Now is the time for cyber deception

March 21, 2019

Sponsored by Carbon Black.

@BlackHatEvents / #BlackHatWebcasts
Speakers

Featured Presenter:

John Strand, @strandjs
Owner,
Black Hills Information Security and Active Countermeasures

Sponsor Presenter, @network232

David Balcar,
Security Strategist,
Carbon Black
Brought To You By!

One interesting omission, Moss said, was the apparent lack of use of deception technology. "I never heard one speaker say: 'And then I checked the canary or, and then I [reviewed] the deception tech," he said. "Who here uses deception technology?"

Let’s Change that
Why?

• Another useless rant on Threat Intelligence Feeds
• But there is value in understanding attackers
• How about attackers that are attacking you right now?
• What if we (as an industry) got better tracking attackers?
• Broken Windows
ADHD

https://www.activecountermeasures.com/free-tools/
What Is Cyber Deception?

• Cyber deception is the deliberate and calculated process of deceiving attackers in an effort to wage a better defense
  • Slow them down, confuse them, deceive them ... make them work harder
  • Serves to significantly increase your chances of detection
  • Designed to make \( D_t + R_t < A_t \) (\( D_t + R_t < A_t \))

• Cyber deception does not replace other efforts or layers of defense
• It should complement and feed the other layers
• Militaries have employed deception strategies since the beginning of time. Why don’t we?
Advanced Persistent Thieves (APTs)

• So who’s after your electrons?
  • China?
  • Russia?
  • The Five Eyes?
  • Other nation-states?
  • Organized crime?
  • Insiders?
  • All of the above!?
Susan v. Absolute

• Substitute teacher buys a stolen laptop
• The laptop has tracking software and software to “spy” on the potential “thief”
• Embarrassing pictures are taken
  • "It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down," Rice wrote in his decision. "It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop." –Judge Walter Rice
• Absolute settled out of court
• Just because they do something bad to you, it does not give you the right to violate their rights
Active Directory
HoneyAdmin
Go on.. Be obvious!
Disable Logon Hours

User logon name:
admin

User logon name (pre-Windows 2000):
winlab\admin

Logon Hours...
Log On To...

Unlock account

Logon Hours for Admin ADM. Administrator

Logon Permitted
Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM
### SNARE Network Configuration

The SNARE Agents are issued as both a free Open Source download (this agent) as well as an Enterprise version. They include maintenance, upgrades, and bug fixes as released by the SNARE project. The Open Source Agent does not support TCP, caching, custom event logs, UTC or regular expression support. The Enterprise Agents which include the ability to support TCP, caching, custom event logs, UTC or regular expression support.

1. **Support** - If you need a supported security platform, then you need to use the Enterprise Agent. Wondering how to determine the type of Agent your organization should use? Ask yourself the following questions to aid in selecting the right Agent.
2. **Complete and Factual** - If your organization needs to know that absolutely every event that is generated is provided to the open source community free of charge for the community; then you need to use the Open Source Agent.
3. **Sensitivity and Confidentiality** - Should your organization work with sensitive data? Do you want to maintain practices and encryption protocols.

Click [Here](#) for more information on the Snare Enterprise Agent.

The following network configuration parameters of the SNARE unit is set to the following values:

<table>
<thead>
<tr>
<th>Override detected DNS Name with:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Snare Server address</td>
<td>10.232.232.245</td>
</tr>
<tr>
<td>Destination Port</td>
<td>514</td>
</tr>
<tr>
<td>Allow SNARE to automatically set event log max size</td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:** The table above shows the default values for the network configuration parameters of the SNARE unit.
Set up Kiwi

<table>
<thead>
<tr>
<th>Rule</th>
<th>Type</th>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Action</td>
<td>Display</td>
<td>Display</td>
</tr>
<tr>
<td>Default</td>
<td>Action</td>
<td>Log to file</td>
<td>Log to file</td>
</tr>
<tr>
<td>New Rule</td>
<td>Filter</td>
<td>New Filter Message text-Simple</td>
<td></td>
</tr>
<tr>
<td>New Rule</td>
<td>Action</td>
<td>New Action Display</td>
<td></td>
</tr>
</tbody>
</table>
Password Spray

Administrator: Command Prompt - po...

PS C:\Users\JimmyAdmin\Downloads> Invoke-DomainPasswordSpray -Password Spring2017

[+] Current domain is compatible with Fine-Grained Password Policy.
[+] Now creating a list of users to spray...
[+] There appears to be no lockout policy.
[+] Removing disabled users from list.
[+] Removing users within 1 attempt of locking out from list.
[+] Created a user list containing 293 users gathered from the current user’s domain

Confirm Password Spray
Are you sure you want to perform a password spray against 293 accounts?
[?] Yes [N] No [?] Help (default is "Y")?: Y

[+] Password spraying has begun. Current time is 11:11 AM
[+] This might take a while depending on the total number of users
[+] SUCCESS! User:Jenkin.Admin Password:Spring2017
[+] Password spraying is complete
PS C:\Users\JimmyAdmin\Downloads>
Alerts!

Evil Honeyports: Portspoof

• In addition to our “tripwires,” why not create white noise and chaff as well?
• Portspoof does this
• It generates random responses to service identification requests
• Basically, the ports that get scanned never come back the same
• It can take hours to run a simple service identification scan
### Portspoof in Action

Starting Nmap 6.28 (http://nmap.org) at 2013-07-16 10:48 CEST
Nmap scan report for 172.16.37.145
Host is up (0.00097s latency).

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/tcp</td>
<td>open</td>
<td>pop3</td>
<td>Eudora Internet Mail Server X pop3d 870</td>
</tr>
<tr>
<td>2/tcp</td>
<td>open</td>
<td>honeypot</td>
<td>Network Flight Recorder BackOffice Friendly http honeypot</td>
</tr>
<tr>
<td>3/tcp</td>
<td>open</td>
<td>smtp</td>
<td>Postfix smtpd (Debian)</td>
</tr>
<tr>
<td>4/tcp</td>
<td>open</td>
<td>ssh</td>
<td>(protocol 7)</td>
</tr>
<tr>
<td>5/tcp</td>
<td>open</td>
<td>NULL</td>
<td>XFree86 9 patch level g (Connectiva Linux)</td>
</tr>
<tr>
<td>6/tcp</td>
<td>open</td>
<td>imap</td>
<td>Koria imapd 4.3.9 patch 4</td>
</tr>
<tr>
<td>7/tcp</td>
<td>open</td>
<td>ftp</td>
<td>Samba ftpd</td>
</tr>
<tr>
<td>8/tcp</td>
<td>open</td>
<td>unknown</td>
<td>Cisco VPN Concentrator http config</td>
</tr>
<tr>
<td>9/tcp</td>
<td>open</td>
<td>http</td>
<td>(protocol 3)</td>
</tr>
<tr>
<td>10/tcp</td>
<td>open</td>
<td>ssh</td>
<td>Microsoft NetMeeting Remote Desktop Service</td>
</tr>
<tr>
<td>11/tcp</td>
<td>open</td>
<td>ms-wbt-server</td>
<td>Scalix UAL</td>
</tr>
<tr>
<td>12/tcp</td>
<td>open</td>
<td>scpix-ux</td>
<td>Scalix UAL</td>
</tr>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>smtp</td>
<td>Small Home Server smtpd</td>
</tr>
<tr>
<td>14/tcp</td>
<td>open</td>
<td>telnet</td>
<td>Dreambox 500 media device telnetd (Linux kernel t; Pli image Jade, based on DK)</td>
</tr>
<tr>
<td>15/tcp</td>
<td>open</td>
<td>ftp</td>
<td>ProFTPD (German)</td>
</tr>
<tr>
<td>16/tcp</td>
<td>open</td>
<td>ftp</td>
<td>Lexmark K series printer ftpd (MAC: K)</td>
</tr>
<tr>
<td>17/tcp</td>
<td>open</td>
<td>ftp</td>
<td>ProFTPD</td>
</tr>
<tr>
<td>18/tcp</td>
<td>open</td>
<td>irc-proxy</td>
<td>mih IRC proxy</td>
</tr>
<tr>
<td>19/tcp</td>
<td>open</td>
<td>ftp</td>
<td>ProFTPD</td>
</tr>
<tr>
<td>20/tcp</td>
<td>open</td>
<td>hp-gsq</td>
<td>IEEE 1284.4 scan peripheral gateway</td>
</tr>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>desktop-central</td>
<td>ManageEngine Desktop Central DesktopCentralServer</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>OpenSSH 5.3p1 Debian Subpup7 (Ubuntu Linux; protocol 2.0)</td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td>Blue Coat telnetd</td>
</tr>
<tr>
<td>24/tcp</td>
<td>open</td>
<td>hp-gsq</td>
<td>IEEE 1284.4 scan peripheral gateway</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>vnc</td>
<td>Polycom VSX 7000A VOIP phone ftpd</td>
</tr>
<tr>
<td>26/tcp</td>
<td>open</td>
<td>vnc</td>
<td>UltraVNC 1.0.8.0</td>
</tr>
<tr>
<td>27/tcp</td>
<td>open</td>
<td>ssh</td>
<td>(protocol 133098)</td>
</tr>
<tr>
<td>28/tcp</td>
<td>open</td>
<td>telnet</td>
<td>Blue Coat telnetd</td>
</tr>
<tr>
<td>29/tcp</td>
<td>open</td>
<td>printer</td>
<td>VSE ltd</td>
</tr>
<tr>
<td>30/tcp</td>
<td>open</td>
<td>ssh</td>
<td>SSHTools J2SSH (protocol 0740)</td>
</tr>
<tr>
<td>31/tcp</td>
<td>open</td>
<td>telnet</td>
<td>Lantronix MSS100 serial interface telnetd 8469697</td>
</tr>
<tr>
<td>32/tcp</td>
<td>open</td>
<td>pop3</td>
<td>Dovecot pop3d</td>
</tr>
<tr>
<td>33/tcp</td>
<td>open</td>
<td>telnet</td>
<td>Control DeviceMaster RTS ethernet to serial telnetd (Model 4; NS-Link DqX; MAC Q)</td>
</tr>
<tr>
<td>34/tcp</td>
<td>open</td>
<td>smtp</td>
<td>WebsHieldet smtpd</td>
</tr>
<tr>
<td>35/tcp</td>
<td>open</td>
<td>telnet</td>
<td>HP switch telnetd</td>
</tr>
<tr>
<td>36/tcp</td>
<td>open</td>
<td>upnp</td>
<td>MINIPLNA MISUCEP (DLNA/DDC cmnQnuuF; UPnP YT)</td>
</tr>
</tbody>
</table>
Kippo

• Kippo is different from a simple honeypot because it allows the attacker to interact with a fake SSH service
• Kippo is an outstanding SSH honeypot
• It allows you to intercept and capture logins and activity by attackers
• It is useful for capturing the passwords an attacker has, or at least what he thinks he has
• It can be used for both annoyance and for attribution
Questions & Answers

Featured Presenter:

John Strand, @strandjs
Owner,
Black Hills Information Security
Active Countermeasures

Sponsor Presenter:

David Balcar,
Security Strategist,
Carbon Black

• To join the Black Hat mailing list, email BH LIST to: feedback@blackhat.com
• To join our LinkedIn Group: http://www.linkedin.com/groups?gid=37658&trk=hb_side_g
• To follow Black Hat on Twitter: https://twitter.com/Blackhatevents
• Black Hat’s Facebook Fan Page: http://www.facebook.com/blackhat
• Find out more at www.blackhat.com
• Next Webcast: April 18, 2019
Thank You!

@BlackHatEvents / #BlackHatWebcasts