Active Web Application Defense

OverDrive Conference

Lance Buttars @Nemus801

Updated Slides @

http://www.introtobackdoors.com/

Nemus@dc801.org

Who am I

Twitter @Nemus801

Vice President of Software Engineering

GIAC Web Application Penetration Tester (GWAPT)

Defcon Group **www.dc801.org**
Freenode #dc801

My Defcon Presentations
http://www.introtobackdoors.com/

My Presentations

http://obscuritysystems.com/index.html

DC801 Organizer

https://defcongroups.org/dcgfaq.html

Requirements are that they are open to everyone and they are free.

DC801 is ran by local people.

We recorded our monthly presentations.

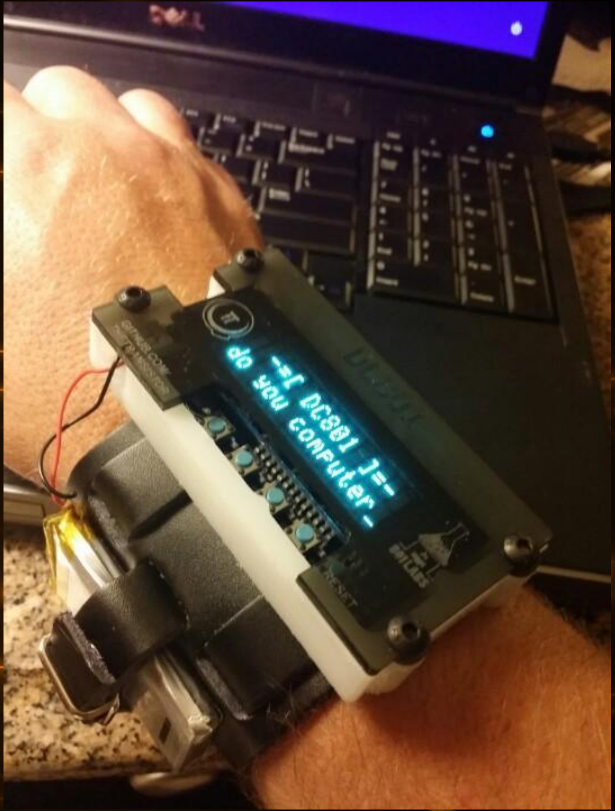
https://www.youtube.com/channel/UCaapPdadqEK-S8RTCBgvhJQ

Twitter @DC801

DC801

IT SECURITY PROJECT MANAGEMENT
HACK PROOFING
HACK PROOFING
HACK PROOFING
SECURITY ASSESSMENT
CYBER SPYING
HACKING THE CODE
SPYWARE IN THE ENTERPRISE
WRITING SECURITY TOOLS & EXPLOITS
BigNum MATH
SPAM CARTEL
SPAM CARTEL
ENEMY AT THE WATER COOLER
SOFTWARE PIRACY EXPOSED
INSIDER THREAT
SOCKETS, SHELLCODE, PORTING & CODING
IM & P2P APPLICATIONS
SPYWARE IN THE ENTERPRISE
PHISHING EXPOSED
BUFFER OVERFLOWS
Running Linux
Learning XML
OpenSSL
SECURITY ASSESSMENT
SMALL BUSINESS SERVER 2003
SECURITY LOG MANAGEMENT
NESSUS
SNIFFER PRO
CISCO PIX FIREWALLS
Network+
Honeypots
Privacy Defended
GRAY HAT HACKING
EXPLOITING
CISSP

801 LABS


-=[DC801]=-
do you computer -
801 LABS

SAINTCON

801 LABS

Local Community Hackerspace of SLC.

Is supported by local members who pay the monthly membership fee.

We are more of a hackerspace and less of a maker space. The difference is the focus. Our hackerspace focuses more on security research than on building and making.

https://www.801labs.org/

Twitter @801labs

Bsides SLC

BSides is a community-driven framework for building events for and by information security community members. The goal is to expand the spectrum of conversation.

https://www.bsidesslc.org/2017.html

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.
- 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.

What is Counter Hacking?

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

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

NOW AND THEN, I ANNOUNCE "I KNOW YOU'RE LISTENING" TO EMPTY ROOMS.
IF I'M WRONG, NO ONE KNOWS.
AND IF I'M RIGHT, MAYBE I JUST FREAKED THE HELL OUT OF SOME SECRET ORGANIZATION.

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>

So?

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

This presentation is about how you can go about fighting back not weather or not you should.

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

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?

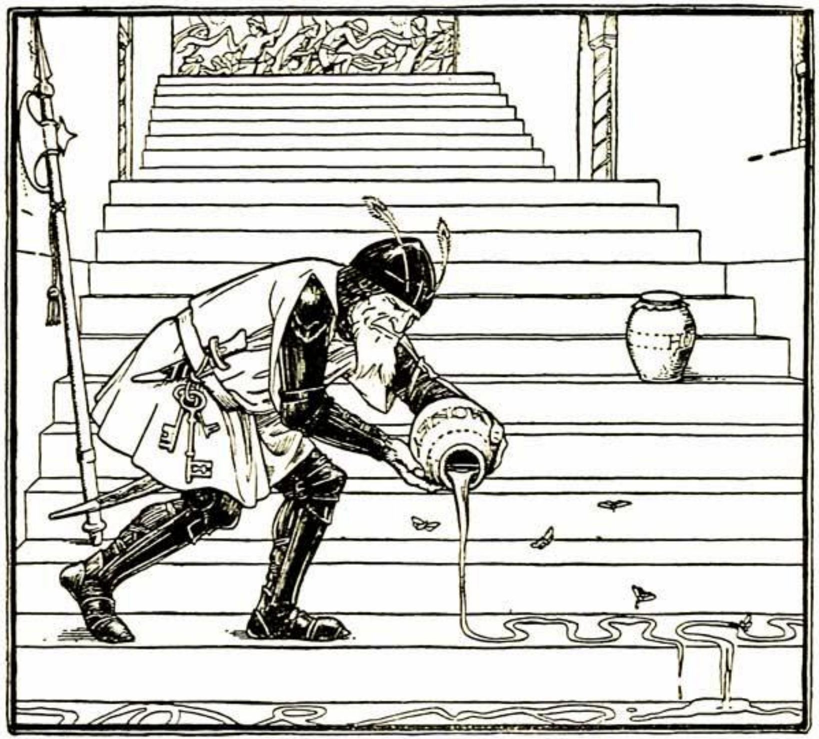
What if our Intrusion Detection System (IDS) misses the attack?

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

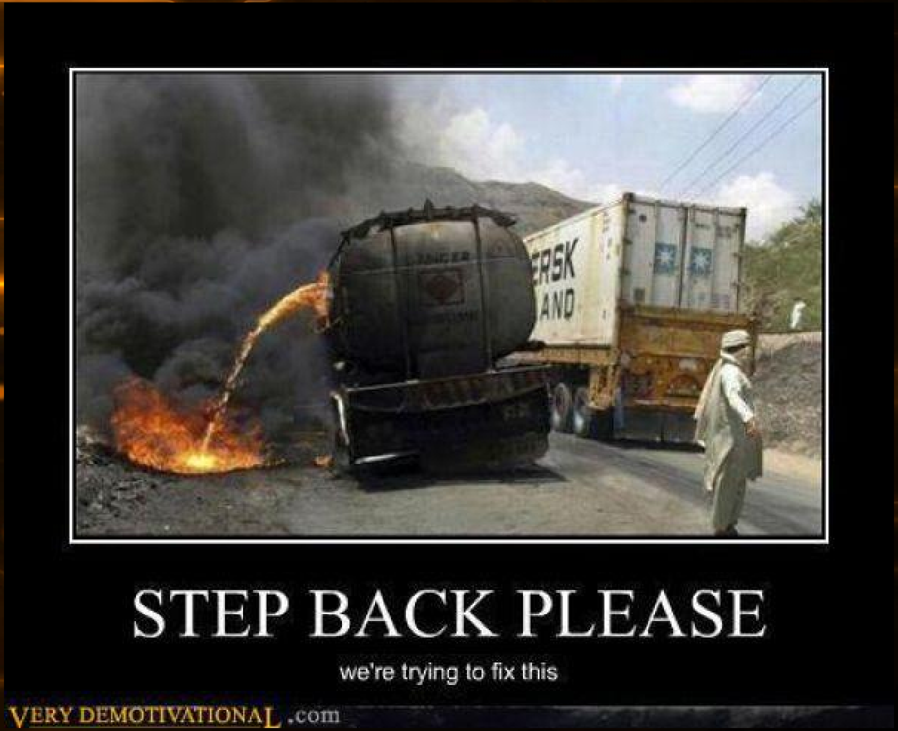
Detection Honeypot

- 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

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.

elastic + + kibana

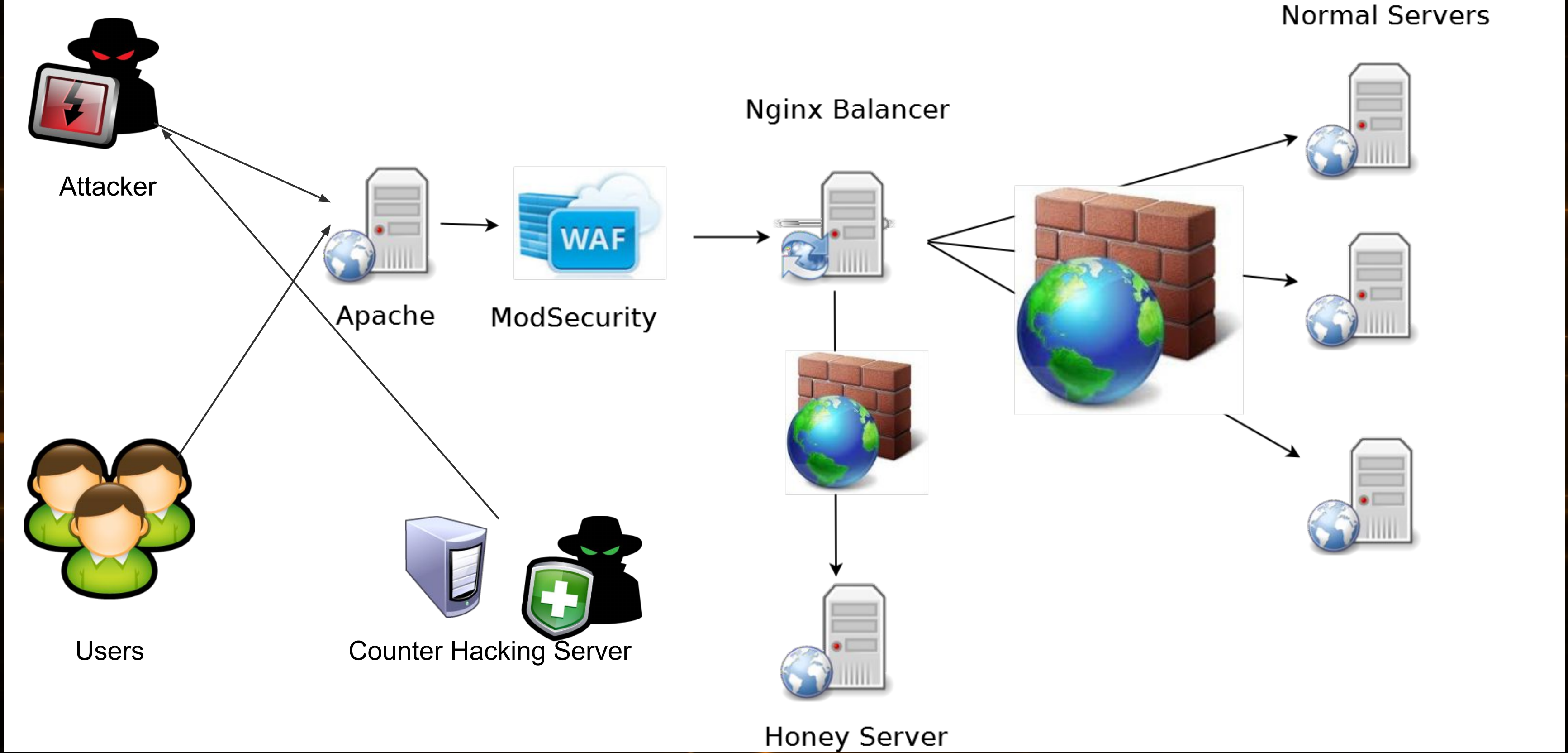
Apache

modsecurity

Open Source Web Application Firewall

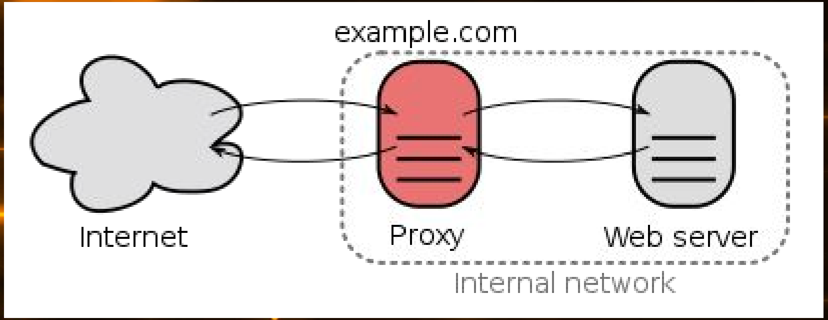
NGINX

Diagram


Normal Servers
Nginx Balancer
Attacker
Apache
WAF
ModSecurity
Users
Counter Hacking 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>
```



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;
     }
```

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
```

```
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
```

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

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

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>
# Initalize 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
```

HTTrack

Httrack is a program that copies websites.

It will download the internet if you let it.

```
httrack <URL of the site> [options] URL Filter -O <location to write copy>
httrack http://www.mycopysite.com -O /tmp/mycopy
```

https://www.httrack.com/html/fcguide.html

http://null-byte.wonderhowto.com/how-to/hack-like-pro-clone-any-website-using-httrack-0152420/

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/

Decloaking Engine

http://decloak.net/ is dead :(

The Decloaking Engine was a tool designed by HD Moore, the father of the Metasploit platform, to de-anonymize Tor users.

Counter Hacking

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?

Auto pawn

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

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

BeEF Part 2

Geolocation

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

Persistence

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

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

Malicious Word Documents

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/

Whats Next?

How can I hide system monitoring from attackers when a system is compromised?

Defensive rootkit to hide system monitoring from hackers.

Send logging packets to random ip addresses to be picked up by IDS systems.

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