GIÁM SÁT & ỨNG PHÓ SỰ CỐ AN TOÀN MẠNG

Chương 2. Hệ thống giám sát an toàn thông tin mạng

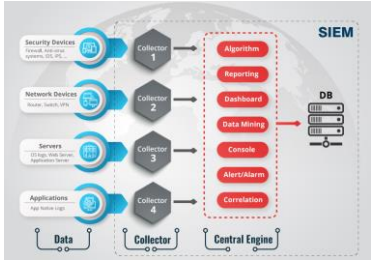
1. Kiến trúc và thành phần
2. Dữ liệu thu thập
3. Phương pháp thu thập
4. Phát hiện xâm nhập

SIEM

- **Hệ thống giám sát an toàn thông tin** (SIEM – Security information and event maagement) là hệ thống được thiết kế nhằm ***thu thập*** thông tin nhật ký sự kiện từ các thiết bị đầu cuối và ***phân tích*** chúng với mục đích phát hiện và kịp thời ứng phó, cho phép cơ quan/tổ chức hạn chế được các rủi ro, tiết kiệm thời gian và nhân lực.

Kiến trúc và thành phần

- Thành phần thu thập dữ liệu (Collector).
- Thành phần phân tích và lưu trữ (Engine+DB).
- Thành phần quản trị tập trung (Management).



Đối tượng

- SIEM thu thập dữ liệu từ 4 nguồn chính:
  - Thiết bị bảo mật (Security devices – IDPS, AV, DLP, Firewall, Honeypots, Web Filters)
  - Thiết bị mạng (Network devices – Routers, Switches, Access Point, Private Cloud Networks)
  - Máy chủ (Servers – App Server, Databases)
  - Ứng dụng (Applications – Web App, SaaS App)

Thành phần thu thập dữ liệu

- Thu thập toàn bộ dữ liệu nhật ký từ các nguồn thiết bị, ứng dụng.
- Kiểm soát băng thông, không gian lưu trữ.
- Phân tách từng sự kiện và chuẩn hóa các sự kiện vào một lược đồ chung.
- Tích hợp các sự kiện.
- Chuyển toàn bộ các sự kiện đã thu thập về thành phần phân tích và lưu trữ.

7

Thành phần phân tích và lưu trữ

- Tập hợp nhật ký tập trung, tiến hành phân tích, so sánh tương quan.
- Môđun phân tích sẽ được hỗ trợ bởi các luật (được định nghĩa trước) cũng như khả năng tuỳ biến, nhằm đưa ra kết quả phân tích chính xác nhất.
- Hỗ trợ kết nối đến các hệ thống lưu trữ dữ liệu giúp nâng cao khả năng lưu trữ và xây dựng kế hoạch dự phòng, chống mất mát dữ liệu.

8

Thành phần quản trị tập trung

- Cung cấp giao diện quản trị. Các giao diện được phân quyền theo vai trò của người quản trị.
- Hỗ trợ các mẫu báo cáo, các giao diện theo dõi, điều kiện lọc, tập luật…
- Hỗ trợ các công cụ cho việc xử lý các sự kiện an toàn mạng xảy ra trong hệ thống.

9

Câu hỏi thảo luận

- Cần lưu ý gì khi xây dựng hệ thống SIEM???

10

Yếu tố cơ bản

- Xác định các đơn vị, hệ thống, thiết bị, dịch vụ cần giám sát.
- Xác định trang thiết bị, giải pháp phần mềm thương mại cần giám sát.
- Xác định phần mềm nội bộ và phần mềm mã nguồn mở phục vụ giám sát.
- Xác định các thiết bị, công cụ, giải pháp hỗ trợ phân tích kết quả giám sát.
- Xác định quy trình giám sát.

11

Chức năng & thành phần quan trọng

1. Data aggregation
2. Threat Intelligence Feeds
3. Correlation
4. Analytics
5. Alerting
6. Dashboard
7. Compliance
8. Log Retention
9. Forensic Analysis
10. Threat Hunting
11. Incident Response
12. SOC Automation

12

Chức năng & thành phần quan trọng

1. Data Aggregation: dữ liệu được thu thập từ nhiều nguồn theo nhiều cách khác nhau:

- Thu thập từ agent
- Kết nối trực tiếp với thiết bị
- Truy cập vào logs được lưu trữ trong DB

13

Chức năng & thành phần quan trọng

2. Threat Intelligence Feeds: Sử dụng các dữ liệu hiện có kết hợp với nghiên cứu, cập nhật các lỗ hổng, các hoạt động đe dọa tiềm tàng, và sau đó ánh xạ với tài sản của khách hàng để thực hiện và nâng cao khả năng phòng thủ chủ động

14

Chức năng & thành phần quan trọng

3. Correlation: giúp liên kết các sự kiện an ninh từ các nguồn khác nhau thành một sự kiện an ninh chính xác.

- Tương quan dựa trên luật
- Tương quan dựa trên thống kê

4. Analytics:

- Sử dụng các kỹ thuật như học máy, mô hình thống kê để xây dựng liên kết sâu hơn giữa các loại dữ liệu.
- Chuẩn hóa log

15

Chức năng & thành phần quan trọng

5. Alerting:

- Thông báo tới các quản trị viên một cuộc tấn công hay một hành vi bất thường đang xảy ra.

6. Dashboards:

- Cung cấp công cụ, giao diện trực quan hóa dữ liệu.
- Cho phép quản trị viên giao tiếp với dữ liệu được lưu trữ trong SIEM.

7. Compliance:

- Khả năng tạo ra các báo cáo tuân thủ các tiêu chuẩn như HIPAA, PCI/DSS, HITECH, SOX.

16

Chức năng & thành phần quan trọng

8. Log Retention: dữ liệu gửi tới SIEM cần phải lưu trữ với mục đích lưu giữ và truy vấn sau này. Có thể lưu trữ theo 3 cách:

- Cơ sở dữ liệu
- Lưu trữ dưới dạng file text
- Lưu trữ dưới dạng nhị phân

17

Chức năng & thành phần quan trọng

9. Forensic Analysis:

- Quá trình phân tích chuyên sâu dữ liệu được lưu trữ để tái cấu trúc toàn bộ sự cố nhằm tìm ra nguyên nhân, nguồn gốc sự việc

10. Threat Hunting

- Khả năng chủ động săn tìm các mối đe dọa và đưa ra các khuyến nghị nhằm ngăn chặn các mối đe dọa tìm được.

18

Chức năng & thành phần quan trọng

11. Incident Response:

- Dữ liệu thu thập được giúp đội ứng phó sự cố xác định nguồn gốc tấn công và phản ứng lại một cách nhanh nhất có thể.

12. SOC Automation:

- Khả năng tự động ứng phó sự cố đối với các hệ thống SIEM tiên tiến

19

Yêu cầu

- Dự phòng: dữ liệu cần được lưu trữ dự phòng ở nhiều nơi khác nhau, giảm thiểu nguy cơ mất mát dữ liệu.
- Xác thực tính chính xác của thông tin (kẻ xâm nhập có thể thay đổi hoặc xóa các bản ghi).
- Sử dụng và kết hợp nhiều phương pháp, kỹ thuật nhằm đảm bảo việc thu thập và phân tích thông tin chính xác và hiệu quả.

20

Hạn chế của SIEM

- Mạng có sử dụng các cơ chế mã hóa (vd: VPN).
- Mạng sử dụng NAT.
- Thiết bị trong hệ thống mạng liên tục di chuyển (vd: Mobile).
- Lưu lượng mạng vượt quá khả năng phần cứng của SIEM.
- Các yếu tố khác liên quan đến chính sách hệ thống như quyền riêng tư, chính sách truy cập…

21

1. Kiến trúc và thành phần
2. Dữ liệu thu thập
3. Phương pháp thu thập
4. Phát hiện xâm nhập

Dữ liệu thu thập

Có rất nhiều dạng dữ liệu như sau:

1. Full content data
2. Extracted content
3. Session data
4. Transaction data
5. Statistical data
6. Alert/log data

23

1. Full content data

1. Full content data - tất cả các dữ liệu thu thập được trong hệ thống mạng
2. Chuyên gia phân tích bảo mật khi làm việc với "Full content data" thường qua 2 giai đoạn:
   - Phân tích tổng quan.
   - Phân tích chuyên sâu.

24

1. Full content data

- Phân tích tổng quan:

```
19:09:47.469646 IP 192.168.238.152.41482 > 217.160.51.31.80:
 Flags [S], seq 953674548, win 42340, options [mss 1460,sackOK,TS val 75892
 ecr 0,nop,wscale 11], length 0

19:09:47.594058 IP 217.160.51.31.80 > 192.168.238.152.41482:
 Flags [S.], seq 272838780, ack 953674549, win 64240, options [mss 1460],
 length 0

19:09:47.594181 IP 192.168.238.152.41482 > 217.160.51.31.80:
 Flags [.], ack 1, win 42340, length 0

19:09:47.594427 IP 192.168.238.152.41482 > 217.160.51.31.80:
 Flags [P.], seq 1:296, ack 1, win 42340, length 295

19:09:47.594932 IP 217.160.51.31.80 > 192.168.238.152.41482:
 Flags [.], ack 296, win 64240, length 0

19:09:47.714886 IP 217.160.51.31.80 > 192.168.238.152.41482:
 Flags [P.], seq 1:316, ack 296, win 64240, length 315

19:09:47.715003 IP 192.168.238.152.41482 > 217.160.51.31.80:
 Flags [.], ack 316, win 42025, length 0
```

25

1. Full content data

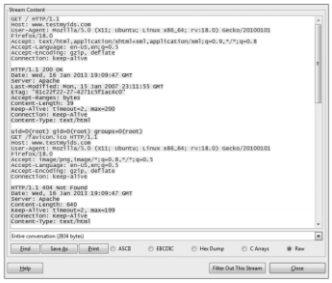
- Phân tích chuyên sâu:

```
19:09:47.594427 00:0c:29:fc:b0:3b > 00:50:56:f0:08:d6, ethertype IPv4 (0x0800), length 349:
192.168.238.152.41482 > 217.160.51.31.80: Flags [P.], seq 1:296, ack 1, win 42340, length 295
        0x0000:  0050 56f0 08d6 000c 29fc b03b 0800 4500  .PV.....)..;..E.
        0x0010:  014f c342 4000 4006 ba65 c0a8 ee98 d9a0  .O.B@.@..e......
        0x0020:  331f a20a 0050 38d7 eb35 1043 307d 5018  3....P8..5.C0}P.
        0x0030:  a564 180c 0000 4745 5420 2f20 4854 5450  .d....GET./.HTTP
        0x0040:  2f31 2e31 0d0a 486f 7374 3a20 7777 772e  /1.1..Host:.www.
        0x0050:  7465 7374 6d79 6964 732e 636f 6d0d 0a55  testmyids.com..U
        0x0060:  7365 722d 4167 656e 743a 204d 6f7a 696c  ser-Agent:.Mozil
        0x0070:  6c61 2f35 2e30 2028 5831 313b 2055 6275  la/5.0.(X11;.Ubu
        0x0080:  6e74 753b 204c 696e 7578 2078 3836 5f36  ntu;.Linux.x86_6
        0x0090:  343b 2072 763a 3138 2e30 2920 4765 636b  4;.rv:18.0).Geck
        0x00a0:  6f2f 3230 3130 3031 3031 2046 6972 6566  o/20100101.Firef
        0x00b0:  6f78 2f31 382e 300d 0a41 6363 6570 743a  ox/18.0..Accept:
        0x00c0:  2074 6578 742f 6874 6d6c 2c61 7070 6c69  .text/html,appli
        0x00d0:  6361 7469 6f6e 2f78 6874 6d6c 2b78 6d6c  cation/xhtml+xml
        0x00e0:  2c61 7070 6c69 6361 7469 6f6e 2f78 6d6c  ,application/xml
        0x00f0:  3b71 3d30 2e39 2c2a 2f2a 3b71 3d30 2e38  ;q=0.9,*/*;q=0.8
        0x0100:  0d0a 4163 6365 7074 2d4c 616e 6775 6167  ..Accept-Languag
        0x0110:  653a 2065 6e2d 5553 2c65 6e3b 713d 302e  e:.en-US,en;q=0.
        0x0120:  350d 0a41 6363 6570 742d 456e 636f 6469  5..Accept-Encodi
        0x0130:  6e67 3a20 677a 6970 2c20 6465 666c 6174  ng:.gzip,.deflat
        0x0140:  650d 0a43 6f6e 6e65 6374 696f 6e3a 206b  e..Connection:.k
        0x0150:  6565 702d 616c 6976 650d 0a0d 0a         eep-alive....
```

26

2. Extracted content data

- Extracted content data – luồng dữ liệu, file, webs, malware…



27

3. Session data

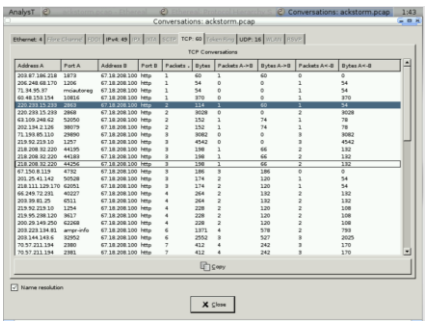
- Session data – dữ liệu trao đổi giữa các nút mạng

```
#fields
ts                      uid         id.orig_h       id.orig_p  id.resp_h       id.resp_p
 proto   service  duration     orig_bytes  resp_bytes    conn_state  local_orig  missed_bytes
 history     orig_pkts  orig_ip_bytes    resp_pkts  resp_ip_bytes  tunnel_parents  orig_cc  resp_cc

#types
time                    string      addr            port       addr            port
 enum    string   interval    count       count          string      bool        count
 string  count        count          count        count   table[string]     string      string

2013-01-16T19:09:47+0000❶  90E6goBBSw3  192.168.238.152❷  41482❸     217.160.51.31❹
 80❺  tcp❻      http     2.548653     877❼        1957❽          SF          T          0
 ShADadfF   9          1257           9          2321           (empty)          -          DE

2013-01-16T19:09:47+0000    49vu9nUQyJf  192.168.238.152  52518     192.168.238.2
 53    udp      dns      0.070759     35          51          SF          T          0
 Dd          1          63             1           79          (empty)          -          -
```

28

3. Session data

- Session data



29

4. Transaction data

- Transaction data - tương tự như "session data" nhưng tập trung vào các "requests" và "replies" giữa các nút mạng.

```
2013-01-16T19:09:47+0000        90E6goBBSw3     192.168.238.152 41482   217.160.51.31   80
1       GET❶     www.testmyids.com       /               -               Mozilla/5.0 (X11; Ubuntu;
Linux x86_64;
rv:18.0) Gecko/20100101 Firefox/18.0    0       39      200❷    OK              -       -
-       (empty) -       -       -       text/plain      -       -


2013-01-16T19:09:47+0000        90E6goBBSw3     192.168.238.152 41482   217.160.51.31   80
2       GET❶     www.testmyids.com       /favicon.ico    -               Mozilla/5.0 (X11; Ubuntu;
Linux x86_64;
rv:18.0) Gecko/20100101 Firefox/18.0    0       640     404❷    Not Found       -       -
-       (empty) -       -       -       text/html       -       -

2013-01-16T19:09:47+0000        90E6goBBSw3     192.168.238.152 41482   217.160.51.31   80
3       GET❶     www.testmyids.com       /favicon.ico    -               Mozilla/5.0 (X11; Ubuntu;
Linux x86_64;
rv:18.0) Gecko/20100101 Firefox/18.0    0       640     404❷    Not Found       -       -
-       (empty) -       -       -       text/html       -       -
```

30

5. Statistical data

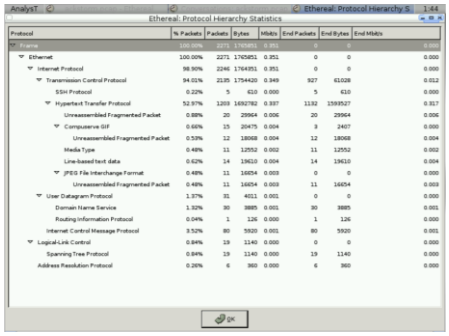
❑Statistical data – mô tả lưu lượng truy cập ví dụ như về giao thức mạng, thông lượng…

```
File name:           capiedit.pcap
File type:           Wireshark/tcpdump/... - libpcap
File encapsulation:  Ethernet
Packet size limit:   file hdr: 65535 bytes
Number of packets:   20
File size:           4406 bytes
Data size:           4062 bytes
Capture duration:    3 seconds
Start time:          Wed Jan 16 19:09:47 2013
End time:            Wed Jan 16 19:09:50 2013
Data byte rate:      1550.44 bytes/sec
Data bit rate:       12403.52 bits/sec
Average packet size: 203.10 bytes
Average packet rate: 7.63 packets/sec
SHA1:                e053c72f72fd9801d9893c8a266e9bb0bdd1824b
RIPEMD160:           8d55bec02ce3fcb277a27052727d15afba6822cd
MD5:                 7b3ba0ee76b7d3843b14693ccb737105
Strict time order:   True
```

31

5. Statistical data

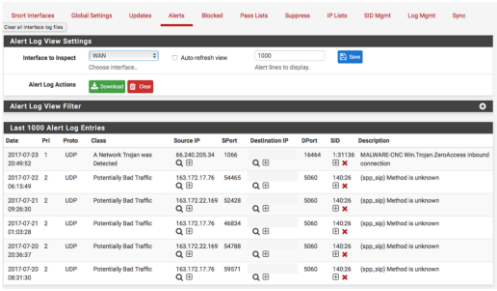
❑Statistical data



32

6. Alert/ Log Data

❑Alert/log data – cảnh báo, dữ liệu từ các thiết bị như Firewall, AV, IDPS, NSM tool…



33

1. Kiến trúc và thành phần
2. Dữ liệu thu thập
3. Phương pháp thu thập
4. Phát hiện xâm nhập

Một số vấn đề

1. Thiết kế Server/sensor như thế nào?
2. Thu thập dữ liệu như thế nào?
3. Thu thập dữ liệu ở đâu?
4. NTP?

35

Sensors và Server

❑ SIEM thường bao gồm server và sensor (agent)

- Sensor thực hiện thu tập dữ liệu
- Server tiếp nhận và xử lý

❑Đối với hệ thống đơn giản thì có thể chỉ cần 1 server và 1 sensor

❑Tuy nhiên đối với những hệ thống phức tạp có thể cần nhiều sensor để thu thập dữ liệu với gửi tới 1 server tập trung

36

Sensors và Server

❑**Thiết kế Server tập trung và nhiều sensor**

- Một vài dữ liệu (vd IDS alert) gửi về server
- Các dữ liệu khác (vd full packet capture) thì lưu lại trên mỗi sensors

❑**Security Onion**

- Dữ liệu gửi về server: NIDS alerts, OSSEC alerts, Bro HTTP logs
- Dữ liệu lưu lại trên sensor: Pcaps, Bro logs, Argus data và raw OSSEC logs

37

Một số vấn đề

1. Thiết kế Server/sensor như thế nào?
2. Thu thập dữ liệu như thế nào?
3. Thu thập dữ liệu ở đâu?
4. NTP?

38

Các mức thu thập dữ liệu

❑ Hub, SPAN ports, TAP để thu thập dữ liệu trung chuyển

- Thông tin dữ liệu trao đổi trong mạng.

❑ Phương pháp đẩy và kéo để thu thập dữ liệu nghỉ

- Dữ liệu nhật ký, sự kiện trên host.
- Dữ liệu nhật ký, sự kiện trên các thiết bị mạng.

39

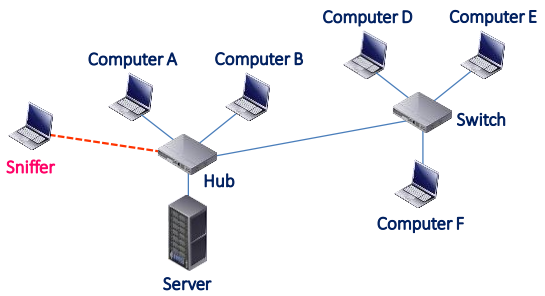
Phương pháp thu thập

❑Để tiến hành nghe lén lưu lượng truy cập yêu cầu thiết bị hỗ trợ "promiscuous" mode

❑Ba phương pháp phổ biến được sử dụng: **hubs**, **span/mirror ports** và **taps**

40

Hubs



41

Hubs

❑**Ưu điểm**

•Giá thành thấp

•Dễ dàng sử dụng

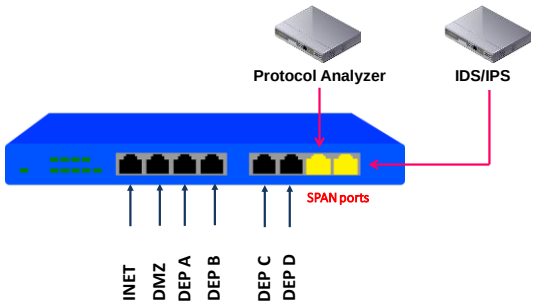
❑**Nhược điểm**

•Hạn chế tốc độ truyền dữ liệu (Hubs hoạt động ở half duplex sẽ làm giảm hiệu suất xuống 100 mbps)

•Dễ gây ra xung đột mạng, khi Hubs bị sự cố sẽ dẫn đến việc kết nối bị ngắt

42

Mirror ports



43

Mirror ports

❑**Ưu điểm**

•Tích hợp sẵn trên hầu hết các switch

•Chi phí tương đối rẻ (60$ - SOHO D-link 8 port gigabit)

•Có khả năng chuyển dữ liệu ở chế độ full duplex

44

Mirror ports

❑**Nhược điểm**

•Việc cấu hình SPAN port khá phức tạp

•Có thể xảy ra tình trạng mất gói khi cấu hình Mirror ports vì dữ liệu được gửi đến cổng giám sát cao hơn so với khả năng của cổng

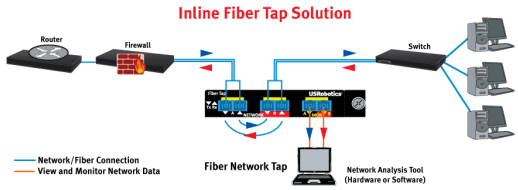
•Loại bỏ nhãn VLAN của gói tin, làm cho việc phân tích VLAN khó khăn hơn

•Một số nhà sx chỉ cung cấp khả năng cấu hình cho một hoặc hai cổng giám sát

•Gây quá tải cho switch, ảnh hưởng đến hoạt động của mạng

45

Network TAPs



46

Network TAPs

❑TAP là thiết bị dùng để sao chép dữ liệu giữa hai điểm trên hệ thống mạng (router-firewall, switch-switch, host-switch…)

❑Tất cả các gói tin được sao chép sẽ chuyển đến cổng giám sát

❑Đây là giải pháp tiên tiến nhất, kết hợp các ưu điểm của Hub và Mirror ports

47

Network TAPs

❑**Ưu điểm:**

•Có khả năng chuyển tiếp được các lỗi tầng vật lý

•Không cần phải cấu hình, dễ dàng kết nối

•Hỗ trợ tối đa khả năng sao chép dữ liệu ở tốc độ cao

•Độ trễ giữa các gói tin được giữ nguyên, hỗ trợ cho quá trình phân tích gói

•Không ảnh hưởng đến hiệu suất của switch

❑**Nhược điểm:**

•Kết nối bị ngắt khi thi công, lắp đặt

•Chi phí cao hơn so với Hubs và Mirroring port

48

Port Overload

❑**Mirror ports và taps có thể bị quá tải**

•Example: Gửi 7 100-megabit streams tới port 100-megabit == mất rất nhiều dữ liệu

❑**Tap buffers có thể làm giảm vấn đề này**

•Tuy nhiên port quá tải trong thời gian dài sẽ dẫn đến việc tiêu tốn tap buffer

•Luôn theo dõi việc sử dụng mirror ports và taps

49

Phương pháp đẩy (Push Method)

- Các sự kiện từ các thiết bị, máy trạm, máy chủ… sẽ được tự động chuyển về các Collector theo thời gian thực hoặc sau mỗi khoảng thời gian phụ thuộc vào việc cấu hình trên các thiết bị tương ứng.
- Collector của Log Server sẽ thực hiện việc nghe và nhận các sự kiện khi chúng xảy ra.

50

Phương pháp kéo (Pull Method)

- Các sự kiện được phát sinh và lưu trữ trên chính các thiết bị sẽ được lấy về bởi các bộ Collector.

51

Một số vấn đề

1. Thiết kế Server/sensor như thế nào?
2. Thu thập dữ liệu như thế nào?
3. Thu thập dữ liệu ở đâu?
4. NTP?

52

Umbrella Sensor

❑**DMZ**

❑**Internal**

•Umbrella

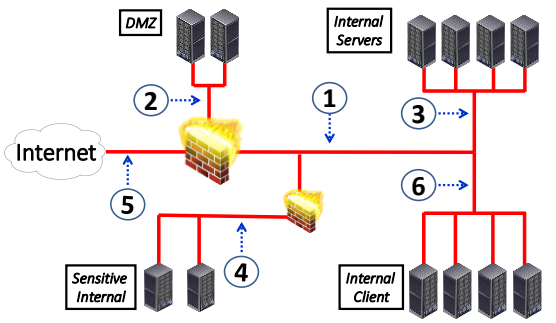
•Focused

❑**External**

•These tend to be used for attack awareness

53

Sensor Placement



54

Một số vấn đề

1. Thiết kế Server/sensor như thế nào?
2. Thu thập dữ liệu như thế nào?
3. Thu thập dữ liệu ở đâu?
4. NTP?

55

NTP

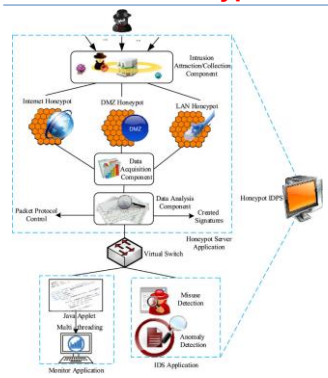
❑Các thiết bị giám sát cũng như hệ thống giám sát phải được đồng bộ với một đồng hồ thời gian tin cậy.

– Máy chủ NTP (Network Time Protocol) được sử dụng cho mục đích này.

– Tổ chức có thể tự xây dựng 1 NTP cục bộ hoặc sử dụng các máy chủ NTP miễn phí trên mạng internet.

56

Honeypot - Honeynet



❑Malware collector

❑SSH Honeypots

❑IoT Honeypots

❑Honeytokens

❑T-pot

Sinh viên tự nghiên cứu !!!

57

Kỹ thuật phát hiện xâm nhập

❑Phát hiện xâm nhập: là một chức năng của phần mềm thực hiện phân tích các dữ liệu thu thập được để tạo ra dữ liệu cảnh báo.

❑Cơ chế phát hiện xâm nhập gồm 2 loại chính:

– Dựa trên dấu hiệu

– Dựa trên bất thường

59

Kỹ thuật phát hiện xâm nhập

❑Cơ chế phát hiện dựa trên dấu hiệu

– Là hình thức lâu đời nhất của phát hiện xâm nhập

– Bằng cách duyệt qua dữ liệu để tìm các ra các kết quả khớp với các mẫu đã biết.

– Ví dụ: một địa chỉ IP hoặc một chuỗi văn bản, hoặc số lượng byte null…

– Các mẫu được chia thành các mẫu nhỏ độc lập với nền tảng hoạt động (dấu hiệu của tấn công)

– Mẫu được mô tả bằng ngôn ngữ cụ thể trong nền tảng của một cơ chế phát hiện xâm nhập, chúng trở thành dấu hiệu

– Có hai cơ chế phát hiện dựa trên dấu hiệu phổ biến là Snort và Suricata

60

Kỹ thuật phát hiện xâm nhập

❑Phát hiện dựa trên danh tiếng

- Là một tập con của phát hiện dựa trên dấu hiệu
- Phát hiện thông tin liên lạc giữa các máy tính được bảo vệ trong mạng và các máy tính trên Internet có thể bị nhiễm độc do đã từng tham gia vào các hành động độc hại trước đó
- Kết quả phát hiện dựa trên các dấu hiệu đơn giản như địa chỉ IP hoặc tên miền

61

Common Public Reputation Lists

- http://www.malwaredomainlist.com/
- http://www.phishtank.com/
- Tor Exit Node http://torstatus.blutmagie.de/
- Spamhaus http://www.spamhaus.org/drop/
- AlientVault Labs IP Reputation Database: http://labs.alienvault.com/labs/index.php/projects/open-source-ip-reputation-portal/
- MalC0de Database: http://malc0de.com/database/
- SRI Malware Threat Center http://www.mtc.sri.com/live_data/attackers/
- Project Honeypot: https://www.projecthoneypot.org/list_of_ips.php
- Emerging Threats Rules: http://www.emergingthreats.net/open-source/etopen-ruleset/

62

Kỹ thuật phát hiện xâm nhập

❑Phát hiện dựa trên bất thường

- Dựa vào quan sát sự cố mạng và nhận biết lưu lượng bất thường thông qua các chẩn đoán và thống kê.
- Có khả năng nhận ra các mẫu tấn công khác biệt với hành vi mạng thông thường.
- Đây là cơ chế phát hiện rất tốt nhưng khó thực hiện.
- Phổ biến với công cụ Bro. Bro là một cơ chế phát hiện bất thường, và thực hiện phát hiện bất thường dựa trên thống kê.

63

Kỹ thuật phát hiện xâm nhập

❑Phát hiện dựa trên honeypot

- Là tập con mới được phát triển của phát hiện dựa trên bất thường.
- Honeypot đã được sử dụng trong nhiều năm để thu thập phần mềm độc hại và các mẫu tấn công cho mục đích nghiên cứu.
- Honeypot có thể được ứng dụng tốt trong phát hiện xâm nhập bằng cách cấu hình hệ thống.
- Được cấu hình cho việc ghi lại dữ liệu, và thường được kết hợp với các loại khác của NIDS hoặc HIDS.

64

Dấu hiệu xâm nhập - IoC

- Indicators of Compromise – IoC: là những thông tin được sử dụng để mô tả khách quan một xâm nhập mạng, độc lập về nền tảng.
- Ví dụ: địa chỉ IP của máy chủ C&C, hay tập các hành vi cho thấy email server là SMTP relay độc hại.
- Được trình bày theo nhiều cách thức và định dạng khác nhau để có thể được sử dụng bởi các cơ chế phát hiện khác nhau.
- Nếu được sử dụng trong một ngôn ngữ hoặc định dạng cụ thể => trở thành một phần của một dấu hiệu.
- Một dấu hiệu có thể chứa một hoặc nhiều IOC.

65

Dấu hiệu xâm nhập – IOC

❑IOC cho mạng:

- Là một mẫu thông tin có thể được bắt trên kết nối mạng giữa các máy chủ, mô tả khách quan một xâm nhập.
- Ví dụ: địa chỉ IPv4, địa chỉ IPv6, tên miền, chuỗi văn bản, giao thức truyền thông,…

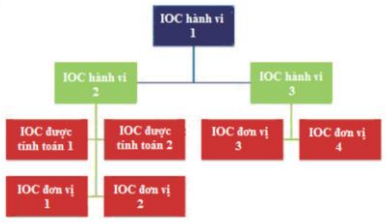
❑IOC cho máy tính

- Là một mẫu thông tin được tìm thấy trên một máy tính, mô tả khách quan một xâm nhập.
- Ví dụ: tài khoản người dùng, đường dẫn thư mục, tên tiến trình, tên tệp tin, khóa đăng ký (registry), …

66

Static Indicators

- Là những IOC mà giá trị được định nghĩa một cách rõ ràng.
- Có ba biến thể của IOC tĩnh: đơn vị, tính toán và hành vi.



67

IOC example

- Người dùng nhận được một e-mail từ chris@appliednsm.com với chủ đề "Thông tin tiền lương" và một tệp PDF đính kèm là "Payroll.pdf". Tệp PDF có một giá trị băm MD5 là e0b359e171288512501f4c18ee64a6bd .
- Người dùng mở tệp PDF, kích hoạt việc tải một tệp tin gọi là kernel32.dll với MD5 là da7140584983eccde51ab82404ba40db. Tệp tin được tải về từ http://www.appliednsm.com/kernel32.dll
- Tệp tin được dùng để ghi đè lên C:/Windows/System32/kernel32.dll.
- Mã trong DLL được thực thi, và một kết nối SSH được thiết lập tới một máy chủ có địa chỉ IP là 216.12.24.75 trên cổng 9966.
- Khi kết nối này được thiết lập, phần mềm độc hại tìm kiếm mọi tệp DOC, DOCX, hoặc PDF trên máy trạm và gửi ra ngoài.

68

IOC example

Phân tích các dấu hiệu thành các phần nhỏ có ích hơn, như các IOC hành vi (B) như sau:

- B-1: Người dùng nhận được một e-mail từ chris@appliednsm.com với chủ đề "Thông tin tiền lương" và một tệp PDF đính kèm là "Payroll.pdf", có một giá trị băm MD5 là e0b359e171288512501f4c18ee64a6bd.
- B-2: Tệp tin kernel32.dll với hàm băm MD5 da7140584983eccde51ab82404ba40db được tải về từ http://www.appliednsm.com/kernel32.dll.
- B-3: Tệp tin C:/Windows/System32/Kernel32.dll bị ghi đè bởi một tệp tin độc hại cùng tên với giá trị hàm băm MD5 da7140584983eccde51ab82404ba40db.
- B-4: Máy tính nạn nhân cố gắng kết nối qua SSH tới máy tính nguy hiểm bên ngoài 216.12.24.75 trên cổng 9966.
- B-5: Các tệp tin DOC, DOCX, và PDF được truyền tới 216.12.24.75.

69

IOC example

- Tiếp tục phân tích IOC hành vi thành các IOC đơn vị (A) và IOC được tính toán (C):
  - C-1: MD5 Hash e0b359e171288512501f4c18ee64a6bd
  - C-2: MD5 Hash da7140584983eccde51ab82404ba40db
  - A-1: Tên miền nguy hiểm: appliednsm.com
  - A-2: Địa chỉ e-mail địa chỉ: chris@appliednsm.com
  - A-3: Tiêu đề thư: "Thông tin tiền lương"
  - A-4: Tên file: Payroll.pdf
  - A-5: Tên file: Kernel32.dll
  - A-6: IP nguy hiểm 216.12.24.75
  - A-7: Cổng 9966
  - A-8: Giao thức SSH
  - A-9: Kiểu file DOC, DOCX, PDF

70

IOC example

IOC được chuyển đổi thành các dấu hiệu để sử dụng trong một loạt các cơ chế phát hiện:

C-1/2: Chữ ký chống vi-rút để phát hiện sự tồn tại của giá trị băm

A-1: Chữ ký Snort/Suricata để phát hiện kết nối với tên miền nguy hiểm

A-2: Chữ ký Snort/Suricata để phát hiện thư nhận được từ địa chỉ e-mail nguy hiểm

A-3: Chữ ký Snort/Suricata để phát hiện dòng chủ đề

A-3: Bro script để phát hiện dòng chủ đề

71

IOC example

IOC được chuyển đổi thành các dấu hiệu để sử dụng trong một loạt các cơ chế phát hiện:

- A-4/C-1: Bro script để phát hiện tên tệp tin hay giá trị băm MD5 được truyền trên mạng
- A-5/C-2: Bro script để dò tìm tệp tin có tên là Kernel32.dll hoặc tệp tin với giá trị băm MD5 truyền qua mạng
- A-6: Chữ ký Snort/Suricata để phát hiện thông tin liên lạc với địa chỉ IP
- A-7/A-8: Chữ ký Snort/Suricata để phát hiện thông tin liên lạc SSH đến cổng 9966
- A-10: Luật HIDS để phát hiện những thay đổi của Kernel32.dll

72

IOC example

- IOC được chuyển đổi thành các dấu hiệu để sử dụng trong một loạt các cơ chế phát hiện:
  - A-4/C-1: Bro script để phát hiện tên tệp tin hay giá trị băm MD5 được truyền trên mạng
  - A-5/C-2: Bro script để dò tìm tệp tin có tên là Kernel32.dll hoặc tệp tin với giá trị băm MD5 truyền qua mạng
  - A-6: Chữ ký Snort/Suricata để phát hiện thông tin liên lạc với địa chỉ IP
  - A-7/A-8: Chữ ký Snort/Suricata để phát hiện thông tin liên lạc SSH đến cổng 9966
  - A-10: Luật HIDS để phát hiện những thay đổi của Kernel32.dll

73

Variable Indicators

- Cần phải coi IOC là các biến, trong đó có những dấu hiệu chưa biết giá trị => để tổng quát hóa cuộc tấn công
- Biến IOC hữu ích trong các giải pháp phát hiện bất thường như Bro

74

Variable Indicators

- Kịch bản tấn công lý thuyết:

1. Người dùng nhận được một e-mail với một tệp tin đính kèm độc hại.
2. Người dùng mở tệp tin đính kèm, kích hoạt việc tải tệp tin từ một tên miền độc hại.
3. Tệp tin được dùng để ghi đè lên một tệp tin hệ thống với phiên bản mã độc của tệp tin đó.
4. Mã trong các tệp tin độc hại thực thi, gây ra một kết nối mã hóa đến một máy chủ độc hại.
5. Sau khi kết nối được thiết lập, một số lượng lớn dữ liệu sẽ bị rò rỉ từ hệ thống.

75

Variable Indicators

- Một số IOC hành vi:
  - VB-1: Một người dùng nhận được một e-mail với một tệp tin đính kèm độc hại.
  - VA-1: Địa chỉ e-mail
  - VA-2: Tiêu đề e-mail
  - VA-3: Tên miền nguồn của e-mail độc hại
  - VA-4: Địa chỉ IP nguồn của e-mail
  - VA-5: Tên tệp tin đính kèm độc hại
  - VC-1: Tệp tin đính kèm độc hại với giá trị băm MD5
  - VB-2: Người dùng mở tệp tin đính kèm, kích hoạt việc tải một tệp tin từ một tên miền độc hại.
  - VA-6: Tên miền/IP chuyển hướng độc hại
  - VA-7: Tên tệp tin độc hại đã tải

76

Variable Indicators

- Một số IOC hành vi:
  - VC-2: Giá trị băm MD5 của tệp tin độc hại đã tải
  - VB-3: Tệp tin được sử dụng để ghi đè lên một tệp tin hệ thống với phiên bản mã độc của tệp tin đó.
  - VB-4: Thực thi mã trong tệp tin độc hại, tạo ra một kết nối mã hóa đến một máynchủ độc hại trên một cổng không chuẩn.
  - VA-8: Địa chỉ IP C2 ngoài
  - VA-9: Cổng C2 ngoài
  - VA-10: Giao thức C2 ngoài
  - VB-5: Sau khi kết nối được thiết lập, một số lượng lớn các dữ liệu đã bị rò rỉ từ hệ thống.

77

Variable Indicators

- Kết hợp các IOC đơn vị, tính toán và hành vi để tạo thành dấu hiệu:
  - VB-1 (VA-3/VA-4) VB-2 (VA-6) VB-4 (VA-8) VB-5 (VA-8): Luật Snort/Suricata để phát hiện các liên lạc với danh tiếng xấu theo địa chỉ IP và tên miền.
  - VB-1 (VA-5/VC-1) VB-2 (VA-7/VC-2): Bro script để kéo các tệp tin từ đường truyền và so sánh tên của chúng và các giá trị băm MD5 với một danh sách các tên tệp tin danh tiếng xấu được biết đến và các giá trị băm MD5.
  - VB-1 (VA-5/VC-1) VB-2 (VA-7/VC-2): Bro script để lấy các tệp tin từ đường truyền và đặt chúng vào trong thử nghiệm phân tích phần mềm độc hại sơ bộ.

78

Variable Indicators

❑Kết hợp các IOC đơn vị, tính toán và hành vi để tạo thành chữ ký:

• VB-2 (VA-6/VA-7/VC-2): chữ ký HIDS để phát hiện các trình duyệt đang được gọi từ một tài liệu.

• VB-3: chữ ký HIDS để phát hiện một tệp tin hệ thống đang bị ghi đè

• VB-4 (VA-9/VA-10) VB-5: Bro script để phát hiện mã hóa lưu lượng đang xảy ra trên một cổng không chuẩn

• VB-4 (VA-9/VA-10) VB-5: một luật Snort/Suricata để phát hiện mã hóa lưu lượng đang xảy ra trên một cổng không chuẩn

• VB-5: script tự viết sử dụng thống kê dữ liệu phiên để phát hiện khối lượng lớn lưu lượng gửi đi từ máy trạm

79

Quản lý IoCs và dấu hiệu

❑Số lượng IoCs và dấu hiệu được quản lý bởi 1 tổ chức có thể phát triển nhanh chóng

– Ví dụ: sử dụng Snort để phát hiện và ghi nhật ký các truy cập vào một tên miền độc hại (IOC đơn vị), thì sau đó các IOC sẽ được lưu thành dấu hiệu Snort, được truy cập trực tiếp bởi Snort

– Điều đó làm ngăn cản sự chia sẻ hoặc chuyển đổi IoCs sang dấu hiệu được thiết kế cho cơ chế phát hiện khác

❑Cần phải có chiến lược lưu trữ, truy cập, quản lý và chia sẻ chúng

80

Indicator/Signature List

GUID	Author	Creation Date	Modified Date	Revision	Source	Classification	Type	Life Cycle Stage	Confidence	Indicator	Deployment
10001	Sanders	3/17/2013	3/20/2013	2	Case # 1492	MD5	Computed/ Static	Mature	Very High	e0b359e1712 8851250114c 18ee64a6bd	Antivirus Signature 42039
10002	Smith	3/18/2013	3/18/2013	1	Malware Domain List	Domain	Atomic/ Static	Mature	Moderate	appliednsm.com	Snort Signature 7100031
10003	Sanders	3/18/2013	3/18/2013	1	Case # 1498	E-Mail Address	Atomic/ Static	Mature	Very High	chris@appliednsm.com	Snort Signature 7100032
10004	Sanders	3/19/2013	3/19/2013	1	Zeus Tracker	IP	Atomic/ Static	Mature	High	192.0.2.99	Custom SLIK Script
10005	Randall	3/20/2013	3/24/2013	4	Analyst	Protocol/Port	Behavioral/ Variable	Immature	Moderate	Encrypted Traffic over Non-Standard Port	Bro Script
10006	Sanders	3/20/2013	3/20/2013	1	RSS Feed	Protocol/Port	Behavioral/ Static	Mature	Moderate	SSH/9966	Suricata Signature 7100038
10007	Sanders	3/21/2013	3/24/2013	3	Internal Discussion	Statistical	Behavioral/ Variable	Immature	Low	Outbound Traffic Volume Ratio Greater than 4:1	Custom SLIK Script

82

Indicator and Signature Framework

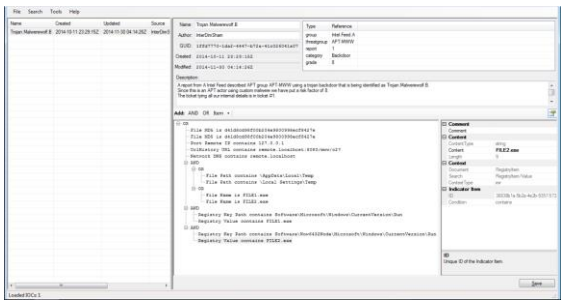
❑OpenIOC

– Dự án của Mandiant dùng để mô tả các đặc điểm kỹ thuật xác định các hoạt động tấn công và được viết bằng XML

– Có thể làm việc với định dạng này bằng công cụ OpenIOC Editor miễn phí của Mandiant

83

IOC metadata



84

Indicator and Signature Framework

❑STIX (Structured Threat Information eXpression)

– Được phát triển mới MITRE cho US Department of Homeland Security để chuẩn hóa thông tin TI

– Thường được sử dụng cho quân đội và chính phủ

– Có thể tìm hiểu thêm tại http://stix.mitre.org

85


QUESTION