

State of the Art Paper

Phasen eines Penetrationstest

Marian Phil Mutschler

mail@mutschler-m.de

DHBW Mannheim

Mannheim, Germany

DATAGROUP ULM GmbH

Ulm, Germany

ZUSAMMENFASSUNG

In diesem State of the Art Paper werden die einzelnen Phasen und Herangehensweisen eines Penetrationstest erläutert und dargestellt. Hierbei wird auf die einzelnen Besonderheiten der Phasen eingegangen und deren Nutzen erläutert. Ebenfalls behandeln wir ein grundsätzliches Durchführungskonzept für Penetrationstests.

7	Abschließend	6
	Abbildungsverzeichnis	6
	Literaturverzeichnis	7

KEYWORDS

Hacking, Gray-Hat, Pen-Test, Penetrationstesting, Phasen, Step-by-Step, Exploitation, Reconnaissance, Informationstechnik

INHALTSVERZEICHNIS

Abstract	1
Inhaltsverzeichnis	1
1 Einführung in die Technik	1
2 Der Begriff Penetrationstest	1
3 Penetrationstests	2
3.1 Ziele eines Penetrationstest	2
3.2 Ansatzpunkte	2
3.3 Bedrohungen	2
4 Durchführungskonzept	2
4.1 Grenzen	2
4.2 Rechtliches	3
4.3 Klassifikation	3
4.4 Organisatorische Voraussetzungen	5
5 Die Phasen	5
5.1 Reconnaissance / Vorbereitung	5
5.2 Informationsbeschaffung	5
5.3 Risikoanalyse / Bewertung der Informationen	6
5.4 Exploitation / Aktive Angriffe	6
5.5 Bericht / Auswertung	6
6 Vorgehensweise	6

1 EINFÜHRUNG IN DIE TECHNIK

Heutzutage sind Netzwerkstrukturen von Unternehmen und öffentlichen Einrichtungen vielfachen Gefährdungen ausgesetzt. Im Laufe der Zeit sind komplexe Kommunikationsstrukturen entstanden, die diese Gefährdungen unterstreichen. Durch die Verknüpfung dieser Kommunikationsstrukturen setzen sich Unternehmen und Einrichtungen Bedrohungen aus, auf die angemessen reagiert werden muss. [1]

2 DER BEGRIFF PENETRATIONSTEST

Penetrationstest haben den Zweck eines umfassenden Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Größe. Unter einem Penetrationstest versteht die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die ein Angreifer anwenden würde, um unautorisiert in das System einzudringen. [2] Der Penetrationstest ermittelt somit die Angreifbarkeit des zu testenden Systems gegen derartige Angriffe. Wesentlicher Teil eines Penetrationstests sind Tools und Werkzeuge, die dabei helfen, möglichst alle Angriffsmuster nachzubilden, die sich aus den zahlreichen bekannten Angriffsmethoden herausbilden. [2]

3 PENETRATIONSTESTS

3.1 Ziele eines Penetrationstest

Ziele eines Penetrationstests sind:

- die Identifikation von Schwachstellen
- das Aufdecken potentieller Fehler, die sich aus der (fehlerhaften) Bedienung ergeben
- die Erhöhung der Sicherheit auf technischer und organisatorischer Ebene und
- die Bestätigung der IT-Sicherheit durch einen externen Dritten.

Durch die ständige Änderung der Bedrohungsbilder und sicherheitsrelevanten Faktoren in der Informationstechnik ist ein Penetrationstest allerdings eher als Momentaufnahme zu begreifen. Im Extremfall kann ein System unmittelbar nach dem Beheben der durch den Test aufgedeckten Schwachstellen durch eine neue Sicherheitslücke wieder verwundbar sein. Allerdings deckt ein Test in der Regel auch die Ursachen auf, welche zu den festgestellten Problemen führen. Jedoch ist die Behebung der Ursachen in der Regel Sache des Betreibers der getesteten Systeme und Anwendungen. Maßnahmen zur Behebung reichen von besserer Betreuung der Systeme und deren Anwendungen bis hin zur Abschaltung oder zum Verkauf.

3.1.1 Erhöhung der Sicherheit. Bevorzugt werden Penetrationstests in Auftrag gegeben mit dem Ziel, die Sicherheit der technischen Systeme zu erhöhen. Hierbei beziehen sich die Tests meistens nur auch technische Aspekte, Themenbereiche wie organisatorische beziehungsweise personelle Infrastruktur werden selten betrachtet.

3.1.2 Identifikation der Schwachstellen. Im Unterschied zu den anderen Zielen ist die Identifikation hier als Entscheidungskriterium das direkte Ziel des Penetrationstest. So kann beispielsweise vor dem Zusammenschalten zweier Netzwerke geprüft werden, ob ein Eindringen von außen möglich ist. Falls dies durch einen Penetrationstest nachgewiesen wurde, können Maßnahmen zur Sicherung ergriffen werden.

3.1.3 Erhöhung der organischen Sicherheit. Eine weitere Besonderheit eines Penetrationstests ist, dass dieser auch die organisatorische sowie die personelle Infrastruktur testet. Hierbei können die Qualität sowie die Einhaltung der Sicherheitsrichtlinien getestet werden.

3.2 Ansatzpunkte

Für Penetrationstests gibt es mehrere Möglichkeiten und Angriffspunkte. Typische sind Firewalls, Webserver RAS¹ Zugänge und Funknetze. Hierbei stellt die Firewall einen beliebten Angriffspunkt dar, da sie als Übergang zwischen Internet und Firmennetz dient.

3.3 Bedrohungen

Mittlerweile existieren viele Möglichkeiten, IT Systeme ihre Funktionsweise oder Unternehmen/Personen zu manipulieren beziehungsweise zu schädigen.

- **Social Engineering**
Hierbei handelt es sich um eine zwischenmenschliche Beeinflussung, bei der Menschen mithilfe von privilegiertem Wissen manipuliert werden, um somit sicherheitsrelevante Informationen zu erlangen. Hierbei kann es sich um Informationen wie Passwörter oder persönliche Daten handeln. Bei dieser Technik ist die Variationsmöglichkeit enorm hoch.
- **Umgehung physischer Sicherheitsmaßnahmen**
Die physische Absicherung der IT-Infrastruktur ist eine Grundvoraussetzung zur Gewährleistung der IT-Sicherheit. Falls einem Angreifer die Überwindung der physischen Maßnahmen gelingt, ist es nur eine Frage der Zeit, bis er diese ausnutzt, um zum Beispiel Daten zu manipulieren.
- **Netzwerk**
Hierunter versteht man Angriffe, welche unter Nutzung der Funktionalität von Netzwerkprotokollen auf Applikationen, Computer oder Systeme eingesetzt werden. Diese Methodik macht sich meist Schwachstellen in Soft- und Hardware zu nutzen. Hierbei handelt es sich häufig um Sniffing, DoS-Attacken, Session Hijacking oder Ähnliches.

4 DURCHFÜHRUNGSKONZEPT

4.1 Grenzen

Ein Penetrationstest alleine kann aufgrund der ständig neuen Schwachstellen nicht aussagekräftig als alleinige Referenz verwendet werden. Systeme, Applikationen sowie auch Angreifer entwickeln sich stetig weiter. So kann es sein, dass unmittelbar nach einem Penetrationstest bereits eine neue Schwachstelle auf den überprüften Systemen aufgekommen ist. Dennoch ist ein

¹Remote Access Service

Penetrationstest keinesfalls nutzlos, dieser kann zwar auch bei gründlicher Durchführung keinen absoluten Schutz bieten, sie reduziert aber die potentielle Gefahr eines Angriffs beträchtlich. Daher ist es zu empfehlen, regelmäßige Penetrationstests anzusetzen, um der Verfügbarkeit der Wirkung entgegenzuwirken. Ebenfalls gilt es zu beachten das ein Penetrationstest keine weiteren Maßnahmen wie Sicherheitsprüfungen, Richtlinien und Konzepte ersetzen kann. Ein Penetrationstest ist als Erweiterung der Sicherheitsmaßnahmen zu betrachten.

4.2 Rechtliches

Bei einem Penetrationstest muss penibel darauf geachtet werden, dass man sich zu jedem Zeitpunkt seines Handelns auf der Seite des Gesetzes aufhält und nicht Widerrechts handelt. Wesentlich lässt sich diese rechtliche Überlegung in drei Punkte aufteilen:

- Rechtliche Überlegungen, die ein Unternehmen oder eine Behörde zur Durchführung eines Penetrationstests veranlassen bzw. motivieren können.
- Rechtliche Vorschriften und Grundsätze, die der Auftragnehmer während der Durchführung eines Penetrationstests beachten sollte und die im Vorfeld des Tests mit dem Auftraggeber geklärt werden sollten.
- Rechtliche Gesichtspunkte, die der Vertragsgestaltung zwischen Auftraggeber und Penetrationstester zugrunde liegen.

Genau genommen existieren keine Vorschriften / Gesetze, welche ein Unternehmen beziehungsweise eine Behörde dazu auffordern Penetrationstests zu veranlassen. Jedoch gibt einige "Richtlinien" welche einen dazu anhalten.

- der Handhabung der Sicherheit und der Verfügbarkeit von steuerrechtlich und handelsrechtlich relevanten Daten,
- des Umgangs mit personenbezogenen Daten,
- der Einrichtung und Ausgestaltung eines internen Kontrollsystems.

Als höchstes Ziel gilt es relevante Daten des Unternehmens, der Behörde bzw. der Organisationseinheit zu schützen. Daher ergreifen Unternehmen Maßnahmen, um die Verfügbarkeit, Vertraulichkeit sowie die Integrität der Daten sicherzustellen. Zu diesen Maßnahmen zählen u.a. Sicherheitskonzepte, Berechtigungskonzepte, Firewallkonzepte und viele mehr.

4.3 Klassifikation

Ein Penetrationstest muss nach mehreren Kriterien kategorisiert werden. Hierbei hat das BSI² mehrere Kriterien vorgeschlagen, diese werden unten aufgeführt. Es muss verschiedene Unterscheidungsmerkmale, wie bspw. den Umfang der geprüften Systeme, die Vorsicht bzw. die Aggressivität des Penetrationstests, charakterisieren. Dies dient einer effektiven Durchführung mit einem kalkulierten Risiko.

In Abbildung 1 ist eine mögliche Klassifikation nach Empfehlung des BSI dargestellt. Links sind die verschiedenen Kriterien aufgelistet, nach denen man den Penetrationstest unterscheiden kann. Rechts hingegen stehen die einzelnen Parameter der Kriterien.

Je nach Auftrag muss ein geeigneter Penetrationstest gewählt werden. Nicht alle Kombinationen ergeben einen sinnvollen Aufbau. Als Beispiel lässt sich hier der aggressive Test heranziehen, da dieser nur schlecht mit einer verdeckten Herangehensweise kombiniert werden kann. Folgend werden die sechs Kriterien erläutert.

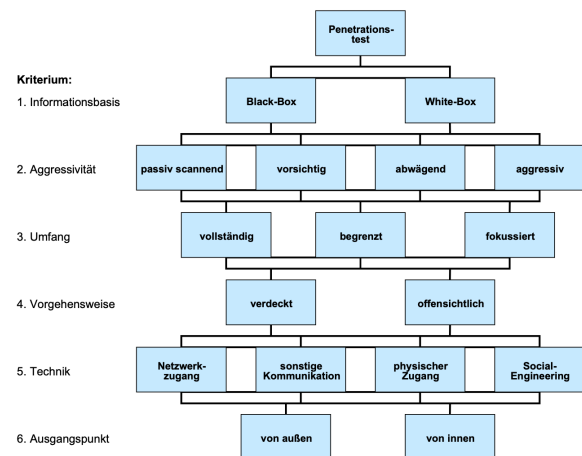


Abbildung 1: Klassifikation nach Kriterien[3]

(1) Informationsbasis

Welchen Wissensstand liegt dem Penetrationstester über das Netzwerk vor? Hierbei wird zwischen zwei Parametern unterschieden **Black-Box**-Test und dem **White-Box**-Test

(2) Aggressivität

Wie aggressiv soll der Penetrationstest durchgeführt werden. Hierbei muss zwischen den einzelnen Parametern differenziert werden.

²Bundesamt für Sicherheit und Informationstechnik

- Wenn man die niedrigste Aggressivitätsstufe ausgewählt wird, werden die Systeme und Strukturen nur "passiv" getestet. Hierbei können gefundene Schwachstellen evtl. nicht ausgiebig getestet werden.
- Bei der zweiten Stufe werden Schwachstellen nur untersucht, wenn eine Beeinträchtigung des Systems ausgeschlossen werden kann. Daher wird diese Stufe als "vorsichtig" betitelt.
- Hier wird versucht, "abzuwägen", ob die gefundene Schwachstelle eine Auswirkung auf das System darstellt. Hierbei betrachtet man die Erfolgchancen und deren Konsequenzen.
- In der Aggressivsten Stufe - "aggressiv" - werden alle gefundenen Schwachstellen ausgenutzt. Dabei muss bewusst sein, dass Beeinträchtigungen auftreten können.

(3) Umfang

Welche Systeme sollen getestet werden? Grundsätzlich ist eine genaue Analyse nötig, welche Systeme getestet werden. Dies dient dazu, dass keine Systeme übersehen werden oder doppelt behandelt werden. Generell unterscheidet man zwischen drei herangehensweisen. Zum einen die **fokussierte**, hierbei wird lediglich ein bestimmter Teil genauestens betrachtet, zum anderen der **begrenzte** hier wird eine begrenzte Anzahl von Systemen und Diensten untersucht. Zu guter Letzt gibt es noch den **vollständigen** Test, dieser überprüft alle erreichbaren Systeme.

(4) Vorgehensweise

Wie sichtbar geht man an den Penetrationstest? Hierbei muss die Frage geklärt werden, ob man neben den primären Sicherheitssystemen auch die sekundären Strukturen / Systeme überprüft.

- Zum Prüfen der sekundären Sicherheitssysteme verwendet man meist den **verdeckten** Penetrationstest. Dieser dient dazu in der Erkundungsphase nicht direkt erkannt zu werden und verhindert somit das direkte Enttarnen von Angriffsversuchen.
- Im Falle, dass die verdeckte Vorgehensweise keine Reaktion auslöst, kann man auch die **offensichtliche** Methode nutzen.

(5) Technik

Welche Techniken werden bei einem Penetrationstest angewendet? Häufig werden Systeme über

das Netzwerk angegriffen, jedoch gibt es auch weitere Möglichkeiten wie zum Beispiel ein Social-Engineering-Angriff oder andere physische Methoden.

- Der "klassische" Penetrationstest erfolgt über das **Netzwerk**. Häufig wird das TCP/IP-Protokoll verwendet. Hierbei spricht man von einem IP-basierten Penetrationstest.
- Es existieren aber noch **weitere Kommunikationsnetze**. Hierbei können Telefon-Netze bzw. auch drahtlose Netze etc. in Erwägung gezogen werden.
- Oftmals stellt es eine größere Hürde, in Systeme einzudringen, da zum Beispiel eine Firewall vorhanden ist. Heutzutage stellen Firewalls ein enorm hohes Sicherheitsniveau dar. Daher wird nach alternativen gesucht, um sich Zugang zu den gewünschten Systemen zu verschaffen. An dieser Stelle bietet sich der **physische Zugriff** oftmals als "einfacher / schneller" an.
- Oftmals ist es möglich in ein System / Netzwerk einzudringen indem man versucht das schwächste Glied in der Kette der Sicherungssysteme anzugreifen. Daher ist es eine beliebte Methode mittels **Social-Engineering**-Methoden den Mensch anzugreifen.

(6) Ausgangspunkt

Von wo wird der Penetrationstest durchgeführt? Hierbei muss man zwischen internen und externen Penetrationstests unterscheiden. Dabei handelt es sich um den Ausgangspunkt an welchem der Penetrationstester sein Rechner in das Netzwerk hängt.

- Die meisten Angriffe erfolgen über extern. Dies bedeutet über das öffentliche Internet. Daher ist es einem Penetrationstest möglich, dieses Ausgangsrisiko zu bewerten. Häufig werden hier Firewalls und Systeme in der DMZ³ betrachtet.
- Ist es dem Angreifer möglich, einen Angriff innerhalb eines Systems zu starten / durchzuführen, kann bewertet werden ob und wie es möglich ist intern in die Netze vorzudringen.

³Demilitarisierte Zone

4.4 Organisatorische Voraussetzungen

Im Vorfeld eines Penetrationstests sind mehrere Dinge zu beachten beziehungsweise gewisse Voraussetzungen einzuhalten. Wenn man diese Voraussetzungen abgeleitet aus dem Durchführungskonzept betrachtet ergeben sich folgende Fragestellungen:

- Wer ist direkt oder indirekt vom Penetrationstest betroffen?
- Sind haftungsrechtliche Risiken angemessen berücksichtigt?
- In welchen Zeitraum finden die Penetrationstests statt?
- Wie verhalten wir uns im Falle eines Systemausfalls?
- Welcher Aufwand ist mit dem Penetrationstest verbunden?

5 DIE PHASEN

Grundlegend lässt sich ein Penetrationstest in fünf Phasen einteilen. Dabei werden die Schritte die bei einem Penetrationstest durchgeführt werden aufgeteilt und betitelt. In Abbildung 2 sind die fünf Phasen und deren

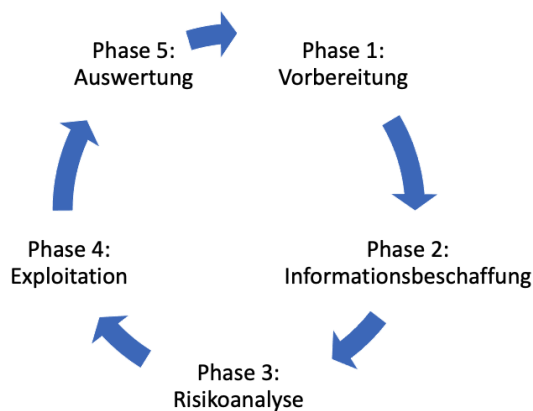


Abbildung 2: Phasen eines Penetrationstest

Zusammenhang dargestellt.

5.1 Reconnaissance / Vorbereitung

Der erste Schritt ist zugleich einer der Wichtigsten. Hierbei handelt es sich um die Informationsbeschaffung, auch Reconnaissance genannt.

Hier unterscheidet sich ein sog. Script-Kiddie⁴ von einem Pentester.

Es ist, sich gründlich vorzubereiten, eine Abstimmung der Ziele des Penetrationstest ist von Bedeutung um auch die Vereinbarten Ziele des Penetrationstest zu erfüllen. Die Nichteinhaltung der klar definierten Ziele kann möglicherweise strafrechtliche und/oder zivilrechtliche Konsequenzen⁵ nach sich ziehen. Ebenfalls kann ein Nichteinhalten auch zum Ausfall eines Produktsystems führen. Es ist also enorm wichtig alle Risiken sowie den Rahmen der Durchführung eindeutig zu definieren und schriftlich festzuhalten. [4]

5.2 Informationsbeschaffung

Da in der ersten Phase sowohl der Umfang, Ziele Vorgehen und Notfallmaßnahmen etc. festgelegt wurden, kann in diesem Schritt mit der Beschaffung von Informationen über das definierte Ziel begonnen werden. Hierbei gilt es zu versuchen eine möglichst detaillierte Aufstellung zu erstellen. Diese Phase wird auch als "Passiver Penetrationstest" bezeichnet. Ebenso wird hier versucht potentielle Angriffspunkte bzw. bekannte Schwachstellen zu erlangen. Abhängig von der Größe des Netzwerks bzw. der Anzahl der zu untersuchenden Objekte kann diese Informationsbeschaffung entsprechend Zeit beanspruchen.

Hier folgt ein kleines Beispiel: Ein Class-C Netzwerk (256 mögliche IP Adressen) wird hinter einer Firewall vollständig gescannt. So kann ein Portscan (65536 Ports), Tage bis Wochen in Anspruch nehmen.

Ferner bietet uns diese Phase eine genaue Übersicht verwendeter Dienste und Anwendungen, sowie möglicherweise deren Spezifikationen wie Versionsnummer, Betriebssystem, Umgebungsvariablen u.v.m.

⁴Ein Scriptkiddie ist ein Stereotyp, das sich alltagssprachlich auf Personen aus dem Bereich der Computersicherheit bezieht. Welche keine fortgeschrittenen Kenntnisse haben.

⁵siehe, 4.2 Rechtliches

5.3 Risikoanalyse / Bewertung der Informationen

Nun haben wir aus Phase 5.2 eine Vielzahl an Informationen. Um mit diesen Informationen ein erfolgreiches, nachvollziehbares und auch wirtschaftliches Ergebnis erzielen zu können, müssen die gesammelten Informationen bewertet werden um so deren Relevanz festzustellen. Die Bewertungskriterien müssen auf die vorab festgelegten Parameter und Ziele zutreffen. Durch diese Bewertung lassen sich die Herangehensweisen für die Phase 5.4 "Exploitation / Aktive Angriffe". Näher lässt sich dieser Schritt als eine Reduktion der Zielsysteme für Phase 5.4 "Exploitation / Aktive Angriffe"beschreiben. Die grundsätzliche Bewertung muss ausführlich begründet werden da diese Auswirkungen auf den restlichen Penetrationstest haben.

5.4 Exploitation / Aktive Angriffe

Anhand der in Phase 5.3 in Betracht gezogenen Bewertung der Schwachstellen werden schließlich die gewählten Systeme aktiv angegriffen. In dieser Phase steckt auch das höchste Risiko, da hier auch an produktiven Systemen gearbeitet wird. Daher muss in dieser Phase des "aktiven Angriffs "besonders sorgfältig und bewusst gearbeitet werden. Bei der Durchführung stellt sich nun heraus welche Schwachstelle wie "relevant "sind, beziehungsweise "tatsächliche "Risiken darstellen.

5.5 Bericht / Auswertung

Neben der Aufzeichnung der einzelnen Phasen wird zuletzt auch ein Abschlussbericht erstellt. Der Bericht dient zur Nachvollziehbarkeit der einzelnen Tests und der dadurch offen gelegten Schwachstellen garantieren. Diese Ergebnisse sollten abschließend in einem Abschlussgespräch erörtert und Maßnahmen daraus abgeleitet werden. Diese Maßnahmen sollten anschließend umgesetzt werden um somit das Potential der Schwachstellen zu entschärfen.

6 VORGEHENSWEISE

Folgend in Abbildung 3 wird das detaillierte vorgehen Schritt für Schritt der Phasen 1-5 niedergelegt. Jedoch muss man erwähnen, dass es trotz dem möglich ist das Szenarien auftreten, in denen sich diese Vorgehensweise nicht explizit anwenden lässt.

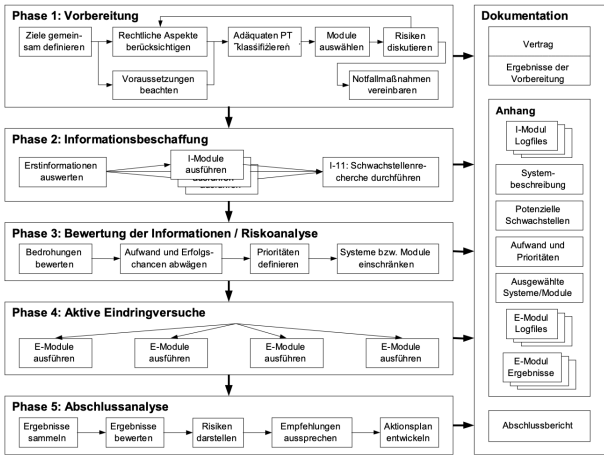


Abbildung 3: Vorgehensweise[3]

7 ABSCHLIESSEND

Abschließend lässt sich ein Penetrationstest sehr gut in eindeutige Phasen kategorisieren. Das ermöglicht einen standardisierten Prozess der Anwendung und legt auch den Grundstein für eine qualitative Durchführung sowie eine fundierte Bewertung des Ergebnisses. Wenn man sich an die Klassifikationen hält und die einzelnen Phasen durchführt sowie rechtlich alle Aspekte beachtet, steht einem erfolgreichen Penetrationstest nichts mehr im Weg.

Dennoch kann es zu Szenarien kommen, in denen eine Durchführung der Norm abweicht. Hierbei sollte man darauf achten, dass man sich bewusst ist, wie man handelt und sich deren Auswirkungen im Klaren sein. Das oben niedergelegte Durchführungskonzept ermöglicht es, einen Penetrationstest in kalkulierbarem Umfang umzusetzen und ein qualifiziertes Ergebnis zu erhalten. Die Gesetzen Kriterien und Strukturen sorgen für ein gleichbleibendes qualitatives Ergebnis. Ebenfalls wird es dadurch möglich vorab die Beeinträchtigung des alltäglichen Betriebs eingegrenzt. Durch den Bericht ist es dem Auftraggeber möglich Maßnahmen zu ergreifen um somit seine Systeme sowie sein Netzwerk gegenüber angriffen zu härten.

ABBILDUNGSVERZEICHNIS

1	Klassifikation nach Kriterien[3]	3
2	Phasen eines Penetrationstest	5
3	Vorgehensweise[3]	6

LITERATURVERZEICHNIS

- [1] Bundesamt für Sicherheit und Informationstechnik. Ein Praxis-Leitfaden für IS Penetrationstests, 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=3.
- [2] Michael Kofler uvm. *Hacking and Security*. Das umfassende Handbuch. Rheinwerk Computing, 2020. ISBN: 978-3-8362-7191-2.
- [3] Bundesamt für Sicherheit und Informationstechnik. Studie - Durchführungskonzept für Penetrationstests, 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3.
- [4] Penetrationtest Austria. DIE INFORMATIONSBESCHAFFUNG ODER RECON. URL: <https://www.penetrationtest-austria.at/penetrationtest-ablauf/reconnaissance/>.