This document was available for public review and comments in the Information Security Fundamentals (ISF) Standards Panel community.

Module Creation Template - Scanning

Maps to:
CSF Function: Protect and Detect

Domains:
Awareness & Training, Data Security, Information Security Processes & Procedures, and Protective Technology

Learning Objectives:
#1748 – Understand the fundamentals of network and application vulnerability scanners, common commercial and open source tools, and how to defend against them

![Diagram of Network Scans]

Figure 1: Prior Classification

Top-level taxonomy of Network Scans

![Diagram of Taxonomy of Network Scanning Techniques]

Figure 4: Taxonomy of Network Scanning Techniques
Situational Knowledge: (Definition should include the target environment and vulnerabilities)
- Target environment: A single-server, 2 node ethernet network
- Weaknesses to be avoided, discovered or managed: Open ports, Exposed services
  - Recursively ask what can go wrong?
    - To guide your analysis, start your rebuttals with the word “Unless...”. Each rebuttal should introduce a doubt in the claim that a learner can successfully avoid, discover or manage the weaknesses identified in the given scenario. Here are a few examples:
      - Unless the ports and services are only visible to certain IP addresses
      - Unless the network scanner IP range does not include the server
      - Unless the scans are being dropped by a firewall
      - Unless the scanner is misconfigured
      - Unless the scanner is improperly updated
      - Unless the results are incorrectly interpreted
      - Unless the scan target is misunderstood
  - For each rebuttal,
    - Think about what learning modules will be necessary to overcome these doubts.
      - The next topics will help you organize the learning materials in to Conditional knowledge, procedural knowledge and declarative knowledge.
    - How will you assess that the instructional materials do in fact help a learner overcome these doubts?
      - Each knowledge component can be paired up with assessments that measure student knowledge and their confidence in that knowledge.

Situational Difficulty Rating
To what extent is this problem (situation) clearly defined?

To what extent is the solution space clearly defined?
  - What adds volatility to this situation? (High rating of the problem, High rating of the solution)
  - What adds uncertainty to this situation? (Low rating of the problem, High rating of the solution)
  - What adds complexity to this situation? (High rating of the problem, Low rating of the solution)
  - What adds ambiguity to this situation? (Low rating of the problem, Low rating of the solution)
    - The presence of a firewall or IDS
Conditional Knowledge: (Choices that must be made between or within procedures to address the situation)
- The selection of appropriate scan types based on the target environment and presented constraints such as the presence of a IDS or firewall
  - This be should motivated by existing literature. See Barnett and Irwin Towards a Taxonomy of Network Scanning Techniques
- The desired results of the reconnaissance

Procedure Knowledge:
- Steps involved in scanning a network using Nmap
- Different configuration options
- Interpreting the results of the scan

Declarative Knowledge Required:
https://docs.google.com/spreadsheets/d/1BKhNWlVms1Vkb4H3Qwia7unVb5c20rh8b_AM5iq0P

- Credentialed vs. non-credentialed vulnerability scanning
- Defensive techniques and measures
- Disabling unused application service ports
- Identify vulnerability
- Intrusive vs. non-intrusive vulnerability scanning
- Network Security
- Nmap
- Passive vs. active threat/vulnerability discovery tools
- Ports:
  - Port 22
  - Port 25
  - Port 443
  - Port 53
- Port scanner
- Protocol analyzer
- Wireshark
- Vulnerability scanner

Suggested Sequence:

1. Take Pre-Assessment/Readiness Declarative Knowledge Assessment (Robin working on this)

2. Watch 1_Scanning_Intro (Lectures\1_Intro_Scanning\Intro_Scanning.mp4) Lecture video

2a. Create Declarative Knowledge Assessment

3. Watch 2_Scanning_Ping_Sweeps
   (Lectures\2_Scanning_Ping_Sweeps\2_Scanning_Ping_Sweep.mp4) Lecture video

3a. Create Declarative Knowledge Assessment (3 questions for each concept)
4. Watch 3_Scanning_with_nmap
(Lectures\3_Scanning_with_nmap\Scannning_with_nmap.mp4) Lecture video

4a. Create Declarative Knowledge Assessment (3 questions for each concept)

5. Watch Scanning_Intro_nmap (Tutorial_Labs\Intro_to_nmap\Intro_to_nmap.mp4) Tutorial video

5a. Create Procedural Assessment (rank order how steps should be executed/included)

5b. Go to Gym and do lab

5c. Create Skills Assessment

6. Watch nmap_Network_Ping_Sweep_Worked_Example
(Tutorial_Labs\nmap_Network_Ping_Sweep_Worked_Example\nmap_Network_Ping_Sweep_WorkeExample.mp4) Tutorial lab

6a. Create Procedural Assessment: should have a question that relates to the use of options/switches and one of the choices should be the wrong option in #6 (nmap_Network_Ping_Sweep_Misuse_Case.mp4)

6b. Go to Gym and do lab: What can vary (the IP address of the target(s)):
   - One host (192.168.1.1)
   - A range of IP addresses (e.g., 192.168.1.1-192.168.1.100)
   - A Network block (e.g., 192.168.1.0/24)

6c. Create Skills Assessment

6d. Watch nmap_Network_Ping_Sweep_Misuse_Case
(Tutorial_Labs\nmap_Network_Ping_Sweep_Misuse_Case\nmap_Network_Ping_Sweep_Misuse _Case.mp4)

7. Create Wireshark functionality & fundamentals Lecture videos (covers Protocol Analyzer from SIG 1 Reference Concepts)

7a. Create Declarative Knowledge Assessment(s) for various Lecture videos

7b. Create Wireshark Functionality & Fundamentals Worked example Tutorial lab videos

7c. Create Procedural Assessment(s) from Worked example Tutorial lab videos

7d. Go to Gym and do various Wireshark labs from 7b.

7e. Create Skills Assessments

7f. Create Wireshark Functionality & Fundamentals Misuse cases
8. Create Ping Sweep with Nmap and Wireshark Tutorial Lecture video (why do you want to use a protocol analyzer when you run a tool like Nmap?)

8a. Create Declarative Knowledge Assessment (3 questions for each concept)

8b. Create Ping Sweep with Nmap and Wireshark Tutorial lab video

8c. Create Procedural Assessment(s)

8d. Go to Gym and do Ping Sweep with Nmap and Wireshark lab

8e. Create Skills Assessment

9. Create UDP Port Scanning Lecture video (be sure to describe what a port scanner is; why hackers and admins alike want to do port scans (to find open ports); covers Port Scanner Reference Topic from SIG 1

9a. Create Declarative Knowledge Assessment (3 questions for each concept)

10. Create UDP Scanning Tutorial video (worked example): be sure to explain how to scan various ports (e.g., no Port switch/option, and explain what nmap scans; all UDP ports; a range (e.g., 53, 161))

10a. Create Procedural Assessment
10b. Go to Gym and do UDP Scanning lab (worked example): What can vary:
   - IP address of target(s)
   - Ports to scan
   - Others?

10c. Create Skills Assessment

10d. Create UDP Scanning video (Misuse Case)

11. Create Understanding Nmap Port States Lecture Video

11a. Create Declarative Knowledge Assessment (3 questions for each concept)

11b. Create Tutorial Video of me analyzing output of a UDP scan

11c. Create Procedural Assessment

11d. Create Skills Assessment

12. Create TCP Scanning Lecture Video (be sure to point them to additional resources for TCP review)

12a. Create Declarative Knowledge Assessment (3 questions for each concept)
13. Create TCP Connect Scan Lecture video

13a. Create Declarative Knowledge Assessment (3 questions for each concept)

13b. Create TCP Connect Scan Tutorial video (Worked example), including analyzing the output; be sure to include Port #s referenced in Reference Topic from SIG 1

13c. Create Procedural Assessment

13d. Go to Gym and do TCP Connect Scan

13e. Create Skills Assessment

13f. Create TCP Connect Scan Tutorial Misuse case video

14. Create TCP SYN Scan Lecture video

14a. Create Declarative Knowledge Assessment (3 questions for each concept)

14b. Create TCP SYN Scan Tutorial video (Worked example), including analyzing the output; be sure to include Port #s referenced in Reference Topic from SIG 1

14c. Create Procedural Assessment

14d. Go to Gym and do TCP SYN Scan

14e. Create Skills Assessment

14f. Create TCP SYN Scan Tutorial Misuse case video

15. Create Service Detection Lecture video

15a. Create Declarative Knowledge Assessment (3 questions for each concept)

15b. Create Service Detection Using Nmap Tutorial video (Worked example), including analyzing the output

15c. Create Procedural Assessment

15d. Go to Gym and do Service Detection Using Nmap lab

15e. Create Skills Assessment

15f. Create Service Detection Using Nmap Tutorial Misuse case video

16. Create Active Stack Fingerprinting Lecture video

16a. Create Declarative Knowledge Assessment (3 questions for each concept)
16b. Create Active Stack Fingerprinting Using Nmap Tutorial video (Worked example), including analyzing the output

16c. Create Procedural Assessment

16d. Go to Gym and do Active Stack Fingerprinting Using Nmap lab

16e. Create Skills Assessment

16f. Create Active Stack Fingerprinting Using Nmap Tutorial Misuse case video

17. Create Active Stack Fingerprinting Lecture video

17a. Create Declarative Knowledge Assessment (3 questions for each concept)

17b. Create Active Stack Fingerprinting Using Nmap Tutorial video (Worked example), including analyzing the output

17c. Create Procedural Assessment

17d. Go to Gym and do Active Stack Fingerprinting Using Nmap lab

17e. Create Skills Assessment

17f. Create Active Stack Fingerprinting Using Nmap Tutorial Misuse case video

18. Create Putting It All Together Lecture video

18a. Create Declarative Knowledge Assessment (3 questions for each concept)

18b. Create Putting It All Together Using Nmap Tutorial video (Worked example), including analyzing the output

18c. Create Procedural Assessment

18d. Go to Gym and do Putting It All Together Using Nmap lab

18e. Create Skills Assessment

18f. Create Putting It All Together Using Nmap Tutorial Misuse case video

Reference Documents (Reading Assignments)
[1]