



Interceptor-NG

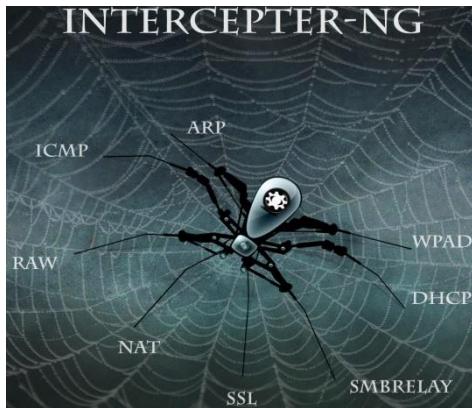
Information Security Inc.

Contents

- About Interceptor-NG
- Features
- Testing Environment
- Installing Interceptor-NG
- Using Interceptor-NG
- References

About Interceptor-NG

- Interceptor-NG is a multifunctional network toolkit for various types of IT specialists.
- The main purpose is to recover *interesting* data from the network stream and perform different kinds of MiTM attacks



Features

- Sniffing passwords, hashes of the types:
ICQ¥IRC¥AIM¥FTP¥IMAP¥POP3¥SMTP¥LDAP¥BNC¥SOCKS¥HTTP¥WWW¥NNTP¥CVS¥
- TELNET¥MRA¥DC++¥VNC¥MYSQL¥ORACLE¥NTLM¥KRB5¥RADIOS

Features

- Sniffing chat messages of:
ICQ¥AIM¥JABBER¥YAHOO¥MSN¥IRC¥MRA
- Reconstructing files from: HTTP¥FTP¥IMAP¥POP3¥SMTP¥SMB



Features

- Sniffing chat messages of:
ICQ¥AIM¥JABBER¥YAHOO¥MSN¥IRC¥MRA
- Reconstructing files from: HTTP¥FTP¥IMAP¥POP3¥SMTP¥SMB

Features

- Promiscuous-mode¥ARP¥DHCP¥Gateway¥Port¥Smart Scanning
- Capturing packets and post-capture (offline) analyzing¥RAW Mode
- Remote traffic capturing via RPCAP daemon and PCAP Over IP



Features

- ARP Watch, ARP Cage, HTTP Injection, Heartbleed exploit, Kerberos Downgrade,
- DNS¥NBNS¥LLMNR Spoofing

Testing Environment

- Windows 8.1 Pro

Windows 8.1 Pro

© 2013 Microsoft Corporation. All rights reserved.

Installing Interceptor-NG

- Download the zip file, unzip and run it

Download

Interceptor-NG-1.0.zip - Primary Windows version.

Installing Interceptor-NG

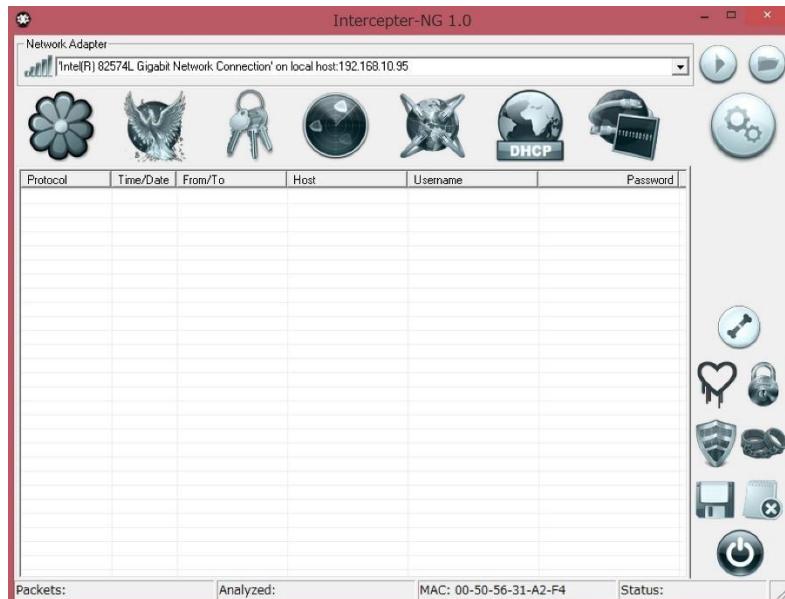
- Download the zip file, unzip and run it



Interceptor-NG.
exe

Using Interceptor-NG

- Main screen



Using Interceptor-NG

- Start sniffing



Using Interceptor-NG

- RAW Mode

The screenshot shows the Interceptor-NG application window. At the top, there is a toolbar with various icons: a flower, a bird, a key, a brain, a star, a globe labeled 'DHCP', a smartphone, and a gear. The 'RAW Mode' icon is highlighted with a blue border. Below the toolbar is a table displaying network traffic. The columns are: No, Time, Source, Destination, Protocol, Len, and Info. The table contains 438 rows of data. Row 437 is highlighted with a pink background. At the bottom of the table, there are two filter fields: 'Pcap Filter' and 'Stream Filter', both containing green bars. At the very bottom, there are status indicators: 'Packets: 475 (0.08Mb)', 'Analyzed: 475', 'MAC: 00-50-56-31-A2-F4', 'Status: Sniffing...', and a power button icon.

No	Time	Source	Destination	Protocol	Len	Info
428	40.467952	192.168.10.1	239.255.255.250	UDP	256	
429	40.467953	192.168.10.1	239.255.255.250	UDP	346	
430	40.467953	192.168.10.1	239.255.255.250	UDP	314	
431	40.467953	192.168.10.1	239.255.255.250	UDP	256	
432	40.467954	192.168.10.1	239.255.255.250	UDP	330	
433	40.467954	192.168.10.1	239.255.255.250	UDP	338	
434	40.467955	192.168.10.1	239.255.255.250	UDP	256	
435	40.467955	192.168.10.1	239.255.255.250	UDP	266	
436	41.797678	192.168.10.111	54.171.131.39	DNS	100	DNS Query: rtm.alk
437	41.797728	192.168.10.95	192.168.10.111	ICMP	128	Redirect
438	41.797771	192.168.10.111	54.171.131.39	DNS	100	DNS Answer: rtm.alk

Using Interceptor-NG

- Password Mode, capturing passwords on the wire

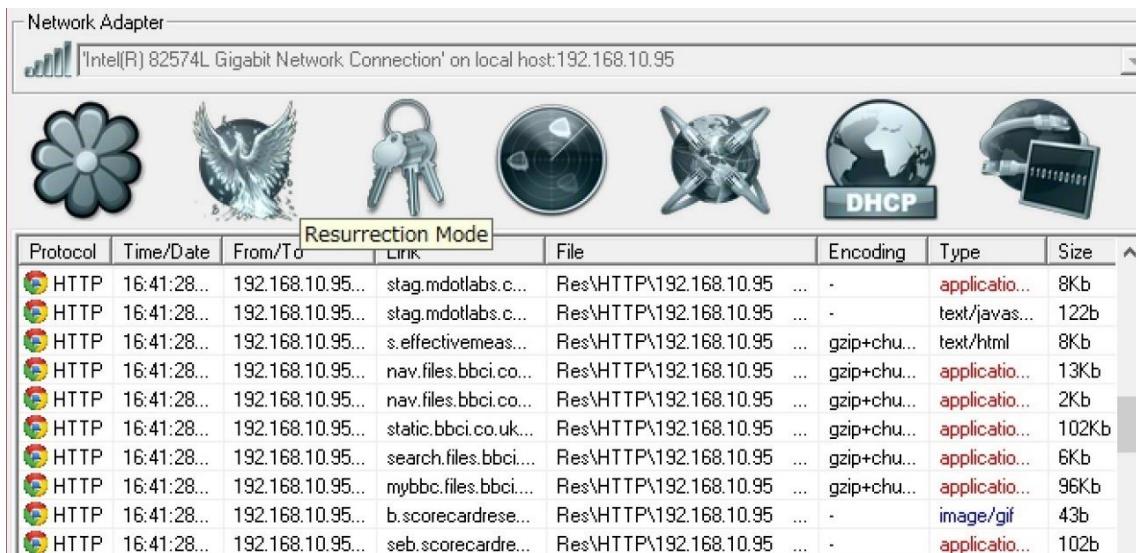
The screenshot shows the Interceptor-NG application window. At the top, it displays the network adapter information: 'Network Adapter' and 'Intel(R) 82574L Gigabit Network Connection' on local host:192.168.10.95. Below this are several icons representing different modes or features: a flower, a bird, a key, a globe, and a gear. The 'Password Mode' icon is highlighted with a blue border. A tooltip 'Password Mode' is visible over this icon. To the right of these icons is a 'DHCP' button. The main area of the window is a table showing captured network traffic:

Protocol	Time/Date	From/To	Host	Username	Password
Web Site visited	16:38:16...	192.168.10.95/19...	192.168.10.95	192.168.10.105	
WWW Basic A...	16:38:22...	192.168.10.95/19...	192.168.10.105/	user	password

Using Interceptor-NG

- Resurrection Mode, reconstructing files from the network stream

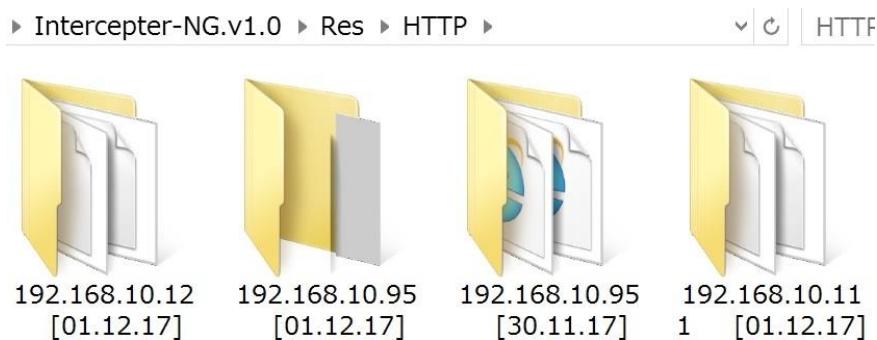
Network Adapter
'Intel(R) 82574L Gigabit Network Connection' on local host:192.168.10.95



Protocol	Time/Date	From/To	LINK	File	Encoding	Type	Size
HTTP	16:41:28...	192.168.10.95...	stag.mdotlabs.c...	Res\HTTP\192.168.10.95 ...	-	application...	8Kb
HTTP	16:41:28...	192.168.10.95...	stag.mdotlabs.c...	Res\HTTP\192.168.10.95 ...	-	text/java...	122b
HTTP	16:41:28...	192.168.10.95...	s.effectivemeas...	Res\HTTP\192.168.10.95 ...	gzip+chu...	text/html	8Kb
HTTP	16:41:28...	192.168.10.95...	nav.files.bbci.co...	Res\HTTP\192.168.10.95 ...	gzip+chu...	application...	13Kb
HTTP	16:41:28...	192.168.10.95...	nav.files.bbci.co...	Res\HTTP\192.168.10.95 ...	gzip+chu...	application...	2Kb
HTTP	16:41:28...	192.168.10.95...	static.bbci.co.uk...	Res\HTTP\192.168.10.95 ...	gzip+chu...	application...	102Kb
HTTP	16:41:28...	192.168.10.95...	search.files.bbci...	Res\HTTP\192.168.10.95 ...	gzip+chu...	application...	6Kb
HTTP	16:41:28...	192.168.10.95...	mybbc.files.bbci...	Res\HTTP\192.168.10.95 ...	gzip+chu...	application...	96Kb
HTTP	16:41:28...	192.168.10.95...	b.scorecardrese...	Res\HTTP\192.168.10.95 ...	-	image/gif	43b
HTTP	16:41:28...	192.168.10.95...	seb.scorecardre...	Res\HTTP\192.168.10.95 ...	-	application...	102b

Using Interceptor-NG

- Resurrection Mode, saving folder



Using Interceptor-NG

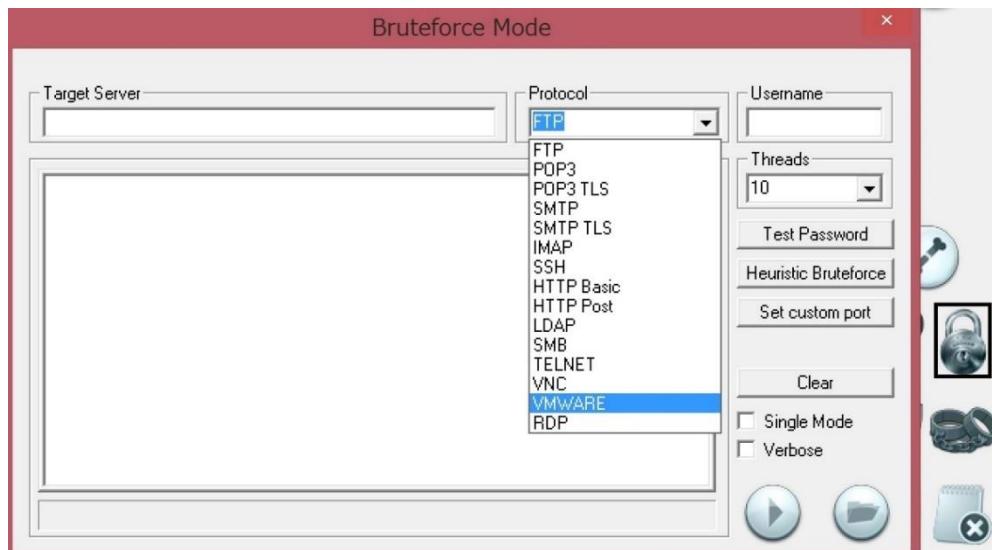
- Resurrection Mode, saving folder

The screenshot shows the 'Res' tab of Interceptor-NG with the URL '192.168.10.95' and timestamp '[01.12.17]'. The search bar also contains '192.168.10.95'. The results list shows numerous files, mostly jpgs, with names like '_98984775_dannyda', '_98984775_dannyda', '_98984775_dannyda', etc., indicating they have been resurrected from a previous session. A red vertical bar highlights the right side of the results list.

File Name
_98984775_dannyda
_98984775_dannyda
_98984775_dannyda
_98996334_cameron
_98999746_oloughlin
_99005326_mediaite
_99005794_gettyima
_99005794_gettyima
_99009988_garethso
_99009988_garethso

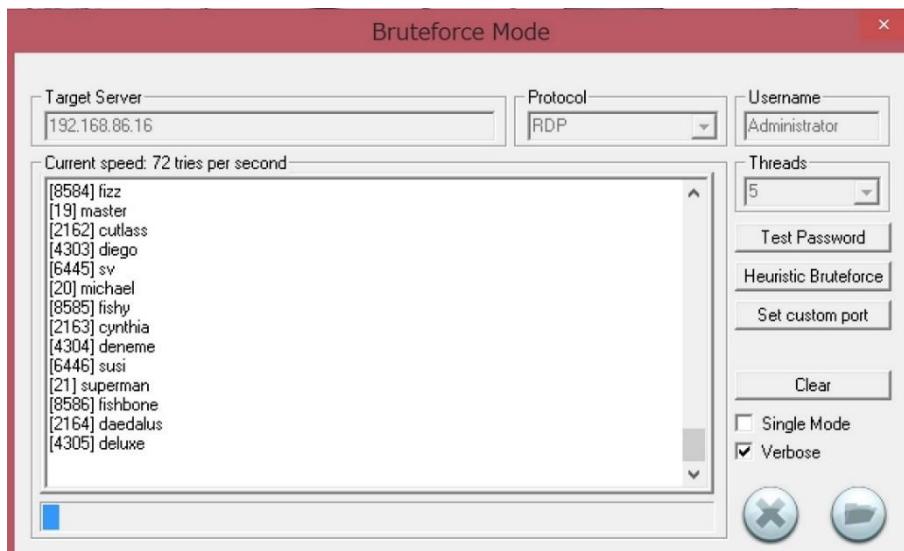
Using Interceptor-NG

- Bruteforce Mode



Using Interceptor-NG

- Bruteforce Mode, RDP



References

- GitHub

<https://github.com/interceptor-ng/interceptor-ng.github.io>

- Official website

<http://sniff.su/about.html>