CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Information Sharing Framework for Penetration Testing

Ihsan Burak Tolga
Gunnar Faith-Ell

NATO CCDCOE

Tallinn 2020

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 25 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual 2.0, the most comprehensive guide on how International Law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise Locked Shields and hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, joining key experts and decision-makers of the global cyber defence community. As the Department Head for Cyberspace Operations Training and Education, the CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations - to this date Austria, Belgium, Bulgaria, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Table of Contents

1. Introduction

In the contemporary interpretation of deterrence theory, maintaining high-level resilience against cyber attacks[1] is one of two pillars of cyber deterrence posture. Particularly in cyberspace, an environment with numerous actors of many sizes, capabilities and attack paths, the first and last lines of defence are merging with the goal of identifying and hindering cyber attacks, or at least making them more costly to the attacker than their associated potential benefit.

The precise domain of resilience in cyber defence varies depending on the context, but in general, critical information infrastructure is a major part. As there is a huge array of systems in various areas of nations' military systems and infrastructure, there are many common systems used by multiple organisations, nations and entities. These are often the same industrial control systems, network components and military systems, manufactured by a single company or consortium and used by the various nations or organisations within those nations. However, their components might differ in configuration, firmware and software versions. [2]

Building a credible, overall resilience for a nation in the cyber domain depends on scale, but consists of different steps and levels, which sometimes overlap. While following a robust risk-management approach would deliver the necessary path to implement complete cyber resilience, it consists of many steps including determining the most valuable assets, threat information sharing,[3] cyber intelligence, increasing cyber awareness, penetration tests, impact analysis, mitigation plans and vulnerability assessment. To stay inside the scope of this report, vulnerability assessment activities are considered in the context of penetration testing while acknowledging their structural differences.

Penetration testing constitutes the technical foundation of improving cyber resilience, apart from known vulnerabilities and threats; while human factors and physical protection are the other major factors in the overall quality of penetration testing. Its results are the major aspect that the other cyber defence / cyber security activities interpret (usually as threats, depending on the context) and direct their focus upon. Therefore, the credibility and success of a given actor's cyber resilience efforts for its critical infrastructure and military systems, be it a nation or a single organisation, are closely correlated with the quality level of its penetration testing.

The threat surface in today's cyber environment is huge, due to the myriad of system components facing the internet and other information networks. In these environments, the ideal scenario for the desired cyber resilience posture is that an actor's domain maintains a flawless overall vulnerability discovery and assessment mechanism by performing penetration testing on every system and combination of systems before integrating it into its existing set. In this sense, it also serves as the product evaluation part of Common Criteria.[4] Whereas in practice, this is difficult for many military systems. It is usually not possible to conduct complete penetration tests on the systems before their production phase, nor to call

[1] Good cyber defences, however, can build resilience or the capacity to recover, which is worthy in itself; they can also reduce the incentive for some attacks by making them look futile. Nye., Joseph S. 2017. 'Deterrence and Dissuasion in Cyberspace.' *International Security, President and Fellows of Harvard College and the Massachusetts Institute of Technology* 44-71.

[2] Jermalavičius, Tomas. 2009. Defence Research & Development: Lessons from NATO Allies. Project Report, Tallinn: ICDS.

[3] Ohl, Martin. 2019. McAfee - Improving Cyber Resilience with Threat Intelligence. 12 06. Accessed 11 July 2019. https://securingtomorrow.mcafee.com/business/improving-cyber-resilience-with-threat-intelligence/.

[4] Common Criteria for Information Technology Security Evaluation (CC) is an international standard (ISO/IEC 15408) for evaluating the security in IT products and systems.

any system invulnerable. Therefore, the usual practice is to perform penetration tests according to a risk-assessment plan before and regularly during the system's life cycle and accept the exposed risks resulting from any missed points.[5]

The variety of alike systems used by different entities, existing partnerships and collaboration mechanisms between actors, and the lessons from previous similar challenges, present an opportunity in this regard. Developing an environment in which different actors share the findings and results of their own penetration testing activities with their partners to improve their overall resilience appears to be a sensible concept. As with any well-functioning multilateral mechanism, the means and methods should be built according to a detailed framework methodology.

This report aims to present a picture of the current situation regarding this sharing and to investigate whether it is possible to benefit from sharing information about penetration testing, examining the potential gains and associated costs. It will track the likely challenges and possible remedies, drawing a scope with respect to legal constraints, and will suggest some draft standards as the first step towards an operative penetration testing platform. The criterion of success for the platform is that its stakeholders benefit by developing robust cyber resilience postures. The final goal of the multiple-stage project is constructing an environment that contains not only the platform, but also common understanding, standards and procedures, an agreed common toolset and ultimately robust cooperation among subject-matter experts working towards a common goal.

[5] Curiel, Johanna. 2019. *App sec best practices: Assess risks before you pen test.* 04. Accessed 11 June 2019. https://techbeacon.com/security/app-sec-best-practices-assess-risks-you-pen-test.

2. Penetration testing

Security assessment of IT systems includes both human and technical aspects. The design, configuration, work routines, supply chain, IT organisations awareness, documentation, TEMPEST,[6] cabling protections and even access to server halls are all parts of a security audit.[7] Penetration testing is a crucial part of cyber security assessment, focusing on the potential vulnerabilities associated with the system at hand. Before an IT system is deployed, best practice mandates that complete penetration tests should be conducted and regularly repeated, both routinely and when the system is reconfigured, to ensure protection from new vulnerabilities.[8] Usually, the observations from penetration tests, along with insights and accompanying material, are compiled into a report for the customer or requesting body. While the main objective of penetration testing is to identify exploitable vulnerabilities, to provide guidance on mitigating them and to determine the security level of information infrastructures, it can have a number of other objectives. These objectives, which are assured by the efforts following penetration testing, include testing security policy and strategy compliance, security assessment, employee security awareness and finally the evaluation of the organisation's security incident identification and response capability.

Penetration testing is usually a simulated attack on resources, systems and networks, depending on the criticality of the system's real-time operations. Since penetration testing could affect the confidentiality, integrity and availability[9] of the system, depending on the client, it is sometimes necessary to take managerial, technical and legal precautions such as conducting the penetration test outside the production phase. In some cases, tests can also be run in a simulated environment.

Usually, the initial classification of penetration test reports is made with knowledge of the technical details regarding the targeted system (i.e. by an interview with a technical representative of the requesting body), which distinguishes black box testing from white box testing. Black box testing assumes no prior knowledge of the targeted system among the personnel who conduct the penetration testing. The attacker first has to locate the target, identifying its surface, before starting the analysis. In white box testing, the attacker has prior knowledge of the targeted system and any other relevant details. While it depends greatly on the client, the system, the budget and the maturity level of the system's cyber security; preferably, the first phase of a penetration test starts as black box, followed by providing the attacker with comprehensive information about the system to be tested.

During the penetration test, the systems are attacked through known vulnerabilities, reconnaissance, checking standard passwords, testing system configuration, network settings and firewall settings to gain access. Use of automated penetration test tools is part of the normal routine. In some cases, tests can affect the system and might even result in the system having to be restored after the test. The penetration test report might contain information that must be addressed by the system's vendor,[10] by the organisation itself, or by other parties such as the network provider.

[6] SANS. 2001. 'An Introduction to TEMPEST.' In *National Communications Security Committee Directive*, by Cassi Goodman. SANS Institute.

[7] United Nations Development Programme. n.d. 'IT Audit Manual.' Albania: United Nations Development Programme.

[8] IT Governance. 2013. 'Why is penetration testing necessary?' *itGovernance.* 04 09. Accessed 11 June 2019. https://www.itgovernance.co.uk/media/press-releases/why-is-penetration-testing-necessary.

[9] CIA Triad. Confidentiality, integrity and availability. For more information on the concept, see https://resources.infosecinstitute.com/cia-triad/

[10] According to Common Vulnerabilities and Exposures (CVE) approach. For more information see https://cve.mitre.org/

Each alteration to the network, to an individual computer or to a firewall, and each security patch, new antivirus definition and configuration setting can introduce new vulnerabilities into the system. As these are regularly included in the penetration tester's tool kits (i.e. scripts of automation tools), the common practice is that penetration testing experts use their own techniques, scripts and manual procedures.

Besides the particular complexity of penetration testing activities in the industry, additional complications are involved with military systems. These are commonly critical systems for nations, and more specific laws and regulations may be in place, in addition to existing legal constraints that protect the intellectual and commercial rights of the stakeholders. Unlike the customer who holds the contract for penetration tests conducted by other parties, the owners of the military systems are subject to regulations that are more restrictive.

3. Current status of penetration testing collaboration

Because of its potential benefits, information sharing across organisations and nations has been a popular subject, with some notable research on the matter. NIST's work is a prominent guide which suggests that '[u]sing shared resources, organisations can enhance their security posture by leveraging the knowledge, skills and abilities of their partners in a proactive way',[11] This leads to the paradigm of allowing 'one organisation's detection to become another's prevention'.[12] Discussing the incentives and challenges for information sharing in this context[13] highlights the implications of the trade-off between challenges (legal implications, poor information quality) and incentives (information value, cost savings, trust-building). However, Barnum[14] argues that there is a need for information sharing with standardised, structured representations to make information tractable. Although these works deal with cyber threat information, their definition of threat also includes vulnerabilities and penetration testing activities.

So far, particularly inside NATO and EU's domain of interest, the Malware Information Sharing Platform (MISP) has been the spearhead[15] among efforts to establish a concurrent information-sharing framework between like-minded nations and organisations who maintain a threat surface in information networks. The earliest and biggest support to MISP project was from NATO in 2012,[16] and several instances of the protocol are now running in various sectors, organisations and national Computer Emergency Response Teams (CERTs). The biggest instance is CIRCL MISP operated by the Computer Incident Response Centre Luxembourg (CIRCL).[17] Aside from the related issues reported by users, it has been a widely used cyber-related information sharing platform on public networks, since it was deemed more beneficial for participating sides.

Another notable initiative for cyber information sharing is the UK National Cyber Security Centre's Cyber Information Sharing Platform (CISP), a joint government and industry-driven platform to exchange cyber threat information in real time.[18] CISP provides a secure environment by registering private companies to the platform only when sponsored by either a government department, existing member, regional cyber police or industry champion. Although the policies are not completely clear and there is no grading mechanism between members to differentiate between their levels of access, this authorisation may still be considered one of the key drivers.

[11] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150.*

[12] This phrase is credited to Tony Sager, Senior VP of Center for Internet Security.

[13] European Network and Information Security Agency. 2010. *Incentives and Challenges for Information Sharing in the Context of Network.* Research Project, European Network and Information Security Agency.

[14] Barnum, Sean. 2014. 'Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).' *MITRE Corporation.*

[15] NCI Agency. 2013. *Malware Information Sharing Platform.* Whitepaper, Brussels: NATO Communications and Information Agency.

[16] MISP-Project. 2019. MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Accessed 11 June 2019. https://www.misp-project.org/who/.

[17] circ.lu. 2019. *Malware Information Sharing Platform MISP - A Threat Intelligence Sharing Platform.* Accessed 11 June, 2019. https://www.circl.lu/services/misp-malware-information-sharing-platform/.

[18] UK National Cyber Security Centre. 2019. *CiSP - Cyber Security Information Sharing Partnership*. Accessed 11 June 2019. https://www.ncsc.gov.uk/section/keep-up-to-date/cisp.

The other large-scale cyber-related information environment is the Cyber Information Sharing and Collaboration Program (CISCP) of the US Department of Homeland Security (DHS).[19] As an unclassified information-sharing programme between DHS and private companies, its focus is mostly on critical infrastructure. Participants are able to share threat actor tactics, techniques and procedures (TTP) and other cyber risk-related information, on an analyst-to-analyst basis. The programme also offers an entire set of products and services, threat broadcasts and periodic reports accessible only to the participants. One of the most significant aspects of CISCP is that all submissions from either government or private participants remain anonymous unless the originator decides otherwise. DHS assures participants that it will provide the required protection and confidence and guarantees that no proprietary or sensitive data will be exposed. The programme adheres to the Traffic Light Protocol (TLP),[20] Freedom of Information Act[21] and Cybersecurity Information Sharing Act.[22] One of the dominant services offered by CISCP is Automated Indicator Sharing (AIS), which operates on STIX[23] and TAXII[24] and enables the participant to distribute and receive cybersecurity information. Compared to its variants, AIS has a prominence that; in 2017, the US and Japan signed an information-sharing agreement for using the AIS platform[25] which adds much to its credibility. Finalising the registration for CISCP is done by signing the Cyber Information Sharing and Collaboration Agreement (CISCA), which sets up the legal aspects of anonymous information sharing among its entities. The main motivation of CISCP is that it provides a certain amount of trust, a feeling of community with a shared goal and valuable insights.

One notable cyber information-sharing platform developed and owned by private industry is Dradis.[26] Its main purpose is to reduce time and efforts spent on reporting activities and to provide collaboration with other parties by integrating with other tools that are widely used by cyber security experts. The tools and software of which Dradis offers include popular tools in penetration testing such as Metasploit,[27] Burp Suite,[28] Nessus[29] and Nmap.[30] Besides the drawback of it being a third-party product designed for private industry, there is no existing study to assess its performance and compatibility for penetration testing information sharing between governmental and military organisations, or across organisations like NATO.

[19] US Department of Homeland Security. 2019. *Cyber Information Sharing and Collaboration Program (CISCP).* Accessed 11 June 2019. https://www.dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp.

[20] US-CERT. 2019. *Traffic Light Protocol (TLP) Definitions and Usage.* Accessed 11 05, 2019. https://www.us-cert.gov/tlp.

[21] Freedom of Information Act (FOIA): NCCIC will not disclose any information that is exempt from disclosure under FOIA consistent with 5 USC 552(b), including but not limited to Exemption (b)(3) as specifically exempt from disclosure by statute, Exemption (b)(4) as trade secrets and commercial or financial information that is privileged or confidential and Exemption (b)(7)(A)-(f) as records or information compiled for law enforcement purposes.

[22] The Department of Homeland Security - The Department of Justice . 2015. 'Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015.' 15 06. Accessed 11 June 2019.

[23] Barnum, Sean. 2014. 'Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).' *MITRE Corporation.*

[24] 2017. TAXII 2.0 Specification. 19 07. Accessed 19 Feb 2019. https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/pub.

[25] US-CERT. 2015. *Automated Indicator Sharing*. Accessed 02 04, 2019. https://www.us-cert.gov/ais.

[26] Dradis. 2019. Dradis Pro. Accessed 11 07, 2019. https://dradisframework.com/ce/.

[27] Porup, J. M. 2019. "'What is Metasploit? And how to use this popular hacking tool.'" *CSO Online.* 25 03. Accessed 11 07, 2019. https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html.

[28] Dafydd Stuttard, Marcus Pinto. 2011. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* Indianapolis: Wiley.

[29] Tenable. n.d. *The Nessus Family.* Accessed 11 07, 2019. https://www.tenable.com/products/nessus.

[30] Lyon, Gordon Fyodor. 2009. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.* Palo Alto: Nmap Project.

Since they bring significant risk to their target systems if compromised, penetration tests results are usually classified. The risks are mainly due to the characteristics of the vulnerability, the purpose of the system, associated risks, and other sensitive data they indirectly expose.

Thus, for the sake of this report's focus, there is no widely adopted cyber information-sharing platform used between nations or domestic organisations in a nation at the moment, and no ongoing public project on the subject. Existing platforms function according to industry-driven requirements. Since they seek to attract a large user base, the trade-off between the focus-in-depth and focus-in-width approaches is leaning towards the latter. Technically, it is possible to utilize existing cyber information-sharing platforms for military-specific penetration testing and vulnerability assessment reports. However, this is impractical due to the risks related to the clear differences between the characteristics of shared information, associatedW costs, the burden of unnecessary overheads caused by legacy structure, dependency on third parties and distinct design concerns between the platforms.

4. Contributions and prospective benefits

A collaboration-oriented platform is only as strong as its active members and it is important to note here that being active is no less important than the number of participants. Especially in a domain like penetration testing, information is the biggest asset. Thus, probably the biggest factor to its overall success is the extent to which the platform can incorporate its members, take initiatives and remain active. Since trust plays a huge role in sensitive information sharing, the overall success depends on how much sense of trust the framework is able to establish for its prospective users.

In addition to dealing with the trust-related drawbacks, it is natural to adopt a risk-based mindset for using the platform. Particularly in the military penetration testing environment, aside from organisations' discomfort, there are legal restrictions and organisational procedures and regulations at play. To overcome these challenges, firm evidence is required to give sufficient assurance to decision-makers that the benefits of being an active participant far exceed the projected risks. The key is making the paradigm better than just fair for all participants. Rough equality between efforts and risks and potential gains usually reinforces inertia and maintains the status quo, and no party willingly takes the initiative because the perception of risks far outweighs the abstract future benefits. Therefore, this paper advocates a strong motivation for prospective participants to join the penetration testing information sharing environment, through agreements on procedures and processes, methods and incentives.

Incentives should be a set of tangible added values to a joining organisation that will improve the quality of either its penetration testing activities, overall cyber security posture or any other aspect to its advantage. Also reducing the associated costs might serve as a strong motivation. These added values must also clearly surpass the required investment needed to realise a return. To establish a functioning paradigm in which participating entities see a substantial surplus of value, a list of contributions and gains is given below.

To build the methodology of the penetration testing information sharing platform, several small-scale analyses and scenarios were conducted. The aim was selected as maximising fairness among participants and the average quality of the information in the exchange, and keeping the framework refined. The following best practices were produced and listed as the expected contributions for the framework. To avoid any conflict with the nature of voluntary information sharing, they are labelled as non-compulsory activities for any participant:[31]

Participating parties should commit to:

- **Sharing penetration test reports (and other related reports) with other identified participants.**
- **Sharing methodologies, best practices and techniques for performing effective penetration testing.**
- **Sharing penetration testing reports of associated systems and applications (auxiliary systems).**
- **Ensuring that shared information maintains a standard level of accuracy, integrity and confidentiality.**
- **Sharing information for prospective systems.**
- **Sharing structured information in given atomic information fields for ease of future data operations.**

[31] Peng Liu, Amit Chetal. February 2005. 'Trust-based Secure Information Sharing Between Federal Government Agencies.' *Journal of the Association for Information Science and Technology Volume 56, Isssue 3.*

- **Acting in accordance with the goal of increasing the overall cyber security and resilience posture of the military systems of the participating entities and allied nations.**
- **Avoiding sharing duplicate information but motivating the enhancement of information by others.**
- **Avoiding sharing unrelated information outside the penetration tests and vulnerability assessment domain of military and associated systems.**
- **Maintaining cooperation with other participants to ensure the overall quality of the information sharing environment.**
- **Taking all necessary measures to protect received information with respect to its classification.**
- **Providing the received information for other participants on request, in accordance with the releasibility set by the originator.**
- **Accurately identifying the systems of interest.**
- **Sharing concise, up-to-date penetration testing information that conforms to the standards of the information-sharing platform.**
- **Supporting the framework in regards of satisfying classification requirements of the information.**

Participating parties should expect to obtain the following benefits:

- **Acquiring standardised penetration testing and vulnerability assessment templates.**
- **Reducing the costs and efforts resulting from penetration testing processes, which are rough duplications of the other processes for the same systems of other participants.**
- **Promoting security by design; reducing the time span between acquiring new systems and their respective vulnerability assessments.**
- **Gaining new insights into the systems possessed by multiple participants.**
- **Staying up-to-date with respect to new techniques, industry standards and tools.**
- **Identifying undiscovered vulnerabilities of systems in use.**
- **Improving overall collaboration with other participants.**
- **Having valuable assessments about prospective systems before resource allocation and investment.**
- **Increasing the number of systems hardened against designated cyber threat vectors.**
- **Fostering the activities of trust-building between participants.**

5. Building synergies between the actors

As several studies report,[32,33] there has been a constant increase in cyber threats over recent years, which calls for enhanced resilience. In NATO countries, major military systems are usually developed or utilized cooperatively.[34] Nations share the overall costs and investments of the entire projects to cut down on cost and risk. Yet, since there is no commonly accepted notion in place, nations (and even different organisations in the same state) conduct penetration tests on military-related systems individually.

Although the overall shared benefit is apparent, information sharing is often perceived as an open-ended endeavour, which makes the potential parties hesitate, given the sensitivity of the assets. The sense of trust is still and always the main principle in information sharing. This is true especially in the case of penetration testing reports, which usually contain information that is extremely sensitive to its owners.[35]

After getting the information-sharing platform up and running, there are several methodologies to govern the process of penetration testing information exchange. The proposed rules and models are not a successor to those of any other in the industry, or a modified version. There are no adapted versions of the rules in the industry or public. The needs expressed by various penetration testing experts, the associated regulations in place and the identified challenges in information sharing are the basis of these rules. The proposed solutions follow a pattern from the simplest to the more complex. At this stage of the project, having several possible methodologies is essential so as to identify the most efficient by using the scenarios and user feedback. As the overall goal, a well-functioning penetration testing information sharing platform is analogous to the desired synergy, resulting from the collaborative efforts of its participating actors, enabling each to gain significantly more benefits than their invested resources. Mutual trust is still the backbone of the entire framework.

Suggested methodologies:

1. **Free for All**

As its name suggests, in this methodology the participants are completely independent in their penetration testing reports exchange, meaning that it is solely up to each participating party to disseminate any information towards others. Disseminating penetration testing information does not call for information in return, and similarly, receiving information reports does not require the receiving participant to act in the same way. This methodology is widely adapted by existing cyber information-sharing platforms, with some minor differences.

[32] Tucker Bailey, Andrea Del Miglio, Wolf Richte. 2014. *The rising strategic risks of cyberattacks. Industry Research,* New York: McKinsey Quarterly.

[33] Symantec. 2019. *Internet Security Threat Report Volume 24.* Industry Research, Mountain View: Symantec Corporation.

[34] n.d. *Eurofighter Typhoon - About*. Accessed 11 07, 2019. https://www.eurofighter.com/about-us.

[35] Jason Creasey, Ian Glover. 2017. A guide for running an effective Penetration Testing programme. Industry Report, Berkshire: CREST.

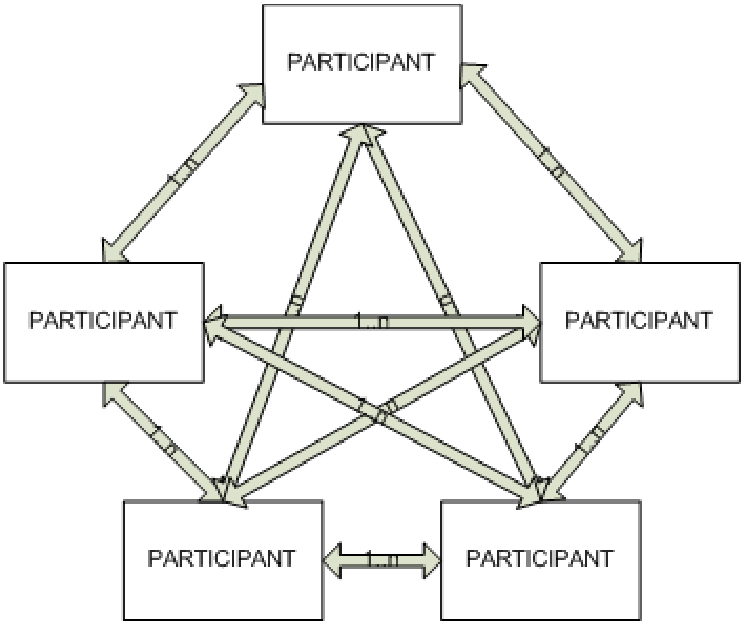


FIGURE 1

As simple as it is and without any tangible incentives for the sharing party, a free-for-all is the most common information sharing method in the industry. However, considering the very sensitive nature of penetration testing reports and their possible implications (technical, intelligence, reputation, credibility), it is a quite ambitious task to have it adopted by organisations and nations.

2. **Credit-based information exchange**

Unlike a free-for-all methodology, there is a quantitative constraint in credit-based information sharing. To initiate the information exchange flow, each authorised participant starts with a small designated amount of credits. Each also provides its interested systems and the applications of penetration testing reports that it requests. These desired reports are visible to other participants on the platform, as a guide for the potential sharing participant.

For each shared penetration testing report beyond the agreed standards, the sharing participant gains credit point for each receiver and for each received report, and a credit point deducted from the receiving participant. With respect to the agreed standards, the quality of the reports should be confirmed by the receiving party prior to gaining credit points. The joining process of new participants to the information-sharing platform should, therefore, follow strict policies, to generate trust among the participants.

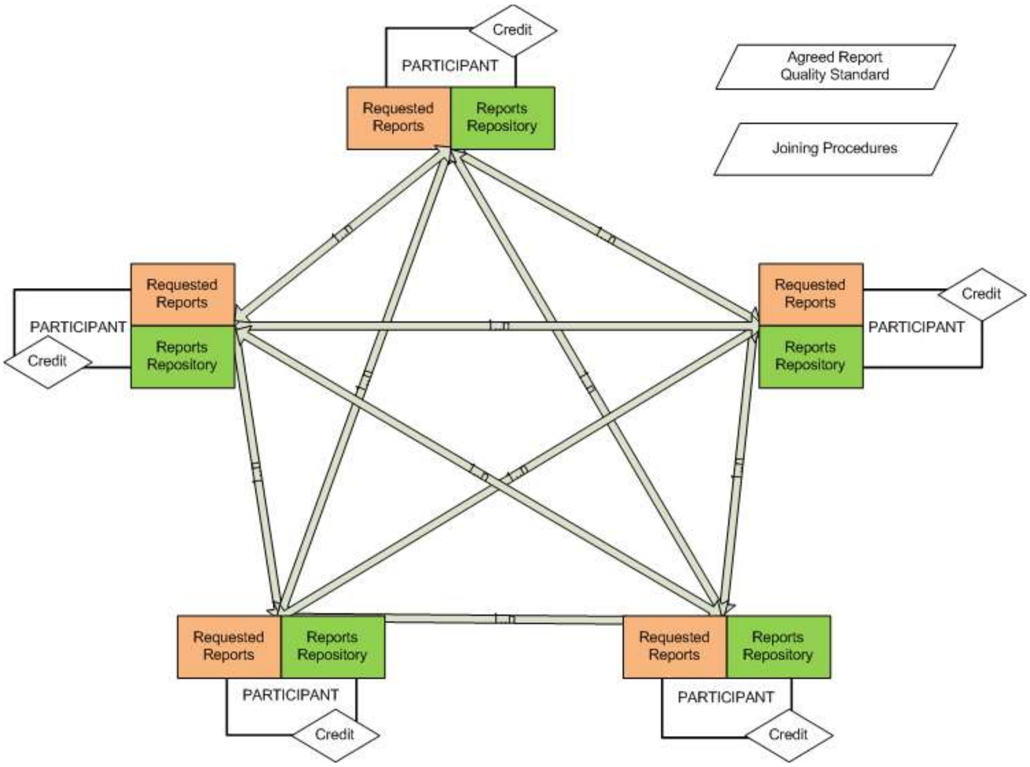


FIGURE 2

3. Centrally Controlled Collaboration

Similar to the credit-based information sharing methodology, each participant is mandated to provide its interested systems and applications of penetration testing reports and additionally its repository of penetration testing reports that it can provide on request. These sets are visible to a designated facilitator body, which assigns reports from potential providers to requesting participants. In a similar fashion, for each shared report beyond the agreed standard, the sharing participant gains credit for each receiver and for each received report, and a deduction of credit from the receiving participant. With respect to agreed standards, the quality of the reports should be confirmed by the receiving party prior to credit gain.

There is the possibility of a deadlock in this model if there is no match between the requested and provided reports. The most likely resolution is that participants continuously update their sets and conduct periodic assessments to track any potential match between those sets.

A potential improvement to the model is that, with respect to overall goal of synergy, the facilitating body can identify the most requested systems and assign them to different potential providers. More parties would then benefit from the single effort of penetration testing of a single system and application.

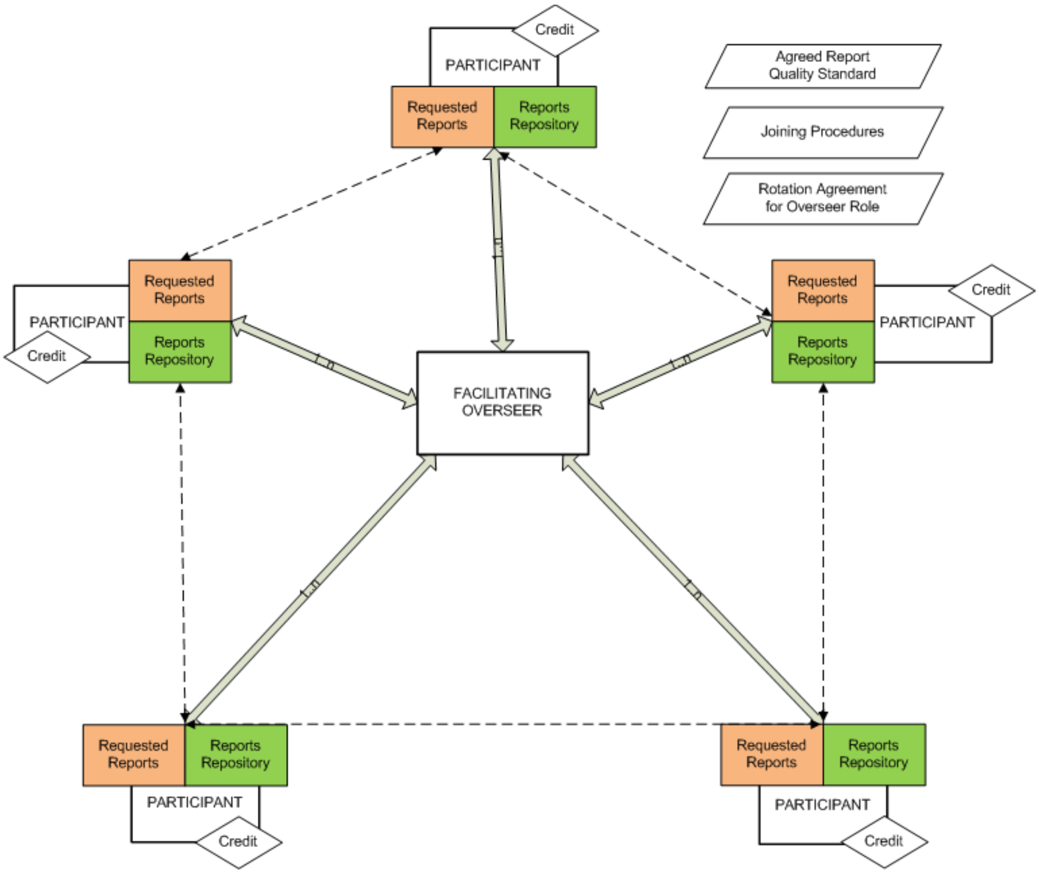


FIGURE 3

A drawback in this methodology is that the facilitating body is in a position to oversee all sets provided and requested by the participants, which could harm the sense of trust. To mitigate this, the role may be set temporarily, allowing participating parties to take turns for mutually agreed periods.

4. Decentralised information exchange

Building on top of centrally controlled and credit-based information sharing methodologies; in the decentralised information exchange model, each participant is again mandated to provide its interested systems and the applications that it requests and the repository of reports that it can provide on request. These sets are visible to other participants on the platform and no facilitating party exists. By running queries on other participants' registered sets, each can invoke any other and request a specific report in exchange for one of its own. Provided that both participants give confirmation, the exchange process takes place.

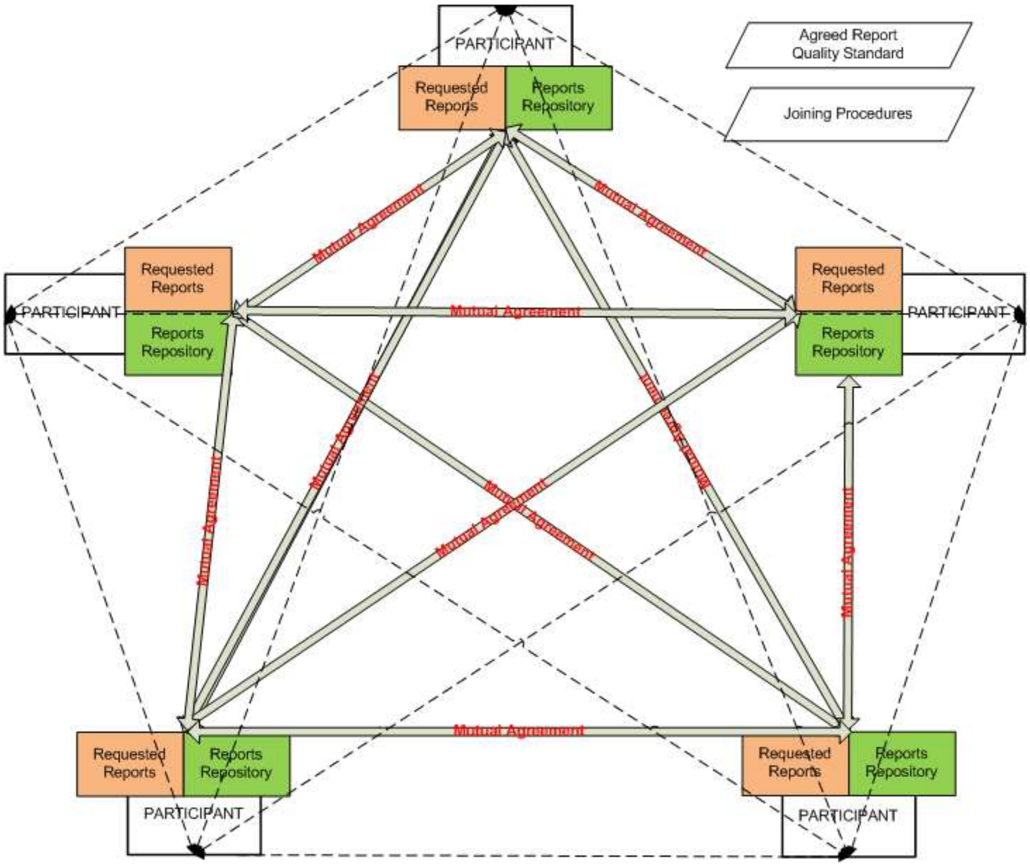


FIGURE 4

To ensure the level of quality, the sharing parties provide feedback on the quality of each received report with respect to quality assurance standards. A mutually agreed course of action in case of failing to fulfil standards should be in place to establish the desired amount of trust in the platform.

Although it is rather early in the course of the project to focus on one of the models, finding the sweet spot between the characteristics of the challenges and the expected values should be the first priority. Following that, it will be perfectly possible to tailor the suggested models to the real case scenarios, due to either changing requirements or any possible shortcoming in any of the models.

6. Expected challenges and possible remedies

Challenges regarding the prospective penetration testing information sharing platform are two-fold, although overlapping to some extent: legal constraints and classification concerns.

Penetration testing-related information, aside from the custom classification policies of its owner, is usually very sensitive, since it contains critical vulnerability information about the target system. Disclosure of such sensitive information is likely to permit adversaries to cause interruptions, data leaks, damage or disruption to the subject system.The laws and regulations for cyber and information security and for sensitive information such as penetration testing reports, are still in the early stages of evolution, but most countries have already adopted stringent cyber security and information security laws, which encompass (or can be interpreted down to) penetration testing activities. The challenge of analysing each country's laws and regulations is out of this report's scope, but to give an overall flavour, the US's recently amended Computer Fraud and Abuse Act,[36] the EU's NIS Directive[37] and the corresponding sections of Estonia's Penal Code[38] (Karistusseadustik) provide a good analogy for the potential implications of penetration testing activities. These acts, along with the recent GDPR in EU countries, set the border between legal and illegal actions in information security and regulate the legal constraints and issues related to operations across information systems, their practitioners and users.[39] Due to its nature and contained sensitive data, penetration testing remains a challenging part of these areas and requires special care for legalities between customers and providers.

The sharing of penetration test information falls under different laws and regulations, such as the US's Cybersecurity Information Sharing Act 2015.[40] Penetration testing information sharing is listed as a security vulnerability, one of the five characterisations of cyber threat indicators. The law does not distinguish between publicly-known vulnerabilities and vulnerabilities that are discovered by in-house penetration testing. In the US federal cyber security information sharing environment, the Department of Homeland Security acts as the overseer, charged with managing the people, processes and technology activities and the methodology of receiving and sharing cyber threat indicators. It gives an assurance of confidentiality and trust, with the statement that '[t]he federal government is limited in its ability to disclose, retain and use shared cyber security information. This information may be used solely for cyber security purposes as defined above'.[41] In this mechanism, while the intended assets to protect are mostly personal information, prior to sharing a cyber-threat indicator, private entities must remove

[36] US Senate. 2015. "'To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes."' Congress.gov. 27 10. Accessed 11 06, 2019. https://www.congress.gov/bill/114th-congress/senate-bill/754.

[37] European Union Directive. 2016. 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.' EUR-Lex. 06 07. Accessed 11 June 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

[38] Riigi Teataja. 2001. *'Karistusseadustik - Penal Code.'* Riigi Teataja. 06 06. Accessed 11 June 2019. https://www.riigiteataja.ee/en/eli/522012015002/consolide.

[39] —. 2016. 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation.' EUR-Lex. 27 04. Accessed 11 July 2019. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679.

[40] US Senate. 2015. 'S.754 - To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats and for other purposes.' Congress.gov. 17 03. Accessed 11 June 2019. https://www.congress.gov/bill/114th-congress/senate-bill/754.

[41] Nolan, Andrew. 2015. *Cybersecurity and Information Sharing Legal Challenges and Solutions*. Legal Research Report, Washington D.C.: Congressional Research Service.

certain personal, confidential information and any other elements that can be used to identify a specific individual. For military systems and penetration tests, the restriction levels are higher.

Assuming the potential participants in the information-sharing platform are military organisations from different allied nations and private organisations and companies working under different legal restrictions such as defence industry contractors, a combination of laws and regulations will apply to each participant resulting in multiple restrictions on each. Usually, these regulations involve restrictions regarding penetration testing and vulnerability assessment information sharing through unclassified or non-secure channels, either directly or by similar overarching statements. In practical terms, it is unlikely that the organisations will take the burden of relaxing the regulations for the sake of being able to participate in information sharing. In addition, unlike the US Cybersecurity Information Sharing Act which allows sharing with bodies in the same jurisdiction, other organisations in other countries do not have the same convenience.

It is possible that states' laws and regulations which administer classified information sharing across partner bodies in organisations like NATO can serve as an overarching code. Here, it is possible to find the lowest common denominator to sustain fair legal grounds for the participants to collaborate on sensitive information. Given the apparent limitations in both legal and classification areas, using existing secure communication networks seems a sensible approach to overcome the challenges at hand. NATO and its member nations have a great deal of experience of cooperation, joint activities and processes at all level of information sharing and operations. To enable such capabilities, NATO operates a set of information networks at various classification levels, and there have been some uses of using cyber information sharing platforms (i.e. MISP) in joint exercises in the past. Member nations (and their armed forces) already have laws and regulations to conduct their communication activities, which enable their participating bodies to exchange classified information with other allied nations. Except for some specific cases, the existing regulations can encapsulate the required legal requirements to exchange information concerning the vulnerabilities of critical systems and their penetration test results, given their willingness to proceed. Using the existing secure communication channels and networks, existing national regulations and multilateral memorandums is a promising remedy for both legal and classification-related challenges.

7. Suggested standards for penetration testing information sharing

Considering the development and implementation of the penetration testing information sharing platform, documentation standards need to evolve throughout the platform's life cycle, after initiating it with a minimum-viable set of principles, in order to avoid loading it with unnecessary sections. In this fashion, the standards and agreed documents will further evolve with respect to the actual customer / user needs.

In order to develop concise and adequate documentation and establish a coherent understanding of all parties, the paper proposes to employ the following standards with respect to general software and cooperation principles:[42]

- **Using agreed templates for documents in both development and production stages.**
- **Tracking each iteration of documents with version control.**
- **Clearly defined roles for developing documents.**
- **Employing user accounts to define user roles and scenarios.**
- **Employing formal proposition and acceptance procedures for importing new information or updating existing information in the documents.**
- **The listed documents will be required during the development and production life-cycle of the framework:**
  - **System and software requirements description.**
  - **Life-cycle plan document.**
  - **Feasibility evidence description.**
  - **Software support plan.**
  - **System and software architecture description.**
  - **Transition plan document.**
  - **Training plan.**
  - **Progress report.**
  - **System security document.**
  - **Client interaction report.**
  - **Client feedback form.**
  - **Test plan and cases document.**
  - **Test procedures and results document.**
  - **User manual.**

One of the most significant parts of the penetration testing collaboration platform is the agreed standards for the report documentation and technical formats between the participants. These are crucial for establishing seamless integration and use of the received information, ensuring a minimum acceptable quality[43] of the shared reports and common language. The standards should involve and be mandatory on:

- **Technical formats.**
- **Penetration testing report documentation.**

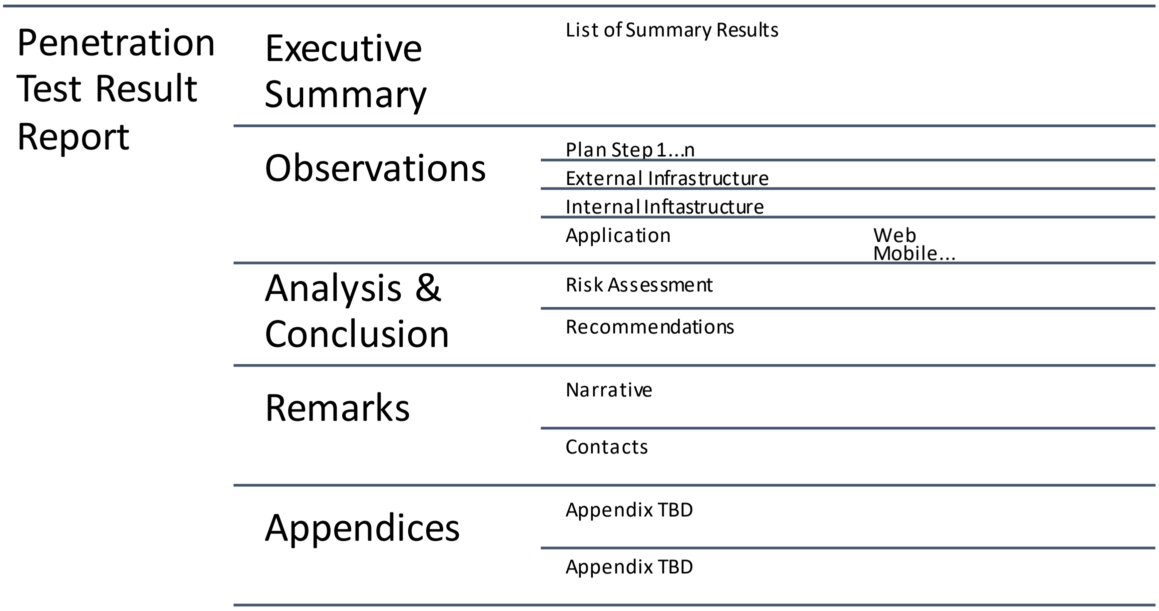
[42] For an overarching set of standards, see OWASP's CLASP (Comprehensive, Lightweight Application Security Process) https://www.owasp.org/index.php/CLASP_Concepts, NIST Special Publication 800-160 'System's Security Engineering' https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf or Microsoft's SDL (Security Development Lifecycle) https://www.microsoft.com/en-us/securityengineering/sdl/

[43] OWASP Documentation Projects can prove useful as a baseline for documentation standards. See https://www.owasp.org

- **Interoperable tools and applications.**
- **Recommended practices documents.**
- **Auxiliary information reports.**

Due to planning and the scope of this research, developing the full standardisation templates for the proposed documents and reports will follow a future workshop with stakeholders and future users of the collaboration environments. However, to establish a foundation on the way forward and the intended pattern of the standards, the following document outlines are provided.

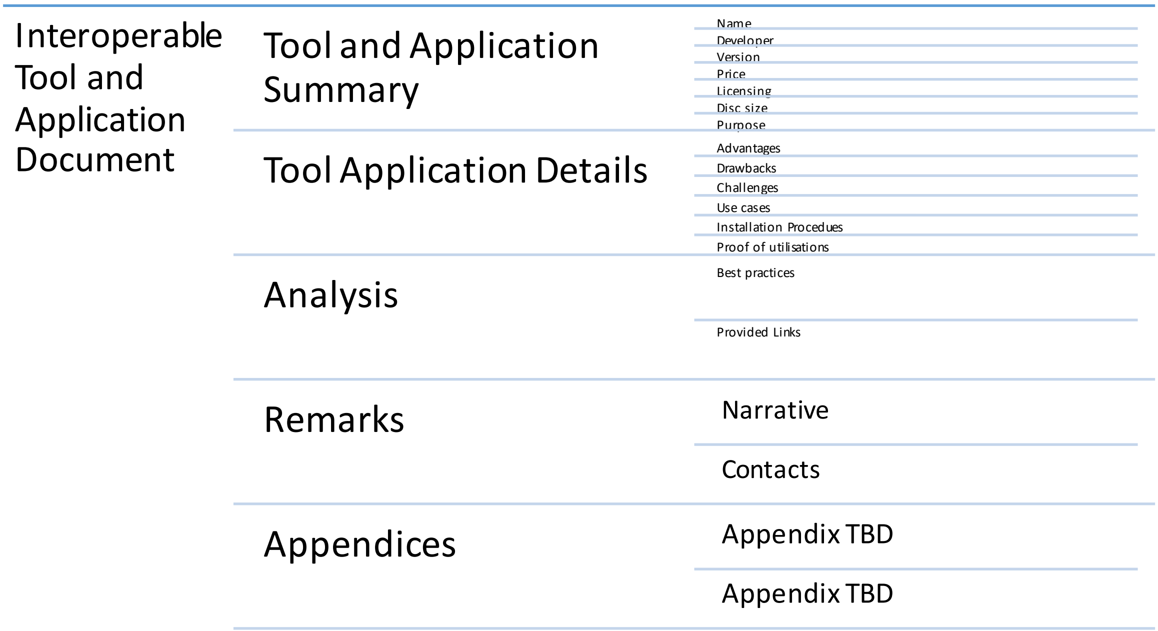
Penetration Test Result Reports:



Penetration Test Result Report	Executive Summary	List of Summary Results	
	Observations	Plan Step 1...n	
		External Infrastructure	
		Internal Inftastructure	
		Application	Web Mobile...
	Analysis & Conclusion	Risk Assessment	
		Recommendations	
	Remarks	Narrative	
		Contacts	
	Appendices	Appendix TBD	
		Appendix TBD	

FIGURE 5

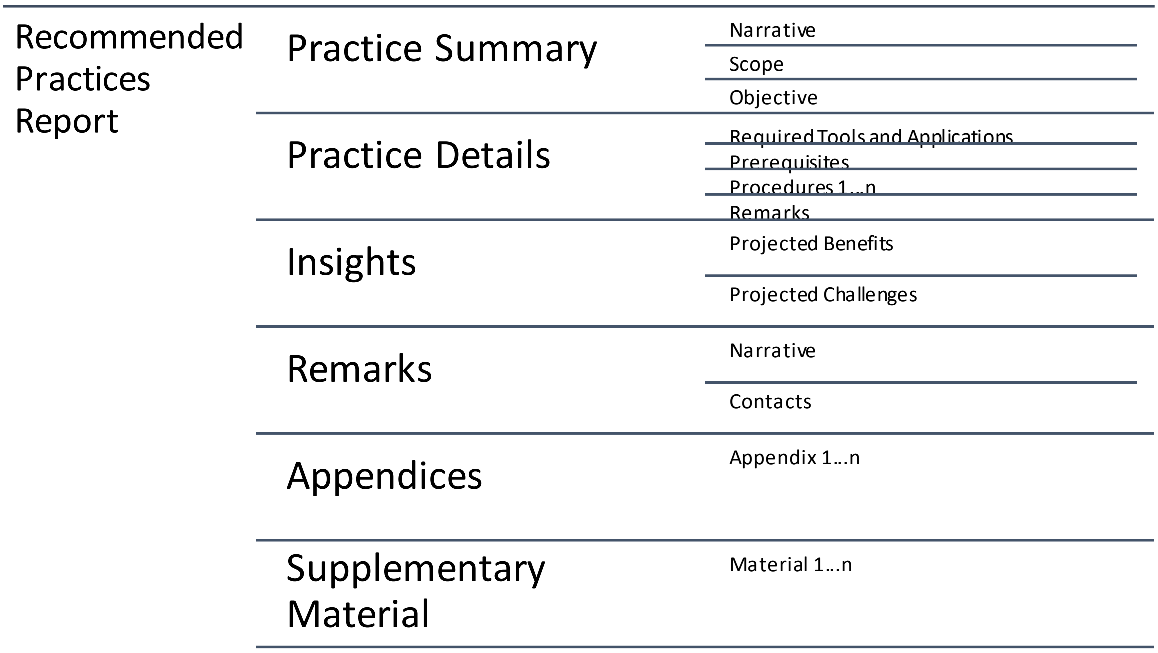
Interoperable Tool and Application Document:



Interoperable Tool and Application Document	Tool and Application Summary	Name Developer Version Price Licensing Disc size Purpose
	Tool Application Details	Advantages Drawbacks Challenges Use cases Installation Procedues Proof of utilisations
	Analysis	Best practices Provided Links
	Remarks	Narrative Contacts
	Appendices	Appendix TBD Appendix TBD

FIGURE 6

Recommended Practices Document:



Recommended Practices Report	Practice Summary	Narrative Scope Objective
	Practice Details	Required Tools and Applications Prerequisites Procedures 1…n Remarks
	Insights	Projected Benefits Projected Challenges
	Remarks	Narrative Contacts
	Appendices	Appendix 1…n
	Supplementary Material	Material 1…n

FIGURE 7

Auxiliary Information Reports

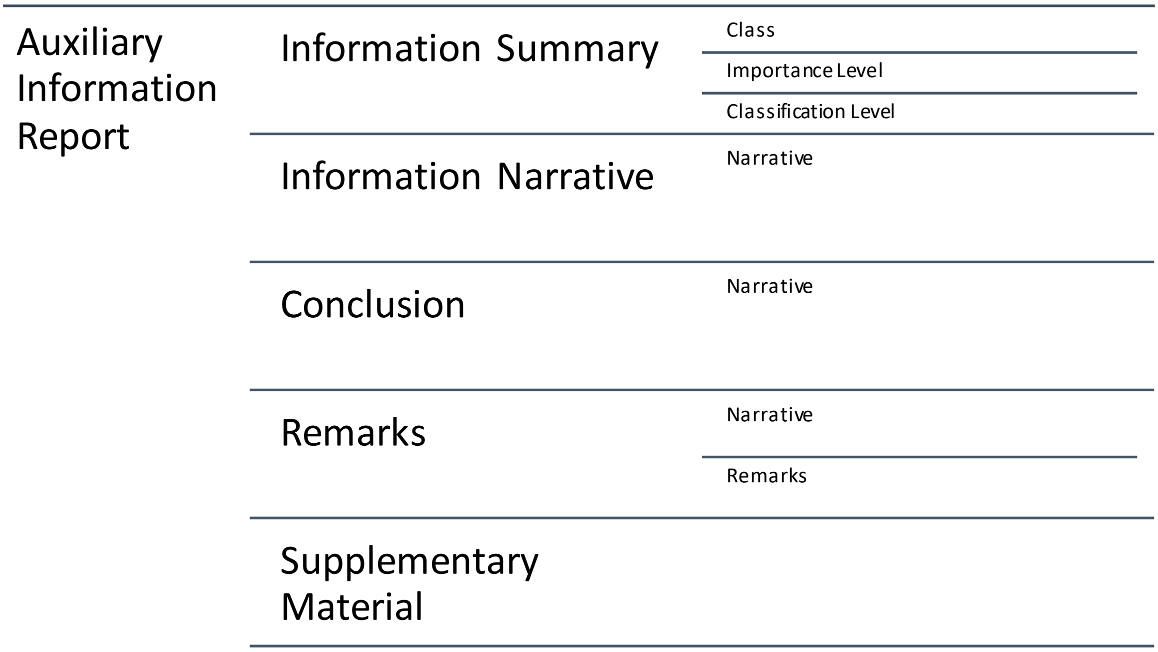


FIGURE 8

Agreed information fields in the reports comprise the atomic data parts of the complete information sharing environment. Instead of comprehensive generic sections, confining the shared information in small structured information fields and sections with specific information will provide great flexibility and ease the process. It then becomes possible to track reports about the same system using identifier values as a unique key, making it possible to form projections for desired systems and for similar uses.

Both a web browser-based portal and standalone software for the platform have advantages and disadvantages regarding compatibility, performance, ease of transition, training needs and licensing. Standalone programs on selected platforms are usually fast, robust and easier to service from a developer's point of view. However, web-based secure portals have the benefits of being platform-independent, real-time maintenance, less training requirements and ease of transition. Currently, MISP runs on Linux platforms and as a web application,[44] yet there are widely adopted methods of running it on containers using OS-level virtualisation and it comes with a robust set of guidelines and documentation. Using the existing MISP platform seems like a tempting option, especially as it is now being tested on secure networks for other purposes. It is specifically designed for sharing cyber threat indicators, which are mostly automated data with small information fields, and this would add significant overheads and unnecessary burden if it were used for sharing penetration testing reports. Additionally, developing a minimum-viable custom web portal for penetration testing information sharing could satisfy user requirements while not giving up the application's agility. Therefore, contrary to the initial assessment, the long-term benefits of developing and running a custom-made web-based portal outweigh the advantages of modified MISP or any other standalone application.[45]

Verification and transparency are challenging aspects. Transparency concerns and classification mechanisms have wide common grounds and are not mutually exclusive. In other words, there is no

[44] MISP-Project. 2019. *MISP - Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing.* Accessed 11 06, 2019. https://www.misp-project.org/features,html

[45] MOMook. 2018. *Web-Based vs. Desktop Software: Which is Better?* 09 10. Accessed 11 July 2019. https://momook.com/web-based-vs-desktop-software-which-is-better/.

practical way of providing transparency without well-functioning classification measures. While it is still valid in many other domains, particularly in the military domain, there are some aspects associated with information sharing which can prove beneficial for our purposes. Due to existing classification, verification and transparency standards adopted by allied nations and their military organisations, a common agreement and understanding already exist when an actor assesses the sensitivity level of the information to be sent, acknowledges the measures and correct practices of the receiving actors in regard to the security of the exchanged information. By operating under the same umbrella of regulations that govern nations' information exchange activities, it should be possible to avoid implementing new rules. Trust in both frameworks and entities will develop over time with each successful step and mitigated problem. Therefore, instead of putting too much effort into building a perfect mechanism at the beginning, starting with a minimum viable framework and evolving towards better versions is more likely to be the path to success.

8. Conclusion and way forward

Building an information sharing environment for penetration tests carries all the familiar challenges of other cyber information-sharing initiatives, besides having its own complications. The overall goal is to produce a platform which allied nations can utilize with an acceptable learning curve and which they can integrate into their daily rhythm with trust, thereby cutting the already high costs of penetration testing of military systems and increasing the alliance's overall cyber resilience.

Albeit there are several cyber information sharing tools currently in use among allied and partner nations, penetration testing and its techniques / practices have different characteristics, and they call for customised solutions. Investing in developing a custom platform with trust in the process will help avoid the sunken costs and future technical problems caused by legacy systems with different design concerns.

The major portion of the penetration test reports is sensitive data and this imposes on its handlers an obligation of extra care due to the associated legal restrictions and classification procedures. Allied nations already have existing legislation enabling the exchange of classified data; and by running the information-sharing platform according to existing regulations on classified networks, nations can benefit from the lowest common denominator of their legal scopes. For the classification concerns, a concise and thorough standardisation is required, which would serve as a reference point for organisations before sharing penetration test reports and even as a guide for implementing the reports.

This report, as the first stage of a longer project, is naturally not in its final form and will require continuous updates and contributions from current and future stakeholders. Standards regarding penetration testing activities, documentation, related efforts and corresponding standards continuously evolve; hence, the standardisation for penetration testing information sharing must follow along.

Standardisations, which are the backbone of the penetration testing information sharing environment, are in their base forms for the initial version of this report. As the report evolves with the exchange of thoughts, best practices and collaboration among stakeholders, the design and structure of the platform will take its mature form. The design and structure phase will be followed by the implementation and testing phases with the participation of its future users.

References

Bailey, Tucker, Andrea Del Miglio, Wolf Richte. 2014. *The rising strategic risks of cyberattacks.* Industry Research, New York: McKinsey Quarterly.

Barnum, Sean. 2014. ‘Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).’ *MITRE Corporation.*

Borys, Christian. 2017. *The day a mysterious cyber-attack crippled Ukraine.* 4 July. http://www.bbc.com/future/story/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine.

circ.lu. 2019. *Malware Information Sharing Platform MISP - A Threat Intelligence Sharing Platform.* Accessed 11 06, 2019. https://www.circl.lu/services/misp-malware-information-sharing-platform/.

CNBC. 2017. *There are 20 billion cyber attacks every day: Cisco.* 11 May. https://www.cnbc.com/video/2017/05/11/there-are-20-billion-cyber-attacks-every-day-cisco-.html.

Creasey, Jason, Ian Glover. 2017. *A guide for running an effective Penetration Testing programme.* Industry Report, Berkshire: CREST.

Curiel, Johanna. 2019. *App sec best practices: Assess risks before you pen test.* 04. Accessed 11 2019, 06. https://techbeacon.com/security/app-sec-best-practices-assess-risks-you-pen-test.

Denning, Dorothy. 2016. ‘Cybersecurity's Next Phase: Cyber Deterrence.’ *The Conversation*, 13 December.

Dradis. 2019. *Dradis Pro.* Accessed 11 07, 2019. https://dradisframework.com/ce/.

Eurofighter Typhoon - About. Accessed 11 07, 2019. https://www.eurofighter.com/about-us.

European Network and Information Security Agency. 2010. *Incentives and Challenges for Information Sharing in the Context of Network.* Research Project, European Network and Information Security Agency.

European Union Directive. 2016. ‘Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.’ *EUR-Lex.* 06 07. Accessed 11 06, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

—. 2016. ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Da.’ *EUR-Lex.* 27 04. Accessed 11 07, 2019. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679.

Gilje Jaatun, Martin, Maria B Line, Tor Olav Grotan. 2009. ‘Secure Remote Access to Autonomous Safety Systems: A Good Practice Approach.’ *International Journal of Autonomous and Adaptive Communications Systems Vol. 2 No. 3* 297-312.ICS-

CERT. 2012. Joint Security Awareness Report (JSAR-12-241-01B) Shamoon/DistTrack Malware (Update B). 16 October. https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B.

InfoSec. n.d. *CIA Triad (Confidentiality, Integrity, Availability).* Accessed 12 05, 2019. https://resources.infosecinstitute.com/cia-triad/.

IT Governance. 2013. 'Why is penetration testing necessary?' *itGovernance.* 04 09. Accessed 11 06, 2019. https://www.itgovernance.co.uk/media/press-releases/why-is-penetration-testing-necessary.

Jermalavičius, Tomas. 2009. *Defence Research & Development: Lessons from NATO Allies.* Project Report, Tallinn: ICDS.

Johnson, Chris, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150.*

Kubecka, Chris. 2015. 'How to Implement IT Security After a Cyber Meltdown.' *[Slideshow].* 3 August. https://www.blackhat.com/docs/us-15/materials/us-15-Kubecka-How-To-Implement-IT-Security-After-A-Cyber-Meltdown.pdf.

Libicki, Martin C. 2009. 'Cyberdeterrence and Cyberwar.' In *Cyberdeterrence and Cyberwar*, by Martin C. Libicki, 27-37. Santa Monica, CA: RAND.

Lyon, Gordon Fyodor. 2009. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Palo Alto: Nmap Project.

MISP-Project. 2019. MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Accessed 11 06, 2019. https://www.misp-project.org/who/.

MOMook. 2018. *Web-Based vs. Desktop Software: Which is Better?* 09 10. Accessed 11 07, 2019. https://momook.com/web-based-vs-desktop-software-which-is-better/.

NCI Agency. 2013. *Malware Information Sharing Platform.* Whitepaper, Brussels: NATO Communications and Information Agency.

Nolan, Andrew. 2015. *Cybersecurity and Information Sharing Legal Challenges and Solutions .* Legal Research Report, Washington D.C.: Congressional Research Service.

Nye, Joseph S. 2017. 'Deterrence and Dissuasion in Cyberspace.' International Security, President and Fellows of Harvard College and the Massachusetts Institute of Technology 44-71.

Ohl, Martin. 2019. *McAfee - Improving Cyber Resilience with Threat Intelligence.* 12 06. Accessed 11 07, 2019. https://securingtomorrow.mcafee.com/business/improving-cyber-resilience-with-threat-intelligence/.

OWASP. 2018. *Offensive Web Testing Framework.* 01 04. Accessed 12 06, 2019. https://owtf.github.io/.

Peng Liu, Amit Chetal. 2005. 'Trust-based Secure Information Sharing Between Federal Government Agencies.' *Journal of the Association for Information Science and Technology.*

Porup, J. M. 2019. 'What is Metasploit? And how to use this popular hacking tool.' *CSO Online.* 25 03. Accessed 11 07, 2019.

https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html.

Riigi Teataja. 2001. ‘Karistusseadustik - Penal Code.’ *Riigi Teataja.* 06 06. Accessed 11 06, 2019. https://www.riigiteataja.ee/en/eli/522012015002/consolide.

SANS. 2001. ‘An Introduction to TEMPEST.’ In *National Communications Security Committee Directive*, by Cassi Goodman. SANS Institute.

SANS ICS. 2016. Analysis of the Cyber Attack on the Ukranian Power Grid. Washingon DC: SANS.

Slayton, Rebecca. 2017. ‘Why Cyber Operations Do Not Always Favor the Offense.’ *International Security, Harvard Kennedy School*, February: 1-3.

Stuttard, Dafydd, Marcus Pinto. 2011. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* Indianapolis: Wiley.

Symantec. 2019. *Internet Security Threat Report Volume 24.* Industry Research, Mountain View: Symantec Corporation.

TAXII 2.0 Specification 2017.. 19 07. Accessed 02 19, 2019. https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/pub.

tenable. n.d. *The Nessus Family.* Accessed 11 07, 2019. https://www.tenable.com/products/nessus.

The Department of Homeland Security - The Department of Justice . 2015. ‘Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015.’ 15 06. Accessed 11 06, 2019. https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

UK National Cyber Security Centre . 2019. *CiSP - Cyber Security Information Sharing Partnership.* Accessed 11 06, 2019. https://www.ncsc.gov.uk/section/keep-up-to-date/cisp.

United Nations Development Programme. n.d. ‘IT Audit Manual.’ Albania: United Nations Development Programme.

US Department of Homeland Security. 2019. *Cyber Information Sharing and Collaboration Program (CISCP).* Accessed 11 06, 2019. https://www.dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp.

US Senate. 2015. ‘S.754 - To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.’ *Congress.gov.* 17 03. Accessed 11 06, 2019. https://www.congress.gov/bill/114th-congress/senate-bill/754.

—. 2015. ‘To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.’ *Congress.gov.* 27 10. Accessed 11 06, 2019. https://www.congress.gov/bill/114th-congress/senate-bill/754.

US-CERT. 2015. *Automated Indicator Sharing.* Accessed 02 04, 2019. https://www.us-cert.gov/ais.

—. 2019. *Traffic Light Protocol (TLP) Definitions and Usage.* Accessed 11 05, 2019. https://www.us-cert.gov/tlp.

Appendix A: NATO initiatives

NATO Communications and Information Agency (NCI Agency)[46] is responsible for strengthening the Alliance through connecting its forces. It delivers secure, coherent, cost-effective and interoperable communications and information systems in support of consultation, command and control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. This includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

NATO FMN - Federated Mission Networking[47] MISSION NETWORKS provide a governed single instance of capability, including the Communication and Information Systems, management, processes and procedures created for the purpose of an operation, exercise, training event, or interoperability verification activity. Mission Networks are established using a flexible and tailored set of non-material (i.e. policy, processes, procedures and standards) and materiel (i.e. static and deployed networks, services, supporting infrastructures) contributions provided by NATO, NATO and non-NATO nations and entities. Federated Mission Networking will be based on trust, willingness and commitment.

NATO NRDC IT Concept The NRDC CIS concept is based on a military tactical CIS system that provides the following secure and insecure information services: Data circuits to provide: the NATO SECRET WAN, the Mission or Theatre Classified WAN, the NATO Unclassified WAN or Internet, C2 Tools, Video Teleconferencing (VTC), Air System and, Functional Area Sub Services.[48]

NATO BICES-X Battlefield Information Collection and Exploitation Systems Extended deliver technical capability and governance to provide multinational intelligence and information-sharing capabilities. It also allows access to intelligence, surveillance and reconnaissance and general IT support to coalition operations and partner nations beyond the original NATO nations and associated partners. It provides secure email, file-sharing, voice [and video teleconferencing], chat, intelligence tools and the ability to support live streaming video feeds.[49]

EU cybersecurity certification framework:[50] As set out in Regulation (EU) 2019/881, the EU cybersecurity certification framework lays down the procedure for the creation of EU cybersecurity certification schemes, covering ICT products, services and processes. Each scheme will specify one or more level(s) of assurance (basic, substantial or high), on the basis of the level of risk associated with the envisioned use of the product, service or process. The purpose of the EU cybersecurity certification framework is to establish and maintain the trust and security on cybersecurity products, services and processes. Drawing up cybersecurity certification schemes at EU level aims at providing criteria to carry out conformity assessments to establish the degree of adherence of products, services and processes against specific requirements. Users and service providers alike, need to be able to determine the level of security assurance of the products, services and processes they procure, make available or use.

EU NIS Directive every EU member state has started to adopt national legislation, which follows or 'transposes' the directive.[51] The directive has three parts:

1. National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.

[46] https://www.ncia.nato.int/Our-Work/Pages/Infrastructure-Services.aspx
[47] https://www.act.nato.int/fmn
[48] https://www.nato.int/nrdc-it/magazine/2003/0307/0307l.pdf
[49] https://www.c4isrnet.com/c2-comms/2016/02/11/how-bices-x-facilitates-global-intelligence/
[50] https://www.enisa.europa.eu/topics/standards/certification
[51] https://www.enisa.europa.eu/topics/nis-directive

2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.

3. National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health and finance sector), ex-post supervision for critical digital service providers (internet exchange points, domain name systems, etc).

Appendix B: IT security standards

The use of IT security standards and frameworks is an important enabler to synchronise different organisations working in IT security:[52]

Common Criteria[53] is a widely recognised standard for security evaluation of IT products which divides products into different evaluation assurance levels. The levels corresponds to how strict the testing of the product has been. It follows the international standard IEC 15408. National certification organisations license companies and evaluate products according to Common Criteria. Certified products are used by both civil and military organisations. Approved products are listed on Common Criteria's website together with their evaluation assurance level[54]

PAS 555 - is primarily intended as a framework for the governance of cyber security which allows executives and senior management to compare the organisation's cyber security measures against the established descriptions at a high level. When implemented, this provides an 'umbrella' under which other standards and guidance can fit to flesh out the results described.

ISO/IEC 27001 is the international Standard for best-practice information security management systems. It is a rigorous and comprehensive specification for protecting and preserving your information under the principles of confidentiality, integrity and availability.

ISO/IEC 27032 – is focusing explicitly on cyber security. This Standard recognises the vectors that cyber-attacks rely on, including those that originate outside cyber space itself. Further, it includes guidelines for protecting your information beyond the borders of your organisation, such as in partnerships, collaborations or other information-sharing arrangements with clients and suppliers.

ISO/IEC 27035 - is the international Standard for incident management and to avoid reoccurrence.

ISO/IEC 27031 - is the international Standard for ICT readiness for business continuity.

ISO/IEC 22301 - is the international Standard for business continuity management systems.

ISO/IEC 15408, Common Criteria (CC)[55] – international standard for computer security. A Common Criteria evaluation allows an objective evaluation to validate that a particular product satisfies a defined set of security requirements. The focus of the Common Criteria is evaluation of a product or system and less on development of requirements. Nevertheless, its evaluation role makes it of interest to those who develop security requirements. The Common Criteria allow for seven Evaluation Assurance Levels (EALs). Functional and assurance security requirements are the basis for the Common Criteria. The higher the level, the more confidence you can have that the security functional requirements have been met. The levels are as follows:

EAL1: Functionally Tested. Applies when you require confidence in a product's correct operation, but do not view threats to security as serious. An evaluation at this level should provide evidence that the target of evaluation functions in a manner consistent with its documentation and that it provides useful protection against identified threats.

EAL2: Structurally Tested. Applies when developers or users require low to moderate independently assured security but the complete development record is not readily available. This situation may arise when there is limited developer access or when there is an effort to secure legacy systems.

[52] https://www.itgovernance.co.uk/cybersecurity-standards

[53] https://www.commoncriteriaportal.org/

[54] https://www.commoncriteriaportal.org/products/

[55] https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

EAL3: Methodically Tested and Checked. Applies when developers or users require a moderate level of independently assured security and require a thorough investigation of the target of evaluation and its development, without substantial reengineering.

EAL4: Methodically Designed, Tested and Reviewed. Applies when developers or users require moderate to high independently assured security in conventional commodity products and are prepared to incur additional security-specific engineering costs.

EAL5: Semi-Formally Designed and Tested. Applies when developers or users require high, independently assured security in a planned development and require a rigorous development approach that does not incur unreasonable costs from specialist security engineering techniques.

EAL6: Semi-Formally Verified Design and Tested. Applies when developing security targets of evaluation for application in high-risk situations where the value of the protected assets justifies the additional costs.

EAL7: Formally Verified Design and Tested. Applies to the development of security targets of evaluation for application in extremely high-risk situations, as well as when the high value of the assets justifies the higher costs.

Frameworks for Security/Penetration Tests:

PRES (Penetration Testing Execution Standard). A group of individuals from different companies has put together a standard framework for penetration testing[56]

OWASP OWTF (OWASP The Offensive (Web) Testing Framework). [57] The flagship project aims to make security assessments as efficient as possible by automating the manual, uncreative part of pen testing. It provides out-of-box support for the OWASP Testing Guide, the NIST and the PTES standards.[58]

Penetration Testing Framework[59]

Information Systems Security Assessment Framework

Open Source Security Testing Methodology Manual[60] (OSSTMM) by Pete Herzog has become a de-facto methodology for performing penetration testing and obtaining security metrics.

Payment Card Industry Data Security Standard (PCI DSS) and security and auditing standard, requires both annual and ongoing penetration testing. The PCI DSS Requirement 11.3 addresses penetration testing like the attempts to exploit the vulnerabilities to determine whether unauthorised access or other malicious activity is possible.

NSA Infrastructure Evaluation Methodology (IEM)

CCM - The Cloud Security Alliance’s Cloud Controls Matrix (CCM) is a set of controls designed to maximise the security of information for organisations that take advantage of Cloud technologies.

[56] See http://www.pentest-standard.org/index.php/Main_Page

[57] See OWASP OWTF Website https://www.owasp.org/index.php/OWASP_OWTF

[58] OWASP. 2018. *Offensive Web Testing Framework.* 01 04. Accessed 12 06, 2019. https://owtf.github.io/

[59] See www.vulnerabilityassessment.co.uk/

[60] See OSSTM Website https://www.isecom.org/research.html#content5-9d

Appendix C: Certifications for penetration testers

Relevant certifications for penetration testers

EC-Certified Ethical Hacker (CEH)

CPEH Certified Professional Ethical Hacker

Licensed Penetration Tester (LPT)

GIAC Penetration Tester (GPEN)

GIAC Web Application Penetration Test (GWAPT)

Certified Penetration Tester

Certified Expert Penetration Tester

CPT: Certified Penetration Tester

CEPT: Certified Expert Penetration Tester

OSCP: Offensive Security Certified Professional

CREA: Certified Reverse Engineering Analyst