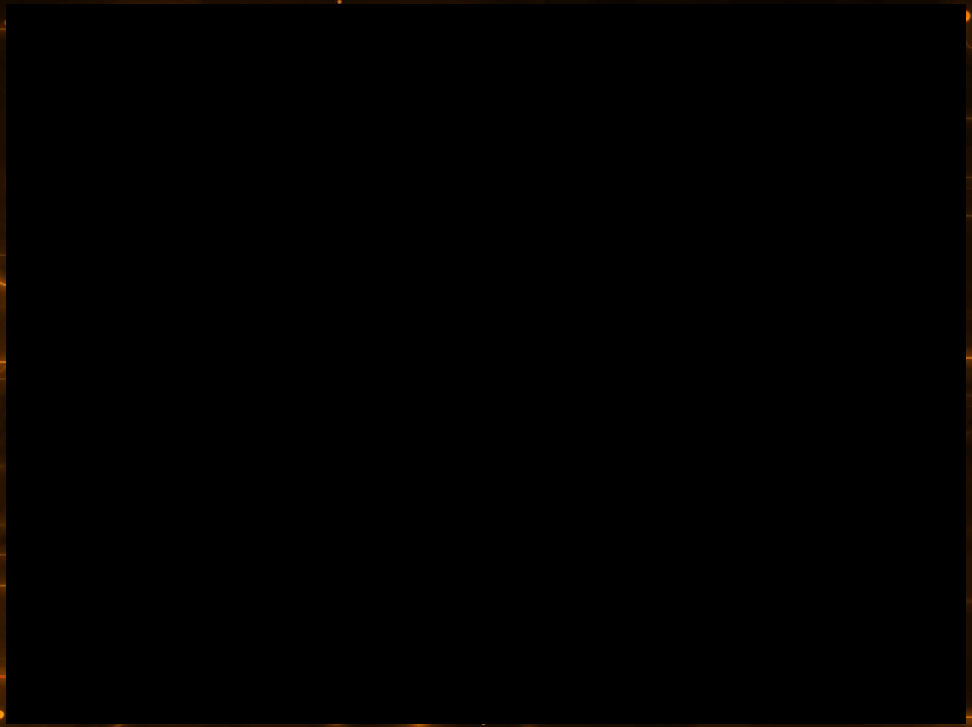
Setting up an Open Source Threat Detection Program

Who am I

- VP of Data Security.
- Long time Developer.
- Founder of hackerspace 801 Labs in Salt Lake City, Utah
- Defcon Group Organizer DC801.
- Blackhat NOC Team.
- https://research.801labs.org/ Twitter @nemus801
- www.801labs.org



https://www.reddit.com/r/Utah/comments/e2pfcy/brian_head_utah_getting_nuked/

Prerequisite

- **Familiarity with Linux, Apache, MySQL, PHP (LAMP).**
  - Linux Operating Systems CLI
  - Apache Server Config
  - Understanding of ModSecurity
    - http://obscuritysystems.com/slides/modsecurity.pdf
  - Understanding of HTTP POST and GET
    - http://www.w3schools.com/tags/ref_httpmethods.asp
  - Understanding of ELK stack and/or other log monitoring tools.
    - http://www.slideshare.net/prajalkulkarni/attack-monitoring-using-elasticsearch-logstash-and-kibana

Disclaimer

- The information provided in this presentation is to be used for educational purposes only.
- My thoughts are my own not of my employer.
- I am in no way responsible for any misuse of the information provided.
- All of the information presented is for the purpose of developing a defensive attitude to provide insight.
- In no way should you use the information to cause any damage directly or indirectly.
- You implement the information given in this presentation at your own risk.
- Contact a Lawyer for legal questions.
- I am not a Lawyer
- **I am also not your Lawyer.**

The Strategic Offensive Principle of War.

“The best defense is a good offense”

Instead of a passive attitude offense will preoccupy the opposition and ultimately hinder its ability to mount an opposing counterattack, leading to a strategic advantage.

My Definition of Security

There is no such thing as “Security”.

The state of being free from danger or threat.

I define something as secure when the “work” of obtaining it is more than it's worth.

A clearer definition is still difficult to obtain.

Obscurity

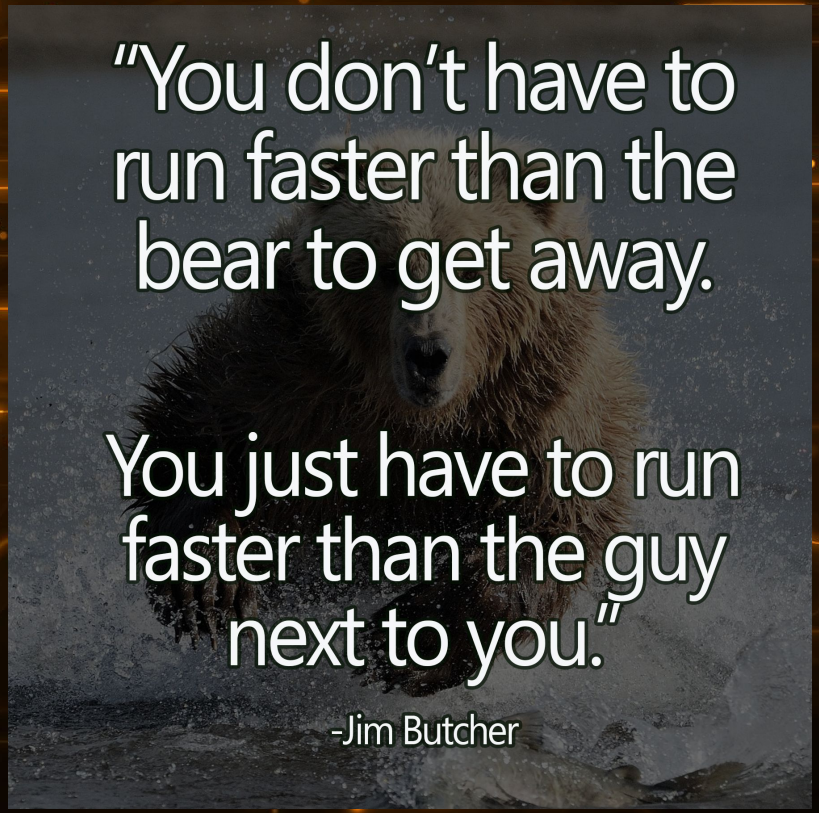
The state of being unknown, inconspicuous, or unimportant.

The quality of being difficult to understand.

A thing that is unclear or difficult to understand.

Don’t be default.

Outrunning the Bear



So Why Are We Turtling and Teching

Turtling is a gameplay strategy that emphasizes heavy defense, with little or no offense. Ostensibly, turtling minimizes risk to the turtling player while baiting opponents to take risks in trying to overcome the defenses. In practice, however, games are often designed to punish turtling through various game mechanics.

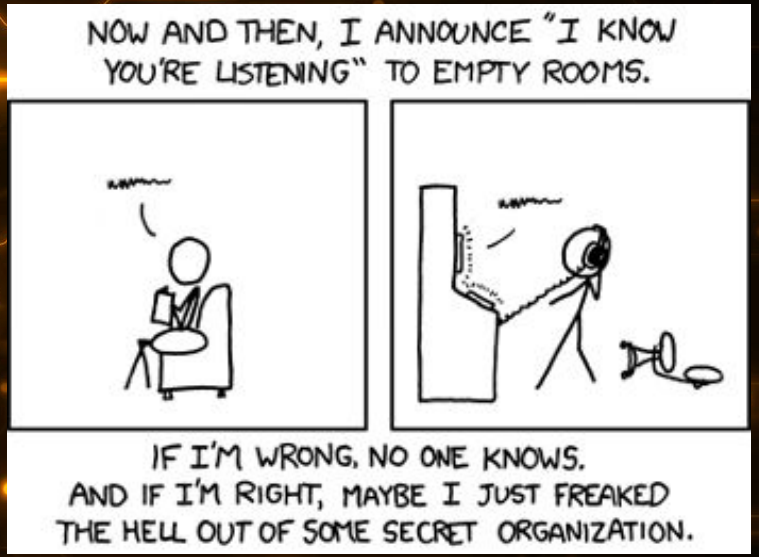
In every RTS, time is the most valuable resource. In every RTS, time is the most valuable resource.

http://www.gamesradar.com/how-to-play-rts-games-competitively-for-newbies/

What is Counter Hacking?

- Counterintelligence
  - Activities designed to prevent or thwart spying, intelligence gathering, and sabotage by an enemy or other foreign entity.

- Counter Hacking
  - Activities designed to prevent or thwart threat actors who seek to compromise digital systems that can involve malicious computer techniques other than just blocking or ignoring attackers. - My Definition



I Know You're Listening/ Digital Image xkcd./ 11/19/2016 <https://xkcd.com/525>

Counter Hacking Debate

- Should we Counter Hack and attack the attackers?
- Is Counter Hacking Legal?
- Do we get a return on investment on Counter Hacking?
- What do we gain by attacking back?
- What do we lose?

Cat Kicking Dog. Imgur . 11/19/2016 <http://i.imgur.com/B4vqFPq.jpg>

Think

This Presentation is the “how” not the “why”.

You should carefully consider what your doing before implementing or following any of technical demonstrations I am going to cover.

Think about what you're doing before you put on the zebra suit.

Scenario

So what do we do about something weird going on in our environment ?

How do we go about catching people that are poking around looking to cause trouble?

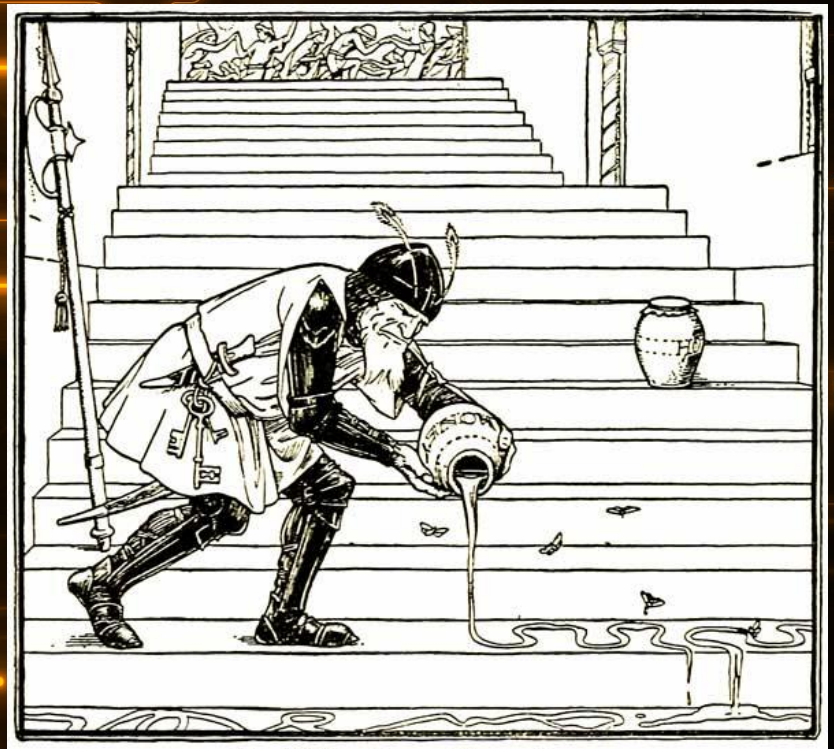
What if our Intrusion Detection System (IDS) misses the attack?

Clown Attempting to Opening Door with Knife. The SUN 10th October 2016 <https://www.thesun.co.uk/news/1945219/terrifying-moment-clown-armed-with-a-knife-is-caught-on-cctv-at-2am-trying-to-break-into-home/>

What is a Honey Pot?

Honey Pots are fake servers or systems setup to gather information about an attacker's methods and techniques.

https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9



The Soldier Lays a Honey Trap

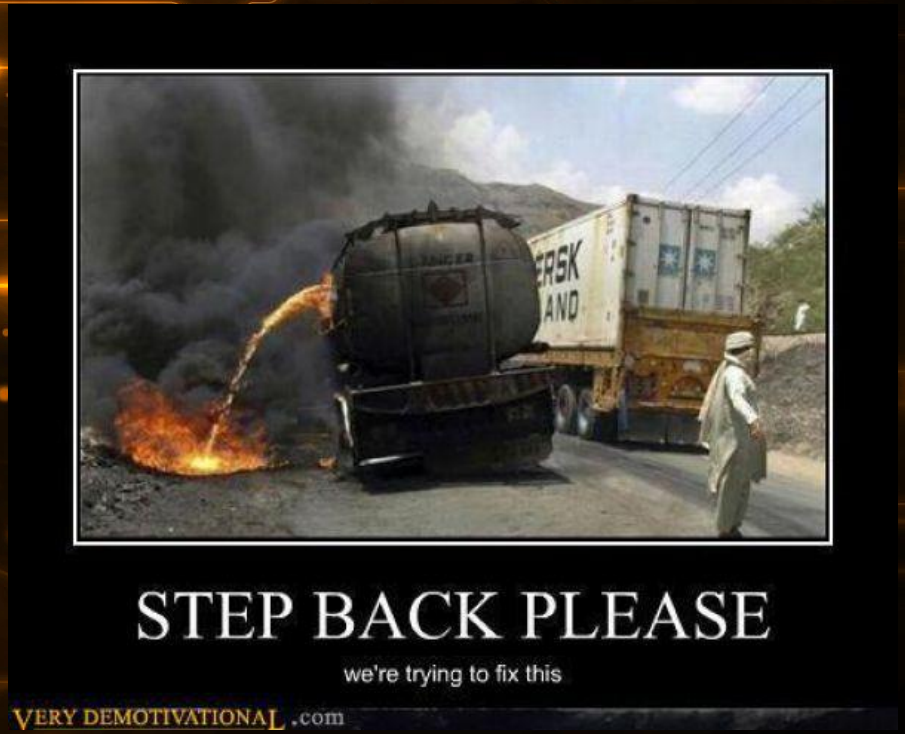
http://tywkiwdbi.blogspot.com.es/2011/09/soldier-lays-honey-trap.html

Detection Honeypot

- Are used to detect threats.
- Complement IDS systems.
- Can help detect false negatives.
- Can detect new or unknown attacks.
- Can provided a clean environment for Incident Response

Research Honeypot

- Adds value by providing a platform from which you can collect information about the threats seeking to gain access to your system.
- The lessons learned from a research honeypot can be applied to improve intrusion prevention.



Honey Pot Pros

- Decrease the rate of false positives, which often plague network IDS.
- Low false positives, high success.
- Able to confuse attackers.
- Help train your security team.
- Understand the intruder’s intentions by observing his interactions.

Honey Pot Cons

They don’t add value to prevention.

They do not block attacks.

If done incorrectly they can lead to a compromise of data and systems in your organization.

Active Defense

Actively Responding to Attacks.

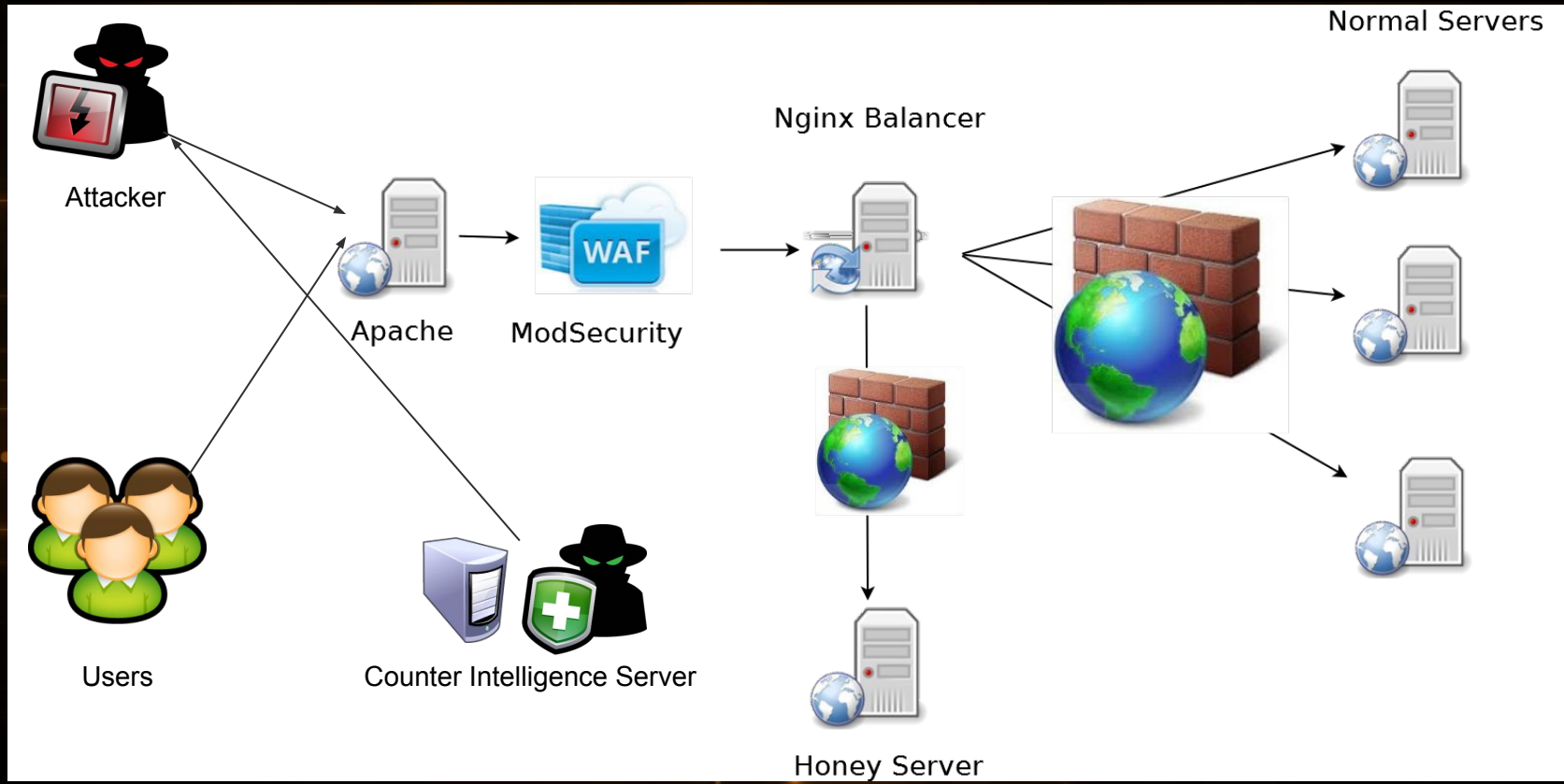
http://weheartit.com/entry/group/40000111

Environment Setup

Monitoring and Detection

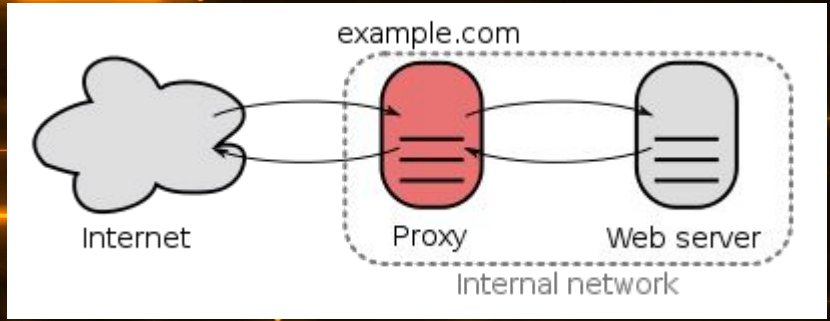
- Setup ELK or another monitoring engine for the purpose of logging malicious actions.
- Setup ModSecurity to detect and redirect traffic before it hits your web application.
- Setup Reverse Proxy to redirect “Clowns” to honey load balancer.
- Setup Nginx to handle proxy conditions.

Diagram


Normal Servers
Nginx Balancer
Attacker
WAF
Apache
ModSecurity
Users
Counter Intelligence Server
Honey Server

Apache Reverse Proxy Setup

```
<VirtualHost *:80>

        ServerName mysite
        ProxyRequests Off
        ProxyVia Off

    <Proxy *>

        Order deny,allow
        Allow from all

    </Proxy>

    ProxyPreserveHost off
    ProxyPass / http://localhost:8080/
    ProxyPassReverse / http://localhost:8080/

</VirtualHost>
```



Apache If Statements

If you want to redirect users you need to wrap you ProxyPass and Redirect directives into the newly introduced If statement: <If expression> ProxyPass… </If>"

Take a look at http://httpd.apache.org/docs/2.4/mod/core.html#if to find out more about the If directive, and http://httpd.apache.org/docs/2.4/expr.html to learn how to write an Apache expression.

Note that this is only valid in Apache httpd 2.4.

https://serverfault.com/questions/605867/apache-2-4-proxy-for-external-redirect-for-internal

Nginx Load Balancer

```
upstream webservers{
       server 192.168.1.1;
       server 192.168.1.2;
       server 192.168.1.3;
}

upstream honeypot  {
       server 192.168.1.6;
}
```

```
server {
        access_log  logs/access.log;
        error_log   logs/error.log;
        index       index.html;
        listen     *:80 default;

    root        /usr/local/nginx/html;

    server_name example.com www.example.com;

    location / {
       proxy_pass  http://webservers;
      if ($http_user_agent ~ Honey) {
        proxy_pass  http:/honeypot;
      }
```

Kong and Openresty

Kong is a scalable, open source API Layer (also known as an API Gateway, or API Middleware). Kong runs in front of any RESTful API and is extended through Plugins, which provide extra functionality and services beyond the core platform.

OpenResty® is a full-fledged web platform that integrates the standard Nginx core, LuaJIT, many carefully written Lua libraries, lots of high quality 3rd-party Nginx modules, and most of their external dependencies. It is designed to help developers easily build scalable web applications, web services, and dynamic web gateways.

ModSecurity Redirect

```
SecRuleUpdateActionById 9888816:5 "setvar:ip.proxy_honeypot=1"

SecRule IP:PROXY_HONEYPOT "@eq 1"
"id:9999999",phase2,t:none,log,msg:'Send to Honey'.
proxy:'http://192.168.1%{REQUST_URI}'
```

https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-%28v2.x%29#proxy

Fail2ban Centos Iptables Setup

```
yum install fail2ban
yum install fail2ban-systemd
systemctl mask firewalld
systemctl enable iptables
systemctl enable ip6tables
systemctl stop firewalld
systemctl start iptables
systemctl start ip6tables
service fail2ban restart
```

```
#how you know its working
iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-N f2b-sshd
-A f2b-sshd -j RETURN
```

```
vim /etc/fail2ban/jail.d/00-firewalld.conf
[DEFAULT]
#banaction = firewallcmd-ipset
banaction = iptables-multiport

vim /etc/fail2ban/jail.conf
[DEFAULT]
bantime = 3600
banaction = iptables-multiport
```

Honey

- Honey Systems
  - Computer systems for the sole purpose of monitoring or catching malicious actors.
- Honey Token
  - Data in table that if it's accessed we know something is going on.
- Honey Tables
  - Tables in a database that if we see access attempts we know we have a malicious actor.
- Honey Domains
  - Sites that are setup to monitor malicious actors.
- Honey Urls
  - Urls we know normal users will never use and only malicious actors will hit.
- Honey Files
  - Files we want malicious actors to find.
- Honey Port
  - Ports we want malicious actors to try and scan or connect to.

Honey Domains

http://tools.kali.org/information-gathering/fierce

Some maybe all

list.somedomain.com
Images1.somedomain.com
club.somedomain.com
business.somedomain.com
update.somedomain.com
fw.somedomain.com

Honey Ports

/etc/fail2ban/action.d/iptables-honeyports.local

```
[INCLUDES]
before = common.conf

[Definition]
_daemon = kernel
failregex = ^%(__prefix_line)s.*HONEYPORT:
.*SRC=<HOST>
ignoreregex =
```

/etc/fail2ban/action.d/iptables-honeyports.local

```
[Definition]
actionstart = iptables -A INPUT -p tcp --syn -m multiport
-i <honeydev> --dports <honeyports> -j LOG --log-prefix
"HONEYPORT: "
actionstop = iptables -D INPUT -p tcp --syn -m multiport
-i <honeydev> --dports <honeyports> -j LOG --log-prefix
"HONEYPORT: "

actioncheck =
actionban =
actionunban =

[Init]
honeyports = 21,8080,9090,3066,
honeydev = enp0s8
```

Honey Port Denied

```
iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent \
  --set
iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent \
  --update --seconds 60 --hitcount 3 -j DROP
```

https://debian-administration.org/article/187/Using_iptables_to_rate-limit_incoming_connections

https://brett.is/writing/about/fail2ban-honeypot/

Rate Limiting

#Limit NEW traffic on port 80

Iptables -A INPUT -s 1.1.1.1/32 -p tcp --dport 80 -m state --state NEW -m limit --limit 30/minute --limit-burst 200 -j ACCEPT

#Second rule – Limit established traffic

Iptables -A INPUT -s 1.1.1.1/32 -m state --state RELATED,ESTABLISHED -m limit --limit 50/second --limit-burst 50 -j ACCEPT

User Agent Strings Blocking

```
#Apache blocking

#module allows you to set internal environment
variables according to whether different aspects of
the request match regular expressions you specify

SetEnvIfNoCase User-Agent "^Wget" denied

<Directory "/var/www">

        Order Allow,Deny
        Allow from all
        Deny from env=denied
</Directory>
```

```
#Dynamic Logging

LogFormat "%a %{User-agent}i" useragent

CustomLog /var/log/httpd/useragents.log useragent
```

#modsecurity

SecDefaultAction
phase:2,pass,status:403,log,auditlog

SecRule REQUEST_HEADERS:User-Agent "!Wget" "phase:2,deny,msg:'get user agent denied"

https://techblog.willshouse.com/2012/01/03/most-common-user-agents/

Useragent String & FAIL2BAN

vim /etc/fail2ban/jail.conf

```
[apache-bad-user-agent]
enabled  = true
port     = 80,443
protocol = tcp
filter   = baduseragent
maxretry = 1
bantime  = 86400
logpath  = /var/log/httpd/useragent.log
```

/etc/fail2ban/jail.conf

```
[apache-bad-user-agent]
enabled  = true
port     = 80,443
protocol = tcp
filter   = baduseragent
maxretry = 1
bantime  = 86400
logpath  = /var/log/httpd/useragent.log
```

Protect Against Brute Force

```
# Block further login attempts after 3 failed attempts

<LocationMatch ^/login>
# Initialize IP collection with user's IP address
SecAction "initcol:ip=%{REMOTE_ADDR},pass,nolog"
# Detect failed login attempts
SecRule RESPONSE_BODY "Username does not exist" "phase:4,pass,setvar:
ip.failed_logins=+1,expirevar:ip.failed_logins=60"
# Block subsequent login attempts
SecRule IP:FAILED_LOGINS "@gt 3" deny

</Location>
```

ModRewrite Traps

RewriteMap badlist txt:~/bad_useragent_list

RewriteCond %{HTTP_USER_AGENT} .* [NC]

RewriteCond ${badlist:%1|white} ^black$ [NC]

RewriteRule (.*) "/itsatrap.php" [L]

https://perishablepress.com/eight-ways-to-blacklist-with-apaches-mod_rewrite/

http://httpd.apache.org/docs/current/mod/mod_rewrite.html

http://serverfault.com/questions/251988/blocking-apache-access-via-user-agent-string

PHP Trap Code

```
<?PHP #random error code
$rand = rand(1,3);
if($rand == 1 ){
	http_response_code(404);
}
if($rand == 2){
	http_response_code(403);
}
if($rand == 3){
	http_response_code(501);
}
```

Honey Url

61.x.x.236 - - [13/Mar/2016:16:43:16 -0400] "GET //phpmyadmin/scripts/setup.php HTTP/1.1" 301 184 "-" "-"
61.x.x.236 - - [13/Mar/2016:16:43:17 -0400] "GET //phpmyadmin1/scripts/setup.php HTTP/1.1" 301 184 "-" "-"
189.x.x.102 - - [12/Mar/2016:16:15:12 -0500] "HEAD http://192.64.80.52:80/PMA2015/ HTTP/1.1" 301 0 "-" "Mozilla/5.0 Jorgee"
183.x.x.26 - - [14/Feb/2016:01:37:16 -0500] "POST /doLogin.do HTTP/1.1" 301 184 "-" "Mozilla/5.0" POST /loginUI.action
183.x.x.187 - - [08/Jan/2016:18:51:43 -0500] "GET /mail/auth/login HTTP/1.1" 301 184 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_4) AppleWebKit/537.36 (KHTML, like Gecko)
61.x.x.236 - - [13/Mar/2016:16:48:25 -0400] "GET //web/scripts/setup.php HTTP/1.1" 301 184 "-" "-"
92.x.x.134 - - [15/Feb/2016:01:36:39 -0500] "GET /scripts/moadmin.php HTTP/1.1" 301 184 "http://www.obscuritysystems.com/scripts/moadmin.php" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461)"

http://www.skepticism.us/2015/05/new-malware-user-agent-value-jorgee/

ModSecurity Redirect Blocking

SecFilterSelective REMOTE_ADDR “!192.168.1.2” chain

SecFilterSelective REQUEST_URI “/wp-login.php”
log,deny,redirect:http://www.somewhere.com/nologin.html

robots.txt

https://www.dc801.org/robots.txt

Disallow:
User-agent: *
Disallow: /admin
Disallow: /passwords
Disallow: /sensitive

Honey Token Detection MySQL

```
#!/bin/bash

honey_token=$(grep "ABCDEF" /var/lib/mysql/queries.log | wc -l)

if [ "$honey_token" -gt 1 ]

then

        logger "Honey Token Alert ABCDEF"

        mail -s "Honey Token Alert ABCDEF" you@somesite.com <<< "Alert Honey Token"

fi
```

MySQL Setup

[mysqld]

general-log
general-log-file=queries.log
log-output=file

https://mariadb.com/kb/en/mariadb/general-query-log/

Named pipes

mkfifo the_pipe
reader_command < the_pipe &
writer_command > the_pipe

http://dba.stackexchange.com/questions/3552/how-do-i-output-mysql-logs-to-syslog/5106#5106

http://lists.mysql.com/mysql/191664

http://dba.stackexchange.com/questions/3552/how-do-i-output-mysql-logs-to-syslog/3571#3571

Honey Table Detection

Same as a honey token but contains data we know attackers want.

Assuming that your system is compromised. Think as if you're a hacker trying to steal data. What would you try pulling down first?

Create tables that look attractive so that hackers try and dump data.

Such as A_PAN A_SSN A_USERNAMES.

The reason we are using A at the beginning of the table names is due to the fact most SQL injection tools start in alphabetical order when probing to determine database names.

ModSecurity Honey Token Detection

```
SecRule RESPONSE_BODY "@rx  honeytoken" \

 "phase:4,log,pass,t:none,msg:'Honey token detected'"
```

Honey File

```
#!/bin/bash

while true; do

    inotifywait -q -e access /root/systempasswords.txt

     mail -s "Honey Token Alert systempassword.txt" you@somesite.com <<< "Alert Honey Token"

    logger "Honey file has been read"

done

#https://linux.die.net/man/1/inotifywait
```

Honey Docs

A honey file might contain instructions for using a “Admin portal” that contains username and passwords used as honey tokens.

The document would be placed in a folder such as https://mysecuresite.com/test/

Counter Hacking and Intelligence Gathering

Active Cyber Defense Certainty Act (ACDC)

The Active Cyber Defense Certainty Act (ACDC) amends the Computer Fraud and Abuse Act to make limited retaliatory strikes against cyber-miscreants legal in America for the first time. The bill would allow hacked organizations to venture outside their networks to identify an intruder and infiltrate their systems, destroy any data that had been stolen, and deploy "beaconing technology" to trace the physical location of the attacker. - Iain Thomson in San Francisco 13 Oct 2017

https://www.theregister.co.uk/2017/10/13/us_hack_back_law/

MalwareTech

@MalwareTechBlog

Follow

I never thought of it this way. It's basically the cyber version of being allowed to murder someone for entering your property.

https://twitter.com/MalwareTechBlog/status/918930856969830400

Section 1030 - Fraud and related activity in connection with computers

A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

https://casetext.com/statute/united-states-code/title-18-crimes-and-criminal-procedure/part-i-crimes/chapter-47-fraud-and-false-statements/section-1030-fraud-and-related-activity-in-connection-with-computers

H.R.3270 - Active Cyber Defense Certainty Act

- Section 3: Exceptions for the Use of Attributional Technology
- Section 4: Exclusion From Prosecution for Certain Computer Crimes for Those Taking Active Cyber Defense Measures
- Section 5: Notification Requirement for the Use of ACDMs
- Section 6: Voluntary Preemptive Review of ACMDs
- Section 7: Annual Report on the Federal Government's Progress in Deterring Cyber Fraud and Cyber-Enabled Crimes

https://www.congress.gov/bill/116th-congress/house-bill/3270

https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act

Client Side Attacks

“Most attacks are conducted against servers, but as services have become harder to attack, easier targets have been selected. Client-side attacks are a result of this, where an attacker will target the various applications installed on the workstation of an employee within a target organization. “ (offensive security)

https://kali.training/topic/types-of-attacks/

Microsoft Office Example

- https://blog.cystack.net/word-based-malware-attack/

Adobe Example

- https://www.offensive-security.com/metasploit-unleashed/client-side-exploits/

SImple Word User Enumeration

By merely embedding an image in a word document, we can enumerate a personal IP address and location by having the document reference images on our web server.

Only works if user isn’t using a VPN or TOR.

AutoSave Off test.docx - Saved Search Sign in

File Home Insert Draw Design Layout References Mailings Review View Help Share Comments

Paste Clipboard Calibri (Body) 11 Font Paragraph Styles Editing Dictate Voice

DEEPSEC
IN-DEPTH SECURITY

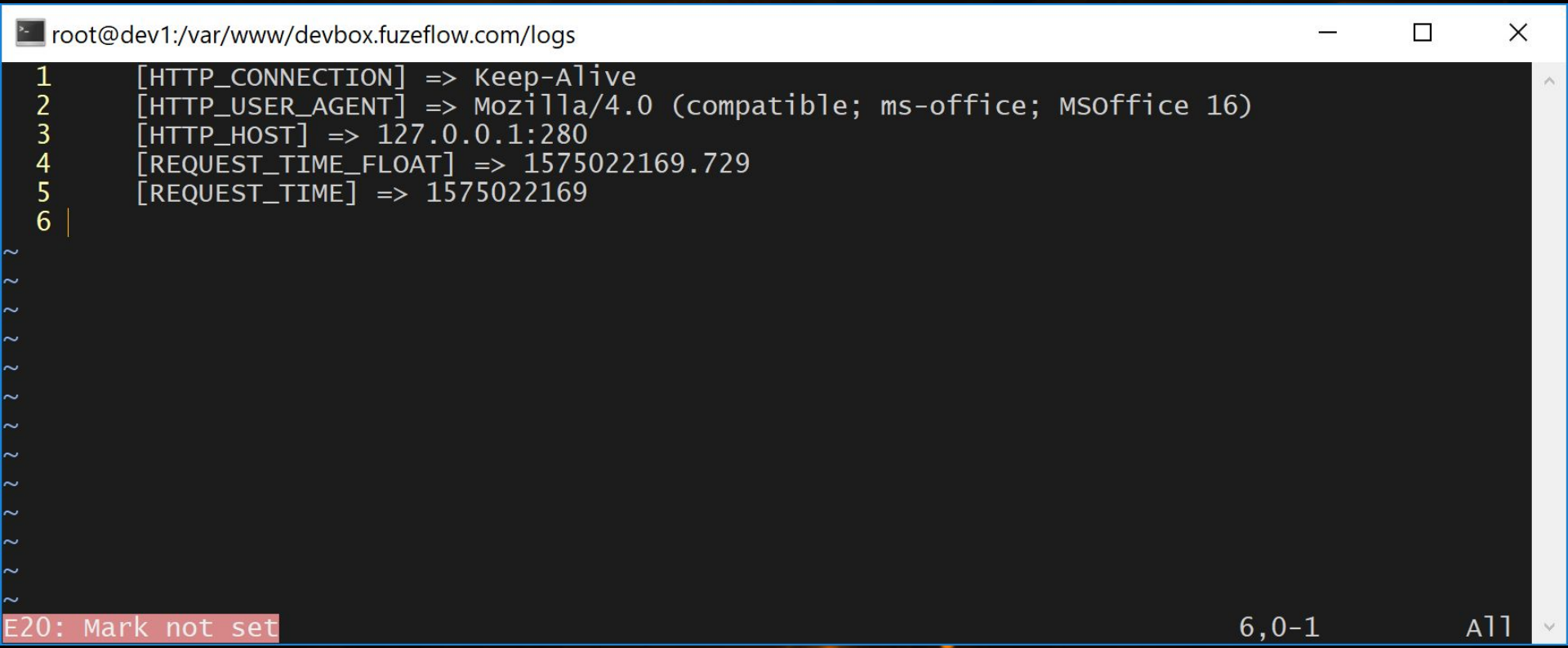
Hello WOrld

Page 1 of 1 2 words Focus 100%

Word Image Enumeration

root@dev1:/var/www/html

```
<?PHP
file_put_contents('/var/logs/server',print_r($_SERVER,true)."\n",FILE_APPEND);
// open the file in a binary mode
$name = 'DeepSec_Hat.png';
$fp = fopen($name, 'rb');

// send the right headers
header("Content-Type: image/png");
header("Content-Length: " . filesize($name));

// dump the picture and stop the script
fpassthru($fp);
exit;
~
                                                    2,25          All
```


root@dev1:/var/www/devbox.fuzeflow.com/logs
[HTTP_CONNECTION] => Keep-Alive
[HTTP_USER_AGENT] => Mozilla/4.0 (compatible; ms-office; MSOffice 16)
[HTTP_HOST] => 127.0.0.1:280
[REQUEST_TIME_FLOAT] => 1575022169.729
[REQUEST_TIME] => 1575022169
E20: Mark not set
6,0-1
All

BeEF

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

https://github.com/beefproject/beef/wiki

http://beefproject.com/

What can Beef do?

Network Discovery
https://github.com/beefproject/beef/wiki/Network-Discovery

Information Gathering
https://github.com/beefproject/beef/wiki/Information-Gathering

Social Engineering
https://github.com/beefproject/beef/wiki/Social-Engineering

Geolocation
https://github.com/beefproject/beef/wiki/Geolocation

Persistence
https://github.com/beefproject/beef/wiki/Persistence

Getting Started | Logs | **Current Browser**

Details | Logs | Commands | Rider | XssRays | Ipec | Network | WebRTC

Category: Browser (6 Items)

Browser Version: UNKNOWN

Browser UA String: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0

Browser Language: en-US

Browser Platform: Win32

Browser Plugins: Shockwave Flash

Window Size: Width: 2234, Height: 975

Category: Browser Components (12 Items)

Flash: Yes

VBScript: No

PhoneGap: No

Google Gears: No

Web Sockets: Yes

QuickTime: No

RealPlayer: No

Windows Media Player: No

WebRTC: Yes

ActiveX: No

Session Cookies: Yes

Persistent Cookies: Yes

Category: Hooked Page (5 Items)

Page Title: BeEF Basic Demo

Page URI: http://10.254.10.165:3000/demos/basic.html

Page Referrer: Unknown

Host Name/IP: 10.254.10.165

Cookies: BEEFHOOK=juo7LqsJ4XF0bVbcEjNb7sMVMIg9b3OJkuijbWHxghmaTXW8skttUyQrMxSqUZbH2fws4VgNWO4ZJh6T

Category: Host (8 Items)

Host Name/IP: 10.254.10.99

Date: Tue Oct 10 2017 00:37:35 GMT-0600 (Mountain Standard Time)

Social Engineer Toolkit

https://www.trustedsec.com/social-engineer-toolkit/

https://github.com/trustedsec/social-engineer-toolkit/raw/master/readme/User_Manual.pdf

Spear-Phishing Attack Vector

Java Applet Attack Vector

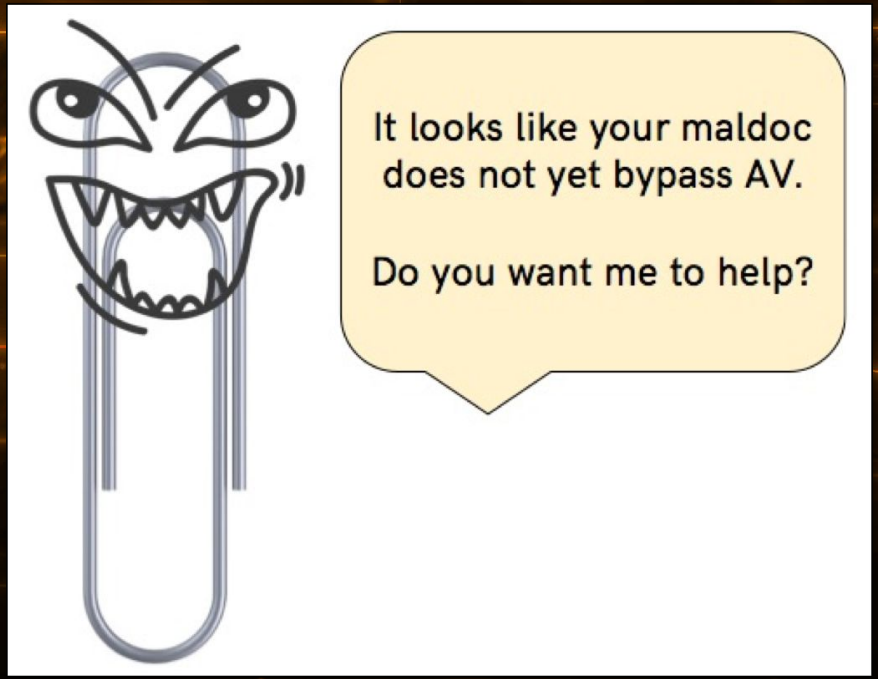
Metasploit Malicious VBA

Metasploit has a couple of built in methods you can use to infect Word and Excel documents with malicious Metasploit payloads.

https://www.offensive-security.com/metasploit-unleashed/vbscript-infection-methods/

Evil Clippy

https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldoc-assistant/



References

http://security.stackexchange.com/questions/24700/is-hacking-back-a-valid-security-technique-for-companies

https://www.upcloud.com/support/installing-fail2ban-on-centos-7/

http://blog.haproxy.com/2012/10/12/scalable-waf-protection-with-haproxy-and-apache-with-modsecurity/

https://blog.inliniac.net/2006/08/09/mod_security-redirection/

https://debian-administration.org/article/187/Using_iptables_to_rate-limit_incoming_connections

http://www.sectechno.com/idenifying-the-real-ip-address-of-a-hiden-hacker/

References part 2

http://www.darkreading.com/vulnerabilities---threats/5-reasons-every-company-should-have-a-honeypot/d/d-id/1140595?

https://www.sans.org/security-resources/idfaq/what-is-p0f-and-what-does-it-do/3/14

https://samhobbs.co.uk/2014/08/introduction-fail2ban

https://www.sans.org/reading-room/whitepapers/attacking/catching-flies-guide-flavors-honeypots-36897

Reference Part 3

US Congress mulls first 'hack back' revenge law. And yup, you can guess what it'll let people do

Iain Thomson in San Francisco 13 Oct 2017 at 22:36 tweet_btn() - https://www.theregister.co.uk/2017/10/13/us_hack_back_law/

Offensive Countermeasures: Making Attackers Lives Miserable

https://docs.huihoo.com/rsaconference/usa-2012/Offensive-Countermeasures-Making-Attackers-Lives-Miserable.pdf