Krutarth Panchal

CIS 450

Week 2 – Nmap Automation (Book)

1. *What are the fourteen listed Nmap basics?*

The fourteen Nmap basics are:

1. Options Summary
2. Target Specification
3. Host Discovery
4. Port Scanning Basics
5. Port Scanning Techniques
6. Port Specification and Scan Order
7. Service and Version Detection
8. OS Detection
9. NMAP Scripting Engine
10. Timing and Performance
11. Firewall/IDS Evasion and Spoofing
12. Output
13. Miscellaneous Options
14. Runtime Interaction
15. *What can a threat actor do with Port Scanning and Service/Version Detection?*

Port Scanning can provide information about the status of the port in the target systems. Service/version detection provides information about the services running on the specific on the targeted machine. With these information threat actors can perform attacks targeting the specific ports and services in the targeted machine.

1. *What is the purpose of Host Discovery? (Hint: There are two clearly defined purposes.)*

The purpose of the host discovery is to determine the active host or IP addresses in the network and focus scanning into the specific host and services running on it.

1. *What default ports are used by Nmap?*

By default, Nmap uses almost 1,000 most common port. The default ports for service used by Nmap are Port 80 (HTTP), HTTPS (443), Port 21 (FTP), Port 22 (SSH), Port 3389 (ms-term-server), Port 25 (SMTP) and so on.

1. *What scanning avenues are used by Nmap?*

The avenues used by nmap are: OPEN. CLOSED, FILTERED, UNFILTERED, OPEN|Filtered, CLOSED|Filtered.

1. *The switch "-sC" is not the correct switch used by all scans. (T or F)*

> False

1. *Scans can target the IP based transport layer. (T or F)*

> True

1. *Version detection is controlled with the -A or -sV switch. (T or F)*

` > True

1. *Port Spec and Scan Order will attempt to identify host info from Session to Application layers. (T or F)*

> True

1. *What readable file formats can NMAP output to?*

The readable file formats that NMAP output to is XML.