CYBERROOKIE

CYBERROOKIE

CYBERROOKIE

CyberRookie Project - Learning Cyber Skills By Building A HomeLab

Trevor Shi

CYBERROOKIE

Week 7 Lesson -Risk/Vulnerability Assessment

CYBERROOKIE

Overview

1. Risk Management/Assessment
2. Vulnerability Assessment
3. WSUS Patch Management
4. LAB Practice
5. Homework

CYBERROOKIE

1. Risk Management/Assessment

1. What is cyber Risk?

The combination of the probability of an event and its consequence(ISO/IEC 73).

2. Key Terms

Asset: Something of either tangible or intangible value that is worth protecting.
Threat: Anything that is capable of acting against an asset in a manner that can result in harm
Vulnerability: Weakness
Likelihood: The measure of frequency of which an event many occur
Impact:

3. Cyber Security is about Risks, Controls and Auditing.

The core duty of cybersecurity is to identify, mitigate and manage cyber risk to an organization’s digital assets.

CYBERROOKIE

Approaches to Cyber Risk

1. **AD HOC**
   implement security with on particular rationale or criteria.

2. **Compliance-based**
   relies on regulations or standards to determine security implementations.

3. **Risk-Based**
   relies on identifying the unique risk as particular organization faces and designing and implementing security controls to address that risk above and beyond the entity's risk tolerance and business needs.

CYBERROOKIE

Risk Management Standards and Frameworks

NIST Special Publication 800-30: Guide for Conducting Risk Assessments
https://www.nist.gov/privacy-framework/nist-sp-800-30

NIST Special Publication 800-39: Managing Information Security Risk
https://csrc.nist.gov/publications/detail/sp/800-39/final

CYBERROOKIE

Online Free Courses

1. **FedVTE Course**
   Fundamentals of Cyber Risk Management - 6 Hours
   https://fedvte.usalearning.gov/publiccourses/fcrmframe.php

2. **EDX Course**
   Cybersecurity Risk Management
   https://www.edx.org/course/cybersecurity-risk-management?source=aw&awc=6798_1616990595_f43a7777a4c29a04f81754b907ace62b&utm_source=aw&utm_medium=affiliate_partner&utm_content=text-link&utm_term=301045_https%3A%2F%2Fwww.class-central.com%2F

CYBERROOKIE

2. Vulnerability Assessment

1. **What is a Vulnerability Assessment**
   the process of identifying the vulnerabilities in your network, systems and hardware, and taking active steps toward remediation.
   https://www.rapid7.com/solutions/vulnerability-assessment/

2. **5 Steps to a VA**

   Planning

   Scanning

   Analysis

   Remediation

   Repeat

CYBERROOKIE

Performing the VA process

1. Install a vulnerability scanner and implement a scanning schedule
2. Scan your organization’s network to address any potential vulnerabilities
3. Scan any devices connected to an associated IP-address or internal network
4. Identify any changes, pending updates or missing software patches
5. Identify and prioritize risks
6. Select strategic risk-based remediation
7. Conduct remediation work

CYBERROOKIE

VA Tools

1. **Qualys VMDR**
   All-in-One Vulnerability Management, Detection, and Response, enterprise solution
   https://www.qualys.com/apps/vulnerability-management-detection-response/

2. **Nessus Essentials**
   Free download scan 16 IPs
   https://www.tenable.com/products/nessus

3. **OpenVAS - Open Vulnerability Assessment Scanner**
   Free, Open-Source, full-featured vulnerability scanner
   https://www.openvas.org/

CYBERROOKIE

Online Courses

1. **Qualys Free Training Online Practice Course**

   Suggest to complete the Vulnerability Management learning path and complete the exam to achieve the certification

   https://www.qualys.com/training/

2. **Tenable University**

   https://university.tenable.com/learn/home

CYBERROOKIE

3. WSUS Patch Management

1. What is Patch Management

https://www.rapid7.com/fundamentals/patch-management/#:~:text=Patch%20management%20is%20the%20process,bugs%E2%80%9D)%20in%20the%20software.&text=When%20a%20vulnerability%20is%20found,be%20used%20to%20fix%20it.

https://www.manageengine.com/patch-management/what-is-patch-management.html

2. What is WSUS

https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

CYBERROOKIE

4. LAB Practice

#1 Implement Nessus Essentials

1. Download Nessus Essentials
   Nessus Essentials Free download scan 16 IPs
   https://www.tenable.com/products/nessus

2. Install it into your Server

3. Prefer a VM Scan for LAB and set up the schedule scan

CYBERROOKIE

4. LAB Practice

#2 Deploy the WSUS on AD server

1. Install the WSUS Server Role

2. Configure WSUS

3. Approve and Deploy Updates in WSUS

4. Configure Group Policy Settings for Automatic Updates

Reference:

Deploy Windows Server Update Services

https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services

CYBERROOKIE

5. HomeWork

1. Install Nessus Essentials,run the scan for LAB, Review the Scan report, remediate the high/Mid level vulnerabilities

2. Deploy the WSUS service and patch all detected Vulnerabilities

CYBERROOKIE

Q&A

Look forward to your feedbacks and suggestions.
Contact: CyberRookieProject@gmail.com

CYBERROOKIE

Thank You