AFRICA INTERNET SUMMIT'14
25 May - 6 June - Djibouti

AfNOG

AAF

JPCERT CC®

Network Forensics Training For CSIRT engineer

Koichiro (Sparky) Komiyama
Toru Yamauchi
From JPCERT Coordination Center

Agenda

- Basics
  - What is “Network Security Analysis”?
  - How is it useful for your security activities?
- Tools
  - Packet capture
  - Packet analysis
- Exercises
  - Using mostly Wireshark
  - Should be fun☺

Knowledge that will be useful

- Basic understanding of TCP/IP and major application protocols
- Basic understanding of Virus, Worms and Malware
- How to use or have at least seen Wireshark

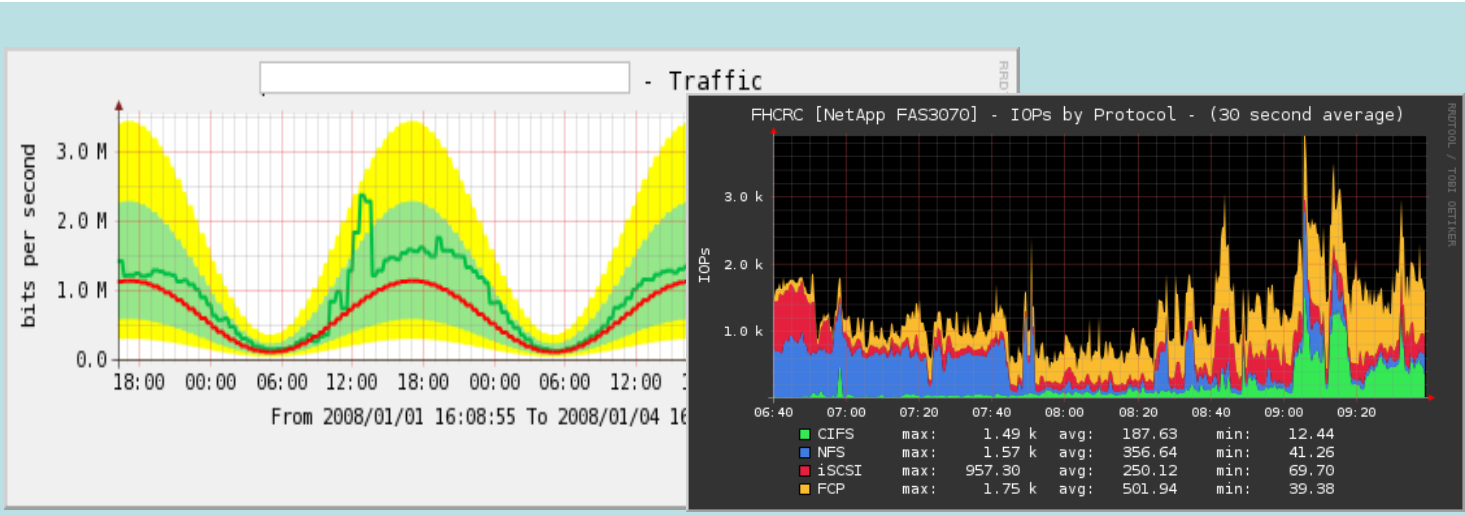
BASICS

What is Network Security Analysis?

- "Network Analysis" for Security
  - important activities for incident responders and security analysts
- Related to many security activities
  - Network monitoring
    - To detect an on-going incident
  - Network forensics
    - To find evidence in the specific incident
    - To recover a system
  - Malware analysis
    - To discover the capability of a malware
      - sending important data to a malicious server
      - bot command & control

Network Security Analysis – Flow based

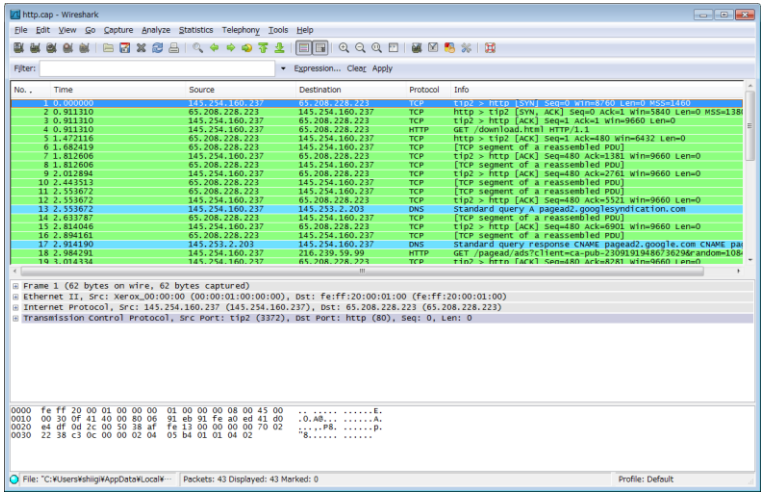
- Features
  - Focus on network flow/traffic instead of each packet
  - Good approach to get high level overview or ‘gist’
- Tools / Techniques
  - Netflow / sFlow
  - MRTG/RRDTool
  - etc…



Network Security Analysis
- Packet Based (1) summary

- Features
  - Focus on each packet or a group of packets
  - Can analyze thoroughly but high cost (time)

- Tools / Techniques
  - tcpdump
  - Wireshark / tshark
  - etc…



WIRESHARK
Network Protocol Analyzer

- **Main Focus of this training☺**

Network Security Analysis - Packet Based (2) How to

- Capturing packet
  - Not recommend to use Wireshark for packet capturing
  - It is recommended to avoid running Wireshark with root privileges

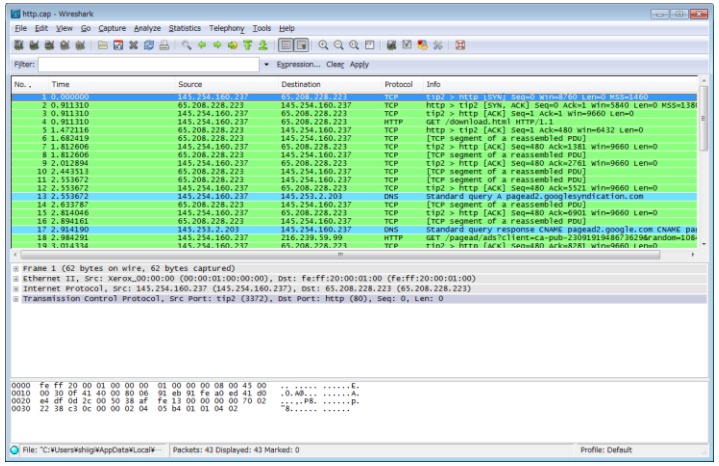
  - Use a more simple program instead
    - e.g. tcpdump, dumpcap

- Analyze packet
  - Wireshark can become your best friend for this purpose
  - **Main focus of this training☺**

Wireshark

About Wireshark

- Free !!
- Runs on many OSs
  - Windows / Linux / *BSD / Solaris and others
- User Interface
  - GUI – 3pane (Packet list / Packet details / Packet Bytes)
  - CUI version : tshark
- Many features
  - Search / Filter / Colorize / Statistics and many others
- Latest: 1.6.1
  - Released July 18, 2011
- Vulnerabilities in Wireshark
  - http://www.wireshark.org/security/



WIRESHARK
Network Protocol Analyzer

Some features of Wireshark that will be used in the exercises.

- "Analyze" => "Follow TCP Stream"
  - See data from a TCP stream in the way the application layer sees it. Very handy tool for looking at data streams.
- "Statistics" => "Conversations"
  - A tabbed window separated by protocol, shows statistics for each protocol. Amount of data, time, etc. is shown here.
- Filters
  - Filters come in handy when you want to see one aspect of the capture. Maybe you want to see just packets originating from a certain port.

** Using a combination of the above features should allow you to solve most of the exercises that follow ☺

Sample filters

- tcp.port==443
  - TCP connections with source or destination port of 443
  - Adding source / destination option can be done by tcp.srcport / tcp.dstport
- tcp.flags.syn==1
  - TCP SYN packets
  - Above will also include ACK packets, to remove ACK packets add tcp.flags.ack==0 using &&
- ip.src==10.0.0.12
  - Connections with source IP 10.0.0.12
  - Changing “src” to “dst” will change to destination IP
- Combinations of the above are possible using:
  - “||” – or, “&&” – and
  - Ex: ip.src==10.0.0.12 && tcp.dstport==80

Set-up

Analysis environment for the exercises

- Attention!!
  - Some pcap files for exercises include malicious data.
  - These files or data may trigger your anti-virus detection
  - Using a virtual environment is recommended
    - e.g VirtualBox / VMware
- Recommendations
  - Wireshark + Supplementary tools (base64 decoder, etc.)

Exercises

Part 1
Basic

Exercise1

Good Old Telnet

Good Old Telnet

- File
  - 01-telnet.pcap
- Question
  - Reconstruct the telnet session.
    - Q1. 192.168.0.1 is a telnet _____.
      192.168.0.2 is a telnet _____.
    - Q2: Who logged into 192.168.0.1 ?
      - Username _____, Password _____ .
    - Q3: After logged in what did the user do?

Exercise 2

Massive TCP SYN

Massive TCP SYN

- File
  - 02-massivesyn1.pcap
  - 02-massivesyn2.pcap
- Question
  - Point out the difference in the two captures.
  - Q1:02-massivesyn1.pcap
    is a _____ attempt.
  - Q2: 02-massivesyn2.pcap
    is a _____ attempt.
- Tip
  - Pay attention to Src IP and Dst Port

Exercise 3

Chatty Employees

Chatty Employees

- File
  - 03-chat.pcap
- Question
  - Q1: What protocol is being used? _____
  - Q2: This is conversation between _____@hotmail.com and _____@hotmail.com
  - Q3: What do they say about you (sysadmin)?
- Tip
  - Your chat log can be monitored by network admin.

Exercise 4

Suspicious FTP activity

Suspicious FTP activity

- File
  - 04-ftp1.pcap
- Question
  - Q1: FTP server's IP address is ___.___.___.___ .
  - Q2: FTP client's IP address is ___.___.___.___.
  - Q3: FTP Err Code 530 means _____ .
  - Q4: 10.234.125.254 is attempting to _____.
- Tip
  - How many login errors are allowed within a minute?

Exercise 5

Unidentified Traffic

Unidentified Traffic

- File
  - 05-Foobar.pcap
- Question
  - Q1: Which application uses TCP/6346?
  - Q2: How many servers was 10.1.4.176 trying to connect to?
  - Q3: Which machines could 10.1.4.176 successfully connect to (at least at the TCP/IP level)?

Exercise 6

Comparing traffic

Comparing traffic

- Scenario
  - You're an IT admin of company X. You get a report that Jim (a new employee) can not browse or email with his laptop. After researching, you found that Risa, sitting next to Jim, can brose without any problem.
- File
  - 06-Risa.pcap
  - 06-Jim.pcap
- Question
  - Compare the capture files from both machines and find out why Jim's machine is not online.
  - Jim must _____
- Tip
  - Pay attention to the first ARP packet.

Part2
Advanced

Exercise 7

Behind the scenes…

Behind the scenes…

- File
  - 07-arp.pcap
- Question
  - Q1: What is the attacker's IP address and MAC address?
  - Q2: What is the direct victim's IP address and MAC address?
  - Q3: What is the victim's role in this network?
  - Q4: What type of packet was malicious in this attack?
  - Q5: What type of attack was happening?
  - Q6: Was this attack successful or not?
  - Q7: What kind of countermeasures may be useful for this attack?

Exercise 8

Someone is already in…

Someone is already in…

- Scenario
  - Alice is a web master. The other day, she browsed several web sites using the same PC for document uploading. Unfortunately one of sites which she visited was defaced and her PC was infected with malware but she was unaware of the infection.
- File
  - 08-gumblar1.pcap
- Question
  - Q1: What is the malicious server's IP address?
  - Q2: What kind of malicious activity did this malware perform?

Exercise 9

Something is stolen…

Something is stolen…

- Scenario
  - Alice cleaned up her pc from infection. But unfortunately, her PC was re-infected by a different malware. This malware seems to be sending some information
- File
  - 09-gumblar2.pcap
- Question
  - Q1: Malicious server's IP address is ___.___.___.___
  - Q2: Data sent by malware includes:
    - (1)____, (2)____, (3)____, (4)_____

Exercise 10

Aurora

Aurora

- Scenario
  - One day, you discovered suspicious activity in your network. It looks like someone was infected by a web-based attack.
- File
  - 10-aurora.pcap
- Question
  - Q1: Which site and which page was defaced?
  - Q2: Which URL looks malicious?
  - Q3: Which software seemed to be the target of this exploit?
  - Q4: What kind of malicious activity was executed after the exploit?

Exercise 11

SSL Storm?

SSL storm?

- Scenario
  - One day you discovered one client in your network has sent many packets outbound from your network via 443/tcp.
- File
  - 11-massive443.pcap
- Question
  - Q1: How many sites did this client send packets to?
  - Q2: Which TCP port did this client send packets other than using 443/tcp?
  - Q3: Which protocol seemed to be used for the session via the port in Q2?
  - Q4: Are there any differences between packets sent via 443/tcp in this pcap and normal SSL?
    - Please compare to 11-normalssl.pcap
    - Please ignore SSL version difference.

Exercise 12

Zero and Infinite

Zero and Infinite (1)

- Scenario
  - One day you are claimed by a user that he couldn't connect the organization's web server. Soon after this, you confirmed the situation, the web server couldn't any reply to requests. You need to identify and solve the problem before you get a flood of claims.

- File
  - 12-zerowindow.pcap

Zero and Infinite (2)

- Question
  - Apply the following display filter: (Just a filtering test!!)
    - Conversation between 10.0.0.12:14856 and 10.0.0.101:80
  - Q1: What does the TCP ZeroWindow mean?
  - Q2: How many TCP ZeroWindow packets were used in this attack?
  - Q3: What is the maximum speed (bps) in this attack? Is it relatively high or low?
  - Q4: Why is 10.0.0.101 sending several Keep-Alive packets after receiving TCP ZeroWindow announcement?
  - Q5: How many sessions are finished or terminated during this attack?
  - Q6: Why could not the client get a reply from the server during this attack?
  - Q7: What type (or class) of attack has occurred?
  - Q1

Exercise 13

Don’t ask me

Don’t ask me

- File
  - 13-dns.pcap
- Question
  - Q1: How big is the DNS reply packet?
  - Q2: Which machines are the victims?
  - Q3: What is the role of the DNS servers in this attack?
  - Q4: What type of packet triggered the problem?
  - Q5: What type of attack was happening here?
  - Q6: What kind of countermeasures may be effective for this attack?

Bonus Exercise

Bonus Exercise

- File
  - 20-gumblar-all.pcap
- Question
  - Analyze the pcap file and reconstruct the incident
    - What kind of sites are related to this incident
    - Identify the role of each sites
    - Reconstruct attack scenario (Provide a network diagram)
- Tips
  - Please use knowledge you used for Exercise 8 & 9 again.