MODULE-2

NETWORK SECURITY

Reflective Piece

MS-CYBERSECURITY | AMIT PAHUJA

TABLE OF CONTENT

UNIT-1 ..... **2**
UNIT-2 ..... **3**
UNIT-3 ..... **5**
UNIT-4 ..... **6**
UNIT-5 ..... **6**
UNIT-6 ..... **7**
REFERENCES **8**

Here are the unit-wise learnings of the “Network Security” module – where I got the opportunity to learn - security assessment methodology, penetration testing approach, a wide variety of tools learned, log management and many more things.

UNIT-1

Description

Studied the network security vulnerabilities, types of testing & security challenges to the digital economy

Analysis & Evaluation

Learned the 4-step network security assessment methodology and two broad assessment flavors (Static analysis & Dynamic Testing) which are further detailed into Network infra / Web App / Web Service testing:

Reconnaissance >> Vulnerability scanning >> Investigation of Vulnerabilities >>

Exploitation of Vulnerabilities.

Every stage of the security assessment uses different tools (active and/or passive) which were used at the later stages to perform security assessment for the website chosen (https://allthegear.org.uk). Submitted the “initial post” on the topic “Digitalization – What are the security implications of the digital economy? “ where cyber security challenges for Bricks & Mortar SMEs wanting to go digital were discussed like Internet of Things (IoT), Point of Sale (PoS), Mobility Security attacks to name a few.

After studying and analyzing the different attack vectors, learned that there are attacks which are client related as well – where attackers with appropriate network access can attack different desktop applications and client software packages (e.g. Web Browsers like Google Chrome, Microsoft office, Putty etc.) – whereas there was a wrong perception in my mind that the attacks are always server/application side.

(McNab, C., 2016)

Initial Post: “Digitalization – What are the security implications of the digital economy?

UNIT-2

Description

Cyber Kill Chain model proposed by Lockheed Martin was revisited and analyzed if it still applies to modern Advanced Persistent Threats (APTs).

Analysis & Evaluation

Learned about Cyber Kill chain, Penetration testing its types (Whitebox & Blackbox), Threat modelling and risk rating mechanisms.

A kill chain which is a step-by-step process to engage and target an adversary is still used as an effective framework. Initially this concept was used in US Military and later expanded to Computer and Network Attacks-

The table below shows the actionable matrix of the cyber kill-chain different phases:

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

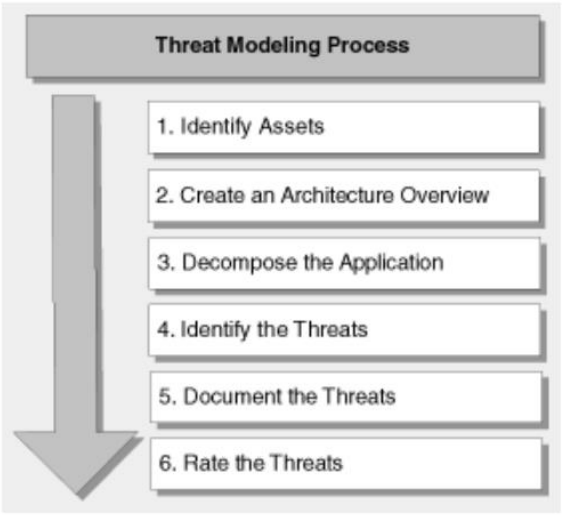
(Eric et al, N.D.)

Explored the Microsoft six-stage threat modelling process which was later used along with the DREAD model for risk rating after website scanning for vulnerabilities.

The below two figures were used to learn:

(1) Six-stage threat modelling process including the risk rating using DREAD model in “step 6” of the first image

(2) The different factors used to decide the risk rating level (High / Medium / Low) in the DREAD model



	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

(Threat Modelling, 2010)

Also, it was interested to read “Initial posts” for many of the students and I responded to two students (Gokul & Rob) as part of “Peer Response” assignment as I found theirs posts a lot meaningful & insightful

Even though there are many threat modelling / risk rating frameworks available, I strongly believe that STRIDE & DREAD are the most matured ones. While reading all these topics I also realized the actual difference between Vulnerability assessment and Penetration testing – Unlike the vulnerability assessment, penetration testing not only identifies but also exploits the vulnerabilities and determine the security gaps - which I thought are same before!

Peer Posts: “Digitalization – What are the security implications of the digital economy?

UNIT-3

Description

During this unit, we were asked to read about different approaches of vulnerability assessment and prepare "**Vulnerability Audit and Assessment - Results and Executive Summary"** including the testing and scanning tools after appropriate evaluation

Analysis & Evaluation

Performed the scanning activity using some of the basic tools:

- **Traceroute**: To calculate the no. of hops to the target website and max. latency
- **Dig & Nslookup**: To find name server and "MX" records
- **WhoIS**: To find the registered contact, email address, name servers etc.

Explored different tools, from Commercial to free, and selected the ones to be used at different stages of the Security Assessment. The selected tools were used during the actual scanning of the website for reconnaissance and finding vulnerabilities.

1) **Reconnaissance:** Web Search Engines. WHOIS databases
2) **Vulnerability Scanning**:
    a. **Network:** OPENVAS, OWASPZAP, Qualys Guard, NESSUS, and NMAP
    b. **Web-APP:** Burp Suite, IBM Security AppScan & Acunetix
3) **Investigation of Vulnerabilities**:
4) **Vulnerabilities Exploitation:** Rapid7 Metasploit & Immunity CANVAS

(Kali Tools, N.D.)

Scanning Activity

Vulnerability Audit and Assessment - Results and Executive Summary

UNIT-4

Description

Learned Kali, a Linux Open-Source penetration testing distribution platform, Biggest Data Breaches and its mitigations

Analysis & Evaluation

Installed Kali in the AWS environment on a virtual Machine. Explored the look and feel of tools of different stages/requirements from Information gathering to Vulnerability Analysis to Exploits.

Submitted the “initial post” on the topic “**The Pros and cons of logging – The impact of log4j**” as part of the assignment, where there was discussion around compliance requirements (FISMA, HIPAA, SOX, PCI-DSS etc.) that mandates the log management and the security of those logs.

(Karen Kent, Murugiah Souppaya, N.D.)

Initial Post- “The Pros and cons of logging – The impact of log4j”

UNIT-5

Description

Logging tools for Windows & Linux and its best practices.

Analysis & Evaluation

Learnt the complete Log Management Strategy –

Logging Events >> Defining Scope >> Timely reviewing logs >> Audit Trails

Explored about different SIEM and Log Management Vendors – ArcSight, Splunk, Log Logic, Nitro Security, Syslog NG & many more.

Also, it was interested to read “Initial posts” for many of the students & all had posted great content, I responded to two students (Iason & Gokul) as part of “Peer Response” assignment as I found theirs posts a lot informative

(David Swift, 2021)

Whilst Splunk covers a fair number of market/enterprises for log management, I worked on only Splunk in all my organizations and was now aware of any other vendors and the study here gave me a fair knowledge about other vendors as well.

Peer-Posts- “The Pros and cons of logging – The impact of log4j”

UNIT-6

Description

Vulnerability Assessment results & Executive Summary, Future of Internet

Analysis & Evaluation

During this week, Created the assignment on “**Vulnerability Audit and Assessment - Results and Executive Summary**”, - Information gathering and vulnerability scanning was performed using different tools like NMAP, DMITRY, WAAFWOOF, OPENVAS, OWASPZAP etc. on the website chosen (https://allthegear.org.uk). The vulnerabilities are rated as per the threat and the solutions are provided to remediate the vulnerability and included executive summary as well. I missed to attend the seminar on “Future of Internet” but went through the slides and recording and found it really interesting.

Vulnerability Audit and Assessment - Results and Executive Summary

REFERENCES:

1. (McNab, C., 2016): Network Security Assessment

2. Eric et al [N.D]: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains http://gauss.ececs.uc.edu/Project4/Documents/kill-chain.pdf

3. (Threat Modelling, 2010) https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

4. (Kali Tools, N.D.) https://www.kali.org/tools/

5. Ekelhart, A., Kiesling, E. and Kurniawan, K. (2018). Taming the logs - Vocabularies for semantic security analysis. Procedia Computer Science

6. Karen Kent, Murugiah Souppaya [N.D]: Guide to Computer Security Log Management https://www.govinfo.gov/content/pkg/GOVPUB-C13-52c3b5520393598b18782a7b55fde7e6/pdf/GOVPUB-C13-52c3b5520393598b18782a7b55fde7e6.pdf

7. David Swift [2021]: Successful SIEM & Log Management Strategies for Audit & Compliance https://sansorg.egnyte.com/dl/GXxMMgSwsV