# ServerSide Attacks (Contd)

## Tools in Kali Linux

## Module #20

# Kali Linux: Exploiting mail system

Email servers hold valuable information making them a high priority target for attackers.

The good news for consumers is that correctly configured modern e-mail systems are extremely difficult to exploit.

This does not mean e-mail systems are not vulnerable to attacks since most e-mail systems have web applications and are accessed through a web interface.

This promotes the possibility of a remote attacker gaining access to a core system that could be leveraged as a jumping point to other internal systems.

# Kali Linux: Mail servers hosting systems?

Which is the mail server to be attacked?

Recall : Reconnaissance method (Using 'fierce' Kali Linux command)
First we need to see if the mail server is vulnerable to direct commands.
The main purpose for which most attackers want to exploit mail servers is to spoof e-mails and use the e-mail server as an unauthorized e-mail relay server.

# Kali Linux: Use netcat?

Netcat is a computer networking service for reading from and writing to network connections using TCP or UDP.
Netcat is designed to be a dependable "back-end" device that can be used directly or easily driven by other programs and scripts.
Netcat is also a feature-rich network debugging and investigation tool with the ability to produce almost any kind of correlation using a number of built-in capabilities.

```
root@kali:~# netcat mail.secmob.net 25
```

Once we connect to the server using Netcat, we use the HELO command to tell the server who we are

# Kali Linux: Use netcat?

If we receive a response, we can manipulate most servers using the SMTP commands (some systems may not be vulnerable based on configuration and system type).

HELO , MAIL FROM , RCPT To , and Data are the only required fields.

You can use other fields to hide who the e-mail is being sent to and change the reply to address.

An example is changing the Reply to address with the goal of tricking a receiver into sending an e-mail to someone else.

# Kali Linux: Brute force attacks?

A brute-force attack is when all possible keys are checked against encrypted data until the right key is found.

Brute-force attacks are extremely costly from a resource & time perspective because the attacker is exploiting vulnerabilities in the encryption by taking advantage of key length and simplicity of the key.

A password is often based on dictionary words meaning the total space an attacker would have to test would be all words in a matching dictionary making the guessing scope significantly smaller than a password using random characters.

Best practice to mitigate brute-force attacks is using long and complicated keys as well as timeouts after a number of attempts and other methods to add more security factors.

# Kali Linux: Hydra?

Hydra is a tool developed by The Hacker's Choice (THC)
Uses the brute-force attack method to test against a variety of different protocols.
It is ideal for attacking e-mail systems because Hydra can target a specific IP and protocol such as the admin account for POP3 and SMTP used by the e-mail systems.
Prior to launching Hydra, you should perform Reconnaissance on a target such as a mail system
Following information should be available for Hydra:

- The target's IP address (for example, 192.168.1.1)
- Open Ports (for example, port 80 or 25)
- Protocol (for example, HTTP for web or SMTP for mail)
- User name (for example, admin)

# Kali Linux: Hydra?

Another Reconnaissance tool that is often used with Hydra is the Firefox plugin Tamper Data

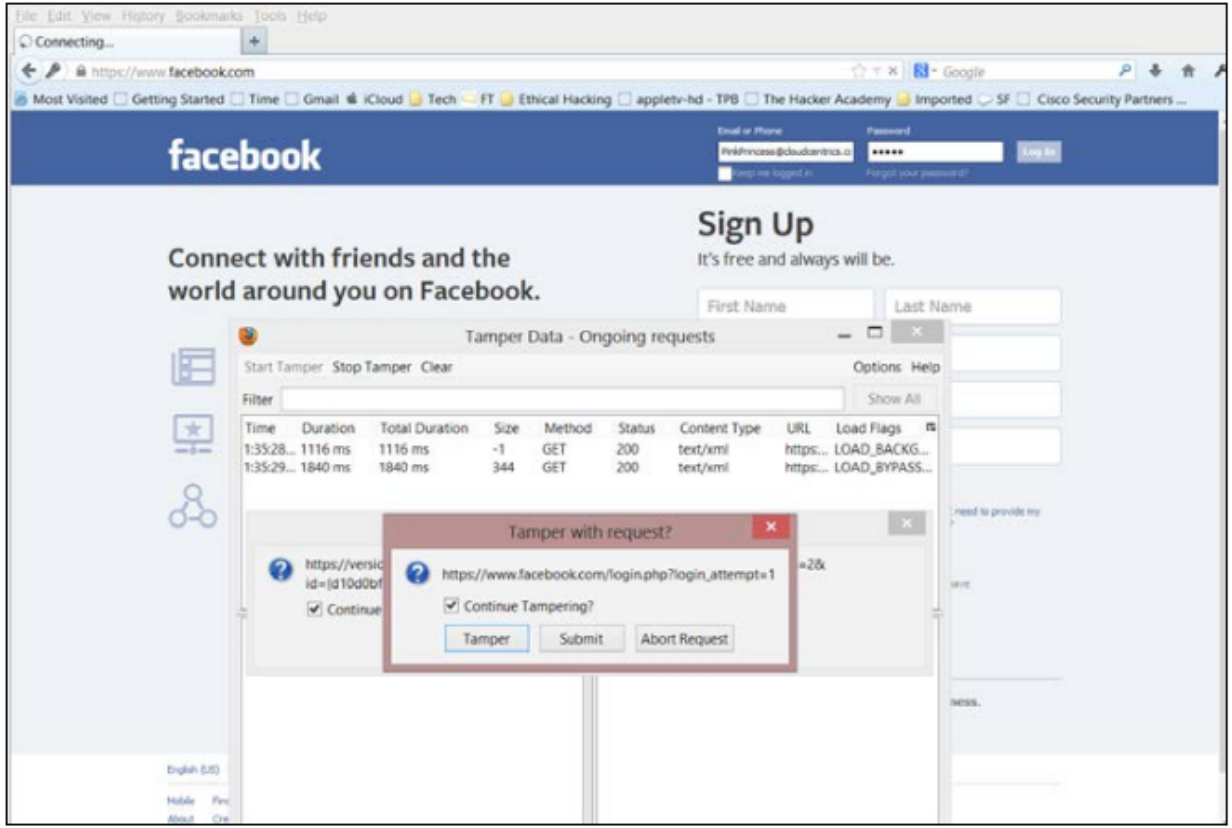
# Kali Linux: Hydra?

Tamper Data is a tool written by Adam Judson that allows an attacker to view HTTP GET and POST information.

This information is useful when using tools such as Hydra to brute-force web forms since you can automate Hydra into opening the webpage and testing the different username and password combinations.

Once we enable the Tamper Data plugin, we can launch the plugin and start it before we submit a name into a web form.

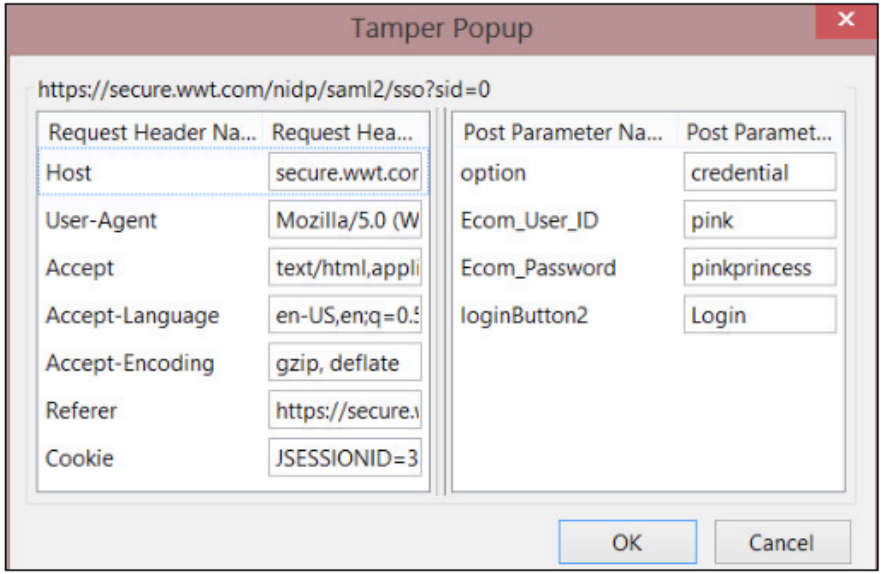
# Kali Linux: Tamper Data plugin?



# Kali Linux: Hydra?

Tamper Data will display information entered in the field groups. Attackers can manipulate and resubmit that data even if the website is encrypted.

In this example, username pink and password pinkprincess are used when the login button was submitted



# Kali Linux: Hydra in Kali Linux?

To access Hydra from the Kali, go to Password Attacks | Online Attacks and select Hydra.
This will open a Terminal window that will auto launch Hydra.

```
Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes.  Newest version available at http://www.thc.org/thc-hydra
The following services were not compiled in: sapr3 oracle.

Examples:
  hydra -l john -p doe 192.168.0.1 ftp
  hydra -L user.txt -p defaultpw -S 192.168.0.1 imap PLAIN
  hydra -l admin -P pass.txt http-proxy://192.168.0.1
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/DIGEST-MD5
root@kali:~#
```

# Kali Linux: Using Hydra

For example, if you want to attack an admin account's password file located at 192.168.1.1 using SMTP,

you would type:
hydra -l admin -p /root/password.txt 192.168.1.1 smtp

If you would like to use Hydra on a web form, we will need to gather the information we collected from the Tamper Data plugin.

The syntax for using Hydra on a web form is
<url>:<formparameters>:<failure string>

URL=https://www.facebook.com/login.php?
login_attempt=1email=pink&passwd=pinkprincessl&login="log in"

# Kali Linux: Using DirBuster

DirBuster is designed to brute-force directories and filenames on web application servers.
Applications and pages are actually hidden within the server.
DirBuster is designed to seek out these hidden factors.

Can be found under Web Applications | Web Crawlers.

Once opened, fields must be filled in before starting an attack.

At the very least, you must enter a target URL, select the number of threads (Suggestion: Max at 100), and the files list.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://www.thesecurityblogger.com

Work Method ○ Use GET requests only ◉ Auto Switch (HEAD and GET)

Number Of Threads 100 Thre... ☐ Go Faster

Select scanning type: ◉ List based brute force ○ Pure Brute Force

File with list of dirs/files

/root/Desktop/wordlist.lst Browse List Info

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ◉ Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files ☐ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

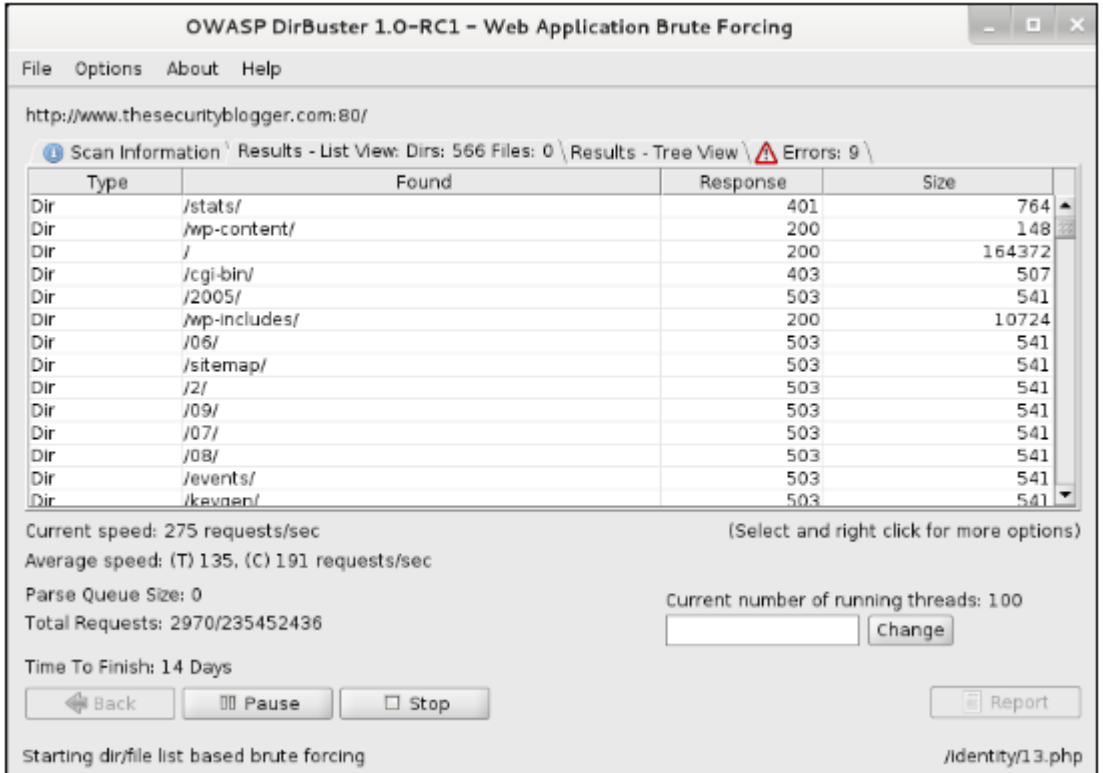
/

Exit Start

Please complete the test details

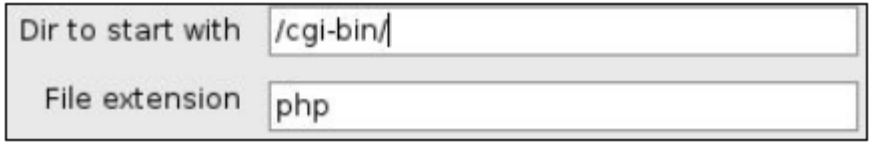
# Kali Linux: Using DirBuster?

Once you fill in the basic information, click on Start and DirBuster will start the vulnerability assessment.



# Kali Linux: Using DirBuster?

To target the /cbi-bin/ folder found during the scan, click on Stop to end the scan and click on Back. On the main dashboard, above Start, is a field for selecting the starting point of the vulnerability assessment. To start inside the /cbi-bin/ folder, place that text in that field and click on Start.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://www.thesecurityblogger.com:80/cgi-bin/

Scan Information | Results - List View: Dirs: 815 Files: 827 | Results - Tree View | Errors: 30

| Type | Found | Response | Size |
|---|---|---|---|
| Dir | /cgi-bin/ | 403 | 505 |
| Dir | /cgi-bin/article/ | 503 | 541 |
| Dir | /cgi-bin/special/ | 503 | 541 |
| Dir | /cgi-bin/support/ | 503 | 541 |
| Dir | /cgi-bin/09/ | 503 | 541 |
| Dir | /cgi-bin/login/ | 503 | 541 |
| Dir | /cgi-bin/2004/ | 503 | 541 |
| Dir | /cgi-bin/18/ | 503 | 541 |
| Dir | /cgi-bin/help/ | 503 | 541 |
| Dir | /cgi-bin/sp/ | 503 | 541 |
| Dir | /cgi-bin/profile/ | 503 | 541 |
| Dir | /cgi-bin/policies/ | 503 | 541 |
| Dir | /cgi-bin/more/ | 503 | 541 |
| Dir | /cgi-bin/info/ | 503 | 541 |

Current speed: 134 requests/sec

(Select and right click for more options)

Average speed: (T) 43, (C) 87 requests/sec

Parse Queue Size: 0

Current number of running threads: 100

Total Requests: 2928/337606829

Change

Time To Finish: 44 Days

Back Pause Stop Report

DirBuster Stopped

/cgi-bin/201/

# Kali Linux: Using DirBuster?

You can click on the Report button to generate a report of your findings.

DirBuster 1.0-RC1 Report Viewer

/root/Desktop/DirBusterReport-www.thesecurityblogger.com-80.txt

Full Text | Simple List | XML | CSV

```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Thu May 09 15:28:10 EDT 2013
--------------------------------

http://www.thesecurityblogger.com:80
--------------------------------
Directories found during testing:

Dirs found with a 403 response:

/cgi-bin/
/cgi-bin/test/

Dirs found with a 503 response:

/cgi-bin/features/
/cgi-bin/page/
/cgi-bin/5/
/cgi-bin/22/
/cgi-bin/docs/
```

Thank You