



Interceptor-NG

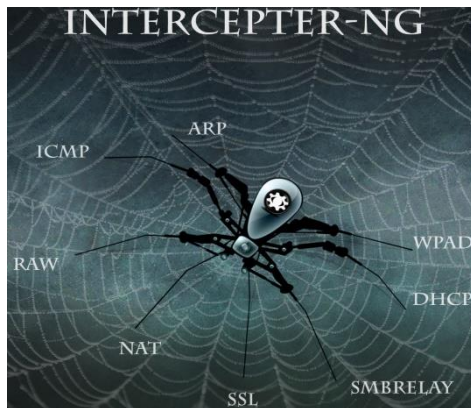
Information Security Inc.

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¥RADIUS

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

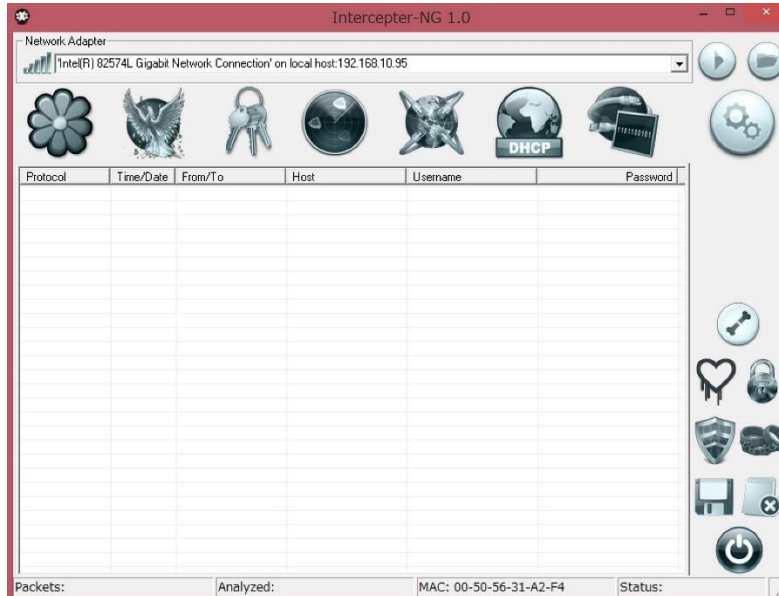
- Download the zip file, unzip and run it



Interceptor-NG.
exe

Using Interceptor-NG

- Main screen



Using Interceptor-NG

- Start sniffing



Using Interceptor-NG

- RAW Mode

The screenshot displays the Interceptor-NG software interface in RAW Mode. The main window shows a table of network traffic with the following data:

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: tlma.tk
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 Query: tlma.tk

The interface also features a sidebar with various icons, including a gear for settings, a padlock for security, and a power button. At the bottom, the status bar shows: Packets: 475 (0.08Mb), Analyzed: 475, MAC: 00-50-56-31-A2-F4, and Status: Sniffing...

Using Interceptor-NG

- Password Mode, capturing passwords on the wire

Network Adapter

Signal strength: [Bar chart] 'Intel(R) 82574L Gigabit Network Connection' on local host:192.168.10.95

Icons: Flower, Eagle, Keys (Password Mode), Globe with slash, Earth with tools, DHCP, Network card


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

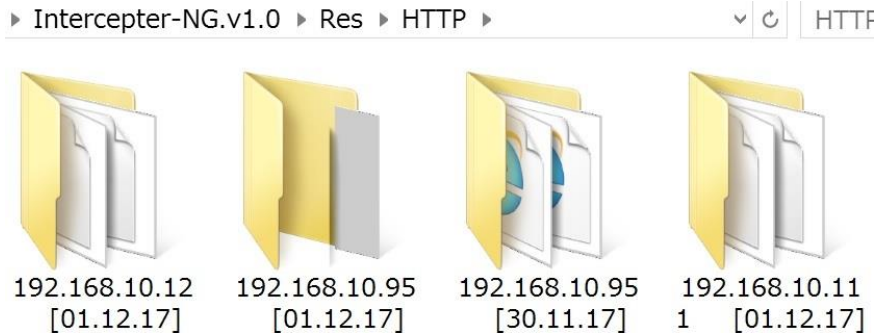


Resurrection Mode

Protocol	Time/Date	From/To	Link	File	Encoding	Type	Size
HTTP	16:41:28...	192.168.10.95...	stag.mdottlabs.c...	Res\HTTP\192.168.10.95 ...	-	applicatio...	8Kb
HTTP	16:41:28...	192.168.10.95...	stag.mdottlabs.c...	Res\HTTP\192.168.10.95 ...	-	text/javas...	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.bbc.co...	Res\HTTP\192.168.10.95 ...	gzip+chu...	applicatio...	13Kb
HTTP	16:41:28...	192.168.10.95...	nav.files.bbc.co...	Res\HTTP\192.168.10.95 ...	gzip+chu...	applicatio...	2Kb
HTTP	16:41:28...	192.168.10.95...	static.bbc.co.uk...	Res\HTTP\192.168.10.95 ...	gzip+chu...	applicatio...	102Kb
HTTP	16:41:28...	192.168.10.95...	search.files.bbc...	Res\HTTP\192.168.10.95 ...	gzip+chu...	applicatio...	6Kb
HTTP	16:41:28...	192.168.10.95...	mybbc.files.bbc...	Res\HTTP\192.168.10.95 ...	gzip+chu...	applicatio...	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 ...	-	applicatio...	102b

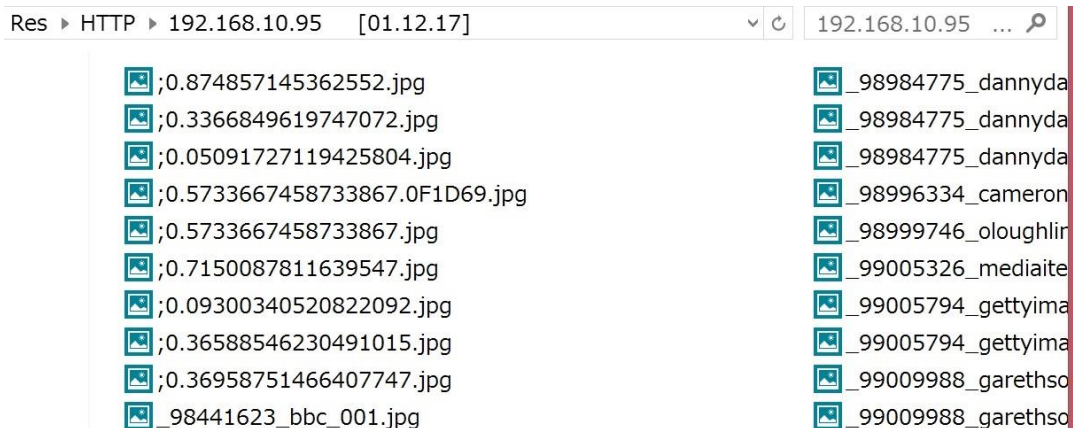
Using Interceptor-NG

- Resurrection Mode, saving folder



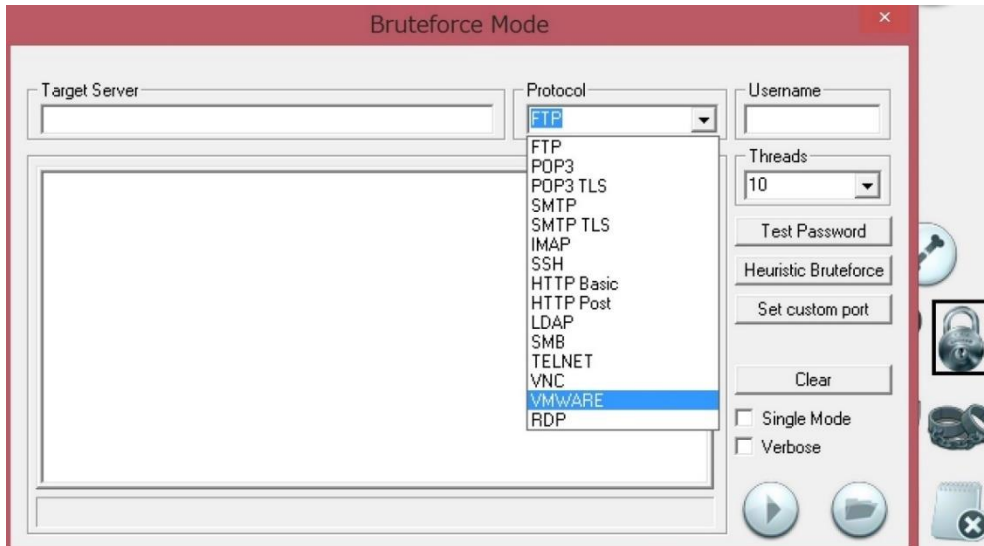
Using Interceptor-NG

- Resurrection Mode, saving folder



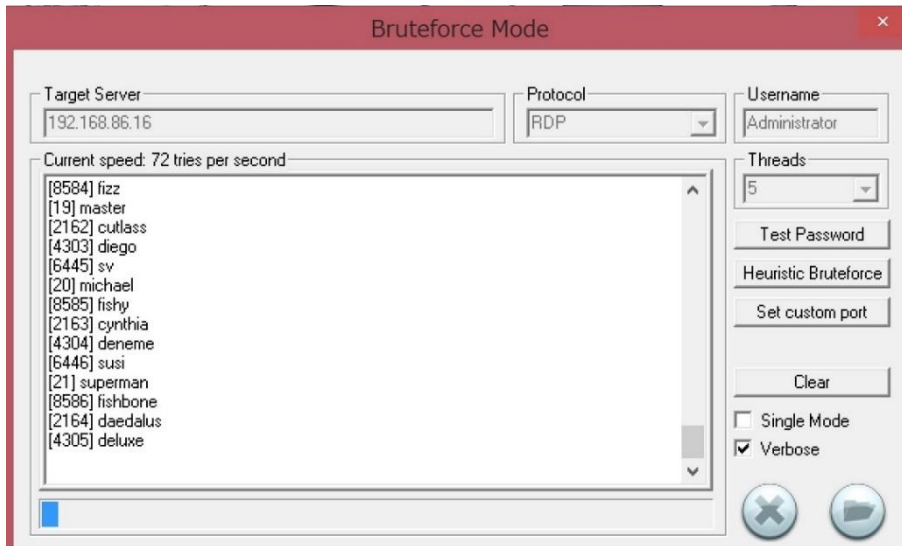
Using Interceptor-NG

- 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>