Epione v1.0
User Guide
26 March 2012

CL BY: 2040808
REASON: 1.5(c)
DECL: X1; 17 June 2028
DRV: COL 1-82

Table of Changes

Date	Change Description	Authority

Table of Contents

Epione User Guide

1.0 (S) Introduction

(S) Epione is designed as a network characterization utility. It contains both an active and passive scanner, both of which can be configured by the user.

(S) The passive scanner creates connection and passively listens in Windows' "promiscuous" mode. All packets to/from the host system are captured, processed, and potentially added to the active scanner.

(S)The active scan actively scans IP-port pairs based on either user configuration or captured packets matching a subnet filter. The active scanner has a configurable time delay between each new scan. The scans are dependent on configurable ports, and will capture banner data.

(S) Epione runs on both Windows and Linux. (Linux executables not provided in v1.0)

1.1 (S) Requirement

(S) The Intelligence Community has identified the need (requirement # 2012-0406) for a capability to scan and characterize networks of interest.

1.2 (S) Purpose

(S) This User Guide describes how to use Epione v1.0. The document provides the Epione configuration process and the installation process.

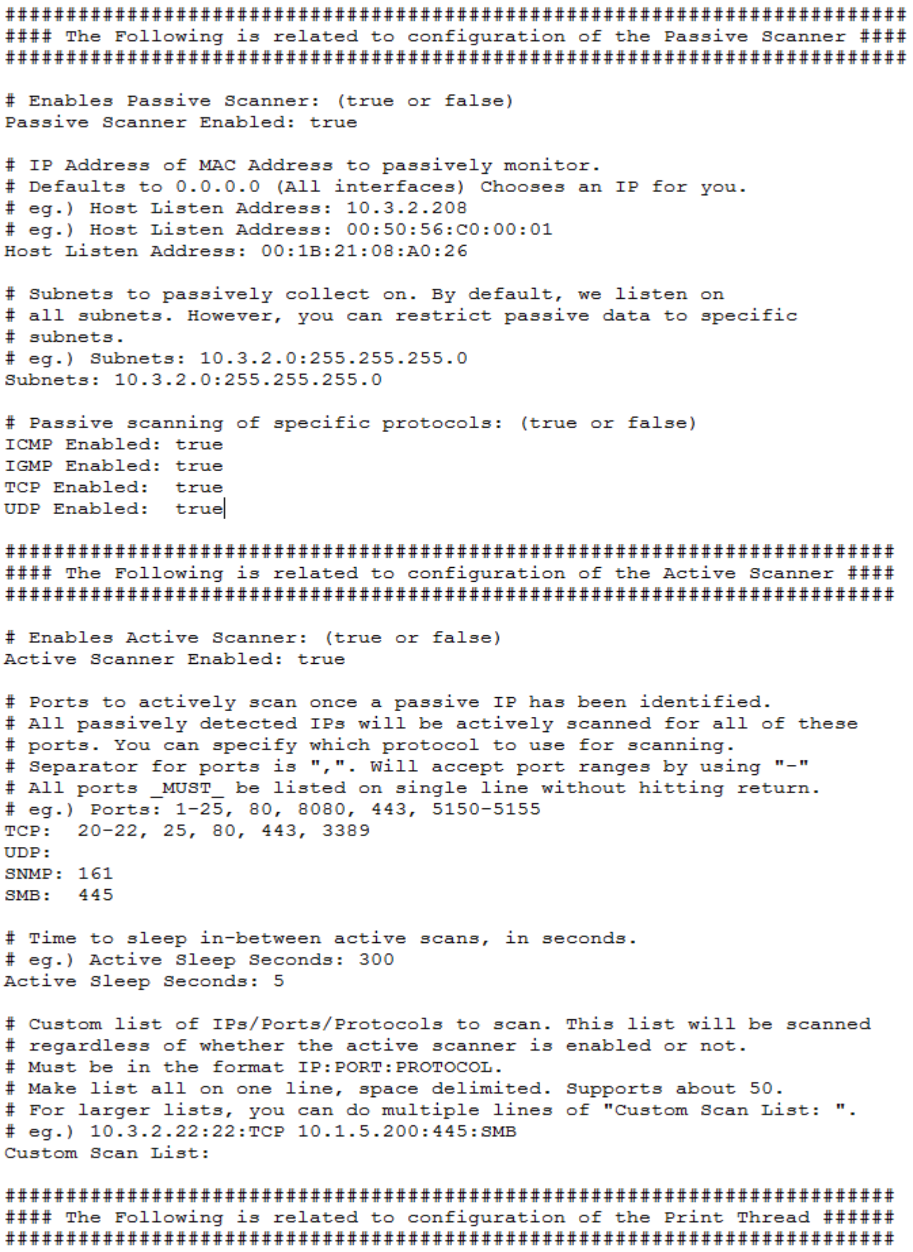
2.0 (S) System Overview

- **(S) Configuration**
    - (S) The configuration for the tool is entirely from the command-line program ConfigureEpione. The usage is:
        - ConfigureEpione -e executable (To read current configuration of exe)
        - ConfigureEpione -f config_file -e executable (To write resources from config file to executable)
        - If config file retains the default name, epione.conf, then simply double-clicking the config tool with both the exe and config file in the same directory will automatically configure the tool for you.
    - (S) See the config file, epione.conf for more information regarding the config options.

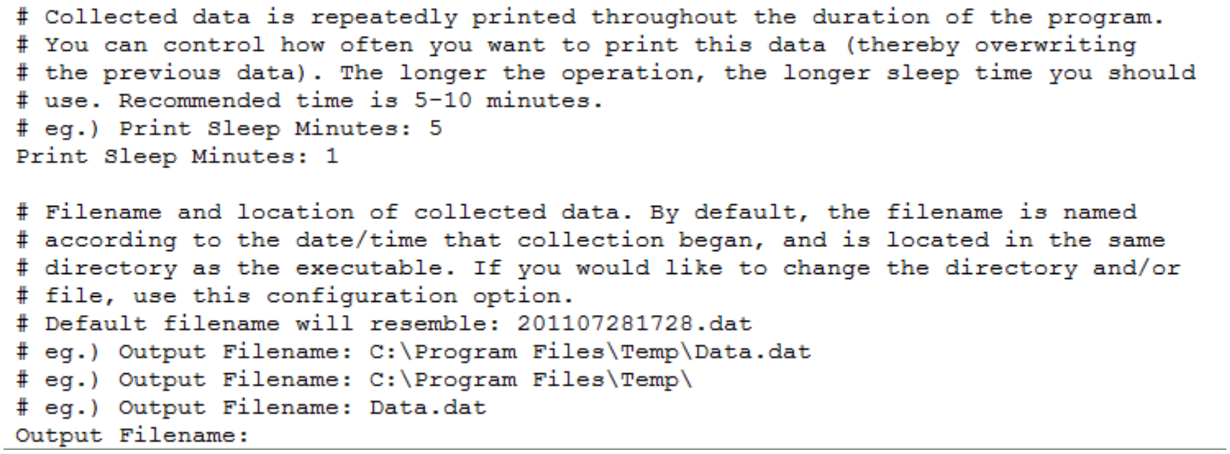
- **(S) Installation and Collection**
  - (S) Once configured, simply drop and run the configured executable on the targeted windows system. It will then run continuously in the background until reboot or the process is killed by the user, and it will continually update the output file every X-configured minutes while running. The output file is compressed and encrypted.

3.0 (S) Getting Started

3.1 (S) Pre-deployment



```
##########################################################################
#### The Following is related to configuration of the Passive Scanner ####
##########################################################################

# Enables Passive Scanner: (true or false)
Passive Scanner Enabled: true

# IP Address of MAC Address to passively monitor.
# Defaults to 0.0.0.0 (All interfaces) Chooses an IP for you.
# eg.) Host Listen Address: 10.3.2.208
# eg.) Host Listen Address: 00:50:56:C0:00:01
Host Listen Address: 00:1B:21:08:A0:26

# Subnets to passively collect on. By default, we listen on
# all subnets. However, you can restrict passive data to specific
# subnets.
# eg.) Subnets: 10.3.2.0:255.255.255.0
Subnets: 10.3.2.0:255.255.255.0

# Passive scanning of specific protocols: (true or false)
ICMP Enabled: true
IGMP Enabled: true
TCP Enabled:  true
UDP Enabled:  true

#########################################################################
#### The Following is related to configuration of the Active Scanner ####
#########################################################################

# Enables Active Scanner: (true or false)
Active Scanner Enabled: true

# Ports to actively scan once a passive IP has been identified.
# All passively detected IPs will be actively scanned for all of these
# ports. You can specify which protocol to use for scanning.
# Separator for ports is ",". Will accept port ranges by using "-"
# All ports _MUST_ be listed on single line without hitting return.
# eg.) Ports: 1-25, 80, 8080, 443, 5150-5155
TCP:  20-22, 25, 80, 443, 3389
UDP:
SNMP: 161
SMB:  445

# Time to sleep in-between active scans, in seconds.
# eg.) Active Sleep Seconds: 300
Active Sleep Seconds: 5

# Custom list of IPs/Ports/Protocols to scan. This list will be scanned
# regardless of whether the active scanner is enabled or not.
# Must be in the format IP:PORT:PROTOCOL.
# Make list all on one line, space delimited. Supports about 50.
# For larger lists, you can do multiple lines of "Custom Scan List: ".
# eg.) 10.3.2.22:22:TCP 10.1.5.200:445:SMB
Custom Scan List:

#########################################################################
#### The Following is related to configuration of the Print Thread ######
#########################################################################
```



```
# Collected data is repeatedly printed throughout the duration of the program.
# You can control how often you want to print this data (thereby overwriting
# the previous data). The longer the operation, the longer sleep time you should
# use. Recommended time is 5-10 minutes.
# eg.) Print Sleep Minutes: 5
Print Sleep Minutes: 1

# Filename and location of collected data. By default, the filename is named
# according to the date/time that collection began, and is located in the same
# directory as the executable. If you would like to change the directory and/or
# file, use this configuration option.
# Default filename will resemble: 201107281728.dat
# eg.) Output Filename: C:\Program Files\Temp\Data.dat
# eg.) Output Filename: C:\Program Files\Temp\
# eg.) Output Filename: Data.dat
Output Filename:
```

3.2 (S) Deployment and Collection

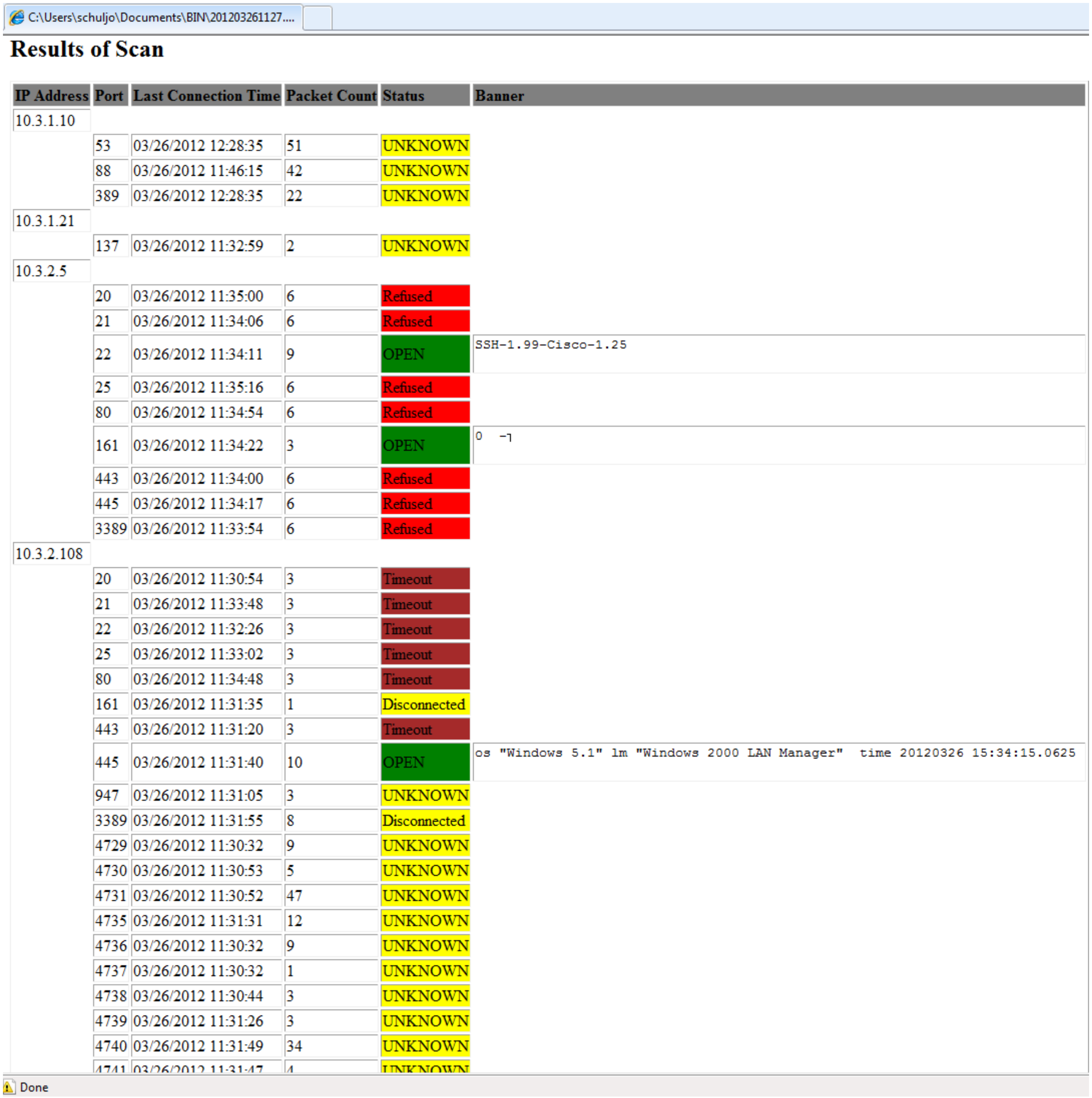
- (S) Simply double-click the executable to begin the network characterization.
- (S) The tool runs indefinitely unless terminated or run with the "-s" parameter from the command-line.

3.3 (S) Post-deployment

(S) After execution, the output will need to be exfiltrated and postprocessed.

(S) Like the config tool, the postprocessor is commandline and expects as arguments, the input file (encrypted take) and an output filename to dump the xml data. If the filename is left unchanged, (the default is a date-time stamp with a .dat extension), then you can simply double-click the postprocessor. Regardless, the decrypted output should be of the same name with a .xml extension and an additionally dropped stylesheet. Then just open the xml file in a web browser or your preferred xml-viewer.

(S) Once decrypted and uncompressed, it should look like the following:



Results of Scan

IP Address	Port	Last Connection Time	Packet Count	Status	Banner
10.3.1.10					
	53	03/26/2012 12:28:35	51	UNKNOWN	
	88	03/26/2012 11:46:15	42	UNKNOWN	
	389	03/26/2012 12:28:35	22	UNKNOWN	
10.3.1.21					
	137	03/26/2012 11:32:59	2	UNKNOWN	
10.3.2.5					
	20	03/26/2012 11:35:00	6	Refused	
	21	03/26/2012 11:34:06	6	Refused	
	22	03/26/2012 11:34:11	9	OPEN	SSH-1.99-Cisco-1.25
	25	03/26/2012 11:35:16	6	Refused	
	80	03/26/2012 11:34:54	6	Refused	
	161	03/26/2012 11:34:22	3	OPEN	0 ¬
	443	03/26/2012 11:34:00	6	Refused	
	445	03/26/2012 11:34:17	6	Refused	
	3389	03/26/2012 11:33:54	6	Refused	
10.3.2.108					
	20	03/26/2012 11:30:54	3	Timeout	
	21	03/26/2012 11:33:48	3	Timeout	
	22	03/26/2012 11:32:26	3	Timeout	
	25	03/26/2012 11:33:02	3	Timeout	
	80	03/26/2012 11:34:48	3	Timeout	
	161	03/26/2012 11:31:35	1	Disconnected	
	443	03/26/2012 11:31:20	3	Timeout	
	445	03/26/2012 11:31:40	10	OPEN	os "Windows 5.1" lm "Windows 2000 LAN Manager" time 20120326 15:34:15.0625
	947	03/26/2012 11:31:05	3	UNKNOWN	
	3389	03/26/2012 11:31:55	8	Disconnected	
	4729	03/26/2012 11:30:32	9	UNKNOWN	
	4730	03/26/2012 11:30:53	5	UNKNOWN	
	4731	03/26/2012 11:30:52	47	UNKNOWN	
	4735	03/26/2012 11:31:31	12	UNKNOWN	
	4736	03/26/2012 11:30:32	9	UNKNOWN	
	4737	03/26/2012 11:30:32	1	UNKNOWN	
	4738	03/26/2012 11:30:44	3	UNKNOWN	
	4739	03/26/2012 11:31:26	3	UNKNOWN	
	4740	03/26/2012 11:31:49	34	UNKNOWN	
	4741	03/26/2012 11:31:47	4	UNKNOWN	

Status decoded:
"OPEN" -- What you want to see: The port is open and was successfully connected
"**Disconnected**"-- Server unexpectedly disconnected, state not known.
"Invalid"-- Winsock error 10049: Cannot assign requested address. (WSAEADDRNOTAVAIL)
"Unreachable"-- Winsock error 10051: Network is unreachable. (WSAENETUNREACH)
"Reset"-- Winsock error 10054: Connection reset by peer. (WSAECONNRESET)
"Timeout"-- Winsock error 10060: Connection timed out. (WSAETIMEDOUT)
"Refused"-- Winsock error 10061: Connection refused. (WSAECONNREFUSED)
"UNKNOWN"-- Active scanner was not tasked to scan this port, data received is passive.
Other errors may exist in numerical form, refer to the Microsoft Windows Winsock error code documentation for further information.