Team: Team 08

Inject Number: 27

Inject Duration: 100 Minutes

Inject Start Date/Time: Sat, 16 Mar 2019 14:39:08 +0000

From: IT Director

To: Infrastructure Team

Subject: M102 - Internal Scan of Services

The CIO recently went to an industry conference and many of his fellow CIOs were lamenting about compromises and breaches at their respective companies. A number of them were caused by servers, services, and ports that were inadvertently exposed to the internet through mis-configured host-based and network firewalls. One of the initial recommendations was to scan the entire infrastructure from inside the environment.

To accomplish this task, utilize the Windows 10 or ubuntu workstation inside the Palo Alto Firewall. Install Zenmap from https://nmap.org and configure it to assess all the networks and devices under your Teams control (including the Windows 8 box itself). This includes: the internal interface of the firewall, the Windows 8 device, the Internal network, the User network, and the Public network. At a minimum, you must scan: 1) all TCP ports (1-65535); 2) UDP for the UDP ports defined for DNS, SNMP, Windows RPC, Netbios Naming Service, Netbios Datagram Service and IPERF common ports as set by vendor default or RFC/standard. If you determine that additional ports or protocols should be scanned, please do so.

Reply with a business memo that documents the current services (tcp/udp ports) that are available on each server and an assessment as to whether they are needed. Submit your complete scan results as an appendix to a business memo in word or pdf format to the CIO that describes 1) what you scanned; 2) an executive summary/analysis of the results (must include description of what you saw that was not expected as well as verifying that you could see the expected services); and 3) what should be done next to secure our environment based on the results and observations.

Thank you.

IT Director