Team: Team 15

Inject Number: 24

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 02 Feb 2019 19:53:56 +0000

From: IT Director

To: Infrastructure Team

Subject: 3.1.20|3.4.7|3.14.5 Assess Network Exposure - Zenmap Scan

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 outside the environment.

To accomplish this task, utilize the Windows 10 machine outside the Palo Alto Firewall. Install Zenmap from https://nmap.org and configure it to assess all the networks and devices under your Team's control (including the Windows 10 box itself) through the firewall. This includes: the external interface of the firewall, the Windows 10 device, the Internal network, the User network, and the Public network. Scanning through firewalls can be complex due to the way firewalls drop packets and ICMP Ping packets may be dropped. To ensure the data is valid and doesn't take in inordinate amount of time, follow the guidance and pick the best options for scanning according to the information at: https://nmap.org/book/determining-firewall-rules.html. At a minimum, you must scan: 1) all TCP ports (1-65535); 2) UDP "version scan" 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.

Once complete, 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