Tool Delivery Review

Epione
Version 1.0

EDG Project Lead: [redacted]

COG Point of Contact: [redacted]

IV&V Lead: [redacted]

CL BY:	2405243
CL REASON:	Section 1.5(c), (e)
DECL ON:	X1
DRV FRM:	COL 1-82

Agenda

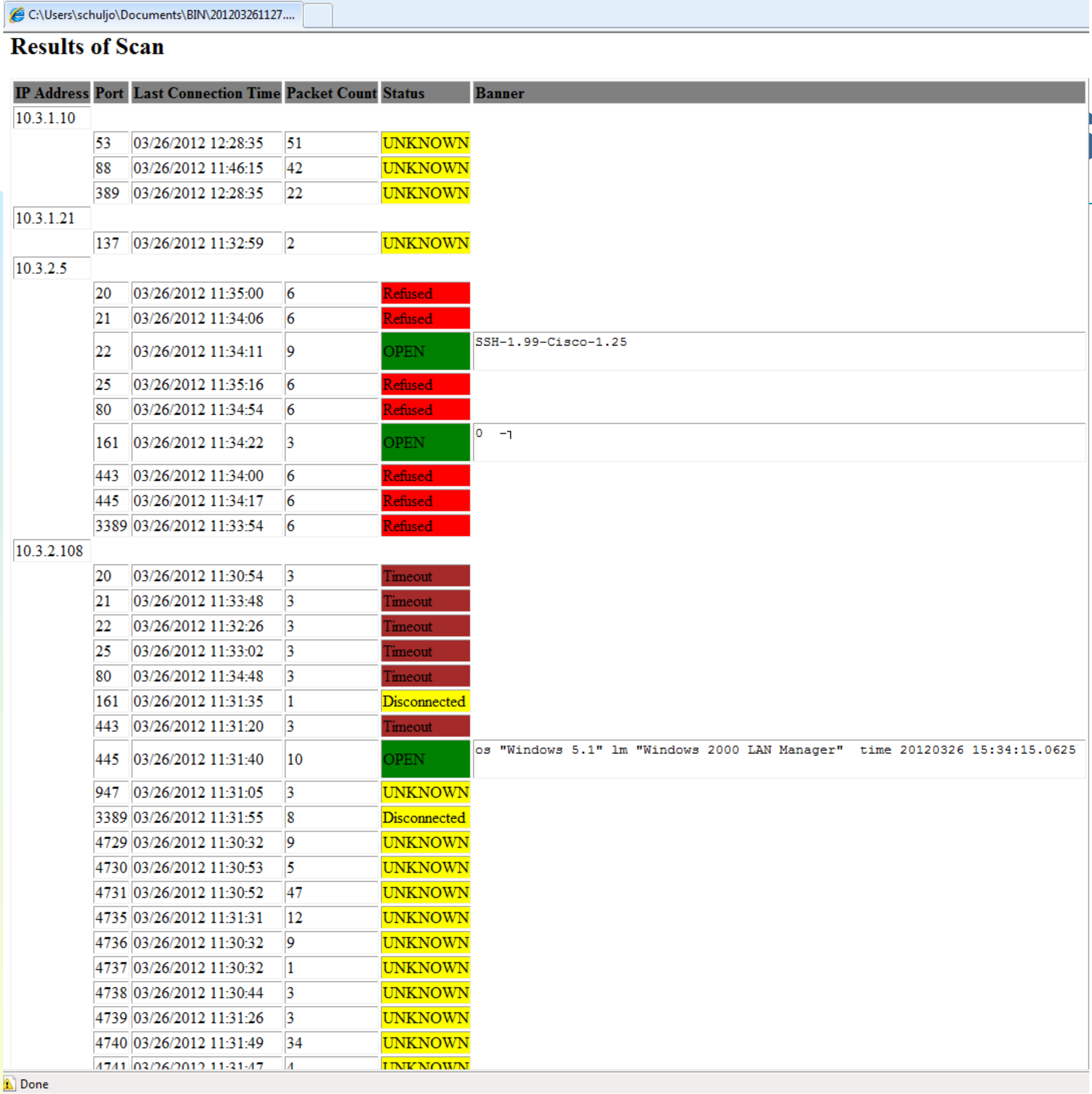
Subject	Briefer
Requirements	[redacted]
Concept of Operations	[redacted]
Capabilities and limits	[redacted]
IV&V	[redacted]
Product Support	[redacted]

Requirements

- Requirement #2012-0406
  - 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.
  - COG/NOD requests this capability to better characterize and enumerate target networks of interest

Concept of Operations

- Epione is designed to be dropped and executed on a target system in order to gain additional information about the target network
  - Epione can be run passively, in which it only listens on all connections and attempts to enumerate the network based on IPs the target encounters
  - Epione can be run actively, in which it targets specific IPs and runs a configured port scan; If run in conjunction with the passive scanner, then it dynamically generates IPs to scan based entirely on the passive scan



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	

Capabilities and Limits

- Configured and postprocessed from the commandline, the tool itself runs indefinitely unless explicitly stopped with the commandline option “-s”. There’s no issue with this since limits are placed on the output file size.
- Additionally, PSPs may detect the fact that the program is attempting a network connection, which cannot typically be hidden

Product Support

Tool and Project Documentation

- Epione v1.0 User Guide_2012-03-26.doc
- Epione v1.0 Test Plan and Procedures.doc
- Epione v1.0 TDR Briefing 2012.ppt

Certification

- Closes requirement for Epione v1.0 #2012-0406
- Discussion and decision
- Recap of assigned Actions