Imaging/Restore

Disk to Disk = simulation

**What may be true for one network, may not be true for another**

Http lets you know when the data starts by 0D 0A 0D 0A

network ada 2

1- Log

2- Traffic

Q1

-

Q2 Tools

- Sysinternals

- WireShark

-

After watching the video, I had learned today about performing network forensics using tools such as Wireshark. Network Forensics is the capture, recording and analysis of network events to discover the source of security attacks or other problem incident. Wireshark can be used to analyse network packets.

Pcap Analysis Methodology

1. Pattern Matching
2. List conversations
3. Isolate and Export
4. Draw conclusions

Network Forensic – Malware

What are we looking for?

1. Where the user contracted the malware from?
2. Malware file (can we assemble it?)
3. What kind of calls to the internet does it make
4. Does it try to self-propagate through the internet network? (is it a worm or a virus?)
5. Possible network traffic signatures

Scenario 1

Malware

* Look for malware using Wireshark and pcap file
* Follow TCP stream on suspicious packet
* check file header and look it up in file signature database
* Check the focused traffic from server to the client
* Show and save data as Raw
* Delete the header of the packet
* get the hash
* filter and find traffic with tcp.stream 5
* Check the packet’s port

The origin of attack

* puskovayaustanovka.ru/pusk.exe
* No User-Agent

Calls

* Seemingly random DNS queries
* Rapid connection attempts to resolved DNS names
* Eventually connects to a web page on port 80 to one of the servers

Does it try to self-propagate through the internal network?

* No connection attempts to RFC 1918, or other 12.x addresses

Possible Network traffic signatures

* We have the DNS names
* High volume of DNS queries followed by high volume of port 80 connection attempts

Where did the user contract the malware from?

* User made a direct call to the executable. Therefore, user either deliberately downloaded the malware, or there was a piece of malware sleeping on the system.

Calls

* DNS queries for a number of domains
* HTTP communication for web sites located on a few of those domains

Does it try to self-propagate

* No communication to other internal addresses

Network traffic signatures

* High volume of DNS queries within a short amount of time

Case Scenario

* User downloaded a malware, or there was a piece of malware sleeping in the system
* The malware made a number of DNS queries within a short amount of time
* User was directed to a fake antivirus website

Network Forensic – DoS attack

What are we looking for?

1. What events led up to the attack on the FTP server?
2. What types of attacks did the attacker perform on the FTP server?
3. What were the results of those attacks? (e.g. Did they login, what did they find, were files stolen, etc.?)

Scenario 2

DoS Attacks

* Click statistics, and conversation (See exactly how many IP addresses we’re dealing)
* check arp.opcode == 2 (filter down to arp reply)
* filter out arp traffic
* Filter the packets by SYN, ACK (tcp.flags ==0x012)
* Because FTP server, filter out port 21 !(tcp.port == 21)
* Filter port 21
* follow one of stream
* check google for ftp code for login success (230)
* filter logged in ([ftp.response.code](ftp://ftp.response.code) == 230)
* carve the png and take the hash

Events led up to the attack on the FTP server

* Arp scan; devices located:
* 192.168.56.1
* 192.168.56.100
* 192.168.56.101
* SYN scan:
* 21
* 445
* 139
* 135
* 49154
* 49152
* 49156
* 49153
* 49155

What were the results of those attacks?

* Attacker logged in with “Anon/anon”
* They listed the directories and downloaded a png

Investigation results