Team Epsilon

Security analysis / Enumeration Tool

\*\*Team Overview\*\*

Bryan Kazunas GitHub:BryanKazunas, Alexander Pratt GitHub: SomewhatCynical, Wenxiao Zeng GitHub: wzeng-01

Our Idea is to build a web-based Security analysis / Enumeration Tool that leverages the concept of browser-based port scanning. The user can provide several parameters for the scan. These include scanning a specific host (i.e.localhost - 127.0.0.1), a range of ports, or exposure to a vulnerability. We would also like to implement scanning based on a range of IPs or DNS names if time and our skillset permit.

The website will ingest information provided by the scan and return a “threat report.” In the case of a host scan, it will detail what ports are open and vulnerable. Subsequent scans will update the “profile” of that workstation to reflect changes. Scans for specific ports or vulnerabilities will return a similar report for that parameter.

Some of the main functions we would like to include are

* Port scanning: Leveraging socket creations and packet time outs, returning whether or not the port is open
* IP parameters: Allowing the user to change the specific target being scanned
* Vulnerability Analysis, allowing the user to search for susceptible ports for a specific vulnerability
* Remediation Steps: Provide the user with instructions on how to prevent a port/ports from being susceptible
* Dynamic Profile: Creating a profile for each new target / updating an existing profile when subsequent scans are run

Time and skillset permitting, we would also like to implement the following,

* Dynamic Vulnerability Updating: Instead of using a predetermined list, we would somehow dynamically update our vulnerability “database” with new threats (ex., from an external repository)
* Scan by IP range: add the ability to scan a network of hosts rather than just one specific one
* Scan by DNS name: add the ability to scan a host using its resolved DNS name and possible extend this to a domain name

**POST FOR SLACK**: (Team Epsilon) Our Idea is to build a web-based Security analysis / Enumeration Tool that leverages the concept of browser-based port scanning. The user can provide several parameters for the scan. These include scanning a specific host (i.e.localhost - 127.0.0.1), a range of ports, or exposure to a vulnerability.The website will ingest information provided by the scan and return a “threat report.” In the case of a host scan, it will detail what ports are open and vulnerable. Subsequent scans will update the “profile” of that workstation to reflect changes. Scans for specific ports or vulnerabilities will return a similar report for that parameter.