Threat Hunting with Network Flow

Austin Whisnant

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
me@linux:~$ echo "Where's my cursor?"
Frame 219: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
Transmission Control Protocol, Src Port: 51376 (51376), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 37
Secure Sockets Layer
<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>No validation</td>
</tr>
<tr>
<td>Automatable</td>
<td>Summary</td>
</tr>
<tr>
<td>Privacy</td>
<td>Yet another tool</td>
</tr>
</tbody>
</table>
Threat Hunting with Network Flow

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.

1. **RECONNAISSANCE**
   - Harvesting email addresses, conference information, etc.

2. **WEAPONIZATION**
   - Coupling exploit with backdoor into deliverable payload

3. **DELIVERY**
   - Delivering weaponized bundle to the victim via email, web, USB, etc.

4. **EXPLOITATION**
   - Exploiting a vulnerability to execute code on victim's system

5. **INSTALLATION**
   - Installing malware on the asset

6. **COMMAND & CONTROL (C2)**
   - Command channel for remote manipulation of victim

7. **ACTIONS ON OBJECTIVES**
   - With 'Hands on Keyboard' access, intruders accomplish their original goal
Adversary

Infrastructure

Capabilities

Victim
Threat Hunting with Network Flow

April 19, 2017

© 2017 Carnegie Mellon University

This material has been approved for public release and unlimited distribution.
Pros

- Small (Quick)
- Automatable
- Privacy
Pros

+ Small (Quick)
+ Automatable
+ Privacy

? Critical thinking
#### Pros
- Small (Quick)
- Automatable
- Privacy
- Critical thinking

#### Cons
- No validation
- Summary
- Yet another tool
Profile

DNS: xxxxxxx

NAT: xxxxxxxxxxx

VPN: xxx

Web: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

...
me@linux:~$ echo "Just Linux command line skills"
Threat Hunting with Network Flow

Austin Whisnant