

Cyber Security Experts Association of Nigeria (CSEAN)  
Society for Multidisciplinary & Advanced Research Techniques (SMART)  
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana  
SMART Scientific Projects & Research Consortium (SMART SPaRC)  
Sekinah-Hope Foundation for Female STEM Education  
ICT University Foundations USA

---

---

Proceedings of the Cyber Secure Nigeria Conference – 2023

---

---

## Addressing the Dilemma of a “Crisis within a crisis”: Exploring the Penetration Testing challenges in a Mobile Field Hospital Setting

<sup>1</sup>Ahmed, N.B., <sup>2</sup>Daclin, N., <sup>3</sup>Olivaux, M. & <sup>4</sup>Dusserre, G.

<sup>1,2&4</sup>IMT Mines Ales, South France

<sup>2</sup>University of Nimes, South France

**E-mails:** nasir-baba.ahmed@mines-ales.fr; nicolas.daclin@mines-ales.fr; marc.olivaux@mines-ales.fr; gilles.dusserre@mines-ales.fr

### ABSTRACT

This paper focuses on evaluating the security challenges faced by mobile field hospitals, which play a crucial role in emergency response and disaster management in remote and austere environments. The authors conducted a penetration test using the Open Source Security Testing Methodology Manual (OSSTMM) framework to assess the security posture of a mobile field hospital. The methodology employed in the study included a combination of automated and manual techniques such as network scanning, vulnerability assessments, social engineering, and exploitation. The penetration test revealed several security vulnerabilities in the mobile field hospital, including weak passwords, unpatched software, and inadequate network segmentation. Additionally, the study identified vulnerabilities in the hospital's medical devices and equipment, posing a risk of cyber-attacks that could disrupt operations and compromise patient safety. The results underscore the importance of implementing enhanced security measures in mobile field hospitals to mitigate cyber threats and ensure the uninterrupted functioning of medical operations during emergencies and disasters. This study provides a comprehensive analysis of the mobile field hospital's security posture using the OSSTMM framework and emphasizes the urgent need for improved security practices in such settings.

**Keywords:** Cybersecurity, Healthcare, Penetration Testing, Mobile Field Hospitals, Data, Emergency Response, Open Source, Security Testing, Ethical Hacking, Security Frameworks,

---

---

#### Proceedings Citation Format

Ahmed, N.B., Daclin, N., Olivaux, M. & Dusserre, G. (2023): Addressing the Dilemma of a “Crisis within a crisis”: Exploring the Penetration Testing challenges in a Mobile Field Hospital Setting. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12<sup>th</sup> July, 2023. Pp 67-80  
<https://www.csean.org.ng/>. [dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P9](https://doi.org/10.22624/AIMS/CSEAN-SMART2023P9)

---

---

## 1.. INTRODUCTION

Mobile Filed Hospitals (MFH) are medical units that provide medical treatment in remote areas inaccessible to regular medical teams [1]. MFH are equipped with all the necessary medical equipment for performing surgical operations and providing care to sick and wounded soldiers. In addition, MFHs have a crew of medical professionals to perform minor surgeries and provide basic first aid in support, or in the absence of a traditional hospital. However, like any other important healthcare facility, MFHs need regular cybersecurity checks to keep them safe from cyber threat actors.

As the healthcare sector continues to evolve and provide life-critical healthcare services, the sector continues in improving the efficiency towards patient care and patient treatments. This is carried out with the aid and implementation of Information Technology and new technology. In turn, this opens up new avenues for cyber threat actors and criminals to explore the weakness in the cyber infrastructure of health sector by exploiting vulnerabilities that emerge with these new innovations. These new avenues leading to cyber vulnerabilities range from malware infections which compromises the integrity of the healthcare information systems and privacy of patients, to a more targeted distributed denial of service (DDoS) attacks that aim to cause major disruptions in the service delivery processes.

While other critical infrastructure sectors experience these types of attacks, the nature of the healthcare industry's mission poses unique challenges. For healthcare, cyber-attacks can have ramifications beyond financial loss and breach of privacy [2]. For example, a ransomware attack on a healthcare facility information system cripples the capability of the healthcare personnel to carry out critical services to patients. In addition, it also compromises the privacy of the patients, and exposes their Electronic Health Records (EHR) to external threats.

### 1.1 Need for Assessment and Testing:

Cybersecurity in MFH and the healthcare sector in general, has become one of the significant threats in the healthcare industry [3]. Thus, I.T experts must persistently aim to address healthcare cybersecurity issues, due to prevention of attacks and safety of patients and specific legislations such as the ones outlined in the health insurance portability and accountability act (HIPAA) in the United States laws. It also applies to the ethical commitment of the healthcare organisations and the MFH to help patients and the damage that healthcare security breaches can have on their lives [3]. With these in mind, there is a need to assess and test the current security posture, to firstly know the current level of the MFH's cybersecurity posture, and secondly to prove that the current security posture is accurate. This will then provide a platform for more understanding of the threats, and vulnerable areas to which MFH needs to be improved to prevent any imminent of future security threats.

## 2. METHODOLOGY & FRAMEWORKS

### 2.1 Major Penetration Testing Frameworks & Methodology Review:

Penetration testing, as important as it is to the general improvement of the security of cyber infrastructure of organizations, can deliver a wide range of results based on standards and methodologies that are implemented.

These penetration testing methodologies offer a range of options to suit the requirement of different ways in which organizations operate, as well as the content and importance of their infrastructure. In this paper, six major penetration testing methodologies are reviewed based on [6] that provide the best possible range of security testing options that can be leveraged and implemented in the cyber infrastructure of a MFH.

#### **I. NIST SP 800-115:**

The US National Institute for Standards and Technology (NIST) provides specific standards and recommendations to be leverage in performing penetration tests. The NIST SP-800-115 (NIST Special Publication) focuses on Critical Infrastructure cybersecurity, even though it provides coverage an overall cybersecurity of organizations in general [6].

The SP-800-115 provides a level guarantee in terms of information security in sectors such as the banking sector, communications sector, energy sector and other industries, including small and medium enterprise businesses, as it can be adapted to the parameters of their needs. In adopting the SP-800-115, the PT is to be carried out on their networks and applications by following a set of guidelines provided in the special publication guided by a set of procedures that have already been established.

In terms of its contribution to performing a PT, it enables the organizations to develop their information security assessment policies, accurately plan and provide guidance on approach to developing assessment plans and legal considerations, safe execution of technical assessment using its methods and techniques. Finally, it covers the handling of technical data from collection, to storage, to transmission and to destruction, during the assessment, as well as conducting analysis and reporting in simpler and technically-translated findings into risk mitigating recommendations [7].

#### **II. ISSAF:**

The Information System Security Assessment Framework (ISSAF) comprises a structured and dedicated approach to PT that requires an advanced methodology entirely tailored to its target organizations or sectors. The standards cover processes from planning and assessment to reporting and destroying artifacts as well as catering for all steps of the process [6]. The ISSAF is a peer reviewed and structured framework that categorizes information system security assessment into numerous fields & points specific evaluation or testing criteria for each of these fields [8]. It may additionally be used as a reference for meeting other information security needs as it includes crucial features of security processes, while aiming to provide a minimal level of an acceptable process. It also aims to provide a baseline for which assessments can be performed, while strengthening the already existing security processes and technology [8].

#### **III. OWASP:**

The Open Web Application Security Project (OWASP) PT describes the assessment of mostly web applications to identify vulnerabilities outlined in its famous OWASP Top 10 list. This PT methodology is designed to identify, safely exploit and help to address these vulnerabilities so that any weaknesses discovered can be addressed with immediate alacrity [9]. In cases of application security, the OWASP is the most recognized standard which is powered by a very well-versed community that stays on top of the latest technologies [6].

It provides a methodology for application PT that can not only identify vulnerabilities commonly found within web and mobile applications, but also complicated logic flaws that stem from unsafe development practices [6]. This methodology helps organizations secure their applications (both web based and mobile-based applications) from common mistakes that can have a potentially critical impact on their organization. When performing a PT with this methodology, the OWASP ensures that no vulnerabilities are omitted and proffers realistic recommendations that can be tailored to specific parameters and cyber infrastructure applications deployed in the organization.

#### **IV. CREST:**

The Council for Registered Ethical Security Testers (CREST) PT, firstly of permits the evaluation of the effectiveness of security controls and policies that are existing, while providing recommendations. The CREST PT also helps in gaining visibility into vulnerabilities which could be exposing organizations to cyber breaches [10]. CREST also provides useful overviews of key concepts that need to be understood to conduct structured penetration tests, by detailing the aspects, defining its' advantages and limitations, as well as describing the reason for implementing the methodology. This is done to help plan for and commence tests efficiently, making sure that vulnerabilities are identified and solutions proffered. The CREST follows a three-stage approach which guides the PT process. This starts from the preparation stage, which is part of the technical security assurance framework, managed by a suitable penetration testing governance structure. The second aspect follows with the actual conducting of the PT throughout the organizations, considering the testing styles, testing type, assessment constraints, identifications and remediation processes. Finally, the follow up actions that aid in maintaining the action plan, as well as improving the delivery of the planned actions [11].

#### **V. MITRE Attack:**

MITRE ATTACK (MITRE Adversarial Tactics, Techniques, & Common Knowledge) is a collection knowledge base and model for how cyber threat actors behave. It reflects the numerous phases involved in a cyber threat actor's attack lifecycle and the platforms they usually target. This provides a common taxonomy of adversary's actions understood by both offensive and defensive sides of cybersecurity. It also provides an appropriate level of categorization for adversary action and specific ways of defending against it [12]. The behavioural model contains core components of its tactics – the goals of the cyber threat actor – and the techniques – the achievement means to the target – that are consisting its implementation.

This methodology framework is a freely-accessible knowledge base of cyber threat actors tactics and techniques based on real-world reflexions, which is used is used as a foundation for the development of specific threat models and methodologies various sectors, and in the cybersecurity service community [13].

#### **VI. Other PT Methodologies:**

Sans Institute Cyber Kill-chain: the cyber kill chain is a concept originally developed and used by the military's model developed by Lockheed Martin, defines it as the steps taken and used by cyber-attackers in the modern day [14]. Theoretically, by understanding these stages used by attackers, organizations can track and identify, detect and remediate attacks in each of the stages.

This mostly focuses on the human element of cyber security, and how the cyber kill chain model is addressed. The cyber kill chain stages include reconnaissance, weaponization, delivery, exploitation, installation, command and control and actions on objectives.\

**Microsoft STRIDE model:**

The Microsoft STRIDE (Spoofing identity, Tampering data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges) model developed by two Microsoft engineers, Loren Kohnfelder and Praerit Garg, in the late 1990s [15]. STRIDE is used as a threat model to detect threats during the design phase of a system. Taking the first step provides better chances of finding potential threats , followed by finding the inherent risks inherent in the way the system has been implemented, and finally preferring solutions. Mainly, STRIDE makes sure that system satisfies the CIA triad (confidentiality, integrity and availability), as it was specifically designed to ensure that Windows software developers considered threats during the design phase.

**2.2 Choice(s) of Implementation & Justification:**

The meticulous review of the PT methodologies that can be used in performing technical tests on the cyber infrastructure of the MFH entailed considerations of the design of the MFH, its size, its limited devices and connectivity. Also the various PT methodologies’ consideration of flexibility of adaptation, especially in implementing in both the health sector services, and miniature structures with limited capabilities.

Due to its restriction to only be used for evaluating application security, the OWASP was graded in red (ruled out) in Table 1 below as being impractical to use in the MFH infrastructure because the MFH has more than just applications as part of its cyber infrastructure. Due to its limited restrictions of simply focusing on theoretical assessments features for its key data, the ISSAF was given the rating yellow (may be considered). Due to its basic design being copied by outside penetration testers, with minimal attention paid to white box test elements, the CREST technique was also given a red rating. While the MITRE framework was given a red rating because to its extensive usage of offensive PT and its extremely sophisticated mapping settings<sup>3</sup>

**3. THE TEST**

Mobile The test presents in details the steps taken, from preparation of the test, to assumptions, to pre-requisite statements, to declaring parameters, and performing the actual scenario tests. This is because the test provides a methodical approach to performing actions guided by the selected test methodology frameworks, as well as presenting the results in a scientific format. The rest is first preceded with a series of processes that declares the actions to be taken, in preparation for the main technical procedures, data recording and data analysis.

The mobile field hospital used in this study was a modular facility designed for rapid deployment in disaster-stricken areas. The penetration test was conducted using a combination of automated and manual techniques, including network scanning, vulnerability assessments, and social engineering. The test was conducted by a team of experienced security professionals with knowledge of the healthcare industry and emergency response operations.

These methods were chosen because they provide a comprehensive view of the security posture of the mobile field hospital and identify potential threats that could be used to disrupt operations and compromise patient safety.

In addition, the test was conducted in a controlled environment, simulating real-world scenarios. The team simulated a scenario where the mobile field hospital was deployed in a disaster-stricken area, and attempted to gain unauthorized access to the facility and its systems by exploiting the identified vulnerabilities. The goal of the test was to identify potential threats and evaluate the security posture of the mobile field hospital.

### **3.1 Test objectives:**

The objective of security testing of the MFH is to:

- define security goals through understanding security requirements of the MFH processes;
- identify the MFH security threats;
- validate that the security controls (if any) operate effectively;
- eliminate the impact of security issues on the safety and integrity of the MFH assets;
- provide response and resilience strategies when MFH is under malicious attacks.

#### **3.1.1 External (Exposure Testing):**

External security testing is conducted from outside the MFH's physical and security perimeter. This offers the ability to view the environment's security posture as it appears outside the security perimeter with the goal of revealing weaknesses that could be exploited by an external attacker [99]. External testing usually takes place first as it provides a chance to perform Black box and Grey box tests, with little or no insider information on network architecture or system configuration of the MFH that would not be available to an adversary.

In accordance with the NISPT SP-800-115 and the cyber-kill chain, external testing often begins with reconnaissance techniques that search public registration data, Domain Name System (DNS) server information, newsgroup postings, and other publicly available information to collect information (e.g., system names, Internet Protocol [IP] addresses, operating systems, technical points of contact) that may help the assessor to identify vulnerabilities. Next, enumeration begins by using network discovery and scanning techniques to determine external hosts and listening services. Since perimeter defences such as firewalls, routers, and access control lists often limit the types of traffic allowed into the internal network, assessors often use techniques that evade these defences—just as external attackers would.

Depending on the protocols allowed through, initial attacks generally focused on commonly used and allowed application protocols such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and Post Office Protocol (POP). Externally accessible servers are tested for vulnerabilities that might allow access to internal servers and private information. External security testing also concentrates on discovering access method vulnerabilities, such as wireless access points, modems, and portals to internal servers.

In addition to the NIST SP-800-115, the OSSTMM complies with a similar but more detailed approach to supplement, by detailing the specific steps in the test procedure, as shown in the Figure 20 below:

### **3.2 MAIN Penetration Testing**

Penetration testing is done manually using the procedures developed for the MFH assets and type of threat & automatically using web application vulnerability scanners, binary analysis tools, proxy tools etc.

The main attacks to be performed during the PT are listed below:

- SQL injection;
- Data manipulation;
- Barcode manipulation;
- Data Exfiltration;
- Denial of Service;
- Command injection.

The list of tools are pointed out in toolset section of each test table. This arrangement is done due to the nature of the test performed in different scenarios and they require a different set of tools.

### **3.3 Attack scenario Diagram:**

The scenario in Figure 2 shows the setting in which the PT generally takes place, within the scope of the test context of the MFH. It details the MFH cyber infrastructure setup, together with annotations to where the possible areas of attacks that are to be tested.

### **3.4 The Test Process**

The test consist of a series of parameters introducing the PT in terms of its category, methods, targets, Test class, test channel, scenario category, attack vectors and techniques. It is also carried out following certain steps that explain the procedures, as well as activities that explain the actions performed. To adequately perform and cover the most cases and possible scenarios, a series of 10 different tests and scenarios are performed.

**Table 4: Test Summary**

S/N	TEST	CATEGORY	TARGET	VECTOR
1	Wi-Fi Access	Wireless	Wireless router, User-PC	Compromised/Weak Credentials, Misconfiguration, Missing/Poor encryption
2	Wi-Fi Interception	Wireless	Wireless router, User-PC	Malicious Insider, Asset Vulnerability
3	Wi-Fi Deception	Wireless	Wireless router, User-PC	Phishing (Social engineering)
4	PC Access	Data	User-PC	Social engineering, Weak credentials, Misconfiguration, Malicious insider
5	Data Exfiltration	Data	User-PC, Local Database	Social engineering (Physical)
6	Data Corruption	Data	User-PC, Local Database	Social engineering (Physical)
7	Device Compromise	Wireless	Medical Device	Wireless sniffing, code injection
8	Data Corruption	Data	Barcode Reader	Social engineering (Physical)
9	Data Compromise	Data	EOS Web-app	Code injection (SQL-injection)
10	Wi-Fi Disruption	Wireless	Wireless router, User-PC	Denial of Service

The tests performed in Table 4 are described in terms of their various scenarios. These are also explained based on their categories, methods, classes, channels, vectors and techniques for better understanding. To conclude each test, the summary is followed by a symmetrical sequence representation of the activities performed in the form of an ‘Activity Flow’. This aims to summarise and highlight the major actions performed from the beginning to the end of each test.

After carrying out 10 separate tests with different scenarios, the methodical approach in describing each step taken to achieve the outcomes was according to the OSSTMM. In addition, the outcome of the tests are presented using the OSSTMM. This is used to convert and quantify the results in terms of the actions, processes, and infrastructural configurations available in the MFH. This will ultimately help in determining the cybersecurity posture of the infrastructure.

**Attack Surface Security Metrics**

OSSTMM version 3.0



Fig 1: OSSTMM RAV Calculator With Test Results Answers And Values

## 4 TEST RESULT

### 4.1 Test Result: The OSSTMM RAV Calculator:

The OSSTMM RAV (Risk Assessment Value) calculator is a tool used to measure the risk level of an organization's attack surface. It takes into account various factors that contribute to an organization's security posture and produces a numerical value that represents the organization's overall risk level. The RAV table is a comprehensive breakdown of the factors that contribute to the RAV score.

Using the OSSTMM RAV Calculator, the results of the questions answered based on the Penetration test methods and process to answer each question. These answers are converted in the RAV calculator based on the “YES or NO” answers and calculated based on the values, as well as the embedded formulae that each aspect of the RAV calculator applies [99].

### 4.2 Results Discussion: MFH ‘Actual security’

The OSSTMM RAV in table 5 is organized into several categories, including Attack Surface, Controls, Infrastructure, and People. Each category contains several items that are scored based on their effectiveness in reducing the organization's overall risk level. The scores for each item are combined to produce a score for the category, which is then used to calculate the overall RAV score. The significance of the values in the RAV table lies in their ability to provide insight into the strengths and weaknesses of an organization's security posture. For example, the Attack Surface category measures the size and complexity of the organization's attack surface, as well as the ease with which an attacker can gain access to it.

A high score in this category indicates that the organization has a large attack surface and is therefore more vulnerable to attack. The Controls category measures the effectiveness of the organization's security controls, including firewalls, intrusion detection systems, and access controls. A high score in this category indicates that the organization has robust security controls that are effective in reducing the risk of a successful attack.

Furthermore, the Infrastructure category measures the security of the organization's IT infrastructure, including servers, network devices, and databases. A high score in this category indicates that the organization has implemented security best practices in its IT infrastructure, making it less vulnerable to attack. The People category measures the security awareness and training of the organization's employees. A high score in this category indicates that the organization's employees are well-trained in security best practices and are less likely to fall victim to social engineering attacks.

Overall, the RAV table provides a detailed breakdown of an organization's security posture, allowing security professionals to identify areas of weakness and develop strategies to address them. By focusing on specific categories and items within the RAV table, organizations can take targeted steps to improve their overall security posture and reduce their risk of a successful attack.

The Actual Security being a nutshell value of the attack surface in the MFH operational environment, the representation of the Controls, Limitations, and the mathematical representation of an attack surface. This also shows where protection measures are lacking and where they are present within the scope of the MFH infrastructure PT. In this case, using a 100 Rav scale for the actual security results shows 81.076, which according to [99] translates as the MFH having far too few controls with respect to its operations and limitations in terms of its quantitative balance. Even though the Rav does not measure the risk of the attack surface, it shows where and how the security resources of the MFH are deployed and configured. For this Rav value, expressed in Table 7 above, to be determined as a consistent value, the tests need to be performed severally, documented, and OSSTMM MFH questions answered, and inputted into the Rav calculator to generate the actual security in each instance. The comparative trend value will provide a better picture of the actual security value for the MFH PT.

## 5. CONCLUSION

The concept of conducting a penetration tests supports the popular saying that “prevention is better than cure”. The MFH’s cyber infrastructure in comparison with the ever growing attack techniques has made it a priority to get Infront of the problem by being more and more proactive, rather than reactive. With PTs simulating and assuming the cyber threat actors roles, conducting penetration tests has now become a necessity for better visibility. The introduction and review of major PT methodologies opened the door to the selection criteria in the adoption in MFH cyber infrastructure. In addition, the PT methods set the foundation and skeletal map to which the test can be performed in each instance and custom real life simulated scenario, to produce results. These test results can now be used as a criteria to be used to answer the OSSTMM MFH questions, which converts the answers to values to be used in the RAV calculator in order to get the actual security value level of the MFH.

Based on the results of the penetration test conducted using the Open Source Security Testing Methodology Manual (OSSTMM) framework, it can be concluded that the mobile field hospital used in this study presented several security vulnerabilities. The test revealed that the hospital's systems and software were vulnerable to cyber-attacks, which could disrupt operations and compromise patient safety. The vulnerabilities identified included weak passwords, unpatched software, and poor network segmentation. The OSSTMM grading system used to evaluate the results of the test revealed that the mobile field hospital scored below the industry standards. The vulnerabilities identified and the level of access gained during the test indicate a significant risk to the continuity of medical operations in emergency and disaster situations. These findings highlight the need for increased security measures in mobile field hospitals to protect against cyber threats.

The recommendations for remediation provided in the test report include implementing security measures such as network segmentation, updating software and devices to reduce vulnerabilities, and providing cybersecurity training and awareness for the staff of mobile field hospitals. In conclusion, this study serves as a call to action for healthcare and emergency response organizations to prioritize cybersecurity and implement effective security measures to ensure the safety and continuity of medical operations in mobile field hospitals.

The use of OSSTMM as a framework for the penetration test provides a systematic and comprehensive approach to testing the security of mobile field hospitals, and the results can be used to identify vulnerabilities and improve the security posture of these facilities. Overall, in simpler terms, all digital devices that are connected to the MFH's network and standalone devices that communicates with other devices by using either the internet or an intranet, can be both tested and or attacked. The conducting of PTs are absolutely not restricted to hardware devices only, but software and management applications also remain a key focus. Even though the Outdated and coding without security in mind has led to leaving devices and stakeholders vulnerable and at the mercy of attackers, the human element also remains a key factor in consideration.

## REFERENCE & BIBLIOGRAPHY

- [1] *Mobile Clinics* (no date) World Health Organization. World Health Organization. Available at: <https://www.who.int/emergencies/partners/mobile-clinics> (Accessed: January 9, 2023).
- [2]. CIS. 2021. *Cyber Attacks: In the Healthcare Sector*. [online] Available at: <https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/> [Accessed 15 September 2021].
- [3]. Culbertson, N., 2021. *Council Post: Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity*. [online] Forbes. Available at: <https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=3bfd0a7b5650> [Accessed 15 September 2021].
- [4]. Happiest Minds. 2021. *What is Penetration Testing?*. [online] Available at: <https://www.happiestminds.com/Insights/penetration-testing/> [Accessed 22 October 2021].
- [5]. VAADATA - Ethical Hacking Services. 2021. *Penetration Testing: Approach, Methodology, Types of Tests and Rates*. [online] Available at: <https://www.vaadata.com/blog/penetration-testing-approach-methodology-types-of-tests-and-rates/> [Accessed 22 October 2021].
- [6]. Vumetric. 2021. *Top 5 Penetration Testing Methodologies and Standards*. [online] Available at: <https://www.vumetric.com/blog/top-penetration-testing-methodologies/> [Accessed 22 October 2021].
- [7]. Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A., n.d. *Technical guide to information security testing and assessment*. pp.ES1-ES2.
- [8]. 2021. *Information Systems Security Assessment Framework (ISSAF)*. 2nd ed. OISSG, pp.18-19.
- [9]. Redscan. 2021. *What is OWASP penetration testing? - Redscan*. [online] Available at: <https://www.redscan.com/news/what-is-owasp-penetration-testing/> [Accessed 22 October 2021].
- [10]. Equilibrium Security. 2021. *What is CREST Penetration Testing? - Equilibrium Security*. [online] Available at: <https://equilibrium-security.co.uk/advice-and-consultancy/penetration-testing/what-is-crest-penetration-testing/> [Accessed 22 October 2021].
- [11]. Crest-approved.org. 2021. *Penetration Testing – A Guide for Running an Effective Programme*. [online] Available at: <https://www.crest-approved.org/2018/07/20/penetration-testing-a-guide-for-running-an-effective-programme/index.html> [Accessed 22 October 2021].
- [12]. Attack.mitre.org. 2021. *MITRE ATT&CK®*. [online] Available at: <https://attack.mitre.org/> [Accessed 22 October 2021].
- [13]. McAfee.com. 2021. *What is the MITRE ATT&CK Framework? | Get the 101 Guide | McAfee*. [online] Available at: <https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html> [Accessed 22 October 2021].

- [14]. Sans.org. 2021. *Applying Security Awareness to the Cyber Kill Chain*. [online] Available at: <<https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/>> [Accessed 22 October 2021].
- [15]. Seale, K., McDonald, J., Glisson, W., Pardue, H. and Jacobs, M., 2018. MedDevRisk: Risk Analysis Methodology for Networked Medical Devices. *Proceedings of the 51st Hawaii International Conference on System Sciences*,.
- [16]. Herzog, P., 2010. OSSTMM 3 – The Open Source Security Testing Methodology Manual. 3rd ed. ISECOM, pp.69-85.