GIÁM SÁT & ỨNG PHÓ SỰ CỐ AN TOÀN MẠNG

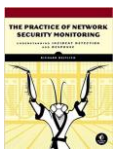
Bài 1. Bài mở đầu

1. Giới thiệu học phần
2. Tổng quan giám sát an toàn mạng
3. Kiến thức nền tảng
4. Công cụ phổ biến

1. Giới thiệu học phần
2. Tổng quan giám sát an ninh mạng
3. Kiến thức nền tảng
4. Công cụ phổ biến

Giáo trình và Tài liệu tham khảo

1. Chris Sander, Jason Smith, **Applied Network Security Monitoring: Collection, Detection, and Analysis.**
2. Richard Bejtlich, **The Practice of Network Security Monitoring: Understanding Incident Detection and Response**
3. Richard Bejtlich, **The Tao of Network Security Monitoring: Beyond Intrusion Detection.**



5

Nội dung học phần

1. Tổng quan về GSATTT
2. Hệ thống GSATTT & Quy trình GSATTT
3. Chiến lược ứng phó sự cố ATTT
4. Xử lý sự cố ATTT

6

Cấu trúc học phần

- **Thời lượng**: 2tc = 36 tiết
- **Đánh giá kết quả học tập**
  - Điểm chuyên cần
    - Đi học đầy đủ, đúng giờ
    - Tham gia xây dựng bài
  - Điểm thực hành + BTL
  - Điểm thi kết thúc học phần
  - Thi cuối kỳ: Tự luận

7

Bài tập lớn

Danh sách và Yêu cầu làm bài tập lớn

8

1. Giới thiệu học phần
2. Tổng quan giám sát an ninh mạng
3. Kiến thức nền tảng
4. Công cụ phổ biến

Operation Aurora

❑**2009, hãng Google bị dính hàng loạt vụ tấn công mang tên Operation Aurora.**

– Ngoài ra, 30 tập đoàn lớn nữa cũng bị ảnh hưởng bởi loại mã độc này như Adobe, Juniper, Intel, Yahoo…

10

Operation Aurora

❑**Mã độc lây lan chủ yếu qua trình duyệt IE.**

– Người dùng bị lừa bấm vào 1 trang web độc hại
– Trình duyệt tải mã độc về máy nạn nhân
– Mã độc thực hiện liên kết tới C&C
– Leo thang đặc quyền
– Mật khẩu Active Directory bị lấy trộm và bẻ khóa
– Kết nối VPN với các tài khoản thu được
– Các dữ liệu có giá trị được gửi về Trung Quốc

➔ **Các giải pháp bảo vệ thông thường như Anti-virus, Firewall không còn hiệu quả.**

11

Giải pháp đảm bảo an toàn thông tin

❑**Giải pháp**:

– Proxy, Firewall, HIDS/NIDS, IPS…

❑**Nguy cơ:**

– "Control" thất bại
– "Prevention" thất bại
– "Initial detection" thất bại

12

Vấn đề thường gặp

– Không có khả năng phân tích toàn bộ nhật ký
– Số lượng cảnh báo lớn, phân tán
– Thiếu khả năng bao quát hệ thống
– Mỗi hệ thống có một định dạng nhật ký khác nhau, gây khó khăn cho việc phân tích

➔ **Xây dựng hệ thống giám sát ATTT**

13

Hệ thống giám sát an toàn thông tin

- **Hệ thống giám sát an toàn thông tin** (SIEM – Security information and event management) là hệ thống được thiết kế nhằm ***thu thập*** thông tin nhật ký các sự kiện an ninh từ các thiết bị đầu cuối và ***phân tích*** chúng với mục đích phát hiện và kịp thời ứng phó, cho phép tổ chức hạn chế được các rủi ro, tiết kiệm thời gian và nhân lực.
- Ví dụ: Phát hiện ra dấu vết các cuộc tấn công, thâm nhập trái phép trong hệ thống.
- Thông thường, GSATTT bao gồm:
  - Giám sát an ninh mạng
  - Giám sat an ninh liên tục

14

Giám sát an toàn thông tin

- **Thông tin an ninh mạng** là những thông tin ghi lại hoạt động của hệ thống mạng có chọn lọc.
- Ví dụ: Xác định vào ngày giờ nào, user nào đã đăng nhập hệ thống, địa chỉ ip, truy cập đến những tài nguyên nào…

15

Trạng thái của dữ liệu số

- **Data in Use**
  - Office apps, PDF…
  - Database access, Cloud apps, Mobile apps
- **Data in Transit**
  - Email, Attachment, Web uploads & downloads
  - LAN transfer, Instant Messaging, P2P
  - Wifi & Mobile network
- **Data at rest**
  - File servers and network shares
  - Database
  - Desktop, laptops, Tablets, Mobile devices
  - USB drives, Cloud Storage

16

Giám sát an ninh mạng

- **Giám sát an ninh mạng** (Network security monitoring - NSM) tập trung vào dữ liệu lưu chuyển:
  - IDPS alerts
  - Packets
  - Flow

17

Giám sát an ninh liên tục

- **Giám sát an ninh liên tục** (Continuos Security Monitoring - CSM) tập trung vào dữ liệu được lưu trữ:
  - Log files
  - Registry Keys
  - Vulnerability assessments
- CSM không phải là giải pháp thay thế cho NSM, chúng bổ sung hỗ trợ lẫn nhau.

18

NSM vs CSM

- **NSM** chủ yếu tập trung vào các **nguy cơ (threat-centric)** còn **CSM** tập trung vào các **lỗ hổng bảo mật (vulnerability-centric)**

NSM	CSM
- Alert data - Packet data - Logs - Sessions - Metadata - Etc…	- Vulnerabilities CVES - Patching and configuration issues - Software weakness

19

Phát hiện tấn công

- GSATTT ***không*** ngăn chặn tấn công.
- GSATTT giúp xác định các mối nguy cơ, hiểm họa và khiến cho kẻ tấn công không thể đạt được mục đích cuối cùng
  - Thời gian là yếu tố chiến lược
  - Thông thường các cuộc tấn công cần một khoảng thời gian nhất định chính vì thế GSATTT cho phép người quản trị có khả năng kịp thời phát hiện tấn công để có biện ứng phó.

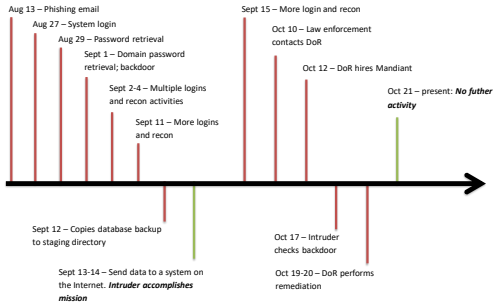
20

Case Study

- CSDL của South Carolina bị tấn công vào năm 2012
- Attacker xâm nhập vào nhờ sử dụng thư lừa đảo
- Dữ liệu bị đánh cắp 4 tuần sau đó
- Sau 4 tuần thì Mandiant được gọi điều tra

21

Case Study



22

Bài học rút ra

- Xâm nhập vào hệ thống chỉ là bước đầu
- DoR có 4 tuần để phát hiện và ngăn chặn
- Nếu kịp thời phát hiện có thể làm giảm các thiệt hại xảy ra

23

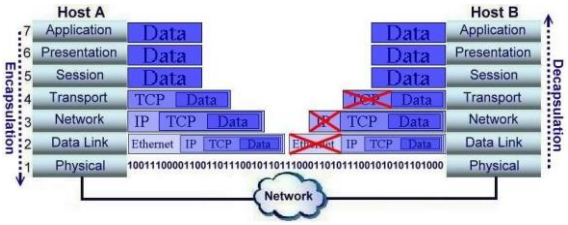
1. Giới thiệu học phần
2. Tổng quan giám sát an ninh mạng
3. Kiến thức nền tảng
4. Công cụ phổ biến

OSI Model

Data	OSI Layers	Activities
Data	**Application** Telnet, FTP, SMTP, HTTP, DNS, SNMP	To allow access to network resources
Data	**Presentation**	To translate, encrypt, and compress data
Data	**Session**	To establish, manage, and terminate session
Segments	**Transport** SCTP, TCP, UDP, Sockets and Ports address	To provide reliable process-to-process Message delivery and error recovery
Packets	**Network** IP, ARP/RARP, ICMP, IGMP, Logical address	To move packets from source to destination; to provide internetworking
Frames	**Data Link** IEEE 802 Standards, TR, FDDI, PPP, Physical address	To organize bits into frames; to provide Hop-to-hop delivery
Bits	**Physical** Medium, Coax, Fiber, 10base, Wireless	To transmit bits over a medium; to provide mechanical and electrical specifications

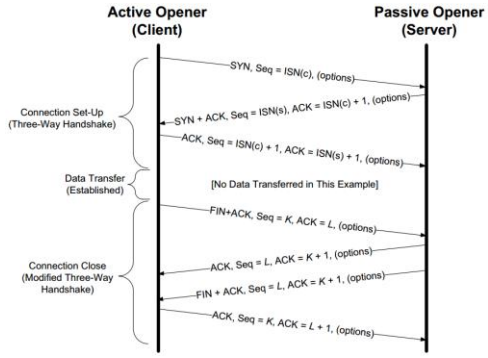
25

Encapsulation-Decapsulation



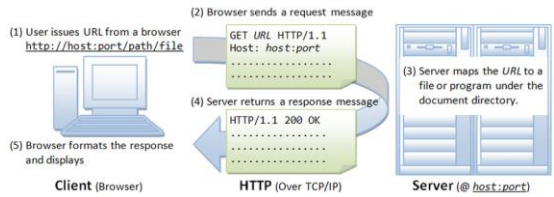
26

TCP/IP Communication



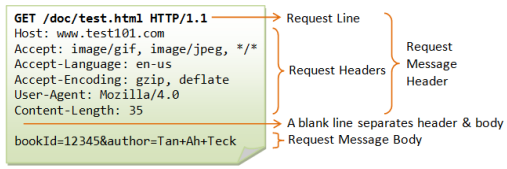
27

HTTP Protocol



28

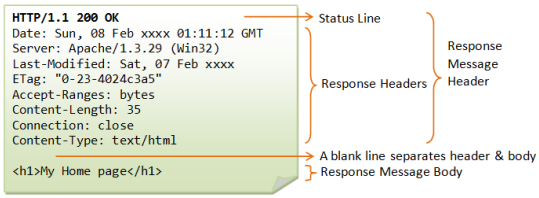
HTTP Request



- **Request-line** = Phương thức+ URI request + HTTP version
- **Phương thức:** GET/POST/HEAD/PUT/DELETE/PATCH…

29

HTTP Response



- **Status-line** = HTTP version + Mã trạng thái + trạng thái
- **Mã trạng thái**: 1xx: Thông tin; 2xx: Thành công ; 3xx: Sự điều hướng lại ; 4xx: Lỗi phía Client ; 5xx: Lỗi phía Server.

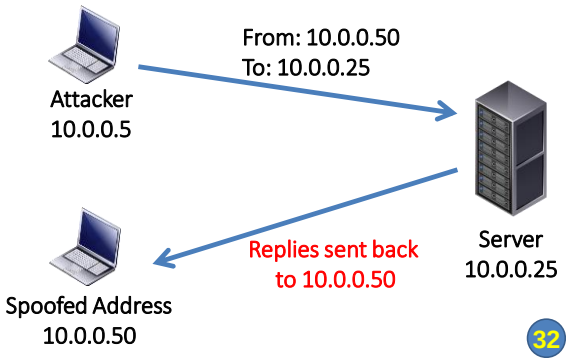
30

Một số tấn công cơ bản

- IP spoofing
- Denial of service
- Man in the middle attack
- Sniffing
- Advanced Persistent Threats
- Client-side exploitation
- Service-side exploitation

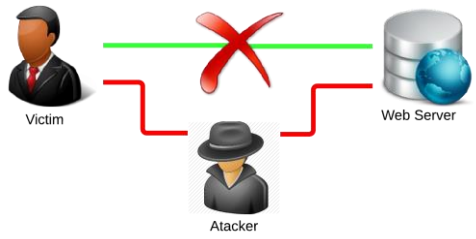
31

IP spoofing



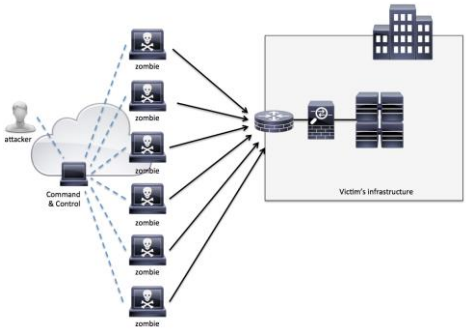
32

MiTM Attack



33

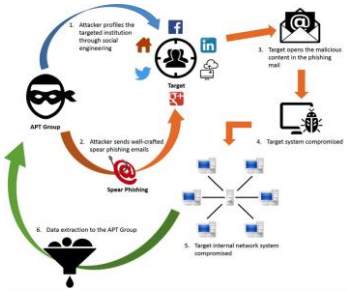
DoS/DDoS Attack



34

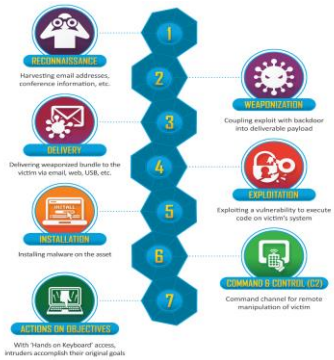
Tấn công APT

A: Advanced – Targeted, Coordinated, Purposeful
P: Persistent – Month after Month, Year after Year
T: Threat – Person(s) with Intent, Opportunity, and Capability



35

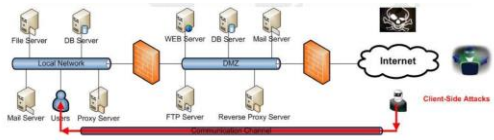
Cyber Kill Chain



- Được phát triển bởi Lockheed Martin (2011)
- Bao gồm 7 giai đoạn, mô tả quá trình tấn công
- Việc tấn công được xem là thành công nếu tất cả 7 giai đoạn đều được thực hiện thành công

36

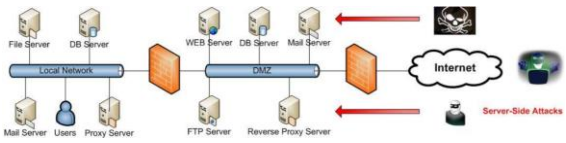
Client-side Attack



- Client-side attacks occur when a user downloads malicious content
- Client-side attacks initiate from the victim who downloads content from the attacker

37

Service-side Attack



- Service-side attacks are initiated by the attacker
- Also known as Server-side attacks

38

1. Giới thiệu học phần
2. Tổng quan giám sát an ninh mạng
3. Kiến thức nền tảng
4. Công cụ phổ biến

NSM Distribution

Secuiry Onion – Linux distribution designed specifically for NSM (https://securityonion.net/)

- Ful packet capture – Tcpdump/Wireshark/NetworkMiner
- Extracted content – Xplico/NetworkMiner
- Session data – Bro/FlowBat/Argus/Ipaudit
- Transaction data – Bro
- Statistical data – Capinfos/Wireshark
- Metadata – ELSA (Whois)
- Alert/Log data – Snort, Suricata, Sguil, Snorby, Syslog

Security Onion

40

NSM/NIDS Frontends

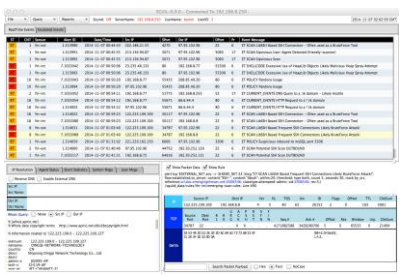
- Có rất nhiều công cụ quản lý sự kiện tập trung được sử dụng cho NSM/NIDS
  - **ACID** (Analysis Console for Intrusion Databases) - last update 2003
  - **BASE** (Basic Analysis and Security Engine) – last update 2013
  - Các công cụ thường được sử dụng hiện tại như **Sguil**, **Snorby** và **Squert**

sguil

41

Sguil

- Sguil perform full packet capture, and allows you to right-click on any event
  - and launch to appropriate tool of choice



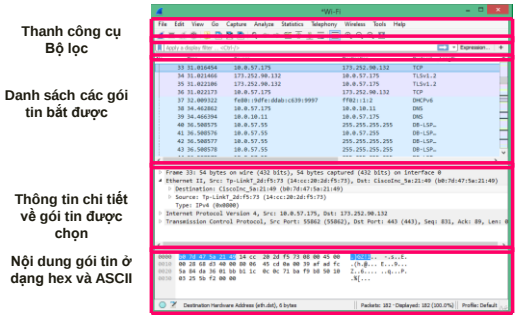
42

NSM Toolbox: Wireshark and Tshark

- Wireshark is a graphical network protocol analyzer (https://www.wireshark.org/)
  - Wireshark is one of the most powerfull tools in the NSM arsenal
- Tshark brings the power of Wireshark to the command line
  - Command line + display filters == awesome!

43

Wireshark



44

Wireshark: Display filter example

- ip.src==10.1.11.00/24
- ip.addr==192.168.1.10 && ip.addr==192.168.1.20
- tcp.port==80 || tcp.port==3389
- !(ip.addr==192.168.1.10 && ip.addr==192.168.1.20)

45

Tshark

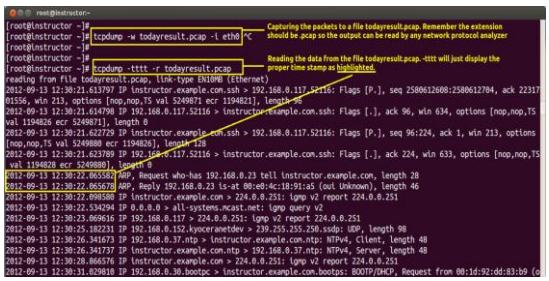
- Tshark marries the power of Wireshark with the command line and scripting!
- One of Tshark's most powerful features: command-line access to display filters

```
ubuntu@ip-172-31-26-215:~/working$ tshark -r dnacat2.pcap -T fields -E header=y
-e ip.src -e ip.dst -e ip.proto -e udp.dstport -e ip.len -e frame.time_delta_d
isplayed ip.dst==165.227.88.15 | head -20
ip.src  ip.dst  ip.proto         udp.dstport     ip.len  frame.time_delta_displa
yed
192.168.88.2    165.227.88.15   17      53      89      0.000000000
192.168.88.2    165.227.88.15   17      53      89      1.074819358
192.168.88.2    165.227.88.15   17      53      89      1.084471967
192.168.88.2    165.227.88.15   17      53      89      1.078728781
192.168.88.2    165.227.88.15   17      53      89      1.069749570
192.168.88.2    165.227.88.15   17      53      89      1.077714934
192.168.88.2    165.227.88.15   17      53      89      1.076642909
192.168.88.2    165.227.88.15   17      53      89      1.070790122
192.168.88.2    165.227.88.15   17      53      89      1.071040506
192.168.88.2    165.227.88.15   17      53      89      1.064914560
192.168.88.2    165.227.88.15   17      53      89      0.993778795
192.168.88.2    165.227.88.15   17      53      89      0.961346162
192.168.88.2    165.227.88.15   17      53      89      1.062188142
192.168.88.2    165.227.88.15   17      53      89      1.065854491
192.168.88.2    165.227.88.15   17      53      89      1.075033821
192.168.88.2    165.227.88.15   17      53      89      1.066068845
192.168.88.2    165.227.88.15   17      53      89      1.063321512
192.168.88.2    165.227.88.15   17      53      89      1.071506357
192.168.88.2    165.227.88.15   17      53      89      1.058017495
ubuntu@ip-172-31-26-215:~/working$
```

46

Tcpdump

- Tcpdump cho phép bắt và lưu lại những gói tin bắt được, từ đó chúng ta có thể sử dụng để phân tích.



47

Others

- Cain and Abel
- Kismet
- Ettercap
- NetStumbler
- Dsniff
- Ntop
- Ngrep
- AtherApe
- ....

48

NIDS

- NIDS (Network Intrusion Detection System) đóng vai trò quan trọng trong việc triển khai SIEM
- Một số NIDS: Snort, Suricata, Bro, OSSEC…

49

SIEM

- Commercial:
  - HP ArcSight
  - Qradar
  - Splunk
  - McAfee/Intel…

50

SIEM

- Open Source:
  - OSSIM
  - ELK Stacks
  - Splunk Free
  - Wazuh
  - Apache Metron

51

52