Meeting Notes

20/05/2021

Team Meeting

Attendance

|  |  |
| --- | --- |
| **Name** | **Present** |
| Anrich Potgieter | Yes |
| Anum Rashid | Yes |
| Panagiotis Tolis | Yes |
| Samiya Nova | No |

Notes

Questions for Tutor

* Is there a page limit for the assignment?
* Is the 1000 word limit a lower limit or an upper limit?
* Will we be marked down if we exceed the word count?

Next Steps

* Each team member needs to experiment with their assigned tool.
* The team member needs to document their findings.
* We will collaborate with the other team to define a domain for their scan.
* Scan through the PCI for Dummies book.
* Every team member needs to deploy an AWS server.

Next Meeting

* Proposed next meeting: **Sun 23rd 4:00 PM GMT + 1**
* Each member should prepare a short paragraph regarding their tool indicating their results and action points.
* We need to consider the methodology of the approach.

Tool Assignment

OpenVas

* Anum Rashid

Nmap

* Anrich Potgieter

TestSSL

* Panagiotis Tolis

dirBuster

* Samiya Nova

Qualys Community Edition

* Panagiotis Tolis is experimenting with this tool.

The Domains for the Assignment

* An industry recruitment site that is used to allow candidates to register themselves on job vacancy sites.
  + GDPR.
  + They will need to provide information about themselves.
* An e-health site provides registrants with medical and fitness information and advice supplied by medical professionals.
  + To receive consultancy, you need to provide your health record; this falls within the remit of GDPR.
  + The type of data provided is within the critical domains of GDPR.
* An e-commerce site used to provide payment services and advice for commercial website operators.
  + Payment Card Industry Data Security Standard.

02/06/2021

Team Meeting

Attendance

|  |  |
| --- | --- |
| **Name** | **Present** |
| Anrich Potgieter | Yes |
| Anum Rashid | No |
| Panagiotis Tolis | Yes |
| Samiya Nova | No |

Notes

For the Tutor

How you will identify, investigate and classify their security challenges

* We could speak about compliance here
* Perform intel gathering to determine whether the infrastructure matches the
* compliance controls
* Comparing the mandatory controls of the regulation with the already implemented security measures.
* These would be the PCI controls.

○ Take a sample of the vulnerabilities found and map these to the PCI controls.

○ We would need to link the Tools to the PCI controls, to determine whether

the domain is within the scope of the assessment we have selected the

following tools.

Hack the Box

● As a result of the ongoing AWS issues, we have decided to scan a hack the box

machine.

Group Members Next Steps

● Each group member needs to sign up for an account at Hack The Box

● Each group member will need to install OpenVPN and download the connect script

from hack the box.

● Each member will be assigned a machine below.

● Each group member needs to scan their respective machine with the assigned tool

and provide screenshots and txt file output from their scans. And a paragraph about

the tool you are using. (Keep in mind the domain which we are scanning)

● Deadline for Sunday:

○ Paragraph about the tool

○ Scans of the server

■ Screen shots

■ txt files of the scans / export of scans

Hack the box allocations

Anrich Potgieter

● Archetype

Anum Rashid

● Pathfinder

Panagiotis Tolis

● Oopsie

Samiya Nova

● Shield

06/06/2021

Team Meeting

# Attendance

|  |  |
| --- | --- |
| **Name** | **Present** |
| Anrich Potgieter | Yes |
| Anum Rashid | Yes |
| Panagiotis Tolis | Yes |
| Samiya Nova | No |

# Notes

## Questions for Nawaz

* A brief overview of the assignment requirements.
* What should be included within the security challenges section?
* Should we include our findings within the security challenges section?
* Business impacts on use of tools and methods?
  + The tools used are non-invasive and we are gathering information rather than attempting to penetrate the application itself.
  + These tools do not generate massive amounts of traffic.
* Limitations and Assumptions

* Discuss regarding Nova’s absence and lack of contribution so far in the module.

### **Unit 11 Assignment**

* Can we copy the information from the design document and use this within the summary?
* We are concerned that if we were to copy the content Turnitin will return a high similarity score.

## Next Steps

## Assignment

### **Methodology (OWASP)**

* <https://owasp.org/www-project-top-ten/>
* <https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/>

* Write a justification of the Methodology.
* Map each tool to an OWASP category.

### **Tasks**

* ~~Test SSL - Paragraph - Panos~~
* ~~Harvester - Paragraph - Panos~~
* OWASP ZAP - Pragraph - Anrich
* Methodology (OpenVas) - Anum

## Next Meeting

Thu 10th @ 5:30 PM GMT + 1

09/06/2021

Team Meeting

Attendance

|  |  |
| --- | --- |
| **Name** | **Present** |
| Anrich Potgieter | Yes |
| Anum Rashid | Yes |
| Panagiotis Tolis | Yes |
| Samiya Nova | Yes |

Notes

* Each tool needs to have a justification
* Threat landscape
  + Define the threat landscape
    - Human Factor (Harverster)
    - Network infrastructure (Nmap)
    - Encryption (Nmap SSL scripts)

* Justification of the Methodology
  + Compare to the best practices.
  + What we did how does this compare to the OWASP methodology.
  + Did we comply with the best practices?
  + We did not just find the methodology, we can say that we selected the steps that applied to our scans.
* Structure of assignment
  + Methodology
    - What is a threat landscape
    - Link the threat landscapes to topics
      * What we were trying to evaluate
      * Why we used the tools
      * Best practices

Tasks

* (Panos) - Prepare the Excel Template.
* (All) - Read about the threat landscape: [Threat Landscape — ENISA (europa.eu)](https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends)
* (All) - The main purpose of the tool.
* (All) - Justify within the methodology the use of the tool and how that forms the threat landscape.
* (Nova) - Write what is the threat landscape.
* (Nova) - Write a short paragraph about DirBuster. (White papers, the documentation from the developers)
* (All) - Find timeline template
* (Anum) - OWASP ZAP - Write a short paragraph
* (Anrich) - Security Challenges

Next Meeting

TBC

27/06/2021

Team Meeting

# Agenda

* Discuss the final group assignment
* Questions for Nawaz
* Tasks for the week

# Attendance

|  |  |
| --- | --- |
| **Name** | **Present** |
| Anrich Potgieter | Yes |
| Anum Rashid | Yes |
| Panagiotis Tolis | Yes |
| Samiya Nova | Yes |

# Notes

* We will update the risk assessment excel spreadsheet
* Panos will share the controls spreadsheet in the channel
* Connect the security controls to the security issues that we have mentioned in the risk assessment.
* Search for controls that refer to Privacy Shield and California Privacy Act.

## Questions for Nawaz

* Unit 11 assignment
  + Can we copy and paste our methodology or will we be required to re-write the methodology, how will this affect turnitin?
  + Summary of data: What is being requested here?

## Next Steps

### **Tasks**

* ~~Set up a meeting with Nawaz~~
* Find technical controls (Privacy Shield | California)
* Find organisational controls (Privacy Sheild | California)
* Make sure to read PCI DSS for Dummys

## Next Meeting

08/07/2021

Team Meeting

Agenda

* Discuss final assignment

Attendance

|  |  |
| --- | --- |
| **Name** | **Present** |
| Anrich Potgieter | Yes |
| Anum Rashid | Yes |
| Panagiotis Tolis | Yes |
| Samiya Nova | Yes |

Notes

The following table is an example of how we can structure the standards.

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Requirements of the directive. | Controls already implemented. | Recommended Mitigation Actions |
|  |  |  |  |

Potential Assignment Structure

1. Introduction
2. Methodology
   1. Refer to the appendix where applicable.
3. GDPR
   1. Introduction to directive
   2. identify the types of personal information that we process
   3. assume the geographical location of our users
   4. Table with vulnerabilities
4. PCI-DSS
   1. 12 Domains
   2. Table of Vulnerabilities
5. Summary of the compliance assessment (with diagrams, charts, etc.)
   1. Diagrams:
      1. How many vulnerabilities
      2. How close are we to being compliant?
6. Conclusion
7. Appendixes

Next Steps

* Paraphrasing the methodology and introduction (Anum and Nova)
* Prepare two Paragraphs for PCI - DSS and GDPR (Anrich and Nova)
* Create tables and introductory text for standards/directives (Anrich and Panos)

Next Meeting

Sunday 11th of July @ 3:00 PM