What Does It Take To Be A 1337 Cyber Analyst?

Presented by: Lorna Hutcheson

SANS Internet Storm Center

18 July 2018

Email: Lorna.Hutcheson@isc.sans.edu
Agenda

- Introduction
- Loss of Fundamental Skills
- Examples
- Path Forward
Cyber Analyst

YOU KEEP USING THAT WORD

I DON'T THINK IT MEANS WHAT YOU THINK IT MEANS
What Does the Trend Look Like?
Agenda

- Introduction
- Loss of Fundamental Skills
- Examples
- Path Forward
Ten Key Points for Intrusion Analysts

8. Analysis is no more about tcpdump than astronomy is about a telescope.

• Whenever I interview someone for any analyst position that’s above entry level I always ask them to describe how they would investigate a typical IDS alert. I get frustrated when someone gives answers along the lines of “I use Tcpdump, Wireshark, Network Miner, Netwitness, Arcsight, Xeyes, etc” with no further clarification. Although their are processes and sciences in intrusion analysis, intrusion analysis itself is not a process or a science, but rather an art. If this wasn’t the case then it wouldn’t even be necessary to have humans in the loop when it comes to intrusion detection. An effective analyst has to understand that while different tools may be the most important part of the job, those things are merely pieces of the puzzle.

• http://chrissanders.org/2011/01/the-10-commandments-of-intrusion-analysis
Some Things NEVER Change

An Introduction to Learning About Network Security

INDEX

Before You Begin
Security Terms
ISO/OSI Model and the TCP/IP Model
Networking Basics
Network Protocols
Network Security Tools
Antivirus Protection
Securing the Operating System
MISC links

Before You Begin

• https://isc.sans.edu/presentations/first_things_first.html
Skill Set Needed?

• What skills do we need to have?

• Example: In addition to required education or equivalent experience
  * 4 years Information technology
  * 2 years network security analysis using intrusion detection systems
  * Packet-level Analysis
  * Intrusion Analysis
  * Troubleshooting
  * Oral and Written Communications
  * TCP/IP
Why These skills?

• Why study this stuff?
  – Network traffic is sent in binary form
  – We look at computer communications
  – We have to speak computer
  – We need to learn normal
  – The bad guys are studying it
  – Cannot be an effective analyst without it
Bad Guys Have A Structured Methodology
OSI Model

The data is broken into "chunks" of a suitable size ...

... pointed to the correct remote port or process, ...

... running on the correct host, ...

... and addressed correctly for the next hop on the local network.
<table>
<thead>
<tr>
<th>Byte Offset 0</th>
<th>Byte Offset 1</th>
<th>Byte Offset 2</th>
<th>Byte Offset 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port Number (16-bit)</td>
<td>Destination Port Number (16-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte Offset 4</td>
<td>Byte Offset 5</td>
<td>Byte Offset 6</td>
<td>Byte Offset 7</td>
</tr>
<tr>
<td>Sequence Number (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte Offset 8</td>
<td>Byte Offset 9</td>
<td>Byte Offset 10</td>
<td>Byte Offset 11</td>
</tr>
<tr>
<td>Acknowledgement Number (32-bit)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte Offset 12</td>
<td>Byte Offset 13</td>
<td>Byte Offset 14</td>
<td>Byte Offset 15</td>
</tr>
<tr>
<td>Hdr Length (4-bit)</td>
<td>Reserved (4-bit)</td>
<td></td>
<td>Window Size (16-bit)</td>
</tr>
<tr>
<td>Byte Offset 16</td>
<td>Byte Offset 17</td>
<td>Byte Offset 18</td>
<td>Byte Offset 19</td>
</tr>
<tr>
<td>Checksum (16-bit)</td>
<td></td>
<td>Urgent Pointer (16-bit)</td>
<td></td>
</tr>
<tr>
<td>Byte Offset 20</td>
<td>Byte Offset 21</td>
<td>Byte Offset 22</td>
<td>Byte Offset 23</td>
</tr>
<tr>
<td>TCP Options (variable...if any)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>data (variable....)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Where Do I Look First?
Agenda

- Introduction
- Loss of Fundamental Skills
- **Examples**
- Path Forward
Network Traffic
What Do You See?
What is Wrong with this Picture?

[Diagram showing a network with echo request and echo response, indicating a UDP attack.]
## Log Example 1

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.727514</td>
<td>220.106.53.75</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.728334</td>
<td>220.106.53.76</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.728896</td>
<td>220.106.53.96</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.728960</td>
<td>220.106.53.97</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.729024</td>
<td>220.106.53.106</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.729202</td>
<td>220.106.53.78</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.729859</td>
<td>220.106.53.111</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.729911</td>
<td>220.106.53.99</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
<tr>
<td>17.730290</td>
<td>220.106.53.128</td>
<td>aaa.bbb.ccc.ddd</td>
<td>ICMP</td>
<td>(Port unreachable)</td>
</tr>
</tbody>
</table>
Log Example 2

Jun 9 03:05:48 a1-33-251-204b 727186: 3w4d: %SEC-6-IPACCESSLOGP: list 120 denied udp 192.228.79.201(53) -> 204.251.33.4(3164), 1 packet
Jun 9 03:05:49 a1-33-251-204b 727187: 3w4d: %SEC-6-IPACCESSLOGP: list 120 denied udp 192.5.5.241(53) -> 204.251.33.4(3164), 1 packet
Jun 9 03:05:52 a1-33-251-204b 727189: 3w4d: %SEC-6-IPACCESSLOGP: list 120 denied udp 198.32.64.12(53) -> 204.251.33.4(3164), 1 packet
Jun 9 03:05:53 a1-33-251-204b 727190: 3w4d: %SEC-6-IPACCESSLOGP: list 120 denied udp 198.41.0.4(53) -> 204.251.33.4(3164), 1 packet
Jun 9 03:05:57 a1-33-251-204b 727192: 3w4d: %SEC-6-IPACCESSLOGP: list 120 denied udp 202.12.27.33(53) -> 204.251.33.4(3164), 1 packet
Jun 9 03:06:00 a1-33-251-204b 727194: 3w4d: %SEC-6-IPACCESSLOGP: list 120 denied udp 192.36.148.17(53) -> 204.251.33.4(3164), 1 packet
Jun 9 03:06:05 a1-33-251-204b 727195: 3w4d: %SEC-6-IPACCESSLOGP: list 120 denied udp 198.41.0.4(53) -> 204.251.33.4(3164), 1 packet
Log Example 3

10:03:47.209149 83.102.166.58 > XX.XXX.XX.XX: udp (frag 27932:25@512) (ttl 53, len 45)
10:04:01.241719 83.102.166.22 > XX.XXX.XX.XX: udp (frag 49984:25@512) (ttl 53, len 45)
10:04:04.712113 83.102.166.217 > XX.XXX.XX.XX: udp (frag 54586:25@512) (ttl 53, len 45)
10:04:17.808917 83.102.166.46 > XX.XXX.XX.XX: udp (frag 57688:25@512) (ttl 53, len 45)
10:04:30.858383 83.102.166.54 > XX.XXX.XX.XX: udp (frag 59613:25@512) (ttl 53, len 45)
10:04:35.341727 83.102.166.46 > XX.XXX.XX.XX: udp (frag 21191:25@512) (ttl 53, len 45)
10:04:40.270574 83.102.166.24 > XX.XXX.XX.XX: udp (frag 55441:25@512) (ttl 53, len 45)
10:04:50.272134 83.102.166.43 > XX.XXX.XX.XX: udp (frag 63235:25@512) (ttl 53, len 45)

0x0000  4500 002d f703 0040 3511 0972 5366 a62b        E..-...@5..rSf.+  
0x0010  XXXX XXXX 11ef 0035 0019 f294 71f7 0100        ?nL....5....q...  
0x0020  0001 0000 0000 0000 0000 0200 0100 ..............
Log Example 4

08:24:29.089688 IP (tos 0x0, ttl 45, id 1, offset 0, flags [none], proto 6, length: 64, bad checksum 5efc ->8db8) 0.0.0.0.2347 > 0.0.0.0.domain: S [bad tcp checksum 5b8e ->8a4a] 1047189198:1047189222(24) win 2048 0 [0q] (22)
08:24:29.186343 IP (tos 0x0, ttl 45, id 2, offset 0, flags [none], proto 6, length: 64, bad checksum 5efb ->8db7) 0.0.0.0.2351 > 0.0.0.0.domain: S [bad tcp checksum 8e22 ->bcde] 2623640264:2623640288(24) win 2048 0 [0q] (22)
08:24:29.315267 IP (tos 0x0, ttl 45, id 3, offset 0, flags [none], proto 6, length: 64, bad checksum 5efa ->8db6) 0.0.0.0.2358 > 0.0.0.0.domain: S [bad tcp checksum 59f0 ->88ac] 1646454613:1646454637(24) win 2048 0 [0q] (22)
08:25:00.717963 IP (tos 0x0, ttl 47, id 1, offset 0, flags [none], proto 6, length: 64, bad checksum a13d ->8bb8) 0.0.0.0.2259 > 0.0.0.0.domain: S [bad tcp checksum 2326 ->da1] 244004491:244004515(24) win 2048 0 [0q] (22)
08:25:01.478019 IP (tos 0x0, ttl 47, id 2, offset 0, flags [none], proto 6, length: 64, bad checksum a13c ->8bb7) 0.0.0.0.2282 > 0.0.0.0.domain: S [bad tcp checksum 4d1a ->3795] 3270760794:3270760818(24) win 2048 0 [0q] (22)
## Network Traffic Example

<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Flags</th>
<th>Seq</th>
<th>Ack</th>
<th>Window</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.008920</td>
<td>192.168.227.128</td>
<td>192.168.227.132</td>
<td>TCP</td>
<td>3474</td>
<td>4444</td>
<td>[SYN]</td>
<td>Seq=0</td>
<td>Len=0</td>
<td>MSS=1460</td>
<td></td>
</tr>
<tr>
<td>0.017993</td>
<td>192.168.227.132</td>
<td>192.168.227.128</td>
<td>TCP</td>
<td>4444</td>
<td>3474</td>
<td>[SYN, ACK]</td>
<td>Seq=0</td>
<td>Ack=1</td>
<td>Win=17520</td>
<td></td>
</tr>
<tr>
<td>0.018564</td>
<td>192.168.227.128</td>
<td>192.168.227.132</td>
<td>TCP</td>
<td>3474</td>
<td>4444</td>
<td>[ACK]</td>
<td>Seq=1</td>
<td>Ack=1</td>
<td>Win=6420</td>
<td>Len=0</td>
</tr>
<tr>
<td>0.082321</td>
<td>192.168.227.132</td>
<td>192.168.227.128</td>
<td>TCP</td>
<td>4444</td>
<td>3474</td>
<td>[PSH, ACK]</td>
<td>Seq=1</td>
<td>Ack=1</td>
<td>Win=17520</td>
<td></td>
</tr>
</tbody>
</table>

0.218717 192.168.227.128 192.168.227.132 TCP 3474 > 4444 [ACK] Seq=1 Ack=40 Win=64201 Len=0
0.227116 192.168.227.132 192.168.227.128 TCP 4444 > 3474 [PSH, ACK] Seq=40 Ack=1 Win=17520 Len=79
You Want Me To Analyze WHAT?

4500 003c 4f14 4000 4006 7417 0af7 0257
4815 222a 8c82 0050 9dc6 5a41 0000 0000
a002 16d0 0ac1 0000 0204 05b4 0402 080a
14b4 1555 0000 0000 0103 0302
Agenda

- Introduction
- Loss of Fundamental Skills
- Examples
- Path Forward
Have to Change Your Thinking

• Learn to think like an attacker
• Learn to think like a packet
• Learn to look at things with your evil hat on
• Learn to think outside the box
• A network can be attacked at ANY time
• NEVER become complacent
Develop Your Technical Skills

• Training never stops! Get Certified!
• Tools: Firewalls, IDS/IPS, Web Proxy, Email Gateway, packet capture, SIEM, Netflow, etc.
• Networking: TCP/IP, networking, routing and switching, DNS, SMTP, HTTP, HTTPS, NTP, etc.
• OS: Windows and Linux operating systems and architecture
• Programming languages – Offensive and Defensive
• Cloud computing
• New Technologies
Develop Your Threat Knowledge

• Web attacks
• Latest Exploits and HOW they work
• Malware Trends
• Current Vulnerabilities
• Penetration Testing Methodologies
• Attacker Tools – Both how they work AND what the traffic looks like
• Supply Chain Attacks
• Vulnerabilities/Weak Points on YOUR network
Develop Your Personal Skills

• Presentation and communications skills (don’t forget written)
• Attention to detail mindset
• Problem solving skills
• Willingness to dig deeper
• Team Player
• Knowledge Sharing (technical, threat, intel, etc.)
• Ability to say “I Don’t Know!!!!!”
• Stay Alert…AVOID Complacency!!!
Ten Key Points for Intrusion Analysts

• 10. Dig deeper.
  – At the end of the day you have to have something to rest your laurels on and that has to be the fact that you’ve done your due diligence and that you’ve given your best. My “motto” per se when it comes to intrusion analysis is “Dig Deeper”. A defender has to control 65,535 ports. An attacker has to compromise one. A defender has to protect 10,000 users. An attacker has to deceive one. A defender has to examine millions of packets. An attacker has to hide a malicious payload in one.

• [link](http://chrissanders.org/2011/01/the-10-commandments-of-intrusion-analysis/)
Don’t Be Overwhelmed!!

• Rome wasn’t built in a day
  – A lot to learn
  – It takes lot of work
  – Get the fundamentals down first
  – PRACTICE, PRACTICE, PRACTICE

• The more you learn the more you will realize how much more you have to learn
Questions??