168.1.92:17500	192.168.1.255:17500	1 sec	Client	516

Showing 1 to 10 of 55 rows

Navigation: ← First Prev 1 2 3 4 5 Next Last →

[1]



Point-in-Time Analysis

- **Wireless Analysis**
 - **Wireless Local Area Network (WLAN) Analysis**
 - **Kismet is a useful WLAN analyzer that detects the WLANs and their characteristics**
 - **Have a baseline in place that is a known good-list of all Wireless Access Point (WAP) and wireless clients**
 - **Perform periodic audits**
 - **For example, with a baseline in place; you would easily see if a rogue access point was set up during the audit**
 - **WPA Enterprise and IEE 802.1x**
 - **Device authentication**
 - **Will help prevent forgery of an end device's identity**

[1]



Correlation Analysis

- **Correlation Analysis**
 - Analyzing multiple collections of data and attempting to find patterns of an incident or event
- **Three tool categories**
 - **SIEM systems**
 - Collects data from an assortment of sensors and generates event and alerts
 - Best-known commercial SIEM product is Splunk
 - Opensource SIEM product is Elasticsearch-Logstash-Kibana(ELK)
 - **Big data analytics solutions**
 - Normally used along with a SIEM system
 - A SIEM systems collect large quantities of data
 - **Locally developed analytics solutions**
 - Scripts developed by the organization's security analysts
 - These tools are normal developed in Python or PowerShell
 - Some time used with a SIEM system or as a substitute for a SIEM system

[1]



Correlation Analysis

- **Baselining**
 - Determining the normal state or flows of a system
- **Anomaly Analysis**
 - Measuring the deviation from the baseline
 - Statistical analysis of the deviation is important given systems to change constantly
 - Significant statistical deviation from the baseline would infer a possible breach
- **Behavioral Analysis**
 - Correlates data points of user behavior such as
 - Time of the day the user may upload files to a cloud folder
 - The user uploads files between 8 am, and 5 pm is normal
 - The user uploads files between 2 am, and 5 am is not normal
 - Location of files being uploaded by a user
 - The user uploads files to Amazon cloud be considered normal
 - The user uploads files to Google cloud be consider not normal

[1]



Correlation Analysis

- **Trend Analysis**
 - Analyzing patterns over time to determine how, when, and why
 - Commonly used to track patterns of attackers' behavior
 - Some security firms will publicly release their trend analysis
 - For example
 - If DDoS attacks were trending upward, then DDoS mitigation efforts would need to be prioritized

[1]



Correlation Analysis

- **Internal Trends**
 - Can reveal emerging areas of risks
 - Example
 - An organization may start increasing the amount of data stored on a cloud service
 - By monitoring the trend in the example; an analyst would be able to decide when it might be best to take action to mitigate the risk
- **Temporal Trends**
 - Can reveal patterns related to time
 - Example
 - An attacker implementing a breach on a Friday night to avoid detection until Monday
 - Increased phishing attacks during tax season
 - Knowing these trends can help users be aware of the risks during that time of day, week, or season

[1]



Correlation Analysis

- **Spatial Trends**
 - **Patterns that show risks related to regions**
 - **Example**
 - **Some countries have a higher risk of stolen technologies than others**
 - **Public areas with free Wi-Fi networks**
 - **Companies might send their employees to certain countries with burner laptops that have limited access and limited files to remediate the risk**
 - **Companies should ensure their employees have had cybersecurity awareness training and know-how to use a virtual private network(VPN)**

[1]



Correlation Analysis

- **Availability Analysis**
 - Analyzing the cost per unit of time the company can afford for its services to be unavailable
- **Heuristics**
 - An approach that is founded on experience rather than theory
 - **Malware is detected through heuristics**
 - The majority of malware exhibits the same characteristics or behaviors such as replicating itself, scanning resources, or adding user accounts
 - **Next-Generation Firewalls (NGFs)**
 - Has the same features as a firewall but also can detect malware

[1]



Tools of the Trade

- **SIEM Systems**
 - **Data analytics platforms**
 - **Splunk and ELK**
 - Can ingest, index, store, and retrieve large volumes of data
 - This data can be applied to network provisioning, marketing, or to enterprise security

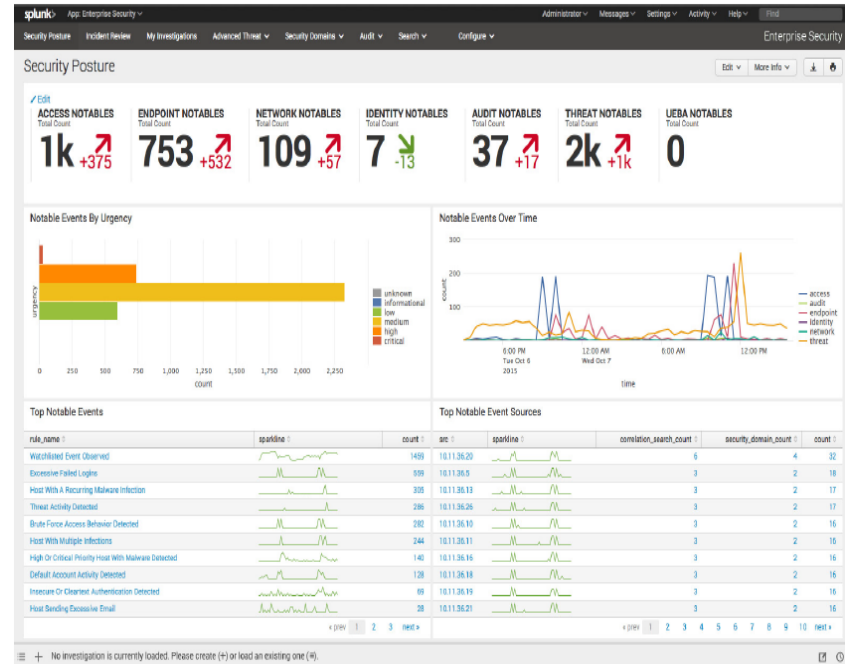
[1]



SIEM Systems cont.

– Splunk

- Data that is captured by Splunk can be easily indexed through sophisticated methods of correlating real-time data in a searchable repository
- Generates graphs of data trends, reports, and security alerts



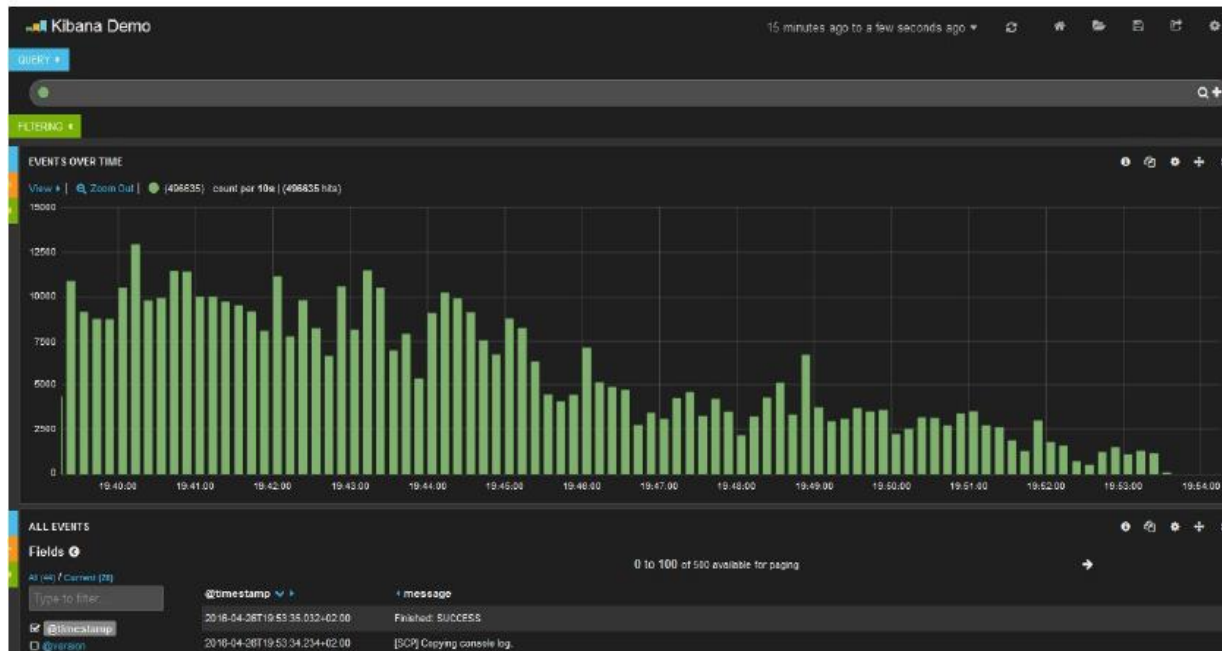
[1]



SIEM Systems cont.

– ELK

- A system of opensource tools, which are Elasticsearch, Logstash, and Kibana
- The three tools in ELK together perform many of the same functions as Splunk



[1]



Tools of the Trade

- **Packet Analyzers**
 - Most widely used packet analyzer is Wireshark
- **Intrusion Detection Systems**
 - **Snort**
 - Best-known opensource NIDS
 - Can also be used as a packet analyzer or as a NIPS



[1,4]



Intrusion Detection Systems con't

– Zeek (formerly Bro)

- Both signature and anomaly-based
- Creates events to indicate something happened on the system
- Collects all data including, embedded files
- Can extract complete executables from network streams to run a malware analysis



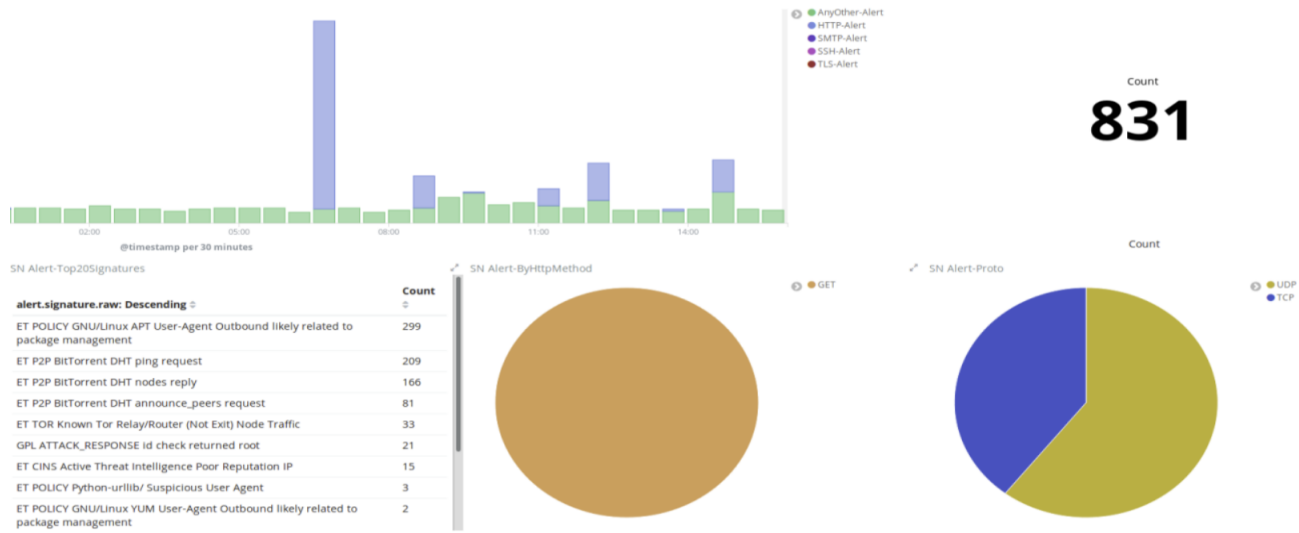
[5]



Tools of the Trade

- **Suricata**

- Can be considered a more powerful version of Snort
- It can utilize Snort signatures to create rules
- Can be used as an IPS
- It can capture packet flows for analysis



Tools of the Trade

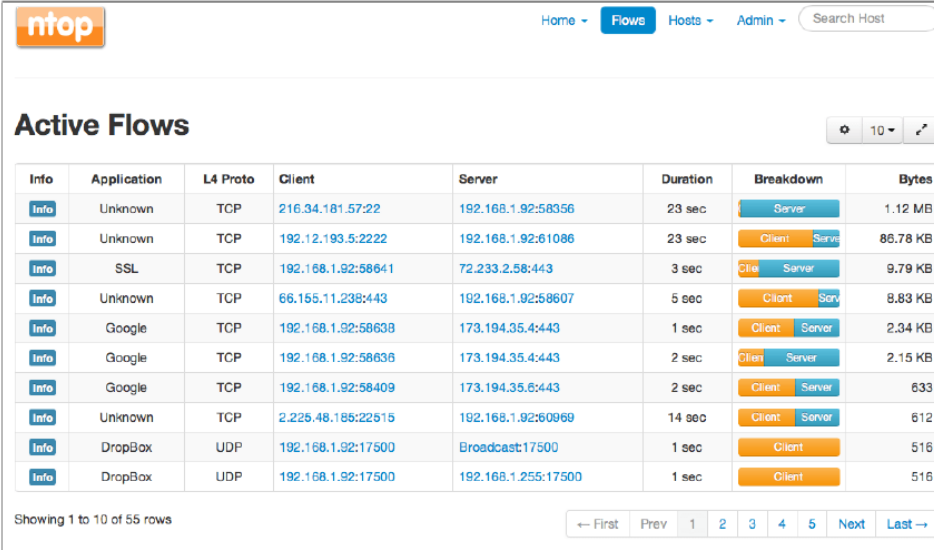
- **Resource-Monitoring Tools**
 - **Nagios Core**
 - **Popular opensource resource-monitoring tool**
 - **Allows the user to track the status of their network devices**
 - **Such as workstations, servers, switches, or routers**
 - **Monitors device processors and disk utilization**
 - **Will log events and send an email to the user of the event**
 - **Is scalable and can handle complex environments**



Tools of the Trade

- **NetFlow Analyzers**

- Allows analysts to view and query data from a collector
- Popular opensource NetFlow analyzer is ntopng
 - Acts as a NetFlow collector and as an analysis console
 - Has a web-based interface and can run on most OSs



Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Bytes
Info	Unknown	TCP	216.34.181.57:22	192.168.1.92:58356	23 sec	Server	1.12 MB
Info	Unknown	TCP	192.12.193.5:2222	192.168.1.92:61086	23 sec	Client Server	86.78 KB
Info	SSL	TCP	192.168.1.92:58641	72.233.2.58:443	3 sec	Client Server	9.79 KB
Info	Unknown	TCP	66.155.11.238:443	192.168.1.92:68607	5 sec	Client Server	8.83 KB
Info	Google	TCP	192.168.1.92:58638	173.194.35.4:443	1 sec	Client Server	2.34 KB
Info	Google	TCP	192.168.1.92:58636	173.194.35.4:443	2 sec	Client Server	2.15 KB
Info	Google	TCP	192.168.1.92:58409	173.194.35.6:443	2 sec	Client Server	633
Info	Unknown	TCP	2.225.48.185:22515	192.168.1.92:60969	14 sec	Client Server	612
Info	DropBox	UDP	192.168.1.92:17500	Broadcast:17500	1 sec	Client	516
Info	DropBox	UDP	192.168.1.92:17500	192.168.1.255:17500	1 sec	Client	516

Showing 1 to 10 of 55 rows

← First Prev 1 2 3 4 5 Next Last →

[1]



Quiz

Chapter 2



Question #1

- **What is the key difference between an intrusion system (IDS) and an intrusion prevention system (IPS)?**
 - A. An IPS only relies on a fixed set of rules, or heuristics, when analyzing traffic.**
 - B. An IDS only analyzes TCP traffic, whereas an IPS analyzes only UDP traffic.**
 - C. An IDS only detects suspicious traffic, whereas an IPS detects and blocks malicious traffic**
 - D. An IPS only detects suspicious traffic, whereas an IDS detects an blocks malicious traffic**

[1]



Answer #1

- **C**
 - **Intrusion detection systems (IDSs) simply detect suspected threats, and intrusion prevention systems (IPSs) actively block them.**



Question #2

- Which of the following transmissions is not provided by the NetFlow network protocol?
 - A. Source IP address
 - B. Destination IP address
 - C. Default gateway address
 - D. TCP source port

[1]



Answer #2

- **C**
 - **NetFlow is traffic-analysis system developed by Cisco that provides information about the arrival interface, source and destination IP addresses and port numbers, and the type of service.**
 - **The default gateway is a network device that facilitates access for a connected device.**

[1]



Question #3

- Which kind of packet capture technique is preferred for a resource-limited environment?
 - A. Header capture
 - B. Footer capture
 - C. Full packet captures
 - D. Payload captures

[1]



Answer #3

- **A**
 - **In a header capture, only the IP header data is recorded for analysis, whereas a full capture requires more storage and processing power.**



Question #4

- **Why might it be useful to analyze individual system logs in addition to network traffic?**
 - A. Activity on the end points is usually much easier to observe than on the network.**
 - B. It is impossible to analyze obfuscated or encrypted network traffic.**
 - C. End point are unable to log their system activity.**
 - D. There aren't any useful standards for logging system activity.**

[1]



Answer #4

- **A**
 - **Monitoring local end-points events provides tremendous insight into the computer's process and network activities.**
 - **Examination of local event logs is an excellent supplement to network analysis and will give a far more accurate picture of the network's state.**

[1]



Question #5

- **When performing a capture for wireless analysis, what mode must the wireless card support?**
 - A. Managed**
 - B. Ad hoc**
 - C. Mesh**
 - D. Monitor**

[1]



Answer #5

- **D**
 - **To capture wireless traffic, especially when it's not associated with an access point, the network interface card must support monitor mode operation.**



Question #6

- The largest unit of data that traverses a network in a single exchange is referred to what?
 - A. ICMP
 - B. MTU
 - C. TCP
 - D. CDMA

[1]



Answer #6

- **B**
 - The maximum transmission unit (MTU) is the largest single unit of data that traverses the network during an exchange.
 - A larger MTU means that more data moves for every exchange, requiring less processing power over time because fewer units can occupy a transmission line at a given time.

[1]



Scenario for Questions 7 - 9

- **Your company has experienced significant growth over the past few months, and increased traffic has proven too much for the existing set of tools. Your analyst team is looking for a solution to manage the alerts generated by all the enterprise's network devices with minimal interruption to the network's current configuration, and they turn to you as their resident expert for guidance.**

[1]



Question #7

- **When searching for a solution, the team comes across the acronym SIEM. What does it stand for?**
 - A. Simulated incident and environmental management**
 - B. Security indicators and event monitor**
 - C. Security information and event management**
 - D. Simulations, indications, and environmental monitors**

[1]



Answer #7

- **C**
 - **SIEM, or security information and event management, is a set of security tools that combine security information management (SIM) and security event management (SEM).**

[1]



Question #8

- **With the new SIEM tool, the team realizes that they can perform point-in-time analysis much more efficiently. What feature of the SIEM are they likely leveraging for this task?**
 - A. Query function to investigate past network activity around the time of an alert**
 - B. Visualization of current network flows**
 - C. Certificate Authority (CA) verification**
 - D. A single syslog warning message**

[1]



Answer #8

- **A**
 - **Point-in-time analysis is the analysis of various data outputs to determine system events that were recorded around a specified time**



Question #9

- **When you're conducting a full packet capture on network traffic, which of the following is not a consideration?**
 - A. Easily identifying the source and destination of the traffic**
 - B. Legal consequences**
 - C. Privacy implications**
 - D. Data storage capacity**

[1]



Answer #9

- **A**
 - Legal and privacy issues must always be considered before capturing packets.
 - Depending on the duration of the capture, storage capacity can become an issue so one would normally ensure the required space is available before starting.
 - Since there are several free and commercial capture and analytic software options that specialize in packet capture and analysis, it is easy to determine the sources and destinations.

[1]



Question #10

- What is the total size, in bytes, of the packet's payload?

- A. 84
- B. 64
- C. 44
- D. 24

The image shows a Wireshark packet capture window titled '*eth0'. The packet list pane shows a table of captured packets. The selected packet (No. 25) is an ICMP Echo (ping) request from 10.10.0.112 to 10.10.0.1, with a length of 98 bytes. The packet details pane shows the following structure:

- Internet Protocol version 4, Src: 10.10.0.112, Dst: 10.10.0.1
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 84
 - Identification: 0x6dba (28090)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: ICMP (1)
 - Header checksum: 0xb80a [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 10.10.0.112
 - Destination: 10.10.0.1
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]
 - Internet Control Message Protocol

The packet bytes pane shows the raw data of the packet, with the first 20 bytes highlighted in blue, corresponding to the IP header. The total length of the packet is 98 bytes, and the payload (ICMP Echo request) is 78 bytes (98 - 20).

[1]



Answer #10

- **B**
 - The total size of the packet (84 bytes) is the size of the header (20 bytes) plus the size of the payload.
 - The payload size is not provided explicitly but can be calculated by subtracting the header size from the total size to get 64 bytes.

[1]



Question #11

- Roughly how much time elapsed between the first ping request and reply?
 - A. 35 seconds
 - B. 35 milliseconds
 - C. 350 milliseconds
 - D. .350 milliseconds

The image shows a Wireshark capture on interface eth0. The packet list pane shows several ICMP Echo (ping) packets. The first packet at time 25.445725580513 is a request from 10.10.0.112 to 10.10.0.1. The second packet at time 26.445725930952 is a reply from 10.10.0.1 to 10.10.0.112. The third packet at time 27.446749575480 is another request. The fourth packet at time 28.446749897763 is another reply. The fifth packet at time 29.447773571740 is a request. The sixth packet at time 30.447773908808 is a reply. The packet details pane for the selected packet (Internet Protocol version 4, Src: 10.10.0.112, Dst: 10.10.0.1) shows the following fields: Version: 4, Header Length: 20 bytes (5), Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT), Total Length: 84, Identification: 0x6dba (28090), Flags: 0x02 (Don't Fragment), Fragment offset: 0, Time to live: 64, Protocol: ICMP (1), Header checksum: 0xb86a [validation disabled], [Header checksum status: Unverified], Source: 10.10.0.112, Destination: 10.10.0.1, [Source GeoIP: Unknown], [Destination GeoIP: Unknown], and Internet Control Message Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Time	Source	Destination	Protocol	Length	Info
25.445725580513	10.10.0.112	10.10.0.1	ICMP	98	Echo (ping) request id=
26.445725930952	10.10.0.1	10.10.0.112	ICMP	98	Echo (ping) reply id=
27.446749575480	10.10.0.112	10.10.0.1	ICMP	98	Echo (ping) request id=
28.446749897763	10.10.0.1	10.10.0.112	ICMP	98	Echo (ping) reply id=
29.447773571740	10.10.0.112	10.10.0.1	ICMP	98	Echo (ping) request id=
30.447773908808	10.10.0.1	10.10.0.112	ICMP	98	Echo (ping) reply id=

[1]



Answer #11

- **D**
 - The time value display in Wireshark is in seconds.
 - The difference between the first and second values listed is about .350 milliseconds.

[1]



Question #12

- **What is the name of the Windows utility that allows you to easily monitor various program, security, and system activity logs on your computer?**
 - A. Nmap**
 - B. Event Viewer**
 - C. Console**
 - D. Putty**

[1]



Answer #12

- **B**
 - **The Event Viewer is a utility that helps administrators troubleshoot problems on their computers by providing an easy-to-use interface for reviewing system logs, including error, informational, and warning messages.**

[1]



References

1. **Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.**
2. **Nmap. [Online]. Available: <https://nmap.org/>. [Accessed: 30-Sep-2020].**
3. **Suricata. [Online]. Available: <https://suricata-ids.org/>. [Accessed: 30-Sep-2020].**
4. **E. Acar, “What is Snort?,” Medium, 17-Dec-2018. [Online]. Available: <https://medium.com/@acaremullahkku/what-is-snort-547916bece5f>. [Accessed: 30-Sep-2020].**



References cont.

5. “The Zeek Network Security Monitor,” Zeek. [Online]. Available: <https://zeek.org/>. [Accessed: 30-Sep-2020].

