Fighting the Good Fight

Reactive Security in a DDOS World
Additional Information by:

Christopher Howard - Director, Network Engineering

Michael Dinkins - Senior Information Security Officer

&&

Jeff Kell - Too many to list....
Follow your company's policies and procedures!

Get a CYA letter signed by your CIO!

Never react in anger or pride!

You are responsible for any damage you cause!
Reacting Without Invoking the Wrath of the Skiddies

- Use “Drop” instead of “Reset”
- Practice Defense in Depth. Security is about layers.
- Put honeypots “outside” your firewall. Do recon “outside” your firewall.
- Enable host based detection with passive reaction. Whitelists!!
- Perform centralized logging and correlation.
- Do analysis in virtualized or isolated environments. Connect via remote access.
- Do not make contact with a “hacker” or “script kiddie.”
- Report your findings as appropriate.
What is a DDOS?

When the bad guys bring down your site(s) by using a distributed denial of service (DDOS) attack. Usually performed by a BotNet or Zombie Horde.

Why?

● Financial Gain
● Differences in Philosophy
● Just for the LoLs

Example: Distributed DNS Amplification Attack, NTP, TFTP.
Q2 2015 Attacks > 100 Gbps

Figure 1: Ten of the mega attacks targeted the Internet and telecom industry

DDOS attacks have become cheaper than one can think, just because of the era of DDOS-for-hire services. However, such attacks are easier to launch now and don’t cost much, but when it comes to the victim - it costs $40,000 per hour to them considering the loss.
More Information on DDoS

- http://www.digitalattackmap.com/
Network Security Monitoring: Network Based

- [https://www.snort.org/](https://www.snort.org/) (Grand Daddy. Signature Based. SINGLE THREADED!)
- [http://oisf.net/suricata/](http://oisf.net/suricata/)
- [https://www.bro.org/](https://www.bro.org/)
- [https://quadrantsec.com/sagan_log_analysis_engine/](https://quadrantsec.com/sagan_log_analysis_engine/)
Network Security Monitoring: Host Based

- http://aide.sourceforge.net/ (Linux, BSD. File Signing)
- https://sourceforge.net/projects/logwatch/files/ (Linux. Signature)
- http://nerderies.blogspot.com/ (Windows. RDP. Blocking)
Network Security Monitoring: Honeypots

- [http://bruteforce.gr/honeydrive](http://bruteforce.gr/honeydrive) (Multiple Honeypot VM)
- [http://www.atomicsoftwaresolutions.com/](http://www.atomicsoftwaresolutions.com/) (Windows Based)
- [https://github.com/micheloosterhof/cowrie](https://github.com/micheloosterhof/cowrie) (SSH)
- [https://www.honerix.com/](https://www.honerix.com/) (Web Attack Honeypot)
- [http://threatstream.github.io/mhn/](http://threatstream.github.io/mhn/) (Manage Multiple Honeypot Servers)
Network Security Monitoring: Centralized Logging

- Forward WiFi Access!
- Monitor Syslog Server Disk Space. Rotate Logs w/Compression. [https://support.rackspace.com/how-to/understanding-logrotate-utility/](https://support.rackspace.com/how-to/understanding-logrotate-utility/)
Network Security Monitoring: Snorby
Network Security Monitoring: Kibana
Network Security Monitoring: The Security Onion

- “All in One” Solution VM or ISO.
- Network and Host based Intrusion Detection Systems (Snort, OSSEC)
- Log Capture (Syslog)
- Event Correlation and Analysis (Kibana, ElasticSearch, Bro, Suricata,...)
- Packet Capture (tcpdump)
Intermission 1: Shodan.io

- [https://account.shodan.io/register](https://account.shodan.io/register) (email [support@shodan.io](mailto:support@shodan.io) for a free upgrade to your educational account)
- Find vulnerable services on your network and ports you didn’t know were open.
- Book by the creator of Shodan [https://leanpub.com/shodan](https://leanpub.com/shodan)
- [https://www.youtube.com/watch?v=XB-vjRCwa9E](https://www.youtube.com/watch?v=XB-vjRCwa9E)
- Google redirects to Shodan
Reactive Security Example: Labrea Tarpit

Snort - Watch’ Em. [https://snort.org/](https://snort.org/)
SnortSam - Block’ Em. [http://www.snortsam.net/](http://www.snortsam.net/)

2016/01/28, 20:11:18, 150.xxx, 2, snortsam, Blocking host 111.255.75.82 completely for 3600 seconds (Sig_ID: 3133700).
2016/01/28, 20:11:54, 150.xxx, 2, snortsam, Blocking host 222.189.40.171 completely for 3600 seconds (Sig_ID: 3133700).
2016/01/28, 20:12:05, -, 2, snortsam, Removing 3600 sec complete block for host 58.214.233.179.

Tarpit Count: 03/15 00.00.00-08:54:21

<table>
<thead>
<tr>
<th>Port</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>3389</td>
<td>178</td>
</tr>
<tr>
<td>5900</td>
<td>120</td>
</tr>
<tr>
<td>118</td>
<td>118</td>
</tr>
<tr>
<td>22</td>
<td>99</td>
</tr>
<tr>
<td>443</td>
<td>61</td>
</tr>
<tr>
<td>80</td>
<td>49</td>
</tr>
<tr>
<td>23</td>
<td>47</td>
</tr>
<tr>
<td>902</td>
<td>24</td>
</tr>
<tr>
<td>49919</td>
<td>24</td>
</tr>
<tr>
<td>8080</td>
<td>23</td>
</tr>
<tr>
<td>11211</td>
<td>17</td>
</tr>
</tbody>
</table>
Reactive Security Example: Cowrie and Dshield

Cowrie (Kippo) Honeypot

https://www.dshield.org/howto.html (Ports, SSH, and 404 Errors)

https://isc.sans.edu/diary/Dockerized+DShield+SSH+Honeypot/20845
Reactive Security Example: OSSEC Active Response

The first is the `<command>` section. This details the command to be run, and the options it will use.

```xml
<ossec_config>
  <command>
    <!--
    Command options here
   -->
  </command>
  <active-response>
    <!--
    active-response options here
   -->
  </active-response>
</ossec_config>
```

The second is the `<active-response>` section. This section defines when the command will be run.

Feb 19 15:23:50 rackmonkey useradd[3500]: failed adding user `apache', data deleted
Reactive Security Example: UFW and DShield

https://isc.sans.edu/howto.html
https://isc.sans.edu/clients/ubuntu.html
Reactive Security Example: Top 20 Dshield Block List

#    This list summarizes the top 20 attacking class C (/24) subnets
#   over the last three days. The number of 'attacks' indicates the
#   number of targets reporting scans from this subnet.


https://isc.sans.edu/forums/diary/Subscribing+to+the+DShield+Top+20+on+a+Palo+Alto+Networks+Firewall/19365/


Reactive Security Example: Fail2Ban

Utilizes host firewall (IPTables)

http://www.fail2ban.org/

2016-01-26 07:19:45.872 fail2ban.actions[26095]: WARNING [apache-badbots] Ban 173.161.52.213
...
Reactive Security Example: LogWatch

Dovecot disconnects:
Logged out: 432 Time(s)
no reason: 7 Time(s)

**Unmatched Entries**
dovecot: pop3-login: Aborted login (no auth attempts): rip=66.240.219.146,
dovecot: pop3-login: Disconnected (no auth attempts): rip=66.240.219.146,
dovecot: pop3-login: Disconnected (no auth attempts): rip=66.240.219.146,
Reactive Security Example: Syslog, Cron, and Grep

```
cat /var/log/auth.log | grep -i root | grep -iv cron | uniq | mail -s secure_root mike-ward@utc.edu
```
Reactive Security Example: Phishing

From: Online Apploid <replyonline@ts.apple.com>
Date: 01/19/2016 6:12 PM (CMT: 06:39)
To: "Safety, Safety And Risk Management" <safety@utc.edu>
Subject: ID475166730

Hey safety@utc.edu,

Please update your ID as soon as possible - if no action is taken, you may be required to contact Customer Support to continue using your ID.

We’re committed to keeping Apple a vibrant, good professional community.

Update ID

Thanks for being our customer!
The iTunes Team

© 2015 Initial registered trademark in the United States and/or other countries. All rights reserved.

If you need assistance or have questions, please contact Customer Service.
Registered as a private limited company. Company Number 477441.
Registered Office: Wilton Place, Wilton Place.
Reactive Security Example: Phishing Cont.
Reactive Security Example: Phishing Cont.
Reactive Security Example: Phishing Cont.
Reactive Security Example: Phishing Cont.
Reactive Security Example: Phishing Cont.
Reactive Security Example: Phishing Cont.
Reactive Security Example: Phishing Cont.
Reactive Security Example: Phishing Cont.

When sending email do not include phishing links as text as good spam filters will prevent delivery. Instead send image files or pdfs.
Reactive Security Example: Phishing Cont.

---

[GV-807-20980]: Phishing from one of your sites. Please investigate.

Bryan Abraham <abuse@support.totalchoicehosting.com>

to me

Hi Michael,

Thank you for letting us know about this issue. The phishing site has been taken down and no longer available.

Kind Regards,

Bryan Abraham
Lead Administrator Assistant
Technical Support
TotalChoice Hosting Inc.
http://www.totalchoicehosting.com

------------------------

I can be reached via instant messenger if you would like to discuss any issues that you may have.

AOL Instant Messenger :: chgurubryan
Yahoo Messenger :: chgurubryan

------------------------

IMPORTANT: Please do not change subject line when you replying back in connection with the same issue. It will help us to provide you better and faster solution on your issues.

Ticket Details

Ticket ID: GJV-807-20980
Department: Abuse
Type: Issue
Status: Open
Priority: --

Helpdesk: https://support.totalchoicehosting.com/index.php?
Intermission 2: What To Read

- [https://www.reddit.com/r/netsec/](https://www.reddit.com/r/netsec/)
- [https://www.reddit.com/r/sysadmin/](https://www.reddit.com/r/sysadmin/)
- [https://www.reddit.com/r/computerforensics](https://www.reddit.com/r/computerforensics)
- [https://www.reddit.com/r/Malware](https://www.reddit.com/r/Malware)
- [https://news.ycombinator.com/newest](https://news.ycombinator.com/newest)
- [https://www.grahamcluley.com/](https://www.grahamcluley.com/)
- [https://www.sans.org/newsletters/newsbites/](https://www.sans.org/newsletters/newsbites/)
- Twitter: @edskoudis @e_kaspersky @GabeAul @SGgrc @NakedSecurity @gcluley @msftsecurity @briankrebs @Carlos_Perez @thurrott @hdmoore @USCERT_gov @sans_isc @schneierblog
Reactive Security Example: Cowrie Binaries
Reactive Security Example: Cowrie Binaries Cont.

2016-03-20 15:15:40-0400 [SSHService ssh-userauth on HoneyPotTransport,10990,208.109.54.40] pi trying auth password
2016-03-20 15:15:40-0400 [SSHService ssh-userauth on HoneyPotTransport,10990,208.109.54.40] pi authenticated with password
2016-03-20 15:15:40-0400 [SSHService ssh-userauth on HoneyPotTransport,10990,208.109.54.40] starting service ssh-connection
2016-03-20 15:15:40-0400 [SSHService ssh-userauth on HoneyPotTransport,10990,208.109.54.40] got channel session request
2016-03-20 15:15:40-0400 [SSHChannel session () on SSHService ssh-connection on HoneyPotTransport,10990,208.109.54.40] channel open
2016-03-20 15:15:40-0400 [SSHChannel session () on SSHService ssh-connection on HoneyPotTransport,10990,208.109.54.40] Command found: sh null.sh &
2016-03-20 15:15:40-0400 [SSHChannel session () on SSHService ssh-connection on HoneyPotTransport,10990,208.109.54.40] sending eof
2016-03-20 15:15:40-0400 [SSHChannel session () on SSHService ssh-connection on HoneyPotTransport,10990,208.109.54.40] sending close 0
2016-03-20 15:15:48-0400 [HoneyPotTransport,10990,208.109.54.40] connection lost
2016-03-20 15:15:48-0400 [HoneyPotTransport,10990,208.109.54.40] Connection lost
Nmap scan report for ip-208-109-54-40.ip.secureserver.net (208.109.54.40)
Host is up (0.13s latency).
Not shown: 82 closed ports

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td>Pure-FTPD</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>OpenSSH 5.3 (protocol 2.0)</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp?</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>Apache httpd 2.4.10 ((Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4)</td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop3</td>
<td>Dovecot pop3d</td>
</tr>
<tr>
<td>135/tcp</td>
<td>filtered</td>
<td>msrpc</td>
<td></td>
</tr>
<tr>
<td>139/tcp</td>
<td>filtered</td>
<td>netbios-ssn</td>
<td></td>
</tr>
<tr>
<td>143/tcp</td>
<td>open</td>
<td>imap</td>
<td>Dovecot imapd</td>
</tr>
<tr>
<td>179/tcp</td>
<td>filtered</td>
<td>bgp</td>
<td></td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>http</td>
<td>Apache httpd 2.4.18 ((Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4)</td>
</tr>
<tr>
<td>465/tcp</td>
<td>open</td>
<td>ssl/smtp</td>
<td>Exim smtpd 4.86_1</td>
</tr>
<tr>
<td>587/tcp</td>
<td>open</td>
<td>smtp</td>
<td>Exim smtpd 4.86_1</td>
</tr>
<tr>
<td>993/tcp</td>
<td>open</td>
<td>ssl imap</td>
<td>Dovecot imapd</td>
</tr>
<tr>
<td>995/tcp</td>
<td>open</td>
<td>ssl/pop3</td>
<td>Dovecot pop3d</td>
</tr>
<tr>
<td>1028/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>3128/tcp</td>
<td>filtered</td>
<td>squid-http</td>
<td></td>
</tr>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
<td>MySQL (unauthorized)</td>
</tr>
</tbody>
</table>
"secsureserver.net"

All News Videos Maps

About 339,000 results (0.66 seconds)

Email Login
https://email.secsureserver.net/
A description for this result is not available because of this site's robots.txt – learn more.

Email - LOG IN
https://sso.secsureserver.net/login?app=email&realm=pass
Welcome to our new login page. Please log in with your current username and password. Having trouble logging in? See this article for more information.

LOG IN
https://sso.secsureserver.net/
Username or Customer # I forgot. Password I forgot. Keep me logged in. Protect your account. Uncheck if using public/shared device. LOG IN. Copyright © 1999 ...

attacks - Break in attempts from secsureserver.net ...
security.stackexchange.com/.../break-in-attempts-from-se... Stack Exchange
May 18, 2015 - Over the last few weeks I have seen dozens if not hundreds of ... Very odd that the attacks came from secsureserver.net Being a previous customer...
Reactive Security Example: Cowrie Binaries Cont.
### Reactive Security Example: Cowrie Binaries Cont.

<table>
<thead>
<tr>
<th>PORT</th>
<th>STATE</th>
<th>SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td>Pure-FTPD</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>OpenSSH 5.3 (protocol 2.0)</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp?</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>nginx 1.8.1</td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop3</td>
<td>Dovecot pop3d</td>
</tr>
<tr>
<td>135/tcp</td>
<td>filtered</td>
<td>msrpc</td>
<td></td>
</tr>
<tr>
<td>139/tcp</td>
<td>filtered</td>
<td>netbios-ssn</td>
<td></td>
</tr>
<tr>
<td>143/tcp</td>
<td>open</td>
<td>imap</td>
<td>Dovecot imapd</td>
</tr>
<tr>
<td>179/tcp</td>
<td>filtered</td>
<td>bgp</td>
<td></td>
</tr>
<tr>
<td>405/tcp</td>
<td>open</td>
<td>ssl/smtp</td>
<td>Exim smtfd 4.86_1</td>
</tr>
<tr>
<td>587/tcp</td>
<td>open</td>
<td>smtp</td>
<td>Exim smtfd 4.86_1</td>
</tr>
<tr>
<td>993/tcp</td>
<td>open</td>
<td>ssl/imap</td>
<td>Dovecot imap</td>
</tr>
<tr>
<td>995/tcp</td>
<td>open</td>
<td>ssl/pop3</td>
<td>Dovecot pop3d</td>
</tr>
<tr>
<td>1022/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>3128/tcp</td>
<td>filtered</td>
<td>squid-http</td>
<td></td>
</tr>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
<td>MySQL (unauthorized)</td>
</tr>
<tr>
<td>6000/tcp</td>
<td>open</td>
<td>irc</td>
<td>Unreal ircd</td>
</tr>
</tbody>
</table>
Reactive Security Example: Cowrie Binaries Cont.
Reactive Security Example: Cowrie Binaries Cont.
Reactive Security Example: Cowrie Binaries Cont.
Reactive Security Example: Cowrie Binaries Cont.
Reactive Security Example: Cowrie Binaries Cont.

Oops! The analysis system reported an error:

The file "ed0d5c5fa4ae4b0bbe560af9555f487ce8b34d1e7bf1d1308e320486e6a3c66" has an invalid or corrupt structure.

If you believe this is incorrect behavior, please contact support@payload-security.com providing the SHA256 and sample.

The SHA256 of your submission is: ed0d5c5fa4ae4b0bbe560af9555f487ce8b34d1e7bf1d1308e320486e6a3c66

Analysis Environment:
- Windows 7 32 bit - Usermode Monitor
- Android Static Analysis
- Windows 7 32 bit - Kernelmode Monitor
- Windows 7 64 bit - Usermode Monitor
- Windows 7 64 bit - Kernelmode Monitor
- Windows XP - (32-3 and 64-bit)
- 32/64 bit - Usermode Monitor
- 32/64 bit - Kernelmode Monitor
- 32/64 bit - Usermode Monitor
- 32/64 bit - Kernelmode Monitor

Runtime action script: Execute random desktop theme
Reactive Security Example: Cowrie Binaries Cont.

http://www.ircbeginner.com/ircinfo/ircc-commands.html

Time to email abuse@secureserver.net with gathered data in PDF form.
Reactive Security Example: Submit What You’ve Found

- Follow Your Company’s Policies and Procedures!
- [https://isc.sans.edu/contact.html](https://isc.sans.edu/contact.html)
Reactive Security: Online Resources

- https://zeltser.com/automated-malware-analysis/
- https://exchange.xforce.ibmcloud.com/
- http://www.amanhardikar.com/mindmaps/ForensicChallenges.html
- http://downdetector.com/
- http://www.toolswatch.org/
- https://www.kali.org/
- http://digital-forensics.sans.org/community/downloads
- http://www.docspal.com/viewer
New Find: Heralding Honeypot

Heralding - the credentials catching honeypot

Wed, 03/23/2016 - 23:57 — johnny.vestergaard

Sometimes (actually, most times) you don’t need advanced deception technology, but rather just a simple tool to answer some simple questions. I was recently in that situation, and needed the answers to the following questions:

- Which protocols does my adversary try to brute-force?
- Which username and password did he use?
- At which speed did he brute-force?
- From where did he proxy from?
- What time of day did he brute-force?

To answer these questions, I needed a tool that would output something similar to:

```
2016-03-12 20:35:02.258198, 192.168.2.129, 51551, 23, telnet, bond, james
2016-03-12 20:35:09.658593, 192.168.2.129, 51551, 23, telnet, clark, P@SSwOrd123
2016-03-18 10:31:38.521047, 192.168.2.129, 53416, 22, ssh, guest, guest
2016-03-18 19:31:39.376768, 192.168.2.129, 53416, 22, ssh, HundeLab, katNIPkast
2016-03-18 19:33:07.054594, 192.168.2.129, 53416, 110, pop3, charles, W00FISH
2016-03-18 19:33:11.564403, 192.168.2.129, 53416, 110, pop3, NektarManden, nADInEkter
2016-03-18 19:36:36.077840, 192.168.2.129, 53445, 21, ftp, Joocop, Pooop
```

https://www.honeynet.org/node/1321