DATASHEET

EISA

Exposed Internet Surface Analysis

NSFOCUS

OVERVIEW

Almost every organization today has some kind of connection to the internet. Whether it is to host multiple ecommerce sites or just have email access, internet connectivity is a necessity for doing business. But being on the internet is not without risk. Worse, most organizations do not know how big their risk is.

What is the level of exposure on the internet? Even with a managed network firewall, it can be difficult to know what IP addresses, ports, or services an organization has available on the internet. Is there a rogue server internally hosting a warez FTP site? What prevents a business unit from installing their own link to the internet, bypassing the corporate firewall. What is the effect of mobile devices and PnP services within the organization? Most organizations don't know because they cannot see themselves from the outside.

EISA IDENTIFIES HOW EXPOSED YOU ARE

With NSFOCUS Exposed Internet Surface Analysis, rogue IPs, ports and services can be quickly identified. The NSFOCUS Threat Intelligence (NTI) high-speed Internet Scanning Engine can scan huge IP address spaces such as complete ASNs quickly looking for unknown IPs, unknown ports open on known IPs, and the services running on those ports. EISA can identify services running on non-standard or high ports using NTI's enhanced fingerprinting technology and enriched protocol fingerprint database. Even when services change their default ports, the right service can still be identified. EISA can also identify when an IP address has been hijacked through BGP routing attacks.

IP	Port	Protocol	Application	Version
223.xxxxxx.214	53	UDP	DNS	
223.xxxxxx.215	53	UDP	DNS	
223.xxxxxx.133	21	TCP	FTP	
223.xxxx.226	98	TCP	FTP	
223.xxxx.226	9029	TCP	FTP	
211.xxxxxx.184	21	TCP	HTTP	1.1
223.xxxxxx.10	22	TCP	HTTP	1.1
211.xxxxxx.171	23	TCP	HTTP	1.1
223.xxxxxx.242	6408	TCP	MEMCACHE	
223.xxxxxx.27	11211	TCP	MEMCACHE	
211.xxxxxx.126	20123	TCP	MYSQL	
211.xxxxxx.237	3306	TCP	MYSQL	
211.xxxxxx.236	20412	TCP	MYSQL	
223.xxxxx.9	110	TCP	POP	
211.xxxxx.5	995	SSL	POP	
223.xxxx.131	20110	TCP	POP	
223.xxxx.10	35000	UDP	RLOGIN	
211.xxxx.126	5351	UDP	RLOGIN	
211.xxxx.235	1099	TCP	RMI	
223.xxxx.9	10089	TCP	SSH	
223.xxxx.242	22	TCP	SSH	
223.xxxx.242	902	TCP	VMWARE	
223.xxxx.27	912	TCP	VMWARE	
223.xxxx.132	902	TCP	VMWARE	

Once rogue IPs and IPs with rogue ports and services have been identified, they are automatically correlated with the NTI IP Reputation databases to determine if there is any evidence of malicious activity, what the malicious activity was, when it was seen and what the level of risk is to the organization and to potential targets on the internet.

IP	Malicious Type	Detected Date
199.xxxxxx169	exploit	2016-07-10
31.xxxxxx200	bots	2016-07-10
85.xxxxxx 9	scanner	2016-07-10
78.xxxxxx238	ssh	2016-07-10
143.xxxxxx3	scanner	2016-07-10
211xxxxxx.36	ssh	2016-07-10
91.xxxxxx206	scanner	2016-07-10

EISA will also find any previously unknown domains associated with rogue IP addresses.

Correlated Domains: 111
http://cheaxxxxxxxomchina.com
http://axxxxxxx.com
http://988xxxxxxx.com
http://abxxxxxxxy.com
http://8881xxxxxxx.com
http://1zxxxxxxx.com
http://075xxxxxxx.com
http://daxxxxxxx.com
http://janxxxxxxx.com
http://ystxxxxxxx.com

Based on EISA's comprehensive analysis and review, organizations can develop remediation plans for updating network firewall and IPS policies to block any further malicious activity. System ROI can be improved by shutting off unauthorized services running on desktops, servers, and other appliances that are siphoning off CPU, memory, and network resources.

REAL TIME EISA PROTECTION

The NSFOCUS Exposed Internet Surface Analysis can be run once or as a subscription service with various levels of monitoring SLAs to meet requirements from organizations with the smallest internet footprint to multi-national businesses that own IP ranges all over the world.

NSFOCUS EISA not only identifies your exposure risks on the internet, it can reduce O&M costs by recovering ROI lost to rogue systems and services impacting your environment. Reduce your risk, save money using Security that is Smart and Simple.