

Team: Team 15

Inject Number: 18

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 02 Feb 2019 18:21:17 +0000

From: IT Director

To: Infrastructure Team

Subject: 3.4.7 Internal zenmap scan using windows 8.1 PC

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 8.1 machine inside 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 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 "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