innovate achieve lead

BITS Pilani

Pilani Campus

CC ZG503: Network Fundamentals for Cloud

Lecture No. 15 : Cloud Network Security (Contd.)

RECAP: Defence In Depth

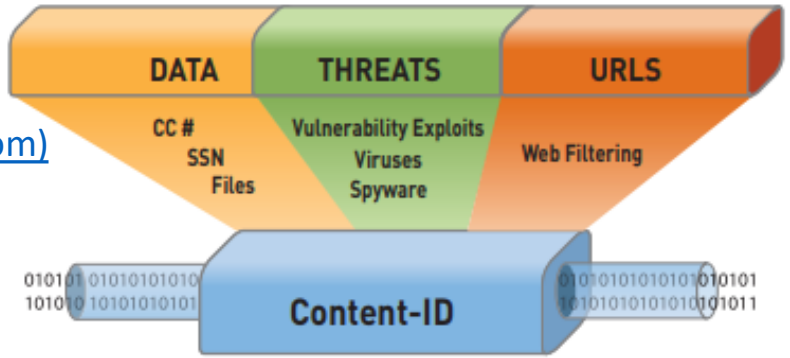
- When developing an enterprise security strategy, a layered approach is the best method to ensure detection and mitigation of attacks at each tier of the network infrastructure
  - *"Defence in depth is a **military strategy** that seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defence in depth relies on the tendency of an attack to lose momentum over time or as it covers a larger area."* Source: Wikipedia
- Although the enterprise network perimeter is changing, the basic network security mechanisms still have their purpose
  - the same types of security mechanisms need to persist, however, where they are implemented may change slightly depending upon the network architecture
- In general, we will not focus much on where the network perimeter is, but on what needs to be protected

RECAP: Next Generation Firewalls

- Standard firewalls simply check for the policy allowing the source IP, destination IP, and TCP/UDP port, without a further deep packet analysis
- Next Generation Firewalls (NGFW) perform more deep packet analysis to mitigate malicious traffic masquerading as legitimate
  - Example: DNS traffic inspected by a standard firewall may look legitimate, but in reality, the DNS packets may be padded with data that is being ex-filtrated from the network
- An NGFW can inspect traffic for data, threats, and web traffic

Content_ID_tech.pdf (paloaltonetworks.com)

Palo Alto
etworks - Contentl



RECAP: IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
  - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
  - this has been abandoned at the network perimeter when a breach is undesirable
  - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
  - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
  - Many IPS devices have purposefully built denial of service mitigation technology
  - can be deployed at the network perimeter
  - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
  - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism

RECAP: Securing Network Services (NS)

- Enterprises provide and leverage Internet services such as DNS, e-mail, and file transfer
  - The latest malware threats utilize these common services in order to redirect internal hosts to Internet destinations under the control of the malware writers
  - However, with correctly implemented architecture, this scenario would mostly be a mute point, and with additional security mechanisms, a rare occurrence

RECAP: Network Segmentation

- Even with the most sophisticated security mechanisms, without network segmentation, their value will be greatly undermined
- Internal segmentation is often overlooked, but is extremely important to prevent spread of malware throughout the enterprise
  - advanced threats are introduced through infected consultant systems, unauthorized introduction of personal devices and business-critical applications

innovate achieve lead

BITS Pilani

Pilani Campus

Case Study: Platform Security Features in Microsoft Azure

innovate achieve lead

BITS Pilani

Pilani Campus

Extra Reading: Can ZTNA replace your VPN?

PDF

ZTNA vs VPN

innovate achieve lead

BITS Pilani

Pilani Campus

Cyber Forensics: Cloud (Network) Forensics

References:

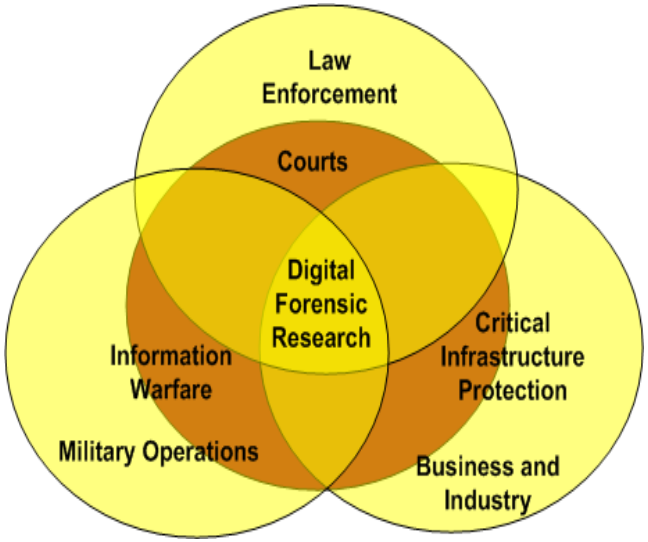
- https://www.infosecurity-magazine.com/opinions/cloud-complicates-digital-crime/
- https://blog.eccouncil.org/cloud-forensics-is-it-important-to-your-cybersecurity-plan/

What is Cyber Forensics….

- "…. is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law."

Source: What is Computer Forensics (Cyber Forensics)? https://searchsecurity.techtarget.com ›

Digital Forensic Science



Source: Cyber Forensics by Eric Katz

Table 1 - Suitability Guidelines for Digital Forensic Research

Area	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution		After the fact
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business & Industry	Availability of Service	Prosecution	Real Time

History of Cyber Forensics

Computer Forensics

- Focused on computing devices
- Requires understanding of Boot Process, File Systems, Registry / Configuration Files, OS Functions etc.
- Static and Live Acquisition of Data

Network Forensics

- Systematic tracking of incoming and outgoing traffic to ascertain how an attack was carried out
- Determine the cause of abnormal traffic (internal bug, attackers)
- Live acquisitions are especially useful

Data Storage Devices

- Requires understanding of data storage devices for data acquisition
- SCSI Disks, IDE/EIDE Disks, SATA Drives
- CD, CD-R, CD-RW, DVD
- RAID Systems (RAID 0, 1, 2, 3, 4, 5, 6, 10)

Evolution of Cyber Forensics

Mobile Device Forensics

- A wealth of information on cell phones/ Smart Phones
- Crimes targeting Mobile Devices
- Requires understanding of Mobile Device Organization, OS, File System and Storage system

Cloud Forensics

- Combines cloud computing with digital forensics
- Requires investigators to work with multiple computing assets, such as virtual and physical servers, networks, storage devices, applications, and much more

IoT Forensics

- IoT is a combination of many technology zones: Device, Network and Cloud
- IoT Forensics thus covers: Cloud forensics, Network forensics and Device forensics.
- Evidence could be from home appliances, cars, tags readers, sensor nodes, medical implants in humans or animals, or other IoT devices

Cloud Forensics Overview

- Cloud forensics combines the realities of cloud computing with digital forensics, which focuses on collecting media from a cloud environment.
- This requires investigators to work with multiple computing assets, such as virtual and physical servers, virtual and physical networks, storage devices, applications, and much more.
- For most of these situations, the cloud environment will remain live and capable of change.
- Despite this wide array of different assets and jurisdiction challenges, the end result must stay the same: evidence must be presented in a court of law.

Source: https://www.infosecurity-magazine.com/opinions/cloud-complicates-digital-crime/

Thank You!