HyperionDev

Welcome to this session: Introduction to Network Forensics

The session will start shortly...

Questions? Drop them in the chat.
We'll have dedicated moderators answering questions.

HyperionDev

What is Safeguarding?

Safeguarding refers to actions and measures aimed at protecting the human rights of adults, particularly vulnerable individuals, from abuse, neglect, and harm.

To report a safeguarding concern reach out to us via email:

safeguarding@hyperiondev.com

HyperionDev

Live Lecture Housekeeping:

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
- No question is daft or silly - ask them!
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- To report a safeguarding concern reach out to us via email: safeguarding@hyperiondev.com
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

HyperionDev

Lecture Overview

- Network forensics

Learning Outcomes

- Define network forensics
- Explain its importance in cybersecurity
- Identify different tools used for network forensics.

Polls

Please have a look at the poll notification and select an option.

Which phase of network forensics involves analyzing logs and correlating events?

A. Packet Capture
B. Log Analysis
C. Traffic Analysis
D. Intrusion Detection

Polls

Please have a look at the poll notification and select an option.

Which of the following is an example of a human risk in cybersecurity?

A. Using encryption
B. Sending more traffic
C. Deleting all logs
D. Turning off their computers

HyperionDev

Network Forensics

You’re a cybersecurity analyst, and your company’s network has been acting strangely. Files are disappearing, systems are slowing down, and no one knows why. Your boss turns to you and says, “We need to figure out what’s going on, fast.

HyperionDev

Network Forensics

- **Definition:** The capture, recording, and analysis of network events to discover the source of security incidents.
- **Comparison with Digital Forensics:**
  - **Digital Forensics:** Focuses on devices (e.g., hard drives, phones).
  - **Network Forensics:** Focuses on network traffic and communication.

HyperionDev

Network Forensics Importance

- **Incident Response:** Helps identify the root cause of breaches.
- **Detecting Threats:** Uncovers data breaches, insider threats, and malware.
- **Legal & Compliance:** Provides evidence for investigations and meets regulatory requirements.

HyperionDev

Types of Network Attacks Investigated

- **Unauthorized Access:** Hackers gaining access to restricted systems.
- **Denial-of-Service (DoS):** Overwhelming a network to disrupt services.
- **Data Exfiltration:** Stealing sensitive data from the network.
- **Malware Propagation:** Spreading malicious software across systems.

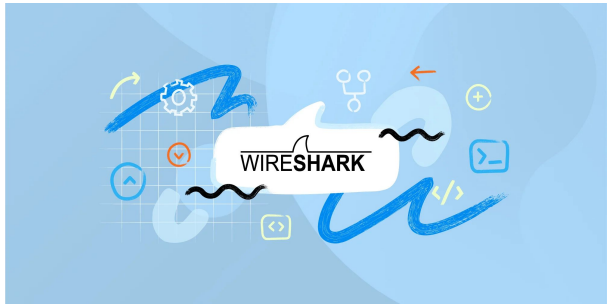
HyperionDev

Let’s take a break

HyperionDev

Tools and Techniques Overview

- **Packet Capture & Analysis:** Wireshark, tcpdump.
- **Log Analysis:** Firewall, IDS/IPS, system logs.
- **Intrusion Detection/Prevention:** Snort, Suricata.
- **Traffic Analysis:** NetFlow, Zeek (Bro).

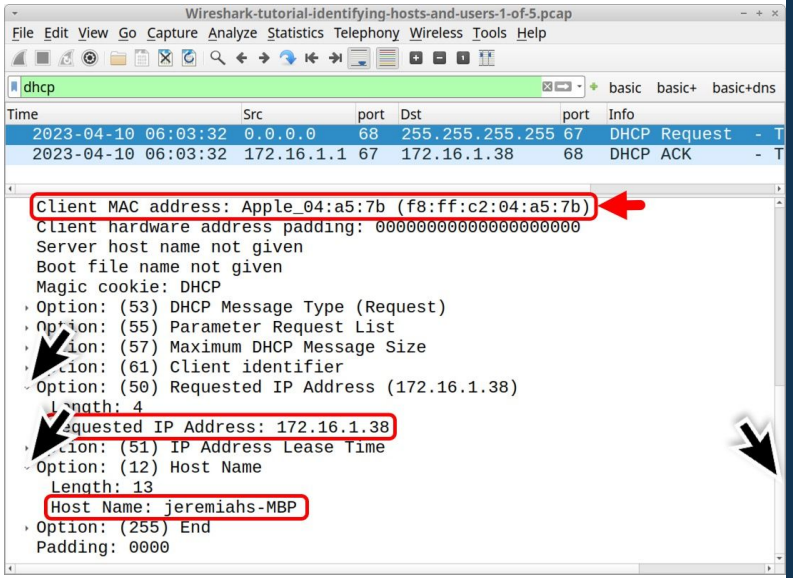


HyperionDev

Packet Capture and Analysis

Tools: Wireshark, tcpdump.

Use Case: Analyzing suspicious traffic patterns or identifying malicious payloads.

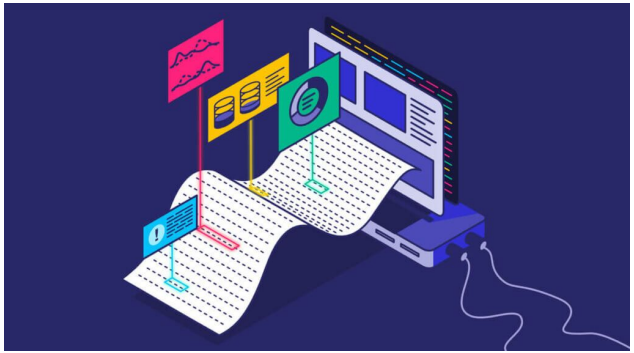


HyperionDev

Log Analysis

Types of Logs: Firewall, IDS/IPS, system logs.

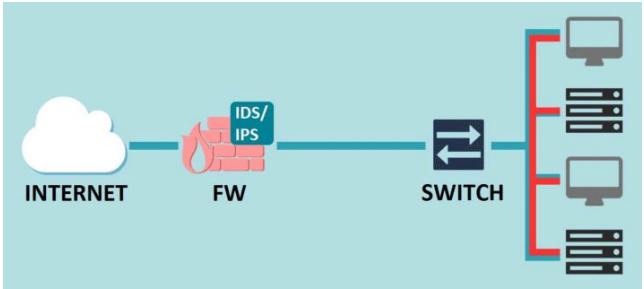
Use Case: Correlating events to trace an attacker's steps.



HyperionDev

IDS and IPS

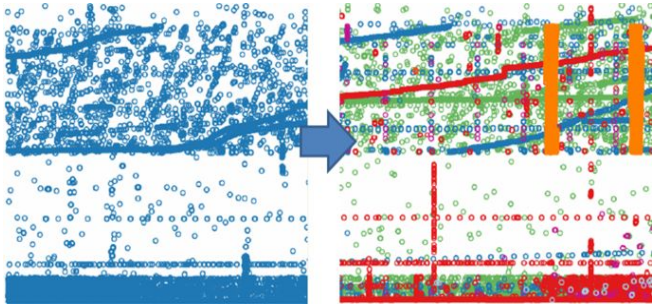
- **Tools:** Snort, Suricata.
- **Use Case:** Detecting and blocking malicious traffic in real-time.



HyperionDev

Network Traffic Analysis

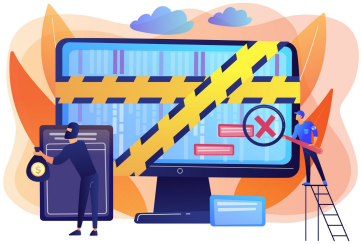
- **Tools:** NetFlow, Zeek (Bro).
- **Use Case:** Monitoring traffic patterns to identify anomalies.



HyperionDev

Challenges in Network Forensics

- **Encryption & VPNs:** Makes it harder to analyze traffic.
- **Data Overload:** Filtering relevant data from massive logs.
- **Evasion Techniques:** Attackers hide their tracks using advanced methods.
- **Legal & Ethical Issues:** Handling sensitive data responsibly.



HyperionDev

Wrap Up

Key Takeaways:

- **Network forensics is critical for incident response.**
- **Use the right tools for packet capture, log analysis, and traffic monitoring.**
- **Overcome challenges like encryption and data overload with smart strategies.**

HyperionDev

Polls

Please have a look at the poll notification and select an option.

Which of the following is a best practice for handling sensitive data during a network forensics investigation?

A. Share findings publicly
B. Ignore legal guidelines
C. Document everything and follow compliance rules
D. Delete evidence after analysis

HyperionDev

Polls

Please have a look at the poll notification and select an option.

What is the purpose of using tools like Snort or Suricata in network forensics?

A. To create network diagrams
B. To detect and prevent intrusions in real-time
C. To encrypt network traffic
D. To delete malicious files

HyperionDev

Q & A SECTION

Please use this time to ask any questions relating to the topic, should you have any.


Thank you
for attending
HyperionDev