Slide 1

Notes

Narration

Slide mockup

Data Collection and Analysis

Course Objectives

After completing this course, you will be able to:

- Define security challenges facing cloud computing.
- Compare the advantages and disadvantages of cloud computing.
- Identify the differences between a threat and a vulnerability.

Narration

Please familiarise yourself with the objectives of this topic.

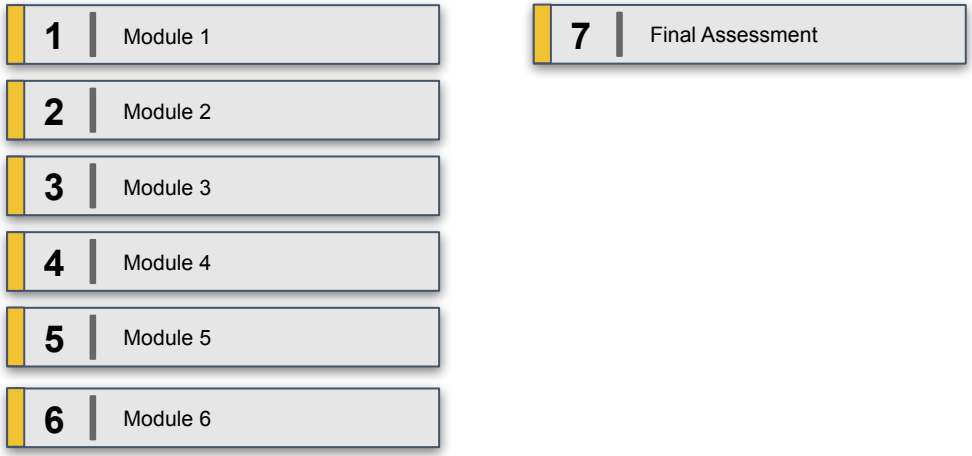
Notes

State the Objectives

Slide mockup

Data Collection and Analysis

Course Map



Narration

Choose a module from the list or click Next to continue.

Notes

Provide the modules for the course

Module 1: Cloud & Network Based Data Sources
Module 2: Cybersecurity & Data Analytics
Module 3: Data Analysis Solutions & Strategies for Processing Data Within Organizations
Module 4: Weapons and Data Analysis
Module 5: Using Windows Tools & Best-Practices
Module 6: Challenges of Secure Data Management

Slide 4

1 Data Collection and Analysis

Module 1: Cloud & Network Based Data Sources

Narration

Welcome to Module 1.

Notes

Slide mockup

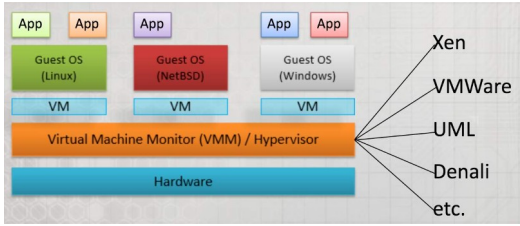
Notes

Data Collection and Analysis

What is a Virtual Machine?

Here are a few examples of virtual machine software:

- **UML-Unified Modeling Language(UML)** is a standardized (ISO/IEC19501:2005), general-purpose modeling language in the field of software engineering. The Unified Modeling Language includes a set of graphic notation techniques to create visual models of object-oriented software-intensive systems
- **Xen**- is a hypervisor providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.
- **Denali Software, Inc.** is an American software company. The company produces electronic design automation (EDA) software, intellectual property (IP) and design cores and platforms for memory, other standard interfaces and system-on-chip (SoC) design and verification
- **Paravirtualization**: Para = “beside”, “with”, or “alongside”. Paravirtualization refers to communication between the guest OS and the hypervisor to improve performance and efficiency.



Narration

A virtual machine allows multiple machines to run on a single computer system, complete with virtual hardware devices. The virtual machine runs as a process in regular window on your current computer or system. The operating system running on your computer is called the host, and any operating system that's running inside your virtual machine are called guests.

Slide mockup

Notes

Data Collection and Analysis

Cloud Computing- Cloud Service Provider (1/2)

Cloud Software as a Service, the Cloud Service Provider:

- Deploys
- Configures
- Maintains
- Updates the operation of the software applications on a cloud infrastructure

Narration

For Cloud Platform as a Service, the Cloud Service Provider manages the cloud infrastructure for the platform, and provisions tools and execution resources for the platform consumers to develop, test, deploy, and administer applications. Consumers have control over the applications and possibly the hosting environment settings, but cannot access the infrastructure underlying the platform including network, servers, operating systems, or storage.

For Cloud Infrastructure as a Service, the cloud provider provisions the physical processing, storage, networking, and other fundamental computing resources, as well as manages the hosting environment and cloud infrastructure for IaaS consumers. Cloud consumers deploy and run applications, have more control over the hosting environment and operating systems, but do not manage or control the underlying cloud infrastructure (e.g., the physical servers, network, storage, hypervisors, etc.).

Slide mockup

Notes

Data Collection and Analysis

Cloud Computing - Five Major Actors (2/2)

Actor	Definition
Consumer	Person or organization that maintains a business relationship with, and uses service from, Cloud Service Providers.
Cloud Service Provider	Person, organization, or entity responsible for making a service available to Cloud Consumers.
Assessor	A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
Broker	An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Service Providers and Cloud Consumers.
Carrier	The intermediary that provides connectivity and transport of cloud services from Cloud Service Providers to Cloud Consumers.

Narration

NIST SP 500-291, the NIST cloud computing reference architecture defines five major actors: cloud consumer, cloud provider, cloud auditor, cloud broker, and cloud carrier. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing.

The table shows the interactions among the actors in the NIST cloud computing reference architecture. A cloud consumer may request cloud services from a cloud provider directly or via a cloud broker. A cloud auditor conducts independent audits and may contact the others to collect necessary information.

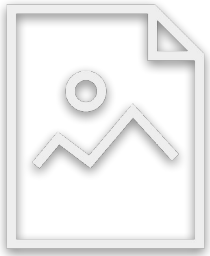
Slide mockup

Notes

Data Collection and Analysis

Advantages to Cloud Computing (1/4)

- Reduced Software Costs
- Lower Computing Costs
- Improved performance
- Instant Software Updates
- Unlimited Storage Capacity
- Increased data reliability
- Universal Document Access
- Device Independence
- Latest version available



Narration

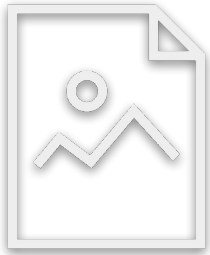
Slide mockup

Notes

Data Collection and Analysis

Disadvantages to Cloud Computing (2/4)

- Requires a constant internet connection.
- When offline, cloud computing does not work.
- Stored data might not be secure.
- Features might be limited.



Narration

Cloud computing is not perfect. So, now that we have discussed the advantages, let's look at some of the disadvantages.Cloud computing is impossible if you cannot connect to the Internet. Since you use the Internet to connect to both your applications and documents, if you do not have an Internet connection you cannot access anything, even your own documents. A dead Internet connection means no work and in areas where Internet connections are few or inherently unreliable, this could be a deal-breaker. When you are offline, cloud computing simply does not work.

Stored data might not be secure

With cloud computing, all your data is stored on the cloud.
The questions is How secure is the cloud?
Can unauthorized users gain access to your confidential data?
Cloud computing companies say that data is secure, but it is too early to be completely sure of that.
Only time will tell if your data is secure in the cloud.
Feature might be limited

Many web-based applications simply are not as full-featured as their desktop-based applications

Slide mockup

Notes

Data Collection and Analysis

Opportunities and Challenges (3/4)

Opportunities of cloud computing:

- Potentially lowers expenses for clients, which they will no longer need to buy their own software or hardware.
- Cost is based on demand.
- Data and services are stored remotely and can be access from anywhere.

Negative perceptions of cloud computing:

- Fosters dependence on other and that could limit flexibility and innovation.
- Proper implementation of security measures is a concern.
- What if remote server goes down? How will customers access data?

Narration

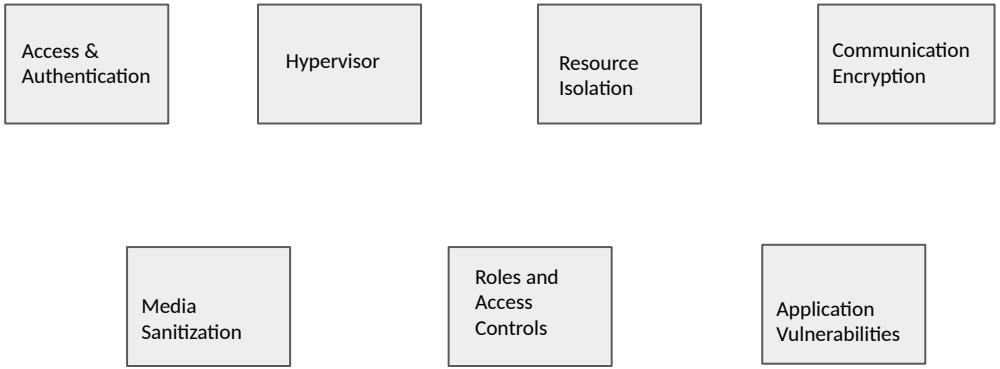
It is important to note that, while cloud computing provides many advantages, there are also challenges associated with its implementation and use. Here are some of the primary opportunities provided by cloud use. Primary among them is the anticipated cost reduction. The use of the cloud provides a number of opportunities as it takes advantage of economies of scale. Dependency on others refers largely to the bigger Internet companies like Google and IBM, who may monopolise the market. Some argue that this use of supercomputers is a return to the time of mainframe computing that the PC was a reaction against. Security could prove to be a big issue: It is still unclear how safe outsourced data is and when using these services ownership of data is not always clear.

Slide mockup

Notes

Data Collection and Analysis

Vulnerabilities of Cloud Computing (4/4)



Narration

The cloud environment has the same threats as traditional data centers. Cloud computing has software vulnerabilities since it runs software within the system.

Let's take a look at cloud computing vulnerabilities broken down in specific details, click on each of the buttons to learn more.

Slide mockup

Notes

Data Collection and Analysis

Third Party Assessor (3PAO)

- Auditing is important to federal agencies.
  - Include a contractual clause enabling third parties to assess security controls of cloud providers.
- Cloud auditor makes an assessment of security control in the information system to establish which controls are to be implemented correctly, operating as intended or producing the correct outcome that are required for system.
- Include verification of the compliance with regulatory requirements and security policy.

Narration

A cloud auditor is a party that can conduct independent assessment of cloud services, information system operations, performance, and security of a cloud implementation. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

Slide mockup

Notes

Data Collection and Analysis

Why Does a Assessor Source Matter? (1/2)

- DoD and Federal systems being authorized will enjoy reciprocal BOE for control assessment and inheritance
- Systems assessed within the Federal environment may have different (but potentially acceptable) control implementations

Narration

Slide mockup

Notes

Data Collection and Analysis

Cloud Broker (2/2)

In general, a cloud broker can provide services in three categories:

- Service Intermediation: A cloud broker enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
- Service Aggregation: A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.
- Service Arbitrage: Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

Narration

A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. A cloud broker is an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

Slide mockup

Notes

Data Collection and Analysis

Cloud Carrier

Consumer can obtain cloud services through the following:

- Network access devices
  - Computers or laptops
  - Mobile devices
  - Mobile Internet devices (MIDs)
- Distribution of Cloud services provided by:
  - Network and telecommunication carriers
  - Transport agents

Note: A cloud provider will set up service level agreements (SLAs) with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and encrypted connections between cloud consumers and cloud providers.

Narration

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers. Cloud carriers provide access to consumers through network, telecommunication, and other access devices.

Slide mockup

Notes

Data Collection and Analysis

Security Concerns (1/3)

- Cloud Providers should ensure that the facility hosting cloud services is secure and that their staff has proper background checks.
- When data or application is moved to a cloud, it is important to ensure that the cloud offering satisfies the security requirements and enforces the compliance rules.
- An independent audit should be conducted to verify the compliance with regulation or security policy.

Narration

It is critical to recognize that security is cross-cutting that spans across all layers of the reference model, ranges from physical security to application security, and in general, shares the responsibility between cloud provider and federal cloud consumer.

For example, the protection of the physical resource layer requires physical security that denies unauthorized access to the building, facility, resource, or stored information.

Slide mockup

Notes

Data Collection and Analysis

Barrier to Successful Cloud Deployments (2/3)

- Security fears have made many organizations hesitant to adopt the cloud.
- To gain trust of organizations, cloud-based services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

Narration

Security refers to a computing system's level of resistance to threats. Privacy most often concerns the digital collection, storage, and sharing of information and data, including the transparency of such practices.

Cloud Computing Impacts Security Implementation in Fundamentally New Ways. In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning resource and applications increases - greatly affecting all aspects of IT security.

Slide mockup

Notes

Data Collection and Analysis

Cloud Security Myths (3/3)

Narration

Slide mockup

Notes

Data Collection and Analysis

What is Cloud Security?

Trends that impact cloud security:

- Changing attackers and threats: Threats are no longer the purview of isolated hackers looking for personal fame. More and more, organized crime is driving well-resourced, sophisticated, targeted attacks for financial gain.
- Evolving architecture technologies: With the growth of virtualization, perimeters and their controls within the data center are in flux, and data is no longer easily constrained or physically isolated and protected.
- Dynamic and challenging regulatory environment: Organizations—and their IT departments—face ongoing burdens of legal and regulatory compliance with increasingly prescriptive demands and the high penalties for noncompliance or breaches. Examples of regulations include Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and the Health Insurance Portability and Accountability Act (HIPAA).

Narration

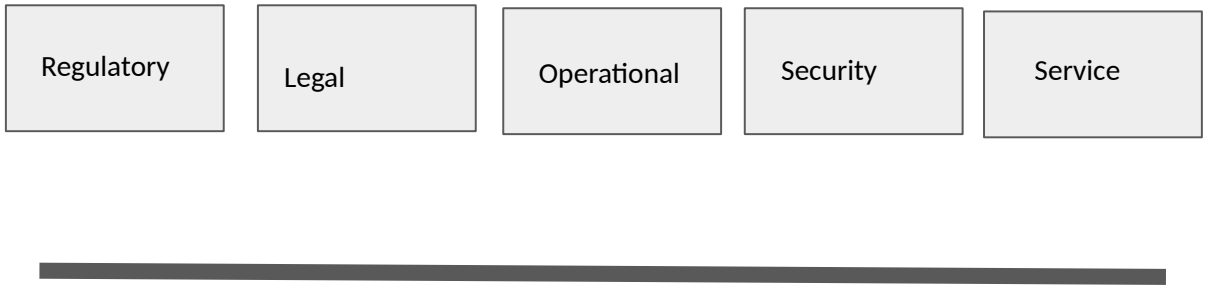
Cloud security is a response to a familiar set of security challenges that are different in the cloud. New technology requires a more thorough approach to defining the system boundary, set of policies, technologies, and controls designed to protect data and infrastructure from attack and enable compliance with layered technologies that create a durable security net or grid. Security is more effective when layered at each level of the stack and integrated into a common management framework. Joint responsibility of an organization and its cloud provider(s). Depending on the cloud delivery model and services that are deployed, responsibility for security comes from both parties.

Slide mockup

Notes

Data Collection and Analysis

Risks



Narration

Slide mockup

Notes

Data Collection and Analysis

Detection and Remediation Tools

- Vulnerability Scanners: Nessus/ACAS, and Nexpose
- Web Application Vulnerability Scanners: WebInspect, and Burp Suite
- Database Vulnerability Scanners: AppDetective Pro, Scuba, and McAfee
- Network Intrusion Detection Systems: Snort, Advanced Intrusion Detection Environment (AIDE), and OSSEC
- Sniffing Tools: Wireshark, Network Miner, and Tcpdump
- Remediation: Patching

Narration

Software vulnerabilities are the entry point of 53% of successful cyber-attacks according to Forrester. Security breaches are known before being exploited, there are numerous tools on the market, let's look at a few.

Slide mockup

Notes

Data Collection and Analysis

Should I Use the Cloud? (1/2)

- Important Steps for Cloud Security
  - Start Planning Early
  - Identify Vulnerabilities to Selected Services
  - Mitigate known vulnerabilities
  - Protect Data - In transit, In Process, and At rest
  - Secure the platform
  - Choose the right Cloud Service Provider

Narration

You must ensure that your business/mission need justifies the risk of cloud operations. Also, ensure using cloud assets is sensible. Having remote connectivity of the cloud introduces risks that would not be present in a local environment.

Slide mockup

Notes

Data Collection and Analysis

Security Considerations (2/2)

Security considerations when choosing a cloud service provider:

- Data Center Risk Management and Security Practices
- Hardware-Based Security
- Technology Segmentation
- Incident Response and Recovery
- System Availability and Performance
- Compliance Capabilities

Narration

Choosing a cloud service provider is complicated on many levels—from the cloud delivery model and architecture to specific applications. Add to that the countless interdependencies and relationships, both technological and business-related, among vendors. To complicate matters, some companies offer not only software, but also hardware and services. Nevertheless, you must be vigilant about making sure the security you need to protect your data and platform are part of the offering.

Slide 24

2 | Data Collection and Analysis

Module 2: Cybersecurity & Data Analytics

Narration

Welcome to Module 2.

Notes

Slide mockup

Notes

Data Collection and Analysis

The Role of Big Data

- Big data and analytics tracking has significantly changed the day to day operations of cybersecurity for both small and large organizations alike.
- A broad agreement on the ability of Big Data to eventually overtake segmented and older research based approaches.
- Requires developing a combined blend of multiple approaches, the limitations of Big Data creates some additional debate about the next steps, best use, and cost effectiveness of data tracking using these progressive tools.

Narration

Big Data is a term used to describe the large amount of data in the networked, and information-driven world. The growth of data is outpacing scientific and technological advances in data analytics. Opportunities exist with Big Data to address the volume, velocity and variety of data through new scalable architectures. To advance progress in Big Data, the NIST Big Data Public Working Group (NBD-PWG) is working to develop consensus on important, fundamental concepts related to Big Data.

Slide mockup

Notes

Data Collection and Analysis

Examples of Machine Learning

Narration

The marketplace for advanced analytics tools in the cybersecurity field today has created competition for individual consumers as well as small and large business owners. Standards such as reliable uptime, consistent reporting, and advanced analytics have become required tools for anyone looking to invest in these types of programs.

Slide mockup

Notes

Data Collection and Analysis

Man and Machine

Overall, data management has created the single largest challenge to successful cybersecurity. For example, in 2017, a research team found that the following data was produced:

- 3,607,080 Google search strings
- 186,000,000 emails sent
- 510,000 comments and 293,000 status updates on Facebook

Narration

With the rise of machine learning, the traditional thought becomes that many human cybersecurity analysts (and their jobs) will become obsolete. Within the field of cybersecurity however, experts agree that the best security solutions will be a blend of both human observation, decision making and the reporting power of open source machine learning.

With the sheer number of data entries becoming too vast for human cybersecurity analysts to realistically review, the need for machine learning analysis was easily apparent. Through steps that we will discuss throughout the rest of this lesson, the pattern recognition, anomaly detection, natural language processing, and general predictive analytics creates the reporting necessary for analysts to make quick and informed decisions.

Slide

3 | Data Collection and Analysis

Module 3: Data Analysis Solutions & Strategies for Processing Data Within Organizations

Narration

Welcome to Module 3.

Notes

Slide mockup

Notes

Data Collection and Analysis

Top Ten Keys to Log Analysis and Log Analytics (1/3)

1. Before you begin, determine a strategy for logging data overall. Because the needs for every organization will be different, you can not apply the same structure to every data set. Your solution should include logging methods, tools used, and data hosting locations.
2. Set a structure to your log data. What exactly would you like each report to look like? Even in smaller systems, not designing a format for easy log review could mean that analysts might not even know or understand what they are looking at. Consider log structuring formats like JSON and KVP (Key Value Pair).
3. Keep your analysis and production environments separate. By allowing analysts a clean environment to test and evaluate issues, you do not run the risk of having your live system compromised. Additionally, centralizing your log data but keeping access set to the lowest possible point will ensure that your logs remain intact even in the event of an actual attack on your system.

Narration

Hacking (either as a white-hat or black-hat) is about the gathering and manipulation of information over time. To do that, attackers gather information through the use of log tools and analytics programs.

Slide mockup

Notes

Data Collection and Analysis

Top Ten Keys to Log Analysis and Log Analytics (2/3)

4. Log analysis requires a broad, holistic view in order to be successful. Don't assume that looking at registry or Windows security logs alone will tell the entire story of potential vulnerabilities across your system. Take the time to look into the system infrastructure pieces, including the application layers and end user machines as well. For those who are able to gather information from the perspective of multiple users, issues like network latency, database delays, and slow web page loading times may illustrate a more comprehensive issue than viewing the same issues from only an administrative level.

5. Correlating data sources gets you ahead of potential problems. Tapping into the streams of data that are continuously received (applications, servers, users) allows for more predictive planning against potential threats and vulnerabilities. Using this type of information will often provide solutions that can be implemented before a large number of users are affected.

6. Identifiers help analysts pinpoint problems in the data sets. Regardless of how much data needs to be reviewed daily, using names and keywords for reported issues helps saves money and allows analysts more diagnosing and repair consultation time before the same problem continues to spread across an organization unchecked overall.

Narration

While some tools will provide more information than others, it's clear to see from this video that it just takes one small entry (or backdoor) into someone's machine or data in order to cause some serious and permanent damage to their reputation and identity.

Slide mockup

Notes

Data Collection and Analysis

Top Ten Keys to Log Analysis and Log Analytics (3/3)

7. Log analysis requires a broad, holistic view in order to be successful. Don't assume that looking at registry or Windows security logs alone will tell the entire story of potential vulnerabilities across your system. Take the time to look into the system infrastructure pieces, including the application layers and end user machines as well. For those who are able to gather information from the perspective of multiple users, issues like network latency, database delays, and slow web page loading times may illustrate a more comprehensive issue than viewing the same issues from only an administrative level.

8. Correlating data sources gets you ahead of potential problems. Tapping into the streams of data that are continuously received (applications, servers, users) allows for more predictive planning against potential threats and vulnerabilities. Using this type of information will often provide solutions that can be implemented before a large number of users are affected.

9. Identifiers help analysts pinpoint problems in the data sets. Regardless of how much data needs to be reviewed daily, using names and keywords for reported issues helps saves money and allows analysts more diagnosing and repair consultation time before the same problem continues to spread across an organization unchecked overall.

10. Get your team to buy in. No one can read, interpret, and discern data decisions on their own. Every member of the team needs to be involved, and a proactive security plan put in place to help you stay ahead of potential issues.

Narration

Regardless of whether you attack (hack) someone for good or malicious purposes, the volume of data provided today to both individual and group organized hacking groups can overwhelm pre-existing motives and agendas.

Slide mockup

Notes

Data Collection and Analysis

Understanding Log Analysis

- Log analysis is the evaluation of these records and is used by organizations to help mitigate a variety of risks and meet compliance standards.
- When breaches do occur, the log data serves to help in the identification of an intruder or an instance of malware.
  - Provides an audit trail for tracking which network resources, processes or users were involved in any potential attack.

Narration

Computers, networks, and other related systems generate operations records called "audit trail records" or "logs" that document system activities and any other related or requested actions. Because logs serve both an important system and potentially legal purpose, for those who work in cybersecurity, they are absolutely essential. While the level of work required in interpreting each one will vary, creating a policy where an analyst can immediately identify key log issues will be beneficial to everyone in the long run.

Slide mockup

Notes

Data Collection and Analysis

Use Cases for Log Analysis

The five main reasons for conducting thorough log analysis:

1. Compliance & Audits
2. Response to Data Breaches
3. Troubleshooting Systems & Networks
4. User Behavior
5. Forensics for Official Investigations

Narration

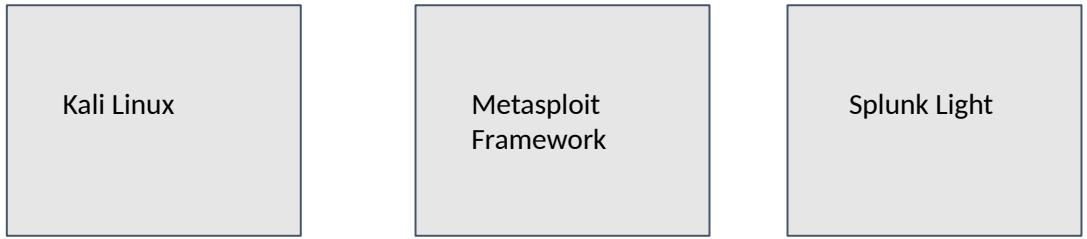
Regardless of what reason motivates an organization to look into its logs, the takeaway here is that being proactive rather than reactive makes the biggest difference in moving past a potentially negative incident. As a leader or CISO, are you reviewing logs regularly, before any issues present themselves, or are you waiting until an incident occurs?

Slide mockup

Notes

Data Collection and Analysis

Popular Log Analysis Software



Narration

While there is virtually no limit to the type of information that can be captured within a log, popular analysis programs specialize in creating dashboards that focus on specific pieces of potential incident data.

Slide mockup

Notes

Data Collection and Analysis

Guide to Predictive Learning (1/2)

> “The time to compromise and exfiltration (how long it takes an attacker to break in and retrieve data from your system) is getting faster and faster. Based on the 2016 numbers, 82% of attackers can compromise your system in minutes and completely extract the data required in less than a week's time."
>
> From the 2016 Data Breach Investigations Report

Narration

In the continual battle between attackers and defenders, the time it takes to process an event and generate the recommended reactive log ultimately defines the success or failure of the attack.

In order to shorten the process, including the reporting and recording time, predictive analytics have pushed log collection past the threshold of collecting digital signatures into capturing data streams across a series of devices and interpreting those signals in order to determine the likelihood of an attack.

Slide mockup

Notes

Data Collection and Analysis

The Future of Log Analytics (2/2)

"The time to compromise and exfiltration (how long it takes an attacker to break in and retrieve data from your system) is getting faster and faster. Based on the 2016 numbers, 82% of attackers can compromise your system in minutes and completely extract the data required in less than a week's time."

From the 2016 Data Breach Investigations Report

Narration

As application systems continue to expand in both size and complexity, creating flexible logging solutions has become a required practice for all organizations. As we learn more about our daily cyber health, additional features and solutions like centralized log capturing and reporting, filtering, and 24/7 real-time alerts are now being pushed to new limits by developer groups in the security and software space. As more operations and development teams roll out these updates, the benefits will begin to quickly outweigh the initial costs.

Slide

4 | Data Collection and Analysis

Module 4: Weapons and Data Analysis

Narration

Welcome to Module 4.

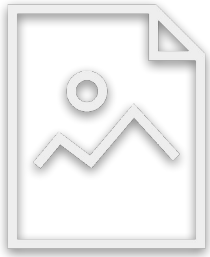
Notes

Slide mockup

Notes

Data Collection and Analysis

Profiling Cyber Attackers



Narration

Although the image of a cyber attacker may vary based on popular films and television shows, the truth behind these individuals is much harder to determine in real life. More often than not, these individuals are funded by foreign military organizations and terrorist groups, which are likely to have the financial backing to hire more hackers to exploit vulnerabilities and attack critical systems. Even with defense and recovery programs in place today with various law enforcement agencies, serious attackers would still not reveal their extent of their activities until it is absolutely necessary.

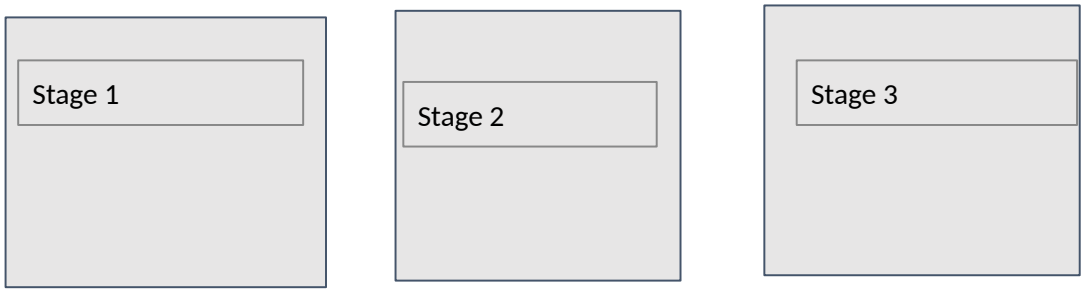
In a recent survey of hackers, responses revealed that 73% of hackers felt that modern security programs that deploy anti-virus and firewalls are either now irrelevant or obsolete. With weak passwords and human error, hackers are able to initiate a targeted cyber attack today easier than ever.

Slide mockup

Notes

Data Collection and Analysis

Cyber Weapon Design



Narration

The range of a cyber weapon is virtually unlimited. Let’s take a look at the three stages of a Cyber weapon design.

Slide mockup

Notes

Data Collection and Analysis

Cyber Arsenal Tools

- Botnets
  - Average size is 5000 computers, some have been as large as 500,000 computers
  - Command and control software allows botnet capacity leasing of subsections of the botnet.
- Phishing
- Targeted Viruses
  - Used to create quick one-time-use botnets.
  - Also used when specifically targeting a single site or organization.
- The usual Internet attack tools.
  - Metasploit, etc.

Narration

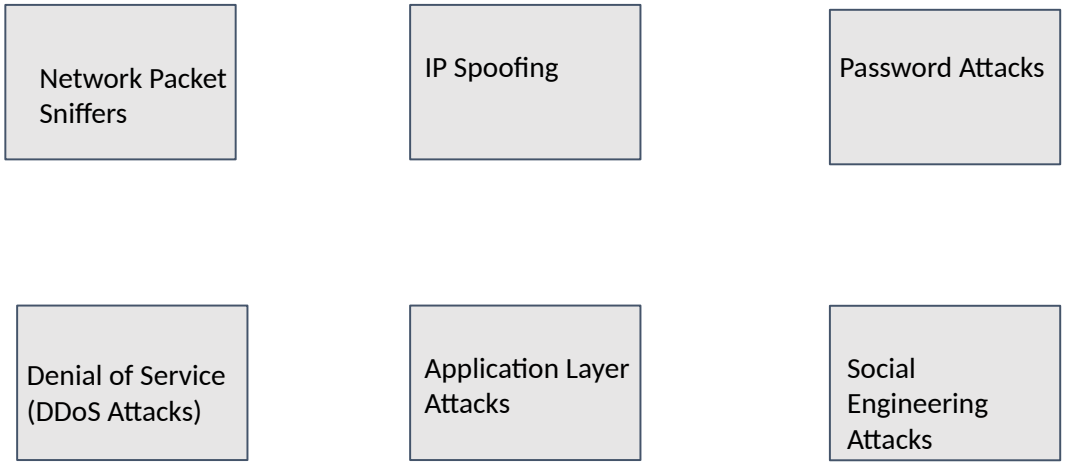
The range of tools in a cyber attackers arsenal will vary, but here are some popular choices among hackers who choose to attack systems.

Slide mockup

Notes

Cyber Incident Response

Common Cyber Attack Methods



Narration

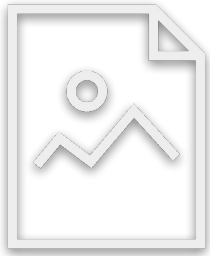
The specific cyber methods used to attack systems and steal personally identifiable data (PII). While most people are aware of these methods, the code to execute these attacks remains available to hackers online; we must all continue to create a defensive plan around our systems, both now and into the future.

Slide mockup

Notes

Data Collection and Analysis

The Rise of the Bots: Working with a Botnet (1/2)



Narration

A robot, or more commonly called a bot, is a piece of highly complex and evolving malicious code that was designed to take control of a user machine without their knowledge or consent. Once discovered by the user, they are still very hard to completely remove from a computer system.

Data Collection and Analysis

The Eight Stages of a Botnet Attack (2/2)

1. The bot master sends malicious Trojan/botnet client over the Internet and infects a victim.
2. The bot client connects to the command center (malicious server) and informs the status of being infected.
3. Command center informs the bot master about the victim.
4. The attacker send attack information to the command center.
5. The command center triggers the victim with the set of instructions sent by the bot master to search for other victim computers with similar vulnerabilities.
6. The compromised computer scans the Internet for other similar systems and infects them with malicious code.
7. This way the attacker creates a huge network of bots that are ready to act based on the instructions sent by the attacker.
8. Bot masters sell access to sections of the botnet as timeshares to bidders online.

Narration

Although the original bots were IRC (Internet Relay Chat) based, the bots used today will vary based on the target of the attack. With the ability to cross-infect thousands of new computers, any new vulnerability in a new system can increase that number by adding thousands of new bots, which in turn will inflict more damage and create more bots over time.

Slide mockup

Notes

Data Collection and Analysis

Proactive Protection Against Botnets

> “The danger of disruptive and even destructive cyber-attack is growing, and the risk of another global economic slowdown remains. The international community’s ability to respond effectively to these and other risks is helped or hindered by the behaviors of major powers. Where progress has been most profound, it is due to the steadfastness of our allies and the cooperation of other emerging powers.”
>
> Former President Barack Obama

Narration

While everyone is at risk in being infected by potential botnets, there continues to be some confusion behind how important it is to actively protect yourself when working online. With our increasing dependence on network infrastructure and the Internet combined with a general lack of understanding and funding for adequate network security tools, the ease of executing a cyber attack remains very likely. Additionally, the difficulty in tracking cyber activity across geographic lines, such as countries and continents, creates more confusion into what happens next after an attack is carried out.

Slide 45

5 | Data Collection and Analysis

Module 5: Using Windows Tools & Best-Practices

Narration

Welcome to Module 5.

Notes

Slide mockup

Notes

Data Collection and Analysis

What is NMAP? (1/3)

Nmap uses raw IP packets in novel ways to determine the following:

- What hosts are available on the network.
- What services (application name and version) those hosts are offering.
- What operating systems (and OS versions) they are running.
- What type of packet filters/firewalls are in use.

Narration

Nmap is short for Network mapper. A open source tool for network exploration and security auditing and was designed to rapidly scan large networks, although it works fine against single hosts.

Slide mockup

Notes

Data Collection and Analysis

Why do we use NMAP? (2/3)

- Network inventory.
- Managing service upgrade schedules.
- Monitoring host or service uptime.

Narration

Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks.

Slide mockup

Notes

Data Collection and Analysis

What do you do with its results?

- Proactively to identify and correct security holes.
- Reconcile found assets with network diagrams.
- Starting place for other types of scans, such as Retina or Nessus.

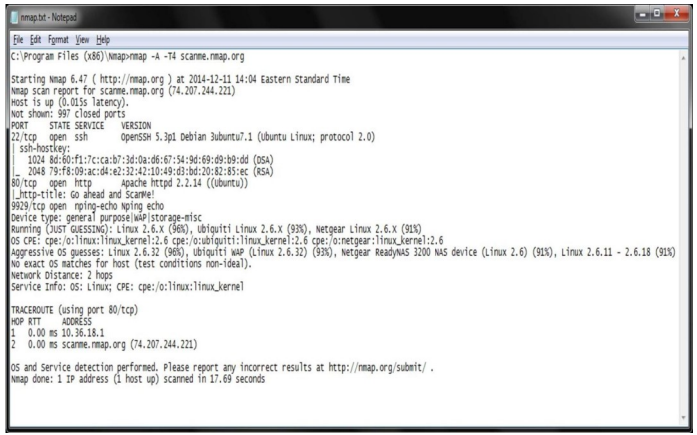
Narration

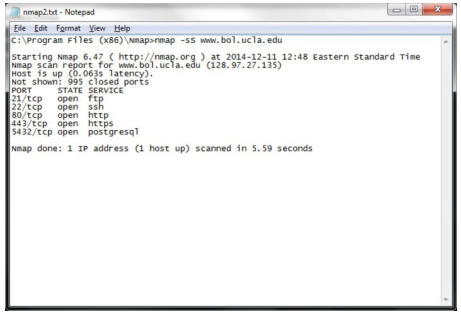
Slide mockup

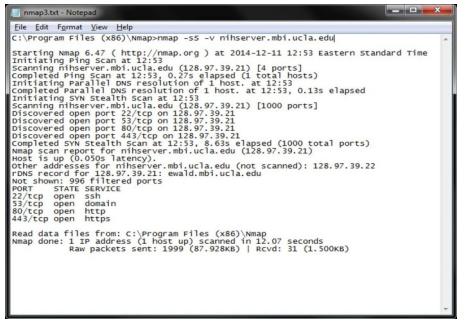
Notes

Data Collection and Analysis

NMAP Examples







Narration

Slide

6 | Data Collection and Analysis

Module 6: Challenges of Secure Data Management

Narration

Welcome to Module 6.

Notes

Slide mockup

Notes

Data Collection and Analysis

Gathering Information

Public records
- WHOIS: information about owner
- DNS : information about IP addresses

Search engines
- Google hacking
- Cache all information gathered
- Tweaking provides additional information

Various websites
- Robtex.com, DNSstuff.com, iptools.com, samspade.org, etc…
- Combine above techniques
- Sort results for nice presentation

Advanced and Automated Scanning
- Specialized (offline) Tools – Kali Linux

Narration

The art of conducting reconnaissance (or footprinting) means determining everything you can about a target (e.g. company, network, system, person) through technical or nontechnical means. In general, hacker's footprint to identify potential targets and identify types of attacks that may be successful against those targets. By comparison, security professionals footprint to determine what information the organization is giving away and what weaknesses are apparent. Overall, the collecting of bits and pieces of information (by both parties) from multiple sources creates a larger picture that can be exploited for specific reasons if desired.

Slide mockup

Notes

Data Collection and Analysis

DNS Lookups

DNS = Domain Name Service

DNS is the utility within the Internet that maps human-readable website names to IP addresses.

DNS is considered to be at either the Application or Network layer.

Since the Internet is huge, its governance and mapping occurs on an international scale.

Narration

Slide mockup

Notes

Data Collection and Analysis

Additional Concepts & Terms - Regional Internet Registries (RIRs) (1/3)

Registry	Geographic Region
AFRINIC	Africa, portions of the Indian Ocean
APNIC	Portions of Asia, portions of Oceania
ARIN	Canada, many Caribbean and North Atlantic islands, and the United States
LACNIC	Latin America, portions of the Caribbean
RIPE NCC	Europe, the Middle East, Central Asia

Narration

Regional Internet Registries (RIRs) are nonprofit corporations that administer and register Internet Protocol (IP) address space and Autonomous System (AS) numbers within a defined region.

Slide mockup

Notes

Data Collection and Analysis

Additional Concepts & Terms - Domain Information Groper (DIG) (1/3)

- Unless specified otherwise, dig will try each server listed in /etc/resolv.conf
- When no options are given, dig performs an NS query for "." (root). Dig defaults to IPv4 lookups.
- Syntax: dig @server name type

Narration

DiG is used to look up the DNS name servers of a domain. Previous utilities that have been deprecated: nslookup and host. Dig is a part of the BIND DNS suite for *nix.

Slide mockup

Notes

Data Collection and Analysis

Additional Concepts & Terms - Traceroute (1/3)

- *nix Command: traceroute www.example.com
- Windows Command: tracert www.example.com

Narration

Traceroute allows users to discover all of the hops taken between a host and target machine.

Slide mockup

Notes

Data Collection and Analysis

Scanning and Enumeration (1/2)

Three Major Types of Scanning

- Port Scanning: determines open TCP/IP ports and services running on a system.
- Network Scanning: identifies IPs on a given network or subnet.
- Vulnerability Scanning: discovers presence of known weaknesses on a system.

Narration

Scanning is the process of detecting live or responding systems on the network. Scanning is conducted after the information gathering, footprinting and reconnaissance stages. Enumeration occurs next and is the process of gathering user names, host or device names, and applications. It involves actively querying or connecting to a target system to acquire these pieces of information.

Slide mockup

Notes

Data Collection and Analysis

Scanning Methodology (2/2)

1. Check for Live Systems
2. Check for Open Ports
3. Service Identification
4. Banner Grabbing/OS Fingerprinting
5. Vulnerability Scanning

Narration

The general steps used when scanning for systems on the network.

Slide mockup

Notes

Data Collection and Analysis

Port Numbers and Ranges

- Well-known (System) ports: 0 to 1023
- Registered (User) ports: 1024 to 49,151
- Dynamic, private, or ephemeral (unassigned) ports: 49,152 to 65,535

Protocol Names	Port Number
FTP data transfer	20
FTP control (command)	21
SSH	22
Telnet	23
SMTP	25
DNS	53
DHCP	68
HTTP	80, 8080
POP3	110
NetBIOS	137, 138, 139
SNMP	161
SSL	443

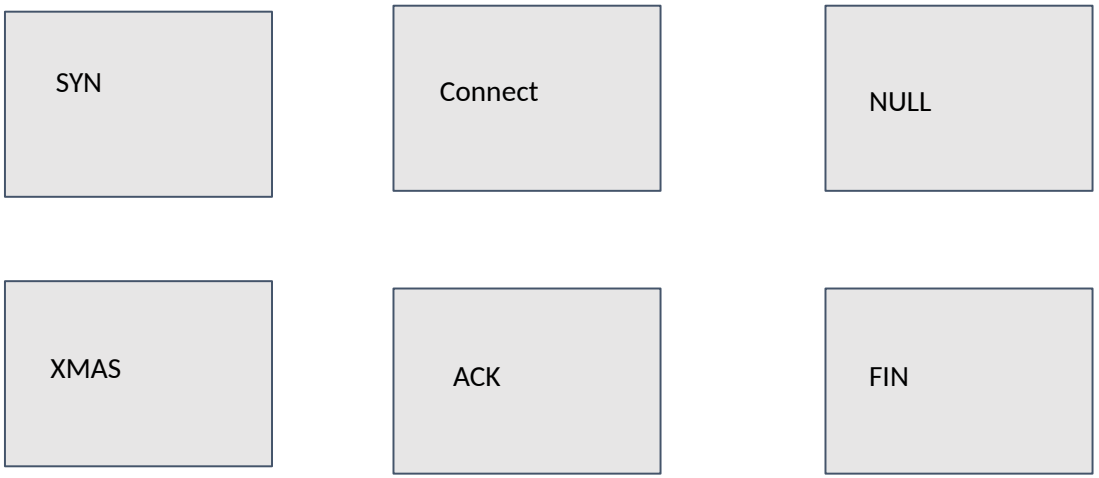
Narration

Slide mockup

Notes

Data Collection and Analysis

Port Scan Types- TCP



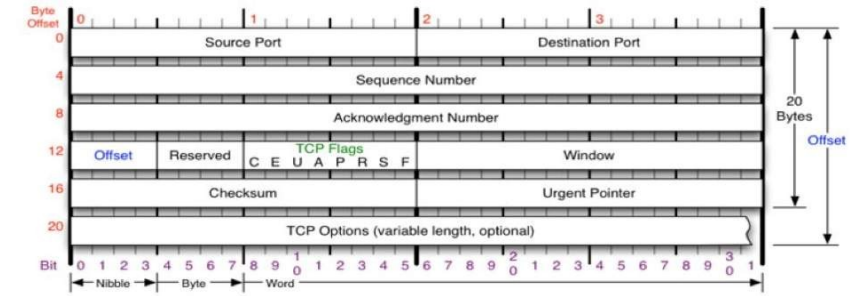
Narration

Slide mockup

Notes

Data Collection and Analysis

TCP Packet Format



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Narration

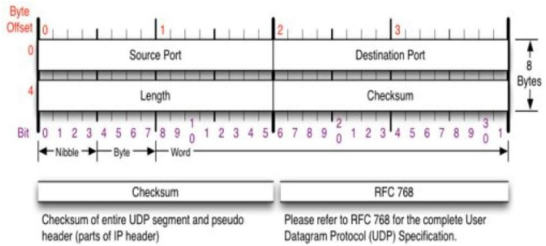
Slide mockup

Notes

Data Collection and Analysis

Port Scan Types - UDP

- Connectionless protocol
- Faster but less reliable than TCP
- UDP packet is sent to target
- If the response is ICMP “Port Unreachable,” the port is closed
  - A lack of response means the port may or may not be open, depending on whether a firewall or other packet filtering device is in place
- Port Return Options
  - Open
  - Closed
  - Filtered
    - False positives and negatives



Narration

Slide mockup

Notes

Data Collection and Analysis

Scanning Countermeasures

- Filter inbound ICMP message types at network border.
- Filter outbound ICMP type 3 at network border.
- Configure firewalls to identify port scan and throttle the connection.
- Configure firewall and IDS to properly handle fragmented packets
- Test router and firewall configurations for bypassing source routing techniques.
- Patch!
- Be aware of network configuration and “normal” traffic.

Narration

Slide mockup

Notes

Data Collection and Analysis

Enumeration & Tools (1/2)

- The process of gathering and compiling:
  - Usernames, Groups and Machine names
  - Username passwords and login times
  - Network Resources or Shares
- Requires an active connection to the target; more intrusive than scanning
- Helps the attacker determine what vulnerabilities may be exploited or the assessor determine what to mitigate

Narration

Once your scanning is complete the next stage is Enumeration.

Slide mockup

Notes

Data Collection and Analysis

Enumeration & Tools- Banner Grabbing (2/2)

- Sending an unsolicited request to an open port to see what, if any, default error message (banner) is returned.
- SNMP can also be used to enumerate user accounts on target systems.

Narration

A common method is using Telnet aimed at a specific port. Many enumeration tools establish a NetBIOS null session to gather information. Unauthenticated connection to a Windows computer without using a logon and password value. Enumerations can be performed using tools built in to Windows or others such as, DumpSec, Hyena, Nessus, Enum, SNMPUtil, onesixtyone, and SNScan. Enumeration of *nix systems can be done with built-in UNIX utilities, such as the finger command, others such as Nessus

Slide mockup

Notes

Data Collection and Analysis

Simple Network Management Protocol

- Client-server application that uses port 161.
- Uses the Management Information Base (MIB) for data.
- Versions 1 and 2 use community strings to protect data.
  - Defaults: public, private
- Version 3 adds encryption
- Can list information about hardware, software, version numbers, network information.

Narration

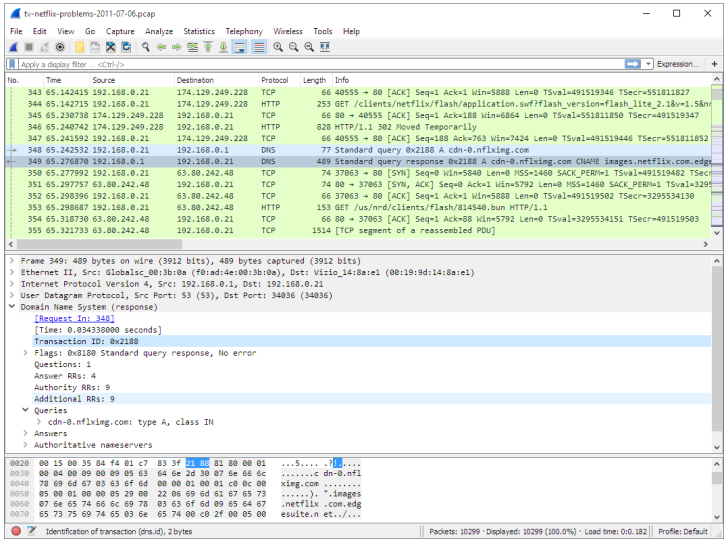
Simple network management Protocol is designed for network administrators to monitor network attached devices.

Slide mockup

Notes

Data Collection and Analysis

Getting Started with Wireshark



Narration

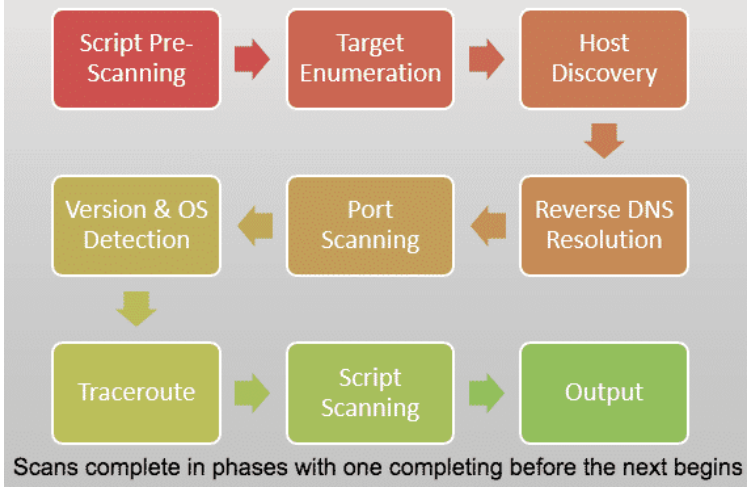
Wireshark is the top network protocol analyzer and is free under the GNU General Public License. It provides deep packet inspection across virtually all major protocols, and can be used for live capture or offline for analysis. The terminal version of the program is called TShark. Here are other threat analysis tools or site, SAINT and sectools.org

Slide mockup

Notes

Data Collection and Analysis

NMAP Network Mapper



Narration

Free and open source utility for network discovery and security auditing. Which uses IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running and used to audit the security and network connections of the devices within the certification boundary. Will identify and validate all systems to be tested and their open ports, network communications, and protocols

Slide mockup

Notes

Data Collection and Analysis

Working with NMAP Syntax

The general syntax used when working with NMAP commands looks like this: nmap [scan type…] [options] {target specification}

Some common syntax commands include:

-sS: TCP SYN scan;-sT: Connect() scan; -sA: ACK scan; -sW: Window scan; -sM: Maimon scan; -sU: UDP scan;-sN: TCP Null scan; -sF: FIN scan; -sX: Xmas scan; -sI <zombie host{:probeport]>: Idle scan-; sY: SCTP INIT scan; -sZ: COOKIE-ECHO scan; -s0: IP protocol scan; -b <FTP relay host>: FTP bounce scan;--scanflags <flags>: Customize TCP scan flags

Narration

Slide mockup

Notes

Data Collection and Analysis

NMAP Syntax: Selected Options (1/3)

Host Discovery

- -sL: List scan (lists targets to scan)
- -sn: Ping scan (Disable port scan)
- --traceroute: Trace hop path to each host

Port Specification

- -p <port ranges>: Only scan specific ports
- -p22 only scans port #22
- -p U:53,11,T:21-8080 scans UDP ports #53 & 11, TCP 21 through 8080

Scan Order and Speed

- -F: Fast mode – scans fewer ports than default
- -r: Scan ports consecutively (don't randomize)
- --top-ports <number>: Scan <number> most common ports

Narration

The lists provides a brief overview into selected NMAP commands, organized by specific objectives and goals needed for scans across a system.

Slide mockup

Notes

Data Collection and Analysis

NMAP Syntax: Selected Options (2/3)

Service/Version Detection

- -sV: Probe open ports to determine service/version info
- OS Detection
- -O: Enable OS detection

Timing and Performance

- Options for <time>: ms, s, m, & h
- -T<0-5>: Set timing template (higher = faster)

Firewall/IDS Evasion and Spoofing

- -f; --mtu <val>: fragment packets (optionally with given MTU)
- -S <IP_address>: Spoof source address
- -g/--source-port <portnum>: Use given port number
- --data-length <num>: Append random data to sent packets
- --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address

Narration

Slide mockup

Notes

Data Collection and Analysis

NMAP Syntax: Selected Options (3/3)

- Output
  - -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename
  - -v: Increase verbosity level (use –vv or more for greater effect)
  - --reason: display the reason the port is in a particular state
  - --open: only show open (or possibly open) ports
- -6: Enable IPv6 scanning
- -A: Enable OS detection, version detection, script scanning, and traceroute
- --datadir <dirname>: Specify custom Nmap data file location
- -h: Print Nmap help summary page

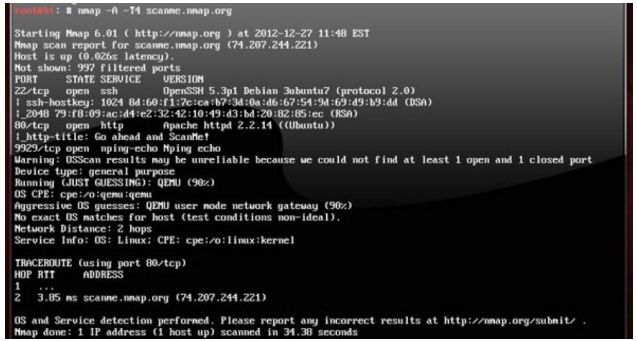
Narration

Slide mockup

Notes

NMAP Syntax: Target Specification

- Can pass: Hostnames, IP addresses, networks, etc.
- Examples: scanme.nmap.org, microsoft.com/24, 192.168.0.1, 10.0.0-255.1-254
- -iL <inputfilename>: Input from list of hosts/networks
- -iR <num hosts>: Choose random targets
- --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
- --excludefile <exclude_file>: Exclude list from file



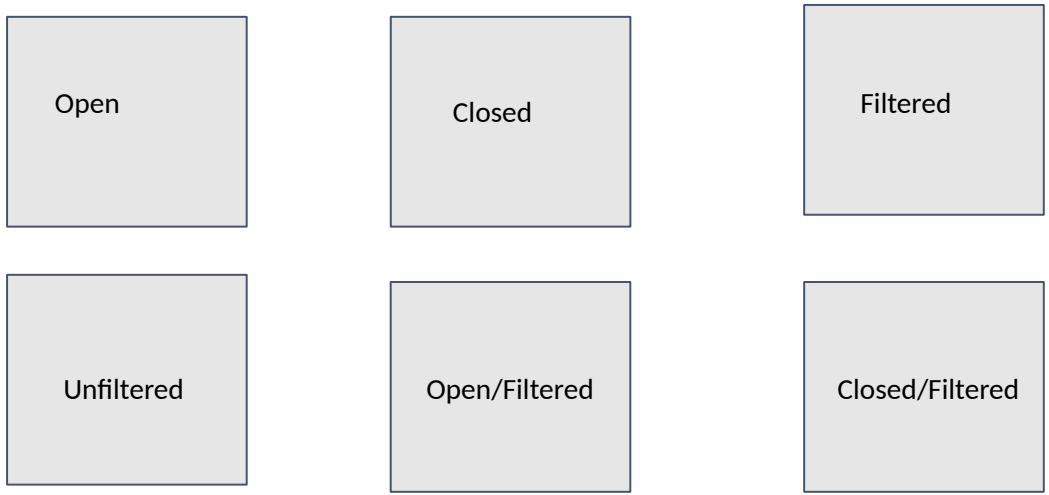
Narration

Slide mockup

Notes

Data Collection and Analysis

Understanding Port States



Narration

Slide mockup

Notes

Data Collection and Analysis

Footprinting/Info Gathering Countermeasures

1. Limit access by allowing search engines only to see what they need to see. Make sure unauthorized users are not able to look into or even see files they do not need to see. Force possible intruders to use methods that can be scanned and monitored.
2. Use the tools of hackers by scanning your systems with the tools hackers use and check the information that is found. Scan for error messages and other things that reveal information about the system and services and remove them.
3. Be aware of all possible sources of information. Create awareness among employees. Assume all information will possibly be abused by cleaning documents and removing all metadata from documents before publishing. Be sure to always audit frequently, which will keep your knowledge up-to-date and scan regularly for information that can be found about your systems or hire professionals do to it for you.

Narration

Slide

7 | Data Collection and Analysis

Final Assessment

Notes

Narration

Welcome to the final assessment. Please familiarize yourself with the instructions and pass requirements.

Slide mockup

Data Collection and Analysis

Assessment

Notes

Narration