Improving Offensive Cyber Security Assessments Using Varied and Novel Initialization Perspectives

Jacob Oakley
Towson University
7800 York Rd.
Towson, USA
joakle2@students.towson.edu

ABSTRACT

Offensive cyber security assessment methods such as red teaming and penetration testing have grown in parallel with evolving threats to evaluate traditional and diverging attack surfaces. This paper provides a taxonomy of ethical hacker conducted offensive security assessments by categorization of their initial evaluation perspectives. Included in this taxonomy are the traditional assessment perspectives which initiate analysis and attack simulation against networks either externally, from within a DMZ or internally. A novel paradigm of critical perspective as an initial point for offensive security evaluation processes is also presented. This initialization from a critical perspective bolsters the holistic capabilities of offensive cyber security assessment by providing a new offensive security assessment option intended to begin evaluation at the last line of defense between malicious actors and the crown jewels of an organization. Then from such a perspective assess outwards from the deepest levels of trust and security. This method will be shown to improve the ability to mitigate the impact of threats regardless of their originating from within or without an organization. As such, the assessment initialization at a critical perspective provides a new approach to offensive security assessment different from what has traditionally been practiced by red teams and penetration testers. [1]

CCS CONCEPTS

• **Security and privacy → Systems security → Vulnerability management →** Penetration testing

KEYWORDS

Cyber Security, Red Team, Penetration Test, Security Assessment, Risk

1 INTRODUCTION

Organizations undergo cyber security assessments to prepare for the dangers posed by malicious threat actors. Utilization of security assessments is increasingly demanded by government and industry regulations [1]. These offensive security assessments aim to identify and leverage vulnerabilities before an attacker finds them. This is done by using ethical hackers to exploit identified vulnerabilities and simulate an attack against the organization. These offensive security assessments are intended to provide true pro-active capabilities enabling organizations to address the identified issues prior to them being exploited in a breach by a real attacker. Typically, offensive security assessments occur in the form of red team engagements or penetration tests. Though there are variances in definitions, red teaming is used to find exploitable gaps in operational concepts with the overall goal of reducing surprises [2]. Alternatively, penetration testing is typically focused specifically on the identification and exploitation of vulnerabilities [3]. The driving factor behind how an offensive security assessment navigates and assesses a target organization is the initial perspective from where it begins. This paper will show correlation between the perspective from which ethical hacking is initialized and the effectiveness of that test. There are several well-known perspectives from which offensive security assessments begin. The decision between which perspective or perspectives best suits the needs of the organization is dependent on the threats faced by that organization and the equities it is trying to protect. This paper will categorically compare typical security assessment perspectives of external, DMZ and internal points of presence.

Also included in the comparison is the critical perspective which utilizes the paradigm of assessing worst-case scenario threats. This is a method already utilized in other industries such as finance and communications to insure the system doesn't fail when subjected to the highest level of stress possible [4] [5]. In cyber security, this requires beginning an assessment from identified items of lethal or critical impact to an organization if compromised. This novel perspective paradigm begins with a comparatively smaller more critical attack surface identified by the organization. This attack surface consists of those devices or data which if compromised would likely prove crippling or lethal to the organization. Assessment from this perspective allows for the most important items to be assessed first and expansion of the

ACM SE '18, March 29–31, 2018, Richmond, KY, USA
© 2018 Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-5696-1/18/03 $15.00
https://doi.org/10.1145/3190645.3190673

attack surface explored during the test expands outwards to points of presence within the organization that allow for an attacker to pivot to the critical or lethal compromise items. This type of critical or lethal perspective is also utilized in the TREsPASS Project which is technology-supported risk estimation by predictive assessment of socio-technical Security [6]. However, no work has been done to analyze the potential benefits for implementing such a view and perspective in ethical hacker conducted manual offensive security assessments.

There is a growing trend of insider threat involvement in security breaches [7] which is something security assessments must adequately address. Attempts to do so are complicated by the different promulgations of inside threats. According to CERT an insider threat is a malicious insider that is a current or former employee, contractor, or business partner who has or had legitimate and authorized access to organization's information systems and advertently misused or abused that privilege [8]. However, a more complete representation of insider threats actually breaks into three separate categories of negligent insiders, malicious insiders, and insiders compromised by malicious external actors [9].

This paper will detail four possible initial assessment perspectives of external, DMZ, internal and critical points of presence. Next, each perspective will be contrasted by its ability to assess and exploit vulnerabilities in an organization. Then, the four perspectives will be compared by their efficiency and manner of attack surface scrutiny. Lastly, disadvantages and advantages of each perspective will be outlined. It is important to note that offensive security assessment is a human conducted process involving tradecraft and skills as much as vulnerability identification and exploitation tools. As such, the process is more art than science and yet is one of the most important tools available to proactively secure a network due by using the resulting findings potentially providing proactive vulnerability mitigation. This being the case, logically deduced assumptions are made in some cases for each initialization perspective and related attributes. The initialization perspective affects nearly all facets of manual offensive security assessment and there has been no research to analyze the potential benefits of differing or transitioning attack perspectives. This paper will lay the ground work for greater analysis and improvement in ethical hacking and offensive security assessment. Additionally, there is clear value in considering the shortcomings of well-known attack perspectives and the potential advantages provided by the paradigm of critical item perspective in offensive security assessment. This following analysis will show that to provide a comprehensive offensive cyber security assessment all four perspectives should be considered.

2 Assessment Initial Perspectives

The initial perspective of an assessment is the point or points of presence from which the assessment will begin and what the initial focus of the ethical hackers will be. Differing perspectives have been adopted to allow for assessments to continue to provide as realistic an attack simulation as possible. This means that as the attack methodologies of attackers changes so to must those used in security assessments.

2.1 External Perspective

External perspective is the most traditional form of security assessment. External assessments typically start from an internet based point of presence and focus at the outside perimeter of the organizations security. This is an efficient way to emulate some of the more prolific threats organizations faced in times when connecting organizations to the internet was in a much less mature state. These early threats consisted of internet based worms [10]. With an attack surface consisting of web and database services hosted on the internet worms such as Code Red, Nimda and SQL Snake wreaked havoc on internet connected organizations in the early 2000's [11] [12] [13]. To help protect organizations from similar threats it was imperative to assess security in a similar way and as such early security assessments focused on this perspective as it presented the largest source of threats.

2.2 DMZ Perspective

DMZ perspective is required to assess networks in response to the popularity of implementing a DMZ in network security. Due to attacker focus on compromising internet facing services of an organization it was a natural evolution to create a DMZ or de-militarized zone where devices hosting these services could be stored and secured in isolation from areas of an organization where users and other devices exist [14]. Assessing a network with the DMZ perspective entails beginning the assessment with a point of presence in the DMZ itself and a focus on exploiting not only the security of internet facing servers from this evolved context but also evaluating the ability to attack the internal organization itself from the DMZ. This insures ensures there is a security assessment of the ability for a malicious actor to pivot from one DMZ-hosted internet facing device to another from within the DMZ, as well as the ability for attackers to move from the DMZ to the internal network.

2.3 Internal Perspective

Internal perspective utilizes points of presence from within the network itself. This perspective is typically manifested with user context on a user machine within the network and the focus of an assessment from this perspective is to assess ability to pivot location and elevate privilege within that internal network. The need for this perspective is a direct result of the increase in compromises originating from this type of access. Two main attack facilitations that drive the need for this perspective are those resulting from insider threats and those attacks which assume such a mantle as a result of social engineering and user executed malware. The fact that socially engineered malware execution represents the lion's share of access vectors for cyber incidents [15] [16] also drives the need for this assessment perspective.

2.4 Critical Perspective

The critical perspective starts at a point or points of presence that are identified as posing the greatest risk to the organization. An attack that affects the availability, integrity or confidentiality of these items is likely to bring down an organization. Thus, the focus of an assessment from this perspective is to identify vulnerabilities local to such devices that would enable an attacker to compromise the critical item. The assessment is then expanded to the points in the organization that would allow an attacker to pivot to the critical items and continues outward.

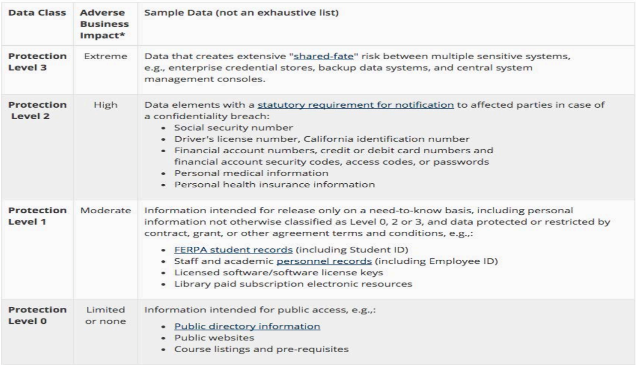
As mentioned in the introduction of this paper this is an implementation of worst case risk and threat assessment into the cyber security assessment vulnerability exploitation process. This purposed fourth perspective is a cyber security assessment paradigm aimed at mitigating the impact of a breach regardless of its source. No matter the vulnerability that allowed an attacker in or the locality of an insider threat should affect this assessment perspective. Beginning security assessments at the goal of a compromise instead of assessing the potential starting points provides an ability to mitigate a myriad of threats to these items of unacceptable loss.

3 Risk

In an effort to classify and contrast the four differing initial perspectives for security assessments a qualitative risk assessment will be utilized. Impact is a traditional component of rating risk being as it is a measure of how damaging different compromises would be to the organization [17]. The other half of risk rating is the likelihood a given impact will occur [17]. In this paper time is used to show likelihood. The time metric represents the amount of time spent assessing from a given perspective that it will take to yield compromises of information with differing impacts and thus is representative of the likelihood an attacker may be able to do the same.

3.1 Impact

To qualify the impact of the findings these assessment perspectives may lead to a classification system created by University of California, Berkeley will be used [18] to determine the impact related to compromised data.



Data Class	Adverse Business Impact*	Sample Data (not an exhaustive list)
Protection Level 3	Extreme	Data that creates extensive "shared-fate" risk between multiple sensitive systems, e.g., enterprise credential stores, backup data systems, and central system management consoles.
Protection Level 2	High	Data elements with a statutory requirement for notification to affected parties in case of a confidentiality breach: • Social security number • Driver's license number, California identification number • Financial account numbers, credit or debit card numbers and financial account security codes, access codes, or passwords • Personal medical information • Personal health insurance information
Protection Level 1	Moderate	Information intended for release only on a need-to-know basis, including personal information not otherwise classified as Level 0, 2 or 3, and data protected or restricted by contract, grant, or other agreement terms and conditions, e.g.,: • FERPA student records (including Student ID) • Staff and academic personnel records (including Employee ID) • Licensed software/software license keys • Library paid subscription electronic resources
Protection Level 0	Limited or none	Information intended for public access, e.g.,: • Public directory information • Public websites • Course listings and pre-requisites

Figure 1: UC Berkeley Data Classification Standard

To identify which type of information each perspective is likely to identify an overlay is created showing which parts of the network are likely to contain which levels of data protection classification.

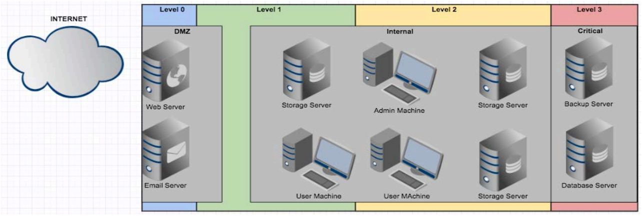


Figure 2: Data Protection Level Locality

3.2 Likelihood

As mentioned earlier the expression of likelihood will be shown as the time it would take an assessment from a given perspective to identify findings that have a given impact. For instance, if an assessment perspective has the ability to almost immediately find data with a given protection level then there is a high likelihood the perspective being used will have that impact. If the perspective requires time and pivoting to get to differing data protection levels the likelihood would be low. It is important to understand that the passing of time during an assessment is likely to transition the assessing perspective as well. An assessment may have the external initial perspective to the network and then via exploitation gain access to a device in the DMZ. From that point forward the assessment is a representation of multiple attack perspectives. This process can continue as an assessment progresses further into the network. The defining delta involved is time, transitioning perspectives and indicating likelihood.

3.3 Risk Assessment: External Perspective

The external initial assessment perspective has a focus on the outer perimeter of the network and may only move on to other parts of the organization after identifying and leveraging vulnerabilities in the outer most layers of the organization. As such early on in the assessment there is a high likelihood that only Level 0-1 data will be endangered by findings. Time may allow the test to compromise data of higher levels via pivoting deeper into the network but as the duration of the test increases the likelihood drops.

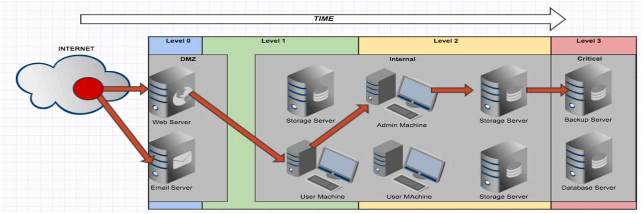
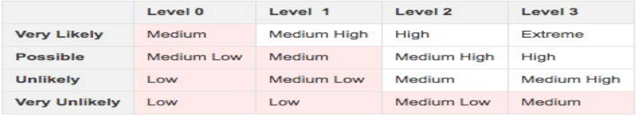


Figure 3: External Perspective Timeline

Using the above timeline representation of an assessment that began with an external point of presence a risk assessment matrix can be created to illustrate the impact and likelihood of threats addressed. Below, cells shaded in red indicate the levels of risk assessed. The impact is represented via the protection level associated with data that can be compromised. As stated earlier the likelihood is demonstrated by how long an assessment needs to realistically compromise a given level of data. Since the external perspective is far from where level 3 data is found in a network the time it would take to reach is greater and is therefore unlikely.



	Level 0	Level 1	Level 2	Level 3
Very Likely	Medium	Medium High	High	Extreme
Possible	Medium Low	Medium	Medium High	High
Unlikely	Low	Medium Low	Medium	Medium High
Very Unlikely	Low	Low	Medium Low	Medium

Figure 4: External Perspective Risk Assessed Matrix

This risk matrix shows that the external perspective provides a high likelihood of identifying findings that could lead to the compromise of level 0 information. Even though the impact of level 0 information is low the almost assured likelihood creates a medium level of risk associated with findings found from this perspective. This perspective is less likely to lead to higher level data as it requires time to discover additional vulnerabilities allowing the assessment perspectives to pivot deeper into the organization. As shown in the external perspective risk matrix, the level of risk likely to be assessed is low to medium.

3.4 Risk Assessment: DMZ Perspective

The DMZ perspective has an advantage over the external perspective as it initially starts from a point of presence already within the DMZ of the organization and does not have to discover a finding that will allow it to pivot into the DMZ from the internet.

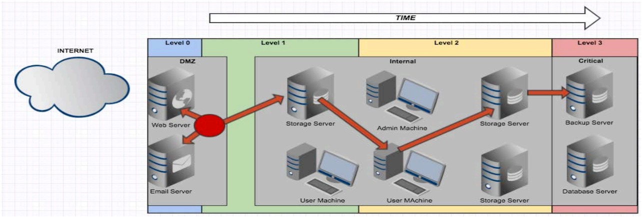
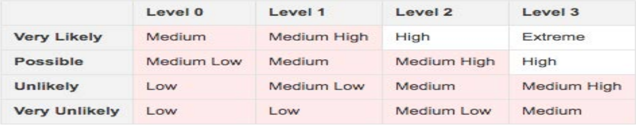


Figure 5: DMZ Perspective Timeline

Since an assessment from this perspective does not need the time to pivot inside that an external perspective requires, the timeline of such an assessment begins already within the perimeter of the network.



	Level 0	Level 1	Level 2	Level 3
Very Likely	Medium	Medium High	High	Extreme
Possible	Medium Low	Medium	Medium High	High
Unlikely	Low	Medium Low	Medium	Medium High
Very Unlikely	Low	Low	Medium Low	Medium

Figure 6: DMZ Perspective Risk Assessed Matrix

This means that findings related to high levels of data protection are more likely as they require less time to identify and increasing the likelihood that impactful threats are found. The DMZ perspective has the greatest potential to evaluate a medium level of risk.

3.5 Risk Assessment: Internal Perspective

With an initial perspective from a point of presence in the middle of the network this perspective is afforded the ability to result in findings early on of level 1-2 data. This position also has the side effect of making an assessment with this initial perspective actually less likely to discover findings that lead to level 0 information than the two perspectives discussed previously. As with the previous two perspectives time is required to get from this initial perspective to a pivot with the capacity to compromise level 3 data.

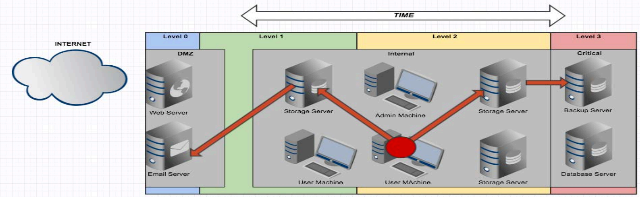
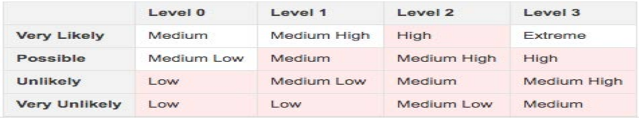


Figure 7: Internal Perspective Timeline

This timeline shows that for an assessment with this initial perspective to lead to findings regarding level 3 data still requires time, as does level 0 data. It is therefore most likely to find data of level 1-2.



	Level 0	Level 1	Level 2	Level 3
Very Likely	Medium	Medium High	High	Extreme
Possible	Medium Low	Medium	Medium High	High
Unlikely	Low	Medium Low	Medium	Medium High
Very Unlikely	Low	Low	Medium Low	Medium

Figure 8: Internal Perspective Risk Assessed Matrix

Since it is not very likely that level 3 data will be compromised by vulnerabilities discovered from this perspective it still does not represent an extreme level of risk assessed. However, the Internal perspective clearly represents a large cross section of the potential risk that can be faced. As a result, the levels of risk evaluated are likely to be medium to high and potentially low as well.

3.6 Risk Assessment: Critical Perspective

An assessment using the critical initial perspective begins deep in the network at the most valuable points. This means that opposite to the other three perspectives, findings of level 3 data compromise will be identified in the beginning. Unfortunately using this perspective actually requires time to get to point in the network that contain level 0-2 data.

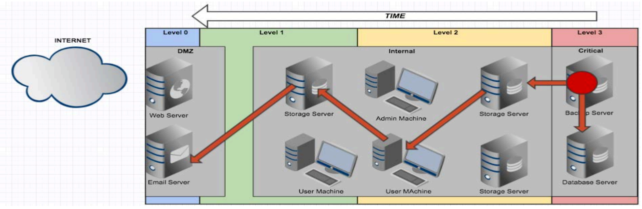
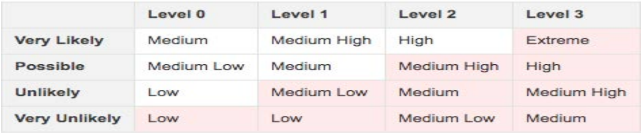


Figure 9: Critical Perspective Timeline

Use of this perspective decreases the likelihood that data of level 1-2 will be discovered during the assessment and is much less likely to encounter findings of level 0 data. In regard to overall assessment efficiency of an organization this initial perspective is probably the least effective at covering all levels of risk.



	Level 0	Level 1	Level 2	Level 3
Very Likely	Medium	Medium High	High	Extreme
Possible	Medium Low	Medium	Medium High	High
Unlikely	Low	Medium Low	Medium	Medium High
Very Unlikely	Low	Low	Medium Low	Medium

Figure 10: Critical Perspective Risk Assessed Matrix

However, it is efficient at finding level 3 data as it begins on devices hosting such information. This assessment perspective is therefore much more likely to discover findings that result in compromise of level 3 data and as such represent an ability to assess the most extreme levels of risk faced by an organization.

4 Attack Surface

The next comparison to be made between the initial perspectives is the ability of each to scrutinize attack surface during an assessment. This is an extremely important attribute in justifying the validity of a security assessment. Although an assessment may not yield results that cover extremely valuable compromise items it may still be extremely effective if it was able to assess a large portion of the organizations attack surface. The attack surface is comprised of the ways in which an adversary can enter the system and potentially cause damage [19]. It is extremely important to reduce the attack surface adversaries can utilize [20]. It is the responsibility of the security assessment to cover attack surface, evaluating it for vulnerabilities. Since attack surface represents the opportunity attackers have to compromise the security of systems [21] reducing that opportunity is a must for any security apparatus.

All attack surface must not be treated equally though as different parts of the overall attack surface represent potential immediate access to different levels of data. Attack surface consists of all the different points where an attacker could get in to a system [22] and that system may be an organization as a whole or individual devices within it. As Stuckman and Purtilo state, “an attack surface metric does not directly measure exploitability (a system with a small attack surface but many vulnerabilities could be more exploitable than a system with a larger attack surface)” [20]. As an example, there is a wider attack surface represented by internet facing surfaces as they are subject to a much higher amount of attack and enumeration attempts. Yet, as has been shown, vulnerabilities allowing access to internet facing servers may not necessarily be initially crippling to an organization. A dissection of how each initial perspective affects the way attack surface is analyzed will further the case for each of them as valid security assessment perspectives as well as how they together comprise the necessary parts of adequate cyber security evaluation of an organization.

4.1 Attack Surface: External Perspective

The SANS Technology Institute defines attack surface as exposure, the reachable and exploitable vulnerabilities [23]. The internet facing portions of an organization are the most exposed and are reachable by the largest audience of users and attackers. As such the internet facing layer of the network can be classified as having the most attack surface. Vulnerabilities present here may not lead to the direst of consequences if exploited yet this is the most likely place they will be found. The nature of creating services available to internet users is something most modern organizations have had to accept. External perspective for security assessment offers the most straight forward method for evaluating this surface.

The external perspective allows for covering large swaths of the attack surface an organization presents however there are periods of time before this assessment reaches deeper into the network if at all during a test. The figure above shows the attack surface evaluated in red and how the assessment transitions to deeper portions of the attack surface with time. At initialization, the first attack surface pyramid shows how the external perspective only sees the external attack surface of the organization. The second pyramid represents the middle of an assessment from the external perspective and how it will have reached an ability to assess attack surface deeper within an organization. The third and last pyramid shows the end of the assessment and how it has assessed parts of the organizations deeper attack surfaces but not all of it.

4.2 Attack Surface: DMZ Perspective

Beginning an assessment in the DMZ removes the need for a vulnerability that allows the assessors to pivot past internet facing defenses. As such, assessments with this perspective are more immediately able to assess the other devices in the DMZ and identify their vulnerabilities presented via lateral enumeration.

A test initiated with the DMZ perspective requires little time to assess devices in the DMZ. It is also able to begin probing the internal network in a quicker fashion than the external perspective. This is due to the external perspective needing the bulk of the organizations external attack surface must first be addressed before moving on. One potential obstacle faced by this assessment perspective however is that it could fail to identify vulnerabilities present to internet based scans and attacks as devices in the DMZ should be talking to the internet but not each other [24].

4.3 Attack Surface: Internal Perspective

Assuming the mantle of the insider threat the internal perspective is the benefactor of starting even deeper in the network and having access to a varied ensemble of an organizations attack surface. This also means that, like the DMZ perspective, assessing an organizations internet facing threat vectors is not easily done and in fact could be quite time consuming from this context.

The benefit of internal assessment perspective as an initial point for an engagement is that the attack surface analyzed in the immediate environment is likely to lead to vulnerabilities that can compromise data an organization has no intention of being made publicly available. This is contrary to the external and DMZ assessment perspectives which may find a lot of less meaningful vulnerabilities across a larger more internet accessible attack surface.

4.4 Attack Surface: Critical Perspective

The critical perspective analyzes by far the least amount of an organizations attack surface. Diametrically opposed to the external perspective which begins focusing on an extremely large surface the critical perspective focuses on very few if not one equity. From this point, it is unrealistic to assume that an assessment beginning from this perspective will be able to assess internet facing services in any reasonable timeframe. As discussed however this method is intended to provide most efficient analysis of the most dangerous attack surface.

The way a critical perspective assessment approaches different parts of the organizations attack surface also varies from the other three methods. For example, the most value can be gained from the external perspective when it finds as many vulnerabilities in the internet facing perimeter of an organization as possible. This likely means that assessors do not even leverage identified vulnerabilities to move deeper into an organization until they deem the entirety of that external surface has been evaluated. This attempted complete attack surface coverage is a necessary part of the other assessment perspectives and allows for the organization to mitigate the largest portion of overall threats post assessment. The critical perspective however does not need to evaluate the next layer completely. The critical perspective instead focuses on how attackers could pivot to the data of unacceptable loss. Instead of looking for all the vulnerabilities in attack surfaces it focuses on those that enable the access to pivot towards lethal and critical items of compromise.

5 Advantages / Disadvantages

Each of the four initial assessment perspectives has been presented as a representation of risk assessment and attack surface analysis. The purpose of security assessment is intended to reduce an organizations overall risk and each of these perspectives are valuable in their own right. The sum of these methods should then result in an affective security assessment strategy that covers as much of an organization attack surface as possible and identifies as many threats as possible allowing the organization to mitigate the maximum amount of risk. When attempting to compile a comprehensive security assessment not all initial perspectives may be realistic due to any number of circumstances. It is therefore imperative to go beyond the value of each with regards to attack surface and risk assessment and delve into additional advantages and disadvantages of each. This will allow assessors to not only know which respective are most needed but which are most feasible in any given assessment scenario. The amount and relevance of attack surface engaged by each initial perspective has been displayed. Additionally, the risk assessment capability for each has been identified. To continue the intent of this paper to compare these initial assessment perspectives some additional attributes will be appropriated to each.

5.1 Introduction of Risk

In any security assessment prior to testing the extremely important steps of establishing the scope and rules of engagement must be completed. These items identify the techniques and methods and especially what is to be tested [25]. The scope of the assessment and the rules of engagement are established as part of the pre-engagement interactions [26]. This means that before the security of an organization can even start being evaluated there are strict processes detailing how the test will be performed. Different initial perspectives present different complexities with regards to understanding and agreeing upon a scope and rules for the test. These two items of scope and rules of engagement are how an organization finds an acceptable level of risk that may be introduced by the test. This risk manifests itself in two ways. First, a security assessment may bring risk to an organization by possibly denying a service which may involve introducing large delays, excessive losses, and service interruptions [27] through assessment activity. Second, the access needed by the assessor to conduct the assessment from a given perspective may increase the overall attack surface or its severity.

5.1.1 External Perspective. The attack surface initially evaluated by the external perspective is intended to be made up of devices and services purposefully made available to the internet. This means they should be expectant of attacks and large amounts of traffic. There are even external entities that help mitigate internet based denial of service to subvert the risk posed by any internet sourced traffic which would include that of the assessor [28]. However, the added strain imposed by scanning and exploitation attempts can still bring devices down. Though low, this source of risk must be considered since loss of one of the internet facing services likely impacts external and internal users of the organization. Since the assessor does not need an established internal access to conduct the assessment from an external perspective there is no additional attack surface added by the execution of such assessments.

5.1.2 DMZ Perspective. Similar to the external perspectives the DMZ perspective initially focuses on devices and services intended for internet based traffic. The risk posed by potential outages caused by the assessment is similarly low. No additional risk should be presented by the assessor accessing devices in the DMZ as the purpose of the DMZ is to isolate accessible hosts from the rest of the organization [29]. There is a slightly higher chance of unintended consequences from scanning and exploitation attempts as the DMZ assessment perspective tests devices from a lateral position in the DMZ instead of from the internet. There is a chance that devices are not prepared to handle this lateral traffic which could cause a denial of service. This perspective requires an established point of presence within the DMZ to begin assessments from. Although this allows the assessor to start one level deeper into the organization the risk is still negligible. The access handed to the assessor is isolated from the internal network by nature of being in the DMZ and therefore poses little additional risk due to the additional attack surface of its initial assessment vector.

5.1.3 Internal Perspective. Assessments from the internal perspective are immediately able to interact with devices and services not intended for public perusal. These devices are much less likely to cope with heavy scanning or exploitation attempts and therefore there is a risk to assessing devices from this perspective. A denial of service here is more likely to result in lack of availability for internal users compared to external users.

Additionally, an outage caused by this assessment is more likely to impact organizational functions. The internal perspective also poses an increase in attack surface. With the necessity of either access being granted by the organization or a successful introduction of malware an assessor using this perspective introduces additional means of access into an organizations interior.

5.1.4 Critical Perspective. Relative to the other initial perspectives the critical perspective represents a high level of risk to an organizations ability to function. The items that constitute the point of presence where such an assessment begins are those identified as extremely critical to an organizations ability to exist. Any issue caused to such devices by the assessment are likely to prove damaging to an organizations ability to function normally. The risk created by an increase to attack surface is also relatively high. Like the internal perspective the critical perspective requires the introduction of an access vector by the organization from which to begin the assessment. The attack surface added to the organization by this access vector is more dangerous as it is a direct line to the critical comprise items. A compromise of the access vector used by the assessor would be extremely dangerous to the organization and extreme care should be taken with this type of assessment.

5.2 Burden of Coordination

In addition to the coordination required to form an acceptable scope and rules of engagement there is also the potential for further burden of coordination before and during an assessment. As mentioned before, different assessments may require collaboration with organizational staff to enable access required for an assessment. There is also a need to maintain communications in varying levels during an engagement to insure there is no confusion between real attack attempts by malicious actors and those of the assessor.

5.2.1 External Perspective. With no need to have an organization enabled point of presence from which to start evaluation this perspective requires little to no collaboration to begin the assessment. There is also minimal need for ongoing communications with the organization staff while engaging from this perspective. The assessor would need to communicate with staff if a vulnerability was discovered that allowed for transition to a new perspective inside the organization to avoid confusion between a real attack and the assessment.

5.2.2 DMZ Perspective. Initially this assessment perspective does require collaboration to introduce an access point within the DMZ from which to conduct the test. Similar to the external perspective ongoing collaboration however is in a limited fashion and typically only to provide de-confliction.

5.2.3 Internal Perspective. Access to conduct an assessment from this perspective is typically achieved in one of two ways. An exploit event is simulated and the outcome of the exploit is simulated to give the assessor contextual access to an internal point of presence. There is also the ability of an assessor to conduct a social engineering campaign in an attempt to get users in the organization to visit a malicious site or open a malicious email that allows the assessor to gain internal access. There is then a need initially to enable access or an ongoing need to monitor the organization to ensure that such a campaign is not confused with a real attempt by an attacker. Additionally, there may be a need to ensure that any notice of the campaign by users in the organization does not impact its ability to compromise others and still allow the assessment to begin from that perspective.

5.2.4 Critical Perspective. This assessment has no way around requiring organization collaboration to create an initial access vector. Unlike the previous examples of perspectives requiring organization enabled access this assessment perspective presents more challenges. In other perspectives, the organization may simply execute a tool for the assessor to enable access. There is a high level of risk involved and atypical traffic requirements potentially necessary to enable access deep within an organization at its critical points. The organization and assessor must create an access vector that creates as little additional risk to the organization as possible and the staff are likely to favour ongoing cognizance of the assessor's activity.

5.3 Emulated Threat

Security assessments such as red teaming and penetration tests are attempting to emulate an attack [30] [31]. The different perspectives discussed in this paper provide and assessor the ability to represent different types of threats to an organization. According to Rusell and Gangemi attackers can be classified in four primary methods, Organized Attackers, Hackers, Amateurs and Insiders [32].Organized attackers are the ones with resources and motivation and are specifically targeting an organization. This category also represents advanced persistent threats or APTs which are intent on breaking into an organization with the goal of stealing or compromising information [33]. Hackers may be perceived as benign explorers, malicious intruders, or computer trespassers [34]. The main difference between hackers and organized attackers is the resources backing the attacker. Amateurs are also known as "script kiddies" and are less skilled often using existing tools and instructions that can be found on the internet [35]. It is worth noting then how each perspective provides emulations of these different threats towards a comprehensive security assessment. An assessment began with any of the four initial perspectives has the potential as time is spent on the engagement to obtain a point of presence in an organization that facilitates assessment from a different perspective. The following statements are strictly with regards to each perspective initial focus and the threats they are most likely to emulate.

5.3.1 External Perspective. With no need for access to the network to perform an assessment the type of threat this perspective most readily represents is amateurs.

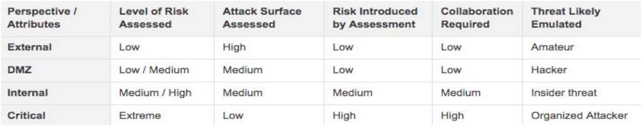
5.3.2 DMZ Perspective. Representing a need for an already successful exploitation of a vulnerability that would provide an attacker the ability to pivot into the DMZ of an organization this perspective closely resembles the ability and intentions of a hacker.

5.3.3 Internal Perspective. The Internal perspective actually represents multiple threats. Here the insider threat is represented since the access needed for an assessment from this perspective requires access to a device within the organization. Additionally, due to the ability of hackers to target individuals who work in an organization using social engineering to deploy their malware it is realistic to assume the threat of hackers can be represented by the initial focus of this perspective.

5.3.4 Critical. This perspective is intended to emulate the targeting of the availability, confidentiality or integrity of critical items. It is therefore most likely to represent the threat of an organized attacker. There is a need to gain access or begin from within the network as an insider or hacker might and then to continue that by pivoting deep into the network with the goal of compromising specific items required by the actor's motivations.

6 CONCLUSIONS

This paper has presented a comparison of initial perspectives for offensive security assessments. This work has also expanded the capabilities of security assessments via proposal of the critical initial perspective as a go-deeper solution to addressing insider and other advanced threats to high risk items. This research represents a dissection and representation of security assessment methodology previously unavailable to researchers. The analysis provided in this paper indicates that all four initial assessment perspectives bring advantageous and disadvantageous aspects to cyber security evaluations.



Perspective / Attributes	Level of Risk Assessed	Attack Surface Assessed	Risk Introduced by Assessment	Collaboration Required	Threat Likely Emulated
External	Low	High	Low	Low	Amateur
DMZ	Low / Medium	Medium	Low	Low	Hacker
Internal	Medium / High	Medium	Medium	Medium	Insider threat
Critical	Extreme	Low	High	High	Organized Attacker

Figure 11: Taxonomy of Initial Perspectives

As Such, all four perspectives together comprise the most complete representation of manual attack simulation by ethical hackers against organizations. All must be considered as valuable parts of any security assessment intent on empowering organizations embattled in the current threat landscape. Thus, this taxonomy has indicated that the proposed paradigm of the critical perspective is an assessment initialization point that provides a valid evolutionary step in the genesis of security assessments. It has been shown to allow for better mitigation of insider and advanced threats making it a valid and novel augmentation to existing cyber security assessments.

REFERENCES

[1] AppliedTrust, "The Importance of Periodic Security Assessments," Viawest. [Online]. [Accessed 15 7 2017].

[2] c. s. choo, c. l. chua and s.-h. v. tay, "Automated red teaming: a proposed framework for military application," in *9th annual conference on Genetic and evolutionary computation*, New Yotk, 2007.

[3] A. Applebaum, D. Miller, B. Strom, C. Korban and R. Wolf, "Intelligent, automated red team emulation," in *32nd Annual Conference on Computer Security Applications*, New York, 2016.

[4] s. ghosh and s. juneja, "Computing worst-case tail probabilities in credit risk," in *38th conference on Winter simulation*, 2006.

[5] M. Y. Naghmouchi, N. Perrot, A. R. Mhjoub, N. Kheir and J.-P. Wary, "A New Risk Assessment Framework Using Graph Theory for Complex ICT Systems," in *8th ACM CCS International Workshop on Managing Insider Security Threats*, Vienna, 2016.

[6] The TREsPASS Project, "TREsPASS," 2017. [Online]. Available: https://www.trespass-project.eu/. [Accessed 4 October 2017].

[7] J. Heiser, "Understanding Data Leakage," Gartner Research Report, 2017.

[8] CERT, "Common Sense Guide to Prevention and Detection of Insider Threat," CERT, 2009. [Online]. Available: http://www.ncix.gov/issues/ithreat/csg-v3.pdf. [Accessed 7 2017].

[9] Imperva, "Hacker Intelligence Initiative Report," Imperva, 2016.

[10] V. Yegneswaran, P. Barford and U. Johannes, "Internet Intrusions: Global Characteristics and Prevalence," in *2003 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, 2003.

[11] Eeye Security Inc., "Microsoft IIS Buffer Overflow Advisory," 2001. [Online]. Available: http : //www.eeye.com/html/ − Research/Advisories/AD20010618.html. [Accessed 7 2017].

[12] K. Poore, "Nimda Worm - Why is it Different?," *SANS Institute InfoSec Reading Room,* 11 November 2001.

[13] SANS, "IDFAQ: An analysis of SQL.Spider-B (Digispid.B.Worm, Spida, MSSQL Worm and SQLSnake)," SANS, 2003.

[14] M. Bauer, "Paranoid Penguin: Designing and Using DMZ Networks to Protect Internet Servers," *Linux Journal,* vol. 2001, no. 83es, March 2001.

[15] Verizon, "2017 Data Breach Investigations Report (DBIR)," Verizon, 2017.

[16] Industrial Control Systems Cyber Emergency Response Team, "ICS-CERT Year in Review," NCCIC, 2016.

[17] M. J. Lewis, "Characterizing risk," in *Eighth Annual Cyber Security and Information Intelligence Research Workshop*, 2013.

[18] "Data Classification Standard," 22 April 2013. [Online]. Available: https://security.berkeley.edu/data-classification-standard. [Accessed 16 7 2017].

[19] P. Manadhata, J. Wing, M. Flynn and M. McQueen, "Measuring the attack surfaces of two FTP daemons," in *2nd ACM workshop on Quality of protection*, Alexandria, 2006.

[20] K. Sun and S. Jajodia, "Protecting Enterprise Networks through Attack Surface Expansion," in *2014 Workshop on Cyber Security Analytics, Intelligence and Automation*, Scottsdale, 2014.

[21] J. Stuckman and J. Purtilo, "Comparing and applying attack surface metrics," in *4th international workshop on Security measurements and metrics*, Lund, 2012.

[22] The Open Web Application Security Project (OWASP), "What is Attack Surface Analysis and Why is it Important?," OWASP, July 2015. [Online]. Available: https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet. [Accessed 17 July 2017].

[23] SANS Technology Institute, "Security Laboratory: Defense In Depth Series," SANS, 2016. [Online]. Available: https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface. [Accessed 17th July 2017].

[24] M. Chapple, "Four Tips for Securing a Network DMZ," 18 May 2012. [Online]. Available: https://fedtechmagazine.com/article/2012/05/four-tips-securing-network-dmz-fed. [Accessed 17 July 2017].

[25] That Security Blog, "Penetration Testing and Rules of engagement," 3 September 2016. [Online]. Available: https://fl0x2208.wordpress.com/2016/09/03/penetration-testing-and-rules-of-engagement/. [Accessed 18 July 2017].

[26] pentest-standard, "pre-engagement," 16 August 2014. [Online]. Available: http://www.pentest-standard.org/index.php/Pre-engagement. [Accessed 18 July 2017].

[27] J. Mirkovic, P. Reiher, S. Fahmy, R. Thomas, A. Hussain, S. Schwab and C. Ko, "Measuring denial Of service," in *2nd ACM workshop on Quality of protection*, Alexandria, 2006.

[28] J. Brustoloni, "Protecting electronic commerce from distributed denial-of-service attacks," in *11th international conference on World Wide Web*, Honolulu, 2002.

[29] M. Schmidt, M. Smith, N. Fallenbeck, H. Picht and B. Freisleben, "Building a demilitarized zone with data encryption for grid environments," in *first international conference on Networks for grid applications*, Lyon, 2007.

[30] B. J. Wood and R. A. Duggan, "Red Teaming of Advanced Information Assurance Concepts," in *DARPA Information Survivability Conference and Exposition, 2000*, Hilton Head, 2000.

[31] C. Kirsch, "What is Penetration Testing?," Rapid7, 17 April 2013. [Online]. Available: https://community.rapid7.com/docs/DOC-2248. [Accessed 19 July 2017].

[32] D. Russel and G. T. Gangemi, Computer Security Basics, Sebastopol: O'Reilly & Associates.

[33] S. Siddiqui, M. S. Khan, K. Ferens and W. Kinser, "Detecting Advanced Persistent Threats using Fractal Dimension based Machine Learning Classification," in *2016 ACM on International Workshop on Security And Privacy Analytics*, New Orleans, 2016.

[34] K. Hafner and J. Markoff, Cyberpunk: Outlaws and Hackers on the Computer Frontier, New York: Simon & Shuster, 1991.

[35] C. Han and R. Dongre, "Q&A What Motivates Cyber-Attackers?," Talent First Network, October 2014. [Online]. Available: https://timreview.ca/article/838. [Accessed 18 July 2017].