Advanced Network Security

Network Forensics

Dr. Yaeghoobi
PhD. Computer Science & Engineering, Networking, India
dr.yaeghoobi@gmail.com

00 Introduction

01 Security Analytics

02 Log File as Evidence

03 Data Recovery

04 Evidence Collection and Preservation

Introduction 00

Painful Story

Online Gaming Company in Chaos

Need for Network Forensics

Informed we may be the victim of a breach

Had no way to confirm or deny…

Concerns about brand and reputational impact…

Urgent, high-priority project spun up…

People and big $ thrown at the problem…

“Why can’t you prove if this happened or not”…

Digital Forensics

- Digital forensics is about the investigation of crime including using digital/computer methods
  - تست علمی/قانونی دیجیتال در مورد تحقیقات درباره جرم، از جمله استفاده از روشهای دیجیتالی / رایانه ای است
- Digital evidence may be used to analyze cyber crime (e.g. Worms and virus), physical crime (e.g., homicide) or crime committed through the use of computers (e.g., child pornography)
- شواهد دیجیتالی ممکن است برای تجزیه و تحلیل جرم سایبری (به عنوان مثال کرم ها و ویروس)، جرم بدنی (به عنوان مثال ، خودکشی) یا جرمی مرتکب شده از طریق استفاده از رایانه ها (به عنوان مثال ، پورنوگرافی کودک) استفاده شود.

“Digital forensics, also known as computer forensics, involved the preservation, identification, extraction, and documentation of computer evidence stored as data or magnetically encoded information”
by John Vacca

تست علمی/قانونی دیجیتال به عنوان روشهای علمی رایانه نیز شناخته می شود، شامل حفظ، شناسایی، استخراج و مستندسازی مدارک رایانه ای است که به عنوان داده یا اطلاعات رمزگذاری شده مغناطیسی ذخیره شده است.

Relationship to Intrusion Detection, Firewalls, Honeypots

They all work together with Digital forensics techniques

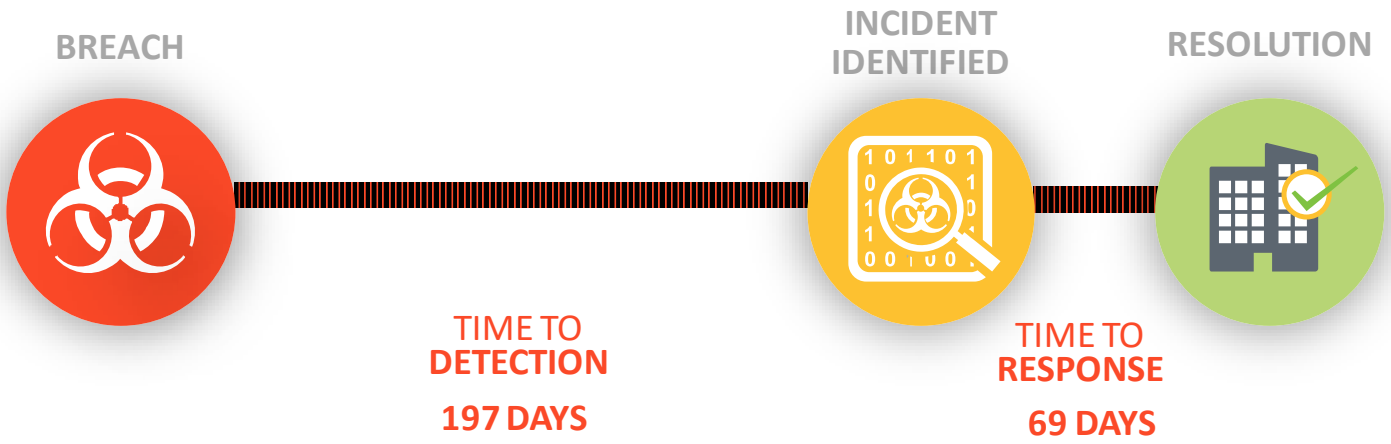
- Intrusion detection
  - Techniques to detect network and host intrusions
- Firewalls
  - Monitors traffic going to and from and organization
- Honeypots
  - Set up to attract the hacker or enemy; Trap
- Digital forensics
  - Once the attack has occurred or crime committed need to **decide who committed the crime**

Computer Crime

- Computers are attacked – Cyber crime
- Computers are used to commit a crime
- Computers are used to solve a crime
  - رایانه ها مورد حمله قرار می گیرند - جرم سایبری
  - از رایانه ها برای ارتکاب جرم استفاده می شود
  - از رایانه ها برای حل یک جرم استفاده می شود
- **FBI's workload**: Recent survey
  - 74% of their efforts on **white collar crimes** such **as healthcare fraud, financial fraud** etc.
  - Remaining 26% of efforts spread across all other areas such as murder and child pornography

The “Average” Enterprise

Cannot Quickly Detect or Accurately Assess Impact of an Incident



- Damage occurring for over six months before detection
- …and is not resolved for over two months after identified

Average Breach Cost - $3.86M

Objective and Priority

Objective

- To **recovery, analyze** and **present computer based material** in such a way that is it **usable as evidence in a court of law**

  - بازیابی، تجزیه و تحلیل و ارائه مطالب مبتنی بر رایانه به گونه ای که به عنوان مدرک در دادگاه قابل استفاده باشد

Priority

- Main priority is with forensics procedures, **rules of evidence and legal processes;** computers are secondary
- Therefore **accuracy is crucial**

  - اولویت اصلی رویه های تست قانونی، شواهد و مراحل قانونی است. رایانه ها ثانویه هستند
  - بنابراین دقت بسیار مهم است

Accuracy vs Speed

- **Tradeoffs between accuracy and speed**
  - Writing a report in a hurry means likely less accurate
- **Accuracy, Integrity** and **Security** of the evidence is crucial
  - No shortcuts, need to maintain high standards
- **Speed may have to be sacrificed for accuracy**.
  - But try to do it as fast as you can provided you do not compromise accuracy

تعادل بین سرعت و دقت

عجله در نوشتن گزارش به معنای دقیق بودن کمتر است

صحت، صداقت و امنیت شواهد بسیار مهم است

بدون میانبر، نیاز به حفظ استانداردهای بالا

ممکن است سرعت بخاطر دقت قربانی شود.

سعی کنید به همان سرعتی که ممکن است انجام دهید به شرط آنکه صحت را پایین‌تر از حد استاندارد نپذیرید.

Security Analytics

01

Job of a Forensics Specialist

- **Determine the systems from which evidence is collected**
- **Protect the systems from which evidence is collected**
- **Discover the files and recover the data**
- **Get the data ready for analysis**
- **Carry out an analysis of the data**
- **Produce a report**
- **Provide expert consultation and/or testimony**

- سیستمهایی را که از آنها شواهد جمع آوری می شود تعیین کنید
- از سیستمهایی که شواهد از آنها جمع می شود ، محافظت کنید
- پرونده ها را کشف کرده و داده ها را بازیابی کنید
- داده ها را برای تجزیه و تحلیل آماده کنید
- تجزیه و تحلیل داده ها را انجام دهید
- گزارش تهیه کنید
- مشاوره و / یا شهادت ارائه دهید

What Net Ops Requires

"Don't complicate our network and don't slow it down!"

Security Analytics

Security Analytics – System of Record

> "At a minimum, organizations should capture 30 days' of packet data. 60 days' worth is even better."

SANS

Records all traffic – 24/7 lossless packet capture (header and payload) – Days/weeks/months

Massive Intelligence – Enriches with Symantec and 3rd party threat and reputation data

Reconstructs All Evidence – Artifacts, flows, files, and activity in human-readable form

Security Analytics doesn't disrupt the Networking/IT department

Incident Response Challenge:

> "Existing tools leave information holes, an incomplete picture, and difficulty in determining the incident source and scope – increasing my time-to-resolution."

Intrusion Process

Enumeration

- Enumeration is the **process of gathering information about a network** that **may help an intruder** attack the network.
- Enumeration فرایند جمع آوری اطلاعات در مورد شبکه است که ممکن است به هکر برای حمله به شبکه کمک کند.
- Enumeration is generally carried out **over the Internet**.
  - **Topology of the network**
  - **List of live hosts**
  - **Network architecture and types of traffic (for example, TCP, UDP, and IPX)**
  - **Potential vulnerabilities in host systems**

Looking for Evidence

Vulnerabilities

- An attacker identifies **potential weaknesses in a system**, **network**, and **elements of the network** and then tries to take advantage of those vulnerabilities.
- The intruder can find known vulnerabilities using various **scanners**.
  - **Viruses**
  - **Trojans**
  - **E-mail infection**
  - **Router attacks**
  - **Password cracking**

Looking for Evidence …

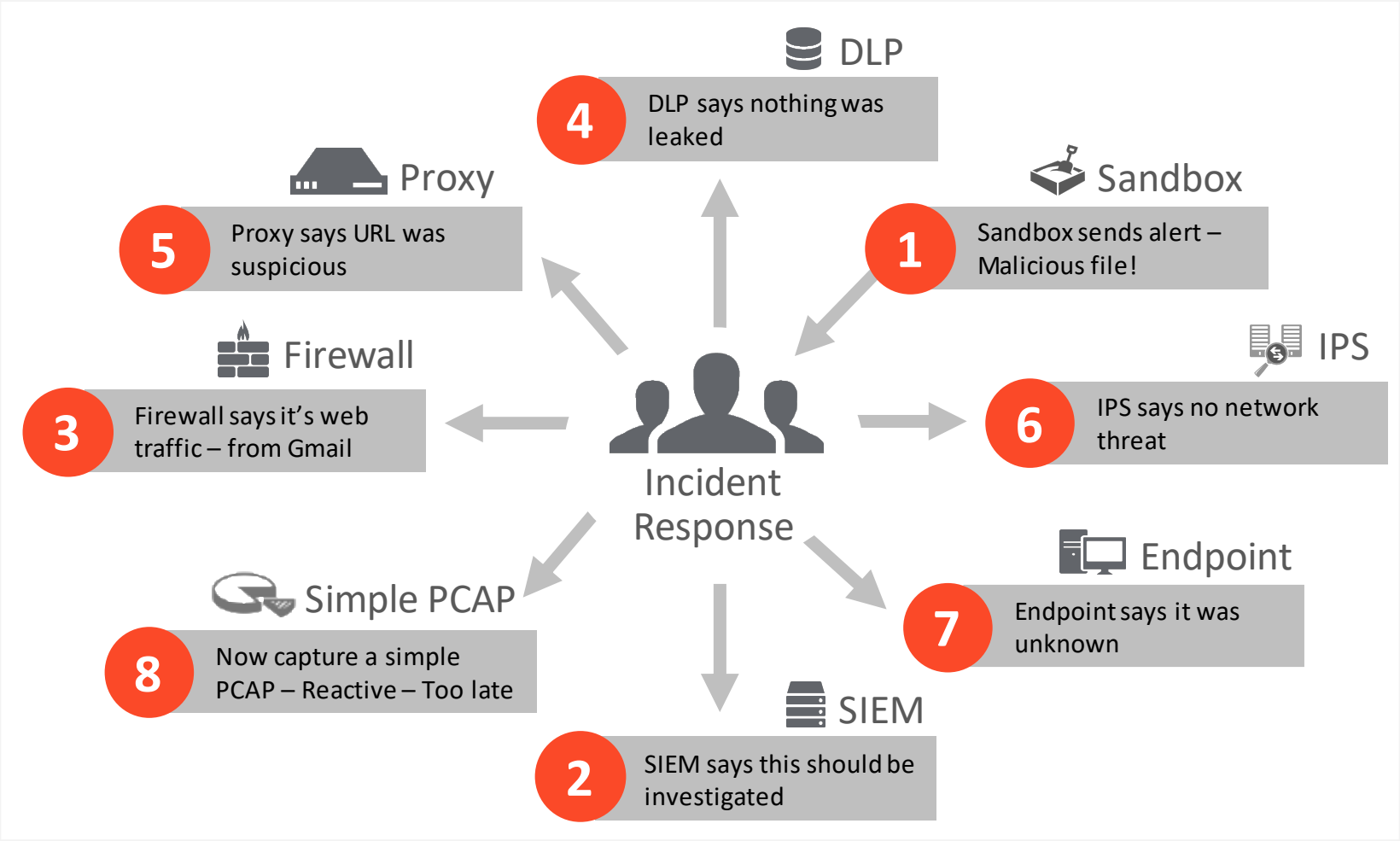
- **From the attack computer and intermediate computers:** This evidence is in the form of **logs, files, ambient data, and tools**.
  - از رایانه حمله کننده و رایانه های واسط: این شواهد به صورت سیاهه‌های مربوط، پرونده ها، داده ها و ابزار است.
- **From firewalls:** An investigator can **look at a firewall's logs.** If the firewall itself was the victim, the investigator treats the firewall like any other device when obtaining evidence.
  - از فایروال‌ها: تحقیق‌کننده می تواند گزارش های مربوط به فایروال را بررسی کند. اگر خود فایروال قربانی باشد، محقق مانند هر وسیله دیگری با فایروال برخورد می کند.

Looking for Evidence …

- **From internetworking devices:** Evidence exists in logs and buffers as available.
  - از دستگاه های بین شبکه‌ای: شواهد موجود در پرونده‌ها و بافرها در دسترس است.
- **From the victim computer:** An investigator can find evidence in **logs, files, ambient data, altered configuration files, remnants of Trojaned files, files that do not match hash sets, tools, Trojans and viruses, stored stolen files, Web defacement remnants, and unknown file extensions.**
  - از رایانه قربانی: محقق می تواند مدارکی را در سیاهه‌های مربوط، پرونده ها، داده ها، پرونده های پیکربندی تغییر یافته، بقایای پرونده های Trojaned، پرونده هایی که با مجموعه هش، ابزارها، Trojanها و ویروس ها مطابقت ندارند، پرونده های دزدیده شده ذخیره شده، بقایای حذف وب و پسوندهای ناشناخته پرونده را پیدا کند .


Working with a fragmented toolset increases workload and delays resolution

Issue: Fragmented Tools and Limited Data



Insufficient for Effective Investigations

Uncertainty

- Multiple disjointed steps and product Interfaces
- No smooth integrated workflow
- No actual evidence and questions go unanswered
- Time-consuming and costly

End-to-End Forensic Investigation

- **The end-to-end concept:** An end-to-end investigation tracks all elements of an attack, including how the attack began, what intermediate devices were used during the attack, and who was attacked.

- تحقیق پایان به پایان، همه عناصر یک حمله، از جمله چگونگی شروع حمله، چه وسایل واسطه ای در طول حمله استفاده می شود، و چه کسی مورد حمله قرار گرفته است را شامل می‌شود.

- **Locating evidence:** Once an investigator knows what devices were used during the attack, he or she can search for evidence on those devices. The investigator can then analyze that evidence to learn more about the attack and the attacker.

- هنگامی که یک محقق می داند در طول حمله از چه وسایلی استفاده شده است، می تواند مدارک را برای آن دستگاه ها جستجو کند. سپس می تواند آن شواهد را تجزیه و تحلیل کند تا اطلاعات بیشتری در مورد حمله و مهاجم کسب کند.

End-to-End Forensic Investigation …

- **Pitfalls of network evidence collection:** Evidence can be lost in a few seconds during log analysis because logs change rapidly. Sometimes, permission is required to obtain evidence from certain sources, such as ISPs. This process can take time, which increases the chances of evidence loss.

- اشکالاتی در جمع آوری شواهد شبکه: شواهد را می توان در طول چند ثانیه در هنگام تجزیه و تحلیل از دست داد زیرا سیاهه‌های مربوط به سرعت تغییر می کنند. بعضی اوقات، برای به دست آوردن شواهد از منابع خاص، مانند ISP، مجوز لازم است. این روند می تواند زمان ببرد، که شانس از دست رفتن شواهد را افزایش می دهد.

End-to-End Forensic Investigation …

- Other pitfalls include the following:
  - An investigator or network administrator may mistake normal computer or network activity for attack activity.
  - There may be gaps in the chain of evidence.
  - Logs may be ambiguous, incomplete, or missing.
  - Since the Internet spans the globe, other nations may be involved in the investigation. This can create legal and political issues for the investigation.

- محقق یا مدیر شبکه ممکن است فعالیتهای رایانه ای یا شبکه ای را به دلیل فعالیت حمله اشتباه کند.
- ممکن است شکافهایی در زنجیره مدارک وجود داشته باشد.
- سیاهه‌ها ممکن است مبهم، ناقص یا مفقود باشند.
- از آنجا که اینترنت در سراسر جهان قرار دارد، ممکن است ملل دیگری نیز در این تحقیقات شرکت کنند. این می تواند مسائل قانونی و سیاسی را برای تحقیقات ایجاد کند.

End-to-End Forensic Investigation …

- **Event analysis:** After an investigator examines all of the information, he or she correlates all of the events and all of the data from the various sources to get the whole picture.

- تجزیه و تحلیل رویداد: بعد از اینکه یک محقق تمام اطلاعات را بررسی می‌کند، برای بدست آوردن کل تصویر، تمام وقایع و کلیه داده های موجود در منابع مختلف را با هم مرتبط می کند.

Smooth Workflow and Resolution

1. Alert from SIEM or other tool – Pivot into Security Analytics Alerts Dashboard (Open API)

2. Narrowed scope of investigation, eliminating noise – malicious file from sandbox results (Customizable Reports/Dashboard)

3. Determine reputation of file and the site sourcing the file (focused threat intel reports)

4. Trace root cause and produce all associated artifacts – Web pages, files, executables, etc. (extractions & Root Cause Explorer)

5. Dive deeper/wider and see related activity (replay traffic, packet analyzer, geolocation, custom reports)

6. With full source/scope resolve with surgical precision

Log File as Evidence

02


Log and event-based investigations lack depth of data to quickly find source/scope

Issue: Log & Event-based Tools Lack Depth

Unable to quickly investigate and identify source of breach

Difficult to acquire and manage data from multiple sources

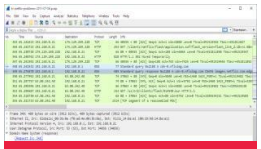
No event reconstruction

SIEM

Can't regenerate human-readable files

No context of what happened before, during and after alert

Full packet capture has been costly and reactive –it's too late



Basic Packet Capture

Simple capture is slow – can't keep up with 10Gb+ Networks

Difficult to navigate – linear search of TBs of data

Lacks enrichment using available threat intel

Legality of Using Logs

The following are **some of the legal issues** involved with **creating and using logs** that organizations and investigators must keep in mind :

- Logs must be created reasonably contemporaneously with the event under investigation.

  سیاهه ها باید همزمان با رویداد مورد بررسی بصورت منطقی ایجاد شوند.

- Someone with knowledge of the event must record the information. In this case, a program is doing the recording; the record therefore reflects the a priori knowledge of the programmer and system administrator.

  شخصی که از واقعه اطلاع دارد باید اطلاعات را ضبط کند. در این حالت، برنامه در حال انجام ضبط است و رکورد بر روی دانش سابق برنامه نویس و مدیر سیستم تاثیرگذار است.

Legality of Using Logs ...

- Logs must be kept as a regular business practice.
  - سیاهه‌های مربوط باید به عنوان یک روش معمول تجاری نگه داشته شوند.
- Random compilations of data are not admissible.
  - گردآوری تصادفی داده ها قابل قبول نیست.
- If an organization starts keeping regular logs now, it will be able to use the logs as evidence later.
- اگر یک سازمان اکنون شروع به نگه داشتن گزارش های منظم کند، بعداً می تواند از سیاهه‌های مربوط بعنوان مدرک استفاده کند.

Legality of Using Logs ...

- A custodian or other qualified witness must testify to the accuracy and integrity of the logs. **This process is known as authentication.**
- The custodian need not be the programmer who wrote the logging software; however, he or she must be able to offer testimony on what sort of system is used, where the relevant software came from, and how and when the records are produced.

- یک شاهد واجد شرایط دیگر باید درباره صحت و تمامیت سیاهه های مربوط گواه باشد. این فرآیند به عنوان احراز هویت شناخته می شود.
- متولی لازم نیست برنامه نویسی باشد که نرم افزار ورود به سیستم را نوشته است. با این وجود، باید بتواند شهادت دهد که چه نوع سیستمی مورد استفاده قرار می گیرد، از کجا نرم افزار مربوطه به وجود آمده است، و چگونگی و زمان تولید رکوردها را بداند.

Legality of Using Logs ...

- A custodian or other qualified witness must also offer testimony as to the reliability and integrity of the hardware and software platform used, including the logging software.
- متولی یا شاهد دیگری نیز باید در مورد اطمینان و یکپارچگی سخت افزار و نرم افزار مورد استفاده، از جمله نرم افزار ورود به سیستم، شهادت دهد.
- A record of failures or of security breaches on the machine creating the logs will tend to impeach the evidence.
- سابقه عدم موفقیت و یا نقض امنیتی دستگاه در ایجاد سیاهه‌های مربوط باعث استیضاح مدارک می‌شود.

Legality of Using Logs ...

- If an investigator claims that a machine has been penetrated, log entries from after that point are inherently suspect.
- In a civil lawsuit against alleged hackers, anything in an organization's own records that would tend to exculpate the defendants can be used against the organization.
- The original copies of any log files are preferred.

- اگر یک بازپرس ادعا کند که یک دستگاه مورد نفوذ قرار گرفته است، ورود به سیستم از بعد از آن نقطه ذاتاً مشکوک هستند.
- در دادخواست مدنی علیه هکرهای ادعا شده، هر چیزی که در پرونده های خود سازمان وجود دارد و برعلیه متهمان، می تواند علیه سازمان استفاده شود.
- نسخه اصلی هر پرونده ورود به سیستم ترجیح داده می شود.

Full Packet Capture = Deep Investigations

- **24/7 enriched recording of all traffic**

Data Capture, Enrichment, Retention

> "Security Analytics gives us the ability to look at historical records…Now we can analyze what happened 15 minutes ago or 15 days ago…what led to a security alert, and what happened."

Ensure you capture the breach before you know you were breached – 24/7 full packet recording

Indexed and enriched packets improve search performance – massive reputation and threat intel

Replay specific traffic to support required workflow – specify timeframe, combine segments, throttle

Retain what you need for long-term, retrospective analysis – Days, weeks, months of metadata and packet retention

Examining Intrusion and Security Events

Examining intrusion and security events includes both **passive and active tasks**.

بررسی رخدادهای امنیتی هر دو وظیفه منفعل و فعال را شامل می شود.

- ***A detection of an intrusion that occurs after an attack has taken place is called a post-attack detection or passive intrusion detection***.
  - تشخیص نفوذی که بعد از وقوع حمله رخ می دهد، شناسایی پس از حمله یا تشخیص نفوذ غیرفعال نامیده می شود.
- In these cases, the inspection of log files is the only medium that can be used to evaluate and rebuild the attack techniques.
  - در این موارد، بازرسی پرونده های لاگ تنها واسطه ای است که می تواند برای ارزیابی و بازسازی تکنیک های حمله مورد استفاده قرار گیرد.

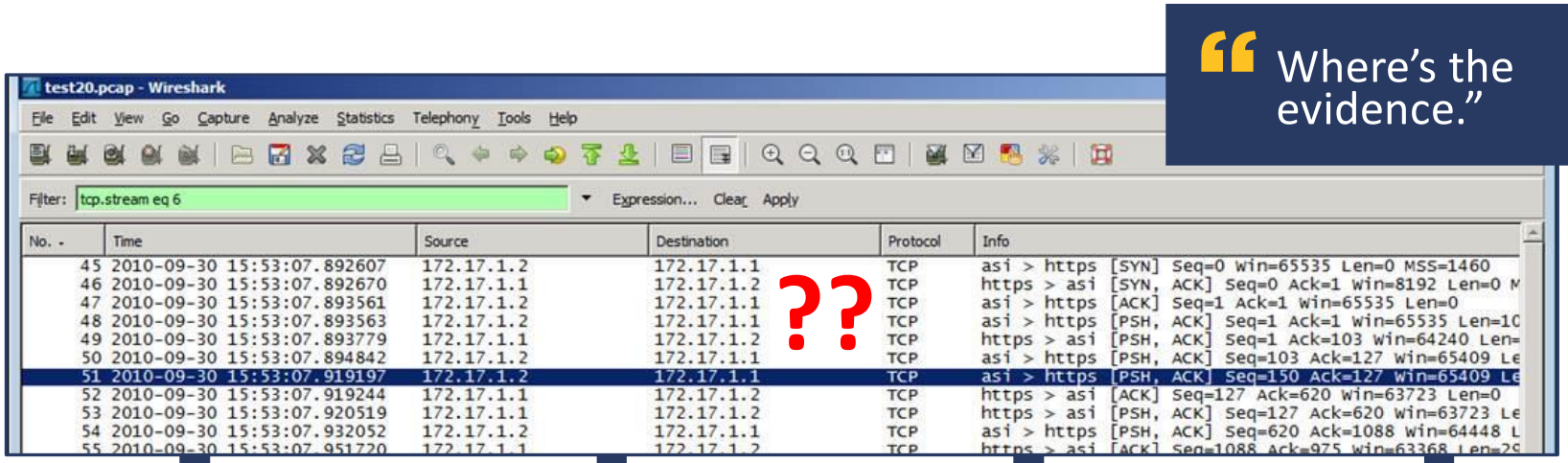
Examining Intrusion and Security Events …

- There are **many attack attempts that can be detected as soon as the attack takes place**.
  - تلاشهای زیادی برای حمله وجود دارد که به محض وقوع حمله قابل شناسایی است.
- This type of detection is known as ***active intrusion detection.***
  - این نوع تشخیص به عنوان تشخیص نفوذ فعال شناخته می شود.
- Using this method, an administrator or investigator follows the footsteps of the attacker and looks for known attack patterns or commands, and blocks the execution of those commands.
  - با استفاده از این روش، یک مدیر یا بازپرس، ردپای مهاجم را دنبال می کند و به دنبال الگوها یا دستورات شناخته شده حمله می رود و اجرای آن دستورات را مسدود می کند.


Inability to recreate exact evidence leads to uncertainty and extended exposure

Issue: Lack of Evidence Means Uncertainty

- Evidence gathering is difficult and time-consuming



Packet analysis requires special skills – It isn’t intuitive

Difficult to visualize actual artifacts – email, texts, html pages, PDF or .exe

Creating timeline of network and file activity is a difficult and time-consuming

Hard to answer “what happened, how, when, what was impacted?”

Using Multiple Logs as Evidence

- **Recording the same information in two different devices** makes the evidence stronger.
- **Logs from several devices collectively support each other.**
- Firewall logs, IDS logs, and TCPDump output can **contain evidence of an Internet user connecting to a specific server at a given time**.

- ضبط اطلاعات در دو دستگاه مختلف، شواهد را قوی تر می کند.
- ورود به سیستم از چندین دستگاه به طور جمعی از یکدیگر پشتیبانی می کند.
- سیاهه‌های مربوط به فایروال، سیاهه‌های مربوط به IDS و خروج TCPDump می‌توانند حاوی اطلاعات اتصال یک کاربر به سرور خاص در یک زمان معین باشند.

Maintaining Credible IIS Log Files

- Many network administrators have faced serious Web server attacks that have become legal issues.
- Web attacks are generally traced using IIS logs.
- بسیاری از سمدیران شبکه با حملات جدی روی سرور وب مواجه شده اند که به مشکلات قانونی تبدیل شده اند.
- حملات وب معمولاً با استفاده از سیاهه‌های مربوط به IIS ردیابی می‌شوند.
- An investigator must secure the evidence and ensure that it is **Accurate, Authentic, and Accessible**.
- یک محقق باید شواهد را تضمین کند و از صحت، معتبر و در دسترس بودن آن اطمینان حاصل کند.

Log File Accuracy

- The accuracy of IIS log files determines their credibility.
- Accuracy here means that the log files presented before the court of law represent the actual outcome of the activities related to the IIS server being investigated.
- Any modification to the logs causes the validity of the entire log file being presented to be suspect.

Logging Everything

- Certain fields in IIS log files might seem to be **less significant**, but **every field can make a major contribution as evidence**.
- Therefore, network administrators should **configure** their IIS server logs **to record every field** available.
- IIS logs must record information about **Web users** so that the logs provide clues about whether an **attack came from a logged-in user or from another system**.

- زمینه های مشخصی در پرونده های ورود به سیستم IIS به نظر می رسد کمتر قابل توجه باشند، اما هر زمینه می تواند به عنوان مدرک نقش مهمی داشته باشد.
- بنابراین ، مدیران شبکه باید گزارش های سرور IISخود را پیکربندی کنند تا هر فیلد موجود را ضبط کنند.
- سیاهه‌های مربوط به مؤسسه باید اطلاعات مربوط به کاربران وب را ضبط کند تا سیاهه‌ها اطلاعاتی راجع به اینکه آیا یک حمله از طریق یک کاربر وارد شده یا یک سیستم دیگر رخ داده است، ارائه دهند.

Logging Everything …

- Consider a defendant who claims **a hacker had attacked his system and installed a back-door proxy server on his computer.** The attacker then used the back-door proxy to attack other systems.
- In such a case, **how** does an investigator **prove** that the traffic came **from a specific user's Web browser** or that it was a proxied attack from someone else?

Paint a Clear Picture of Any Attack

- **Real Evidence for Laser-focused Response**

Evidence Discovery and Delivery

Deliver human-readable evidence: Images Multimedia, Office, PDF, DLL, EXE, HTML, Java, FTP, email and more

Know where your traffic is coming from - Identify traffic and volume on map and filter and alert on traffic to suspect countries

SEE what's crossing your network – View and analyze all images and audio files

Save time finding the source – chain together HTTP referrers

Data Recovery

03

What is Data Recovery

- Usually data recovery means that **data that is lost is recovered** – e.g., when a system crashes some data may be lost, with appropriate recovery procedures the data is recovered
- In digital forensics, **data recovery is about extracting the data from seized computers (hard drives, disks etc.) for analysis**

- معمولاً بازیابی داده به این معنی است که داده های از دست رفته بازیابی می شوند - به عنوان مثال ، هنگامی که سیستم خرابی برخی از داده ها را از دست می دهد ، با روشهای بازیابی مناسب داده ها بازیابی می شوند
- تست علمی/قانونی دیجیتال، بازیابی اطلاعات مربوط به استخراج داده ها از رایانه های توقیفی (هارد دیسک ها ، دیسک ها و غیره) برای تجزیه و تحلیل است.

Role of Backup in Data Recovery

- Databases/files are backed up periodically (daily, weekly, hourly etc.) so that if system crashes the databases/files can be recovered to the previous consistent state

- از پایگاه داده ها / پرونده ها بصورت دوره ای فایل پشتیبان تهیه می شوند (روزانه ، هفتگی ، ساعتی و غیره) به گونه ای که در صورت خراب شدن سیستم، پایگاه داده ها / پرونده ها می‌تواند به حالت قبلی بازیابی شوند.

Role of Backup in Data Recovery …

- Challenge to backup petabyte sized databases/files
- چالش سایز پتابایتی پایگاه داه / فایل‌ها برای نسخه پشتیبان
- Obstacles for backing up موانع پشتیبان گیری
  - Backup window, network bandwidth, system throughout
- Current trends روندهای فعلی
  - Storage cost decreasing, systems have to be online 24x7
- Next generation solutions راه حل های بعدی
  - Multiple backup servers, optimizing storage space

Data Recovery/Backup Solution

- Develop a **plan/policy** for backup and recovery
- **Develop/Hire/Outsource** the appropriate expertise
- **Develop a system design** for backup/recovery
  - Three tier **architectures, caches, backup servers**
- Examine state of the art backup/recovery **products and tools**
- **Implement the backup plan according to the policy and design**

  - تهیه یک طرح / سیاستی برای تهیه نسخه پشتیبان و بازیابی
  - توسعه / استخدام / برون سپاری تخصصی مناسب
  - طراحی سیستم برای تهیه نسخه پشتیبان / بازیابی
    سه نوع معماری ، حافظه ، سرورهای پشتیبان
  - محصولات و ابزارهای بازیابی و ی نسخه پشتیبان را بررسی کنید
  - برنامه تهیه نسخه پشتیبان را مطابق با خط مشی و طرح اجرا کنید

Recover Hidden Data

Hidden data داده های پنهان

- **Files may be deleted**, but until they are overwritten, the data may remain
  - Data stored in diskettes and stored insider another disk
- Need to get all the pieces and complete the puzzle
  - Analysis techniques (including statistical reasoning) techniques are being used to recover hidden data and complete the puzzle

- ممکن است پرونده ها حذف شوند ، اما تا زمانی که رونویسی نشوند ، داده ها ممکن است باقی بمانند
  - داده های ذخیره شده در دیسک ها و دیسک دیسک های داخلی
- نیاز به تمام قطعات و تکمیل پازل
  - از تکنیک های تحلیل (از جمله استدلال آماری) برای بازیابی داده های پنهان و تکمیل معما استفاده می شود

Evidence Collection and Preservation

04


Limited correlation between data, security intel and activity leads to undetected breaches

Issue: Incident Response Isn't Proactive

- I need to now before negative effects

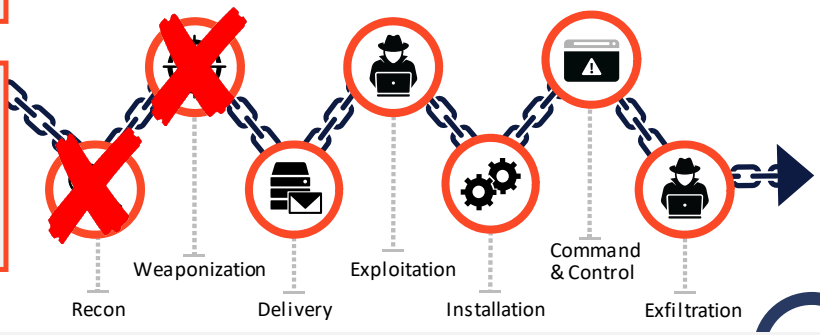
Unknown files are either malicious or safe
Sandboxing is manual and often too late to make a ruling

I don't know what unique threats are targeting my network?
Without knowing "normal" activity, finding "abnormal" activity and targeted attacks is difficult – Too much noise

I need proactive alerts to stop threats early in the "kill chain"?

> At the proactive IR maturity level, unknown data (web pages, PDFs, email attachments, etc.) are also automatically investigated.

SANS



What is Evidence Collection

- Collecting information from the data recovered for further analysis
  - جمع آوری اطلاعات از داده های بازیابی شده برای تجزیه و تحلیل بیشتر
- Collect evidence for analysis or monitor the intruder
  - شواهدی را برای تجزیه و تحلیل جمع آوری کنید یا فرد متجاوز را زیر نظر بگیرید
- Obstacles موانع
  - Difficult to extract patterns or useful information from the recovered data
  - Difficult to tie the extracted information to a person
    - استخراج الگوهای یا اطلاعات مفید از داده های بازیابی دشوار است
    - پیوند دادن اطلاعات استخراج شده به شخص دشوار است

Rules of Evidence

- Admissible قابل قبول
  - Evidence must be able to be used in court
- Authentic معتبر
  - Tie the evidence positively to an incident
- Complete کامل
  - Evidence that can cover all perspectives
- Reliable قابل اعتماد
  - There should be no doubt that proper procedures were used
- Believable باورپذیر
  - Understandable and believable to a jury

Additional Considerations

- Minimize handling and corruption of original data
- Account for any changes and keep detailed logs
- انحراف اطلاعات را به حداقل برسانید
- برای هر گونه تغییر شرح داشته باشید و گزارش های دقیق را نگه دارید

Additional Considerations …

- Need to understand what you are doing
- Follow the security policy established
- Work fast / however need to be accurate
- Proceed from volatile to persistent evidence
- Do not shut down the machine before collecting evidence
- Do not run programs on the affected machine

- درک کنید که چه کاری انجام می دهید
- سیاست امنیتی ایجاد شده را دنبال کنید
- سریع کار کنید / با این حال باید دقیق باشد
- از شواهد بی ثبات و مداوم ادامه دهید
- قبل از جمع آوری مدارک دستگاه را خاموش نکنید
- برنامه های مربوط به دستگاه آسیب دیده را اجرا نکنید

Proactive Detection and Incident Response

- **Reduce effort and respond faster**

Proactive Incident Response

> “Organizations need to understand their environment and what constitutes normal and abnormal behavior”
>
> SANS

Customize Alerts Dashboard and reports to prioritize response	Automate additional analysis based on indicators – alert, export to PCAP, send to sandbox, etc.	Use Sandboxing to turn “unknown” files into known safe or malicious	Leverage Anomaly Detection: Establish a baseline of normal Observe and identify anomalies

Volatile Evidence

- Types
  - Cached data داده‌های ذخیره شده
  - Routing tables جداول مسیریابی
  - Process table جدول پردازش
  - Kernel statistics آمار هسته
  - Main memory حافظه اصلی

- What to do next
  - Collect the volatile data and store in a permanent storage device
  - داده های عیر قابل پیش‌بینی را جمع آوری کرده و در یک دستگاه ذخیره سازی بصورت دائم داده‌ها را ذخیره کنید

Methods of Collection

- Freezing the scene انجماد صحنه
  - Taking a snapshot of the system and its compromised state
  - Recover data, extract information, analyze
    - گرفتن تصویر صحنه‌ای از سیستم و وضعیت به خطر افتاده آن
    - بازیابی اطلاعات ، استخراج اطلاعات ، تجزیه و تحلیل
- Honeypotting
  - Create a replica system and attract the attacker for further monitoring
    - یک سیستم ماکت ایجاد کنید و برای نظارت بیشتر مهاجم را جذب کنید

Steps to Collection

- Find the evidence; where is it stored
- Find relevant data - recovery
- Create order of volatility
- Remove external avenues of change; no tampering
- Collect evidence – use tools
- Good documentation of all the actions

- شواهد را پیدا کنید؛ کجا ذخیره شده است
- داده های مربوط را پیدا کنید - بازیابی
- عدم غیرقابل پیش بینی بودن را ایجاد کنید
- راه های خارجی تغییر را حذف کنید. بدون دستکاری
- جمع آوری شواهد - ابزار استفاده کنید
- مستندات خوب از کلیه اقدامات

Controlling Contamination

- Analyze the evidence
  - Use analysis tools to determine what happened
- Analyze the log files and determine the timeline
- Analyze backups using a dedicated host
- Reconstruct the attack from all the information collected

- شواهد را تجزیه و تحلیل کنید
  - برای تعیین آنچه اتفاق افتاده است از ابزارهای تحلیل استفاده کنید
- پرونده های گزارش را تجزیه و تحلیل کرده و جدول زمانی را تعیین کنید
- تهیه نسخه پشتیبان از یک هاست اختصاصی
- حمله را از تمام اطلاعات جمع آوری شده بازسازی کنید

Computer Evidence MUST be

- Authentic: not tampered with معتبر: دستکاری نشده است
- Accurate: have high integrity صحیح
- Complete: no missing points کامل
- Convincing: no holes قانع کننده
- Conform: rules and regulations انطباق
- Handle change: data may be volatile and time sensitive کنترل تغییرات
- Handle technology changes: tapes to disks; MAC to PC کنترل تغییرات فن آوری
- Human readable: Binary to words قابل خواندن برای انسان

THE SECURITY CAMERA & DVR FOR YOUR NETWORK

Turning Complexity into Context

Providing real-time analysis and full visibility of **everything going in and out of your network**

- Records, classifies and indexes all packets and flows on high-speed networks
- DPI classification of over 2,800 applications and thousands of meta attributes
- On the wire, ***real-time*** visibility and analysis of data exfiltration & infiltration
- Security Context – including reputation, user and social personas, artifacts
- The 'Black Box' for incident response, forensics, root cause and impact analysis

Thanks for your Attention.