**ΠΑΠΑΔΟΠΟΥΛΟΣ ΓΙΩΡΓΟΣ**

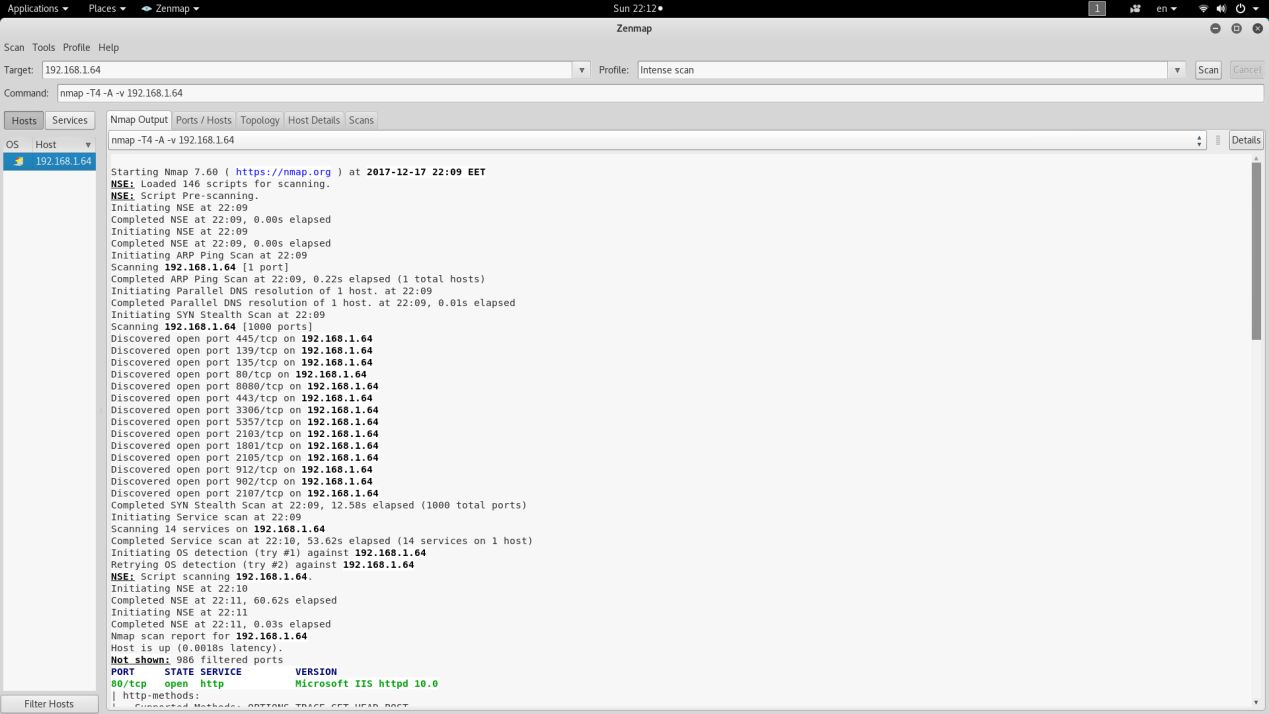
**4Η ΕΡΓΑΣΙΑ – ΤΕΧΝΙΚΟΣ ΕΛΕΓΧΟΣ ΑΔΥΝΑΜΙΩΝ**

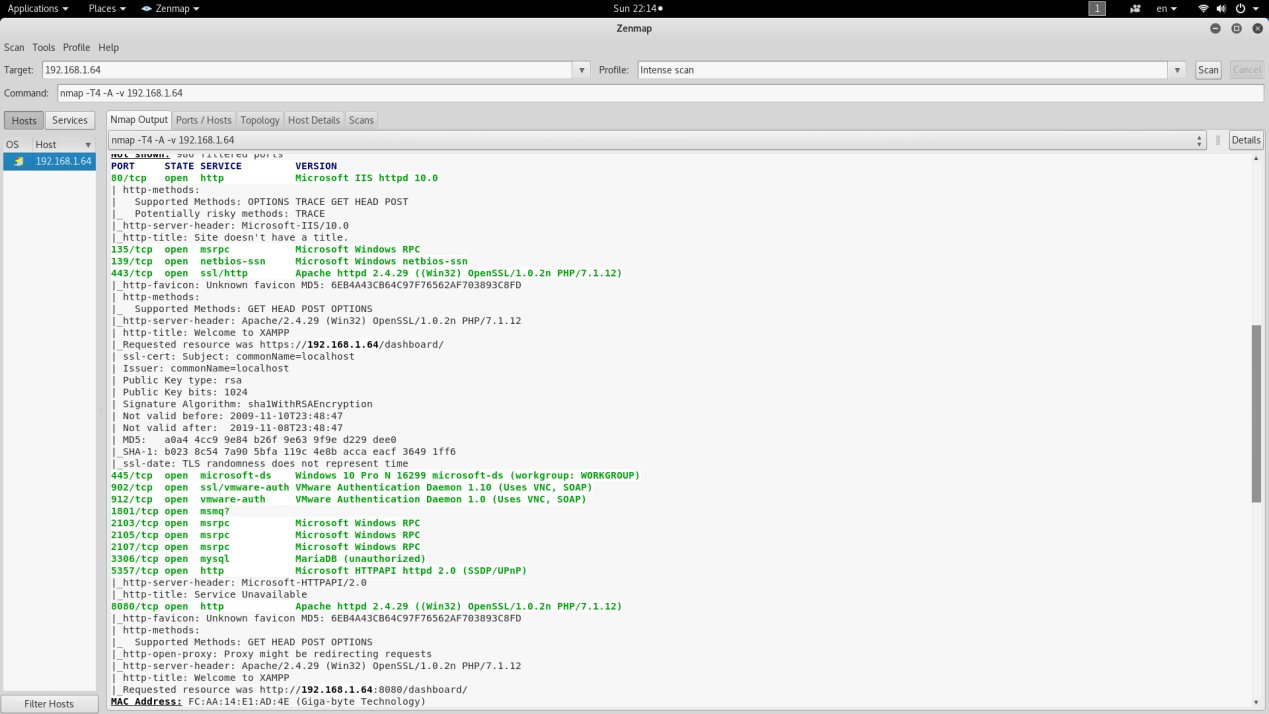
Η IP του στόχου είναι η 192.168.1.64

**NMAP:**

**Τρέξαμε τις εντολές:**

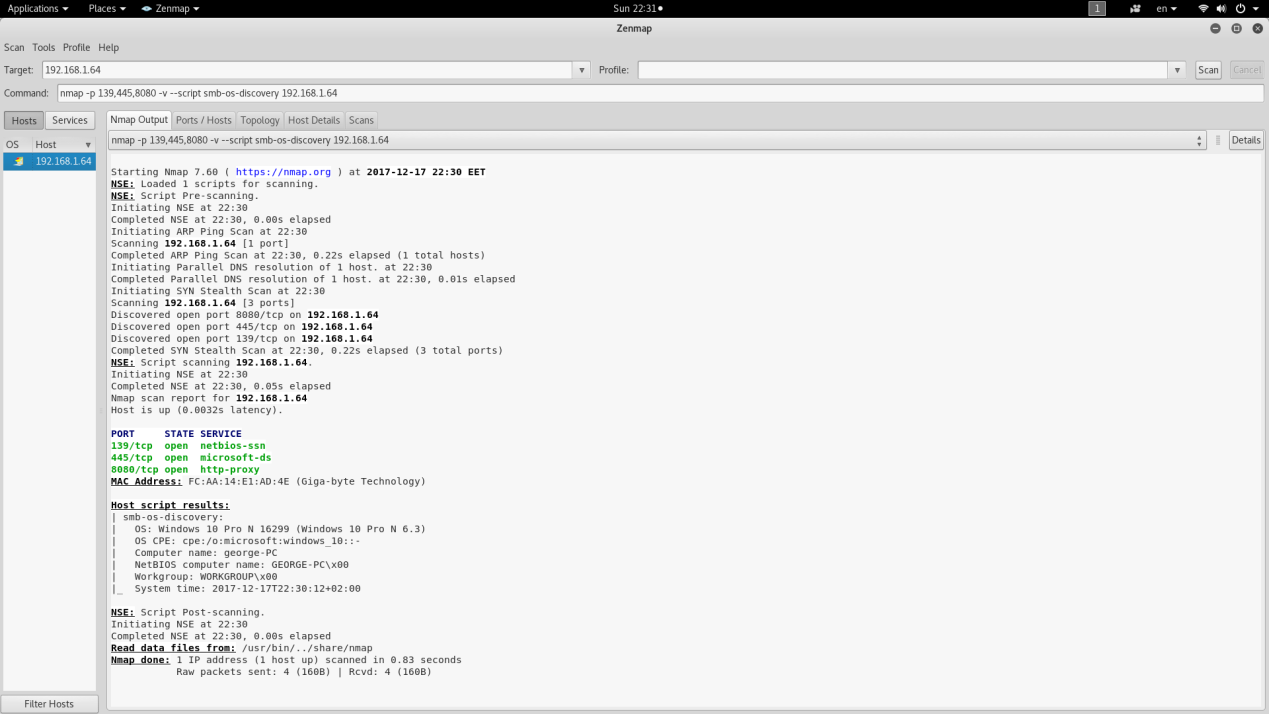
* nmap –T4 –A –v 192.168.1.64



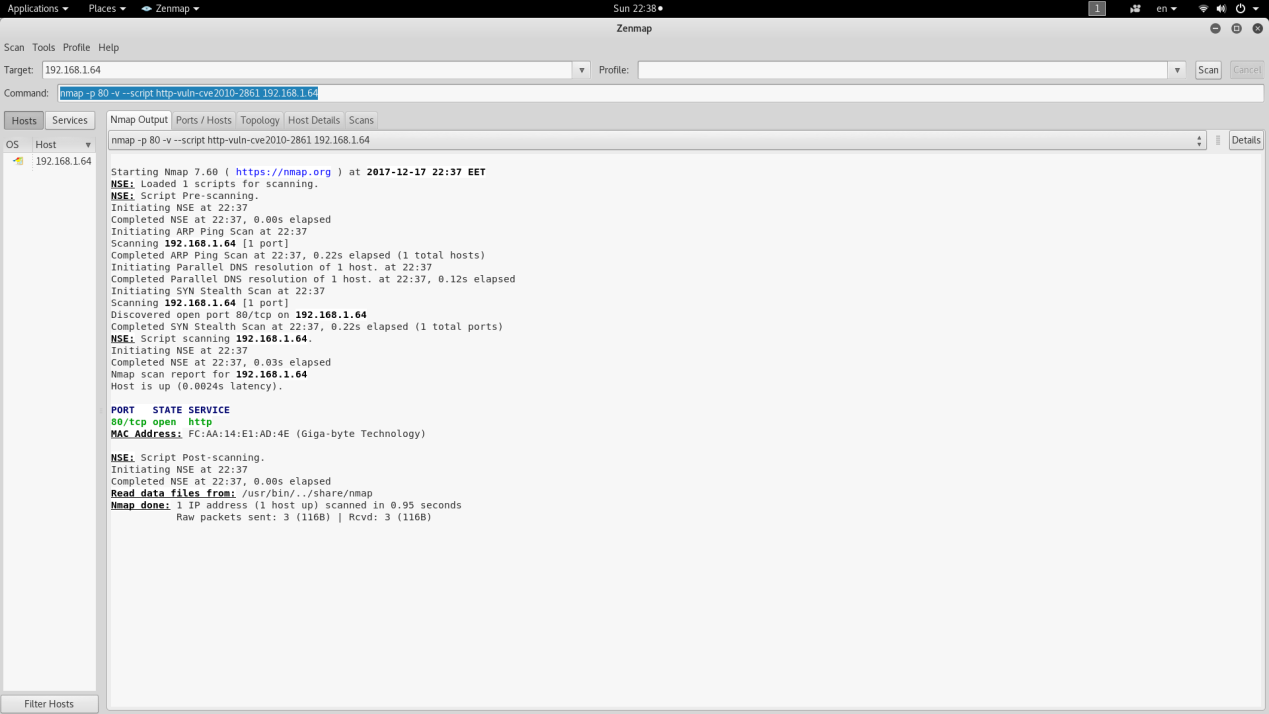




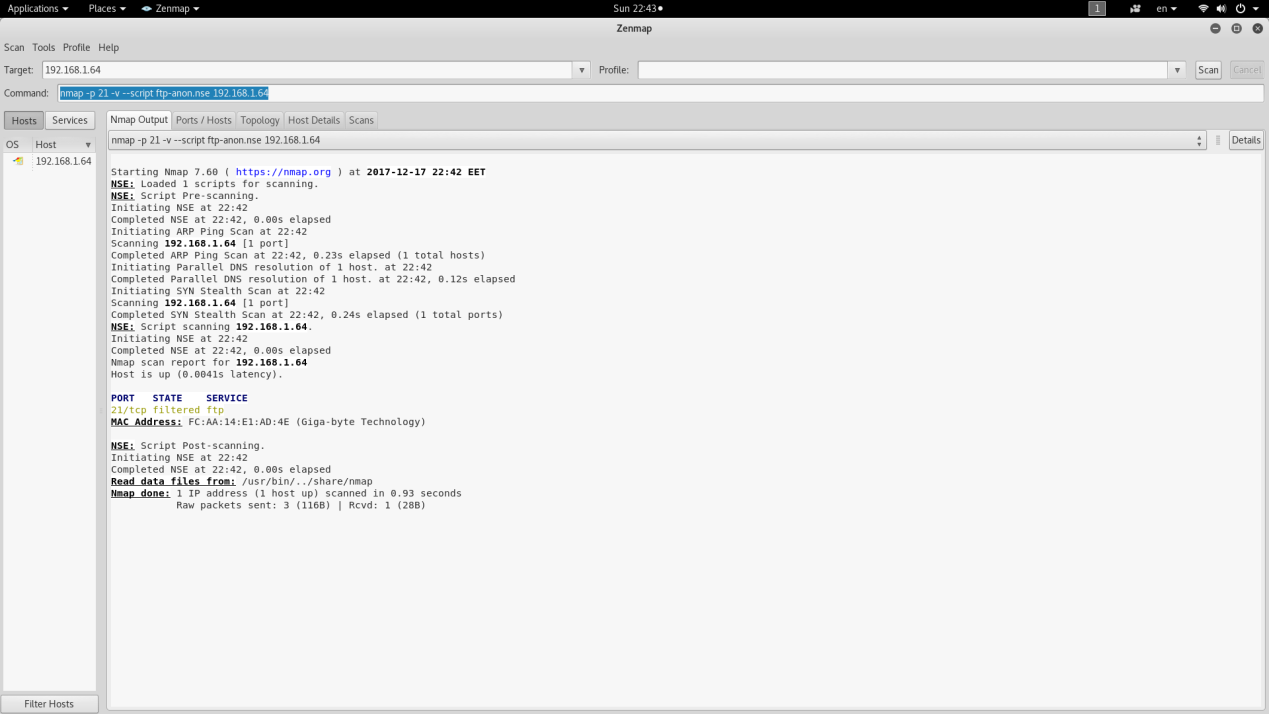
* nmap -p 139,445,8080 -v --script smb-os-discovery 192.168.1.64



* nmap -p 80 -v --script http-vuln-cve2010-2861 192.168.1.64



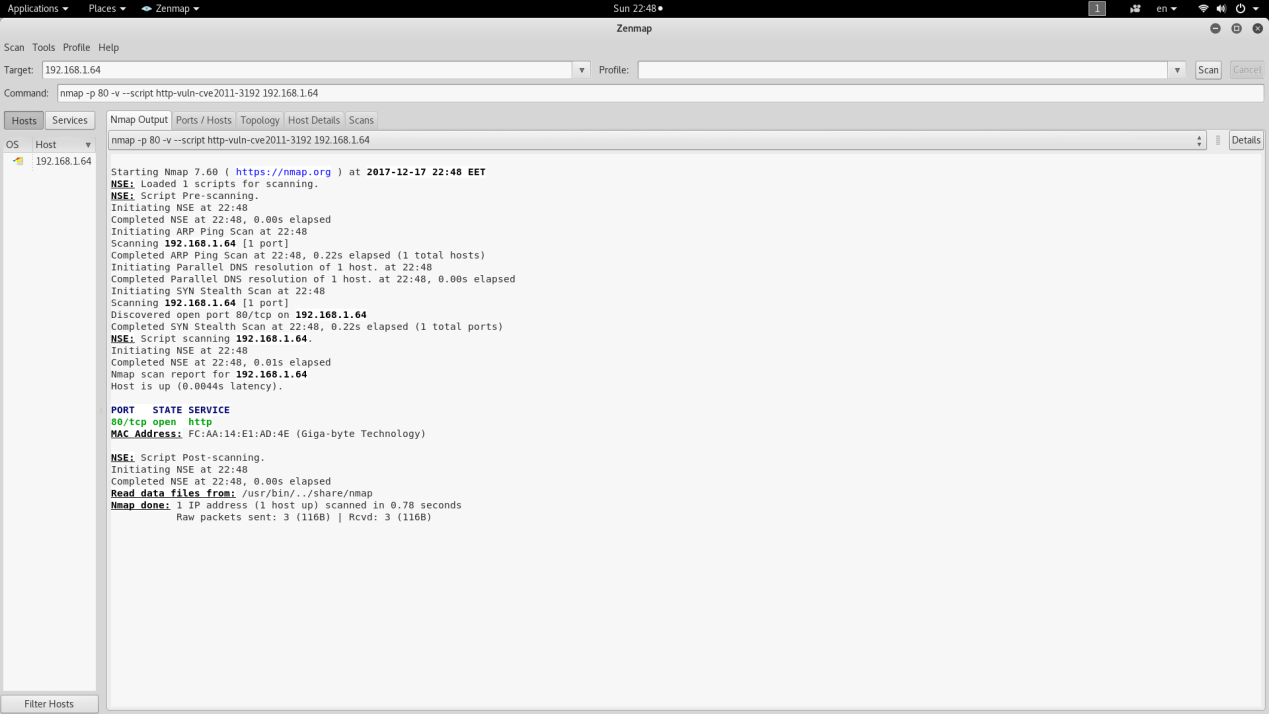
* nmap -p 21 -v --script ftp-anon.nse 192.168.1.64



* nmap -v -p 139, 445 --script=smb-security-mode 192.168.1.64



* nmap -p 80 -v --script http-vuln-cve2011-3192 192.168.1.64



**Και συμπεράναμε ότι *(χαρτογράφηση):***

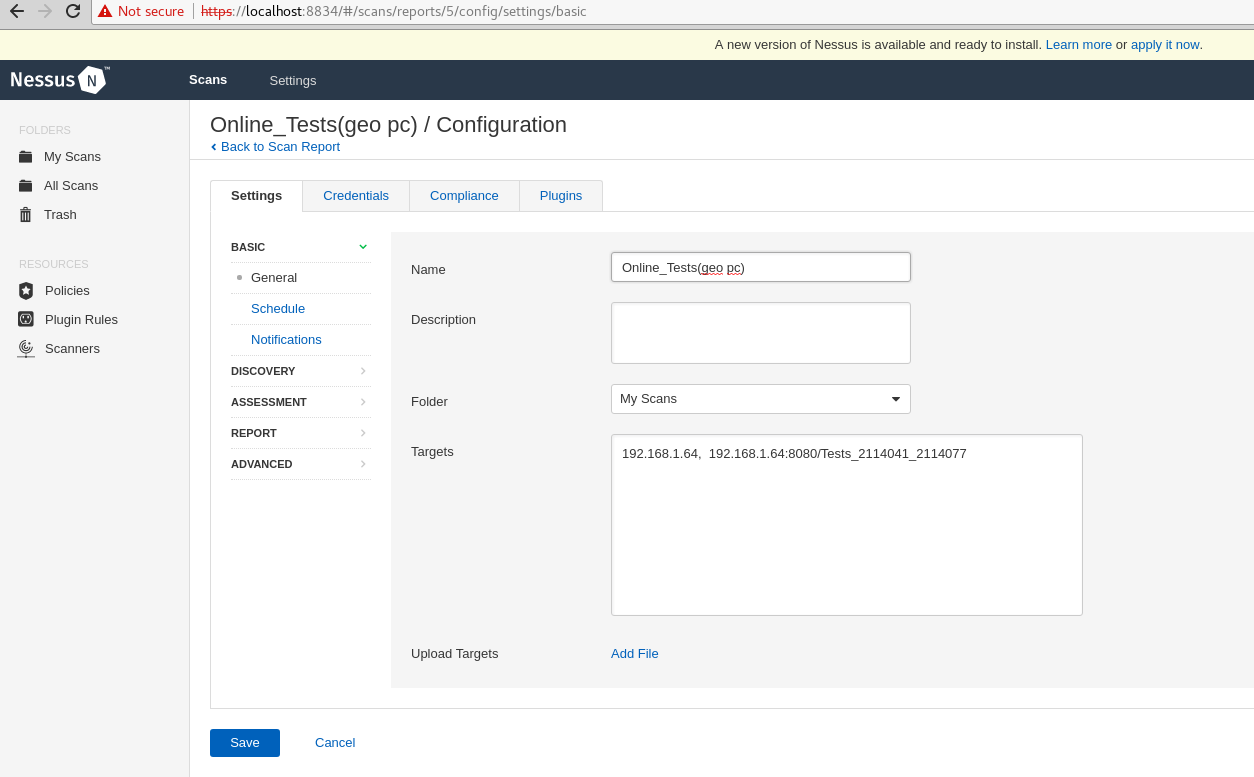
1. Το μηχάνημα τρέχει λογισμικό Windows 10 Pro N
2. Τρέχει apache server στην port 8080 με πρωτόκολλο http (όπως φαίνετε στις εικόνες παραπάνω)
3. Έχει έκδοση PHP/7.1.12
4. ***Βρήκαμε διαθέσιμα ports τα:***

* 80/tcp το οποίο χρησιμοποιεί http με αποτέλεσμα να υπάρχει κίνδυνος υποκλοπής των πακέτων, από την στιγμή που δεν είναι κρυπτογραφημένα.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Port** | **Protocol** | **State** | **Service** | **Version** |
| 80 | tcp | open | http | Microsoft IIS httpd 10.0 |
| 135 | tcp | open | msrpc | Microsoft Windows RPC |
| 139 | tcp | open | netbios-ssn | Microsoft Windows netbios-ssn |
| 443 | tcp | open | http | Apache httpd 2.4.29 ((Win32) OpenSSL/1.0.2n PHP/7.1.12) |
| 445 | tcp | open | microsoft-ds | Windows 10 Pro N 16299 microsoft-ds (workgroup: WORKGROUP) |
| 902 | tcp | open | vmware-auth | VMware Authentication Daemon 1.10 (Uses VNC, SOAP) |
| 912 | tcp | open | vmware-auth | VMware Authentication Daemon 1.0 (Uses VNC, SOAP) |
| 1801 | tcp | open | msmq |  |
| 2103 | tcp | open | msrpc | Microsoft Windows RPC |
| 2105 | tcp | open | msrpc | Microsoft Windows RPC |
| 2107 | tcp | open | msrpc | Microsoft Windows RPC |
| 3306 | tcp | open | mysql | MariaDB (unauthorized) |
| 5357 | tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
| 8080 | tcp | open | http | Apache httpd 2.4.29 ((Win32) OpenSSL/1.0.2n PHP/7.1.12) |

**NESSUS**: Ανίχνευση αδυναμιών σε επίπεδο υποδομής.

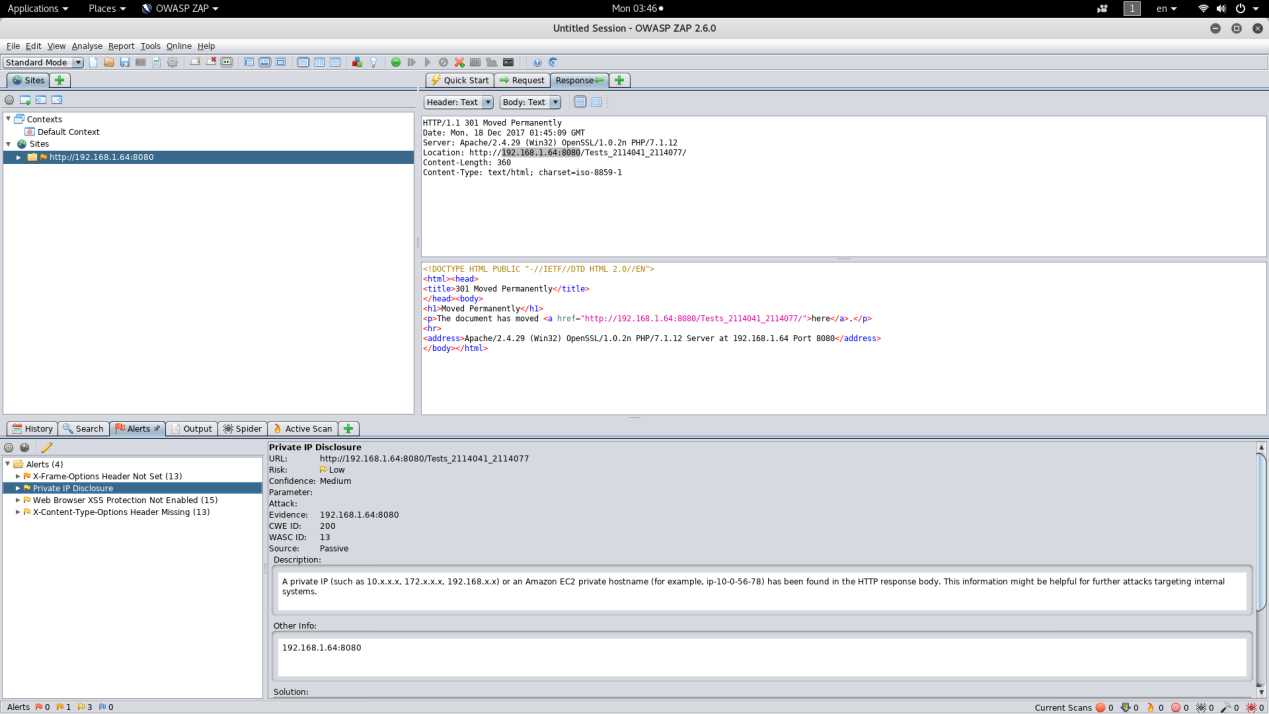
Κάναμε advanced scan με το Nessus :



**Περίληψη των αποτελεσμάτων του scan μέσω Nexus στην IP: 192.168.1.64**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Critical** | | **High** | | | | **Medium** | **Low** | **Info** | **Total** | |  | |  | |  | |  | |  | |  | |  | |
| **0** | | | | 0 | 0 | | | **8** | **1** | **35** | **44** | |  | |  | |  | |  | |  | |  | |  | |
| **Details** | | | |  |  | | |  |  |  |  | |  | |  | |  | |  | |  | |  | |  | |
|  | **Severity** | | |  | **Plugin Id** | | | **Name** |  |  |  | | **State** | |  | |  | |  | |  | |  | |  | |
|  | **Medium (6.4)** | | |  | [5119](http://www.nessus.org/plugins/index.php?view=single&id=51192)2 | | | SSL Certificate Cannot Be Trusted | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Medium (6.4)** | | |  | [5758](http://www.nessus.org/plugins/index.php?view=single&id=57582)2 | | | SSL Self-Signed Certificate | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [1121](http://www.nessus.org/plugins/index.php?view=single&id=11213)3 | | | HTTP TRACE / TRACK Methods Allowed | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [4541](http://www.nessus.org/plugins/index.php?view=single&id=45411)1 | | | SSL Certificate with Wrong Hostname | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [5760](http://www.nessus.org/plugins/index.php?view=single&id=57608)8 | | | SMB Signing Disabled | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [9311](http://www.nessus.org/plugins/index.php?view=single&id=93112)2 | | | OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32) | | | | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Medium (5.0)** | | |  | [9443](http://www.nessus.org/plugins/index.php?view=single&id=94437)7 | | | SSL 64-bit Block Size Cipher Suites Supported (SWEET32) | | | | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Medium (4.0)** | | |  | [3529](http://www.nessus.org/plugins/index.php?view=single&id=35291)1 | | | SSL Certificate Signed Using Weak Hashing Algorithm | | | | | Open | |  | |  | |  | |  | |  | |  | |
|  |  | | |  | | | |  | | | | |  | |  | |  | |  | |  | |  | |  | |
|  | **Low (2.6)** | | |  | [8387](http://www.nessus.org/plugins/index.php?view=single&id=83875)5 | | | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) | | | | | Open | |  | |  | |  | |  | |  | |  | |
|  |  | | |  | | | |  | | |  | |  | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1010](http://www.nessus.org/plugins/index.php?view=single&id=10107)7 | | | HTTP Server Type and Version | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1015](http://www.nessus.org/plugins/index.php?view=single&id=10150)0 | | | Windows NetBIOS / SMB Remote Host Information Disclosure | | | | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1028](http://www.nessus.org/plugins/index.php?view=single&id=10287)7 | | | Traceroute Information | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1039](http://www.nessus.org/plugins/index.php?view=single&id=10394)4 | | | Microsoft Windows SMB Log In Possible | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1073](http://www.nessus.org/plugins/index.php?view=single&id=10736)6 | | | DCE Services Enumeration | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1078](http://www.nessus.org/plugins/index.php?view=single&id=10785)5 | | | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure | | | | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1086](http://www.nessus.org/plugins/index.php?view=single&id=10863)3 | | | SSL Certificate Information | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1101](http://www.nessus.org/plugins/index.php?view=single&id=11011)1 | | | Microsoft Windows SMB Service Detection | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1121](http://www.nessus.org/plugins/index.php?view=single&id=11219)9 | | | Nessus SYN scanner | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1193](http://www.nessus.org/plugins/index.php?view=single&id=11936)6 | | | OS Identification | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [1950](http://www.nessus.org/plugins/index.php?view=single&id=19506)6 | | | Nessus Scan Information | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2030](http://www.nessus.org/plugins/index.php?view=single&id=20301)1 | | | VMware ESX/GSX Server detection | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2164](http://www.nessus.org/plugins/index.php?view=single&id=21643)3 | | | SSL Cipher Suites Supported | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2296](http://www.nessus.org/plugins/index.php?view=single&id=22964)4 | | | Service Detection | |  |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | [2426](http://www.nessus.org/plugins/index.php?view=single&id=24260)0 | | | HyperText Transfer Protocol (HTTP) Information | | |  | | Open | |  | |  | |  | |  | |  | |  | |
|  | **Info** | | |  | | [2691](http://www.nessus.org/plugins/index.php?view=single&id=26917)7 | | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [3571](http://www.nessus.org/plugins/index.php?view=single&id=35716)6 | | | | Ethernet Card Manufacturer Detection | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4311](http://www.nessus.org/plugins/index.php?view=single&id=43111)1 | | | | HTTP Methods Allowed (per directory) | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4381](http://www.nessus.org/plugins/index.php?view=single&id=43815)5 | | | | NetBIOS Multiple IP Address Enumeration | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4541](http://www.nessus.org/plugins/index.php?view=single&id=45410)0 | | | | SSL Certificate 'commonName' Mismatch | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4559](http://www.nessus.org/plugins/index.php?view=single&id=45590)0 | | | | Common Platform Enumeration (CPE) | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [4824](http://www.nessus.org/plugins/index.php?view=single&id=48243)3 | | | | PHP Version Detection | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5084](http://www.nessus.org/plugins/index.php?view=single&id=50845)5 | | | | OpenSSL Detection | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5351](http://www.nessus.org/plugins/index.php?view=single&id=53513)3 | | | | Link-Local Multicast Name Resolution (LLMNR) Detection | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5461](http://www.nessus.org/plugins/index.php?view=single&id=54615)5 | | | | Device Type | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5698](http://www.nessus.org/plugins/index.php?view=single&id=56984)4 | | | | SSL / TLS Versions Supported | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5704](http://www.nessus.org/plugins/index.php?view=single&id=57041)1 | | | | SSL Perfect Forward Secrecy Cipher Suites Supported | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [5732](http://www.nessus.org/plugins/index.php?view=single&id=57323)3 | | | | OpenSSL Version Detection | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [6633](http://www.nessus.org/plugins/index.php?view=single&id=66334)4 | | | | Patch Report | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [7054](http://www.nessus.org/plugins/index.php?view=single&id=70544)4 | | | | SSL Cipher Block Chaining Cipher Suites Supported | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [8450](http://www.nessus.org/plugins/index.php?view=single&id=84502)2 | | | | HSTS Missing From HTTPS Server | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [8482](http://www.nessus.org/plugins/index.php?view=single&id=84821)1 | | | | TLS ALPN Supported Protocol Enumeration | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [9698](http://www.nessus.org/plugins/index.php?view=single&id=96982)2 | | | | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [10087](http://www.nessus.org/plugins/index.php?view=single&id=100871)1 | | | | Microsoft Windows SMB Versions Supported (remote check) | | | | | Open | |  | |  | |  | |  | |  | |  | |
| **Info** | | | [10474](http://www.nessus.org/plugins/index.php?view=single&id=104743)3 | | | | TLS Version 1.0 Protocol Detection | | | | | Open | |  | |  | |  | |  | |  | |  | |

**OWASP-ZAP**: Για ανίχνευση αδυναμιών Web Εφαρμογής



|  |  |  |  |
| --- | --- | --- | --- |
| Εύρημα | Κρισιμότητα | Κατάσταση | Περιγραφή |
| X-frame-Options Header Not Set | Μέτριο | Ανοιχτό | X-frame-Options Header δεν περιέχεται στην HTTP-response για την προφύλαξη ενάντια σε ‘clickjacking’επιθέσεις |
| Private IP Disclosure | Χαμηλό | Ανοιχτό | Μια Private IP (όπως 10.x.x.x, 172.x.x.x, 192.168.x.x) ή ιδιωτικό όνομα κεντρικού υπολογιστή (για παράδειγμα, ip-10-0-56-78) του Amazon EC2 βρέθηκε στην HTTP-Response. Αυτές οι πληροφορίες ενδέχεται να είναι χρήσιμες για περαιτέρω επιθέσεις με στόχο τα εσωτερικά συστήματα. |
| Web Browser XSS Protection Not Enabled | Χαμηλό | Ανοιχτό | Ο web browser δεν έχει ενεργοποιημένο xss-protection ή είναι απενεργοποιημένο από το configuration του “X-XSS-Protection’ HTTP response header του web server |
| X-Content-Type-Options Header Missing | Χαμηλό | Ανοιχτό | To Anti-MIME-Sniffing header X-Content-Type-Options δεν έχει οριστεί σε 'nosniff'. Αυτό επιτρέπει στις παλαιότερες εκδόσεις του Internet Explorer και του Chrome να εκτελούν παρεμβολές MIME-sniffing στο response body, ενδεχομένως προκαλώντας την ερμηνεία και εμφάνιση του response body ως τύπο περιεχομένου διαφορετικό από τον δηλωμένο τύπο περιεχομένου. Οι τρέχουσες (αρχές του 2014) και οι παλαιότερες εκδόσεις του Firefox θα χρησιμοποιούν τον δηλωμένο τύπο περιεχομένου (εάν έχει οριστεί), αντί να εκτελούν MIME-sniffing. |