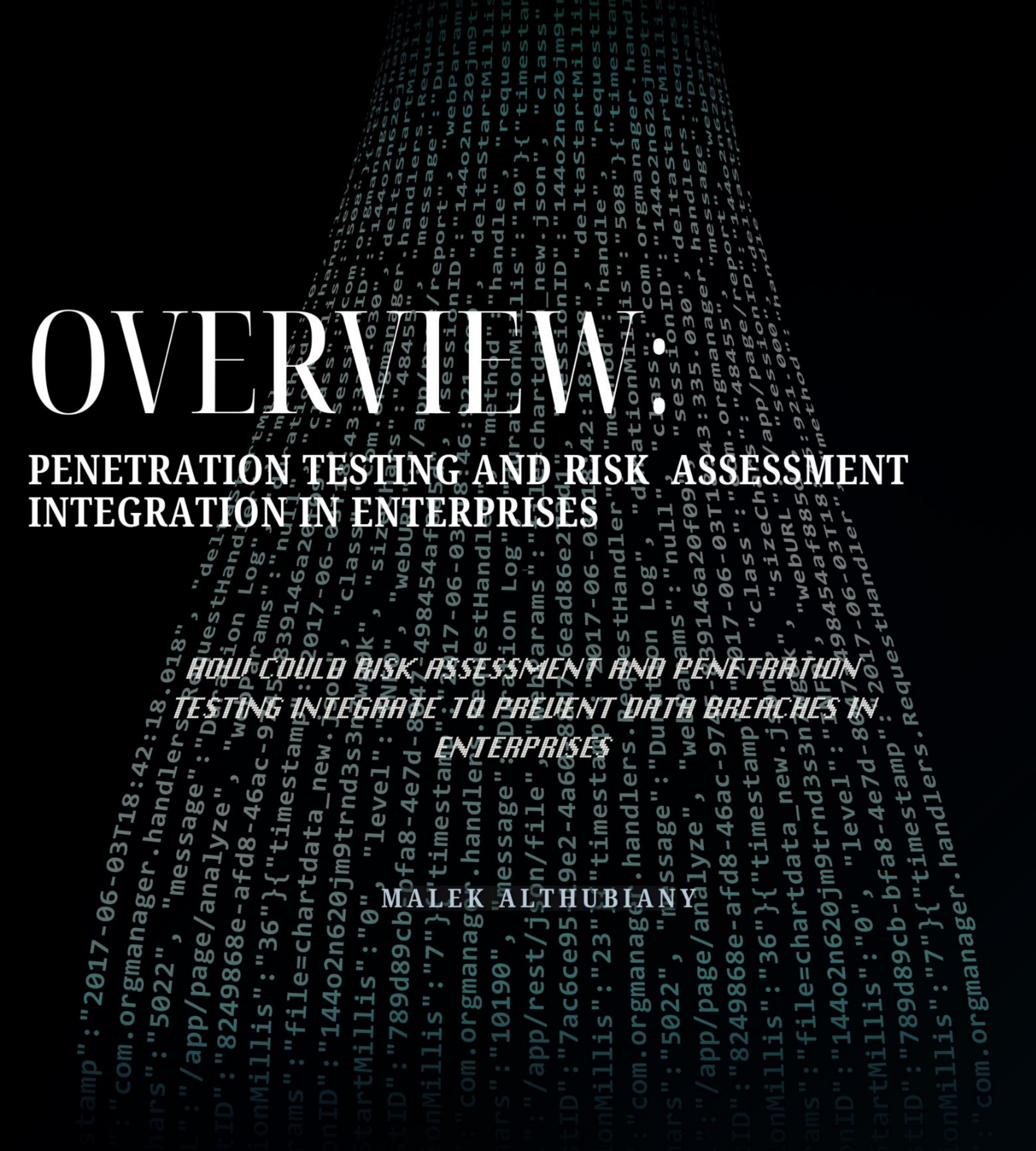


OVERVIEW:

PENETRATION TESTING AND RISK ASSESSMENT INTEGRATION IN ENTERPRISES

HOW COULD RISK ASSESSMENT AND PENETRATION TESTING INTEGRATE TO PREVENT DATA BREACHES IN ENTERPRISES

MALEK ALTHUBIANY

Table of Contents

Introduction

In today's ever-evolving digital landscape, safeguarding sensitive information and infrastructure from cyber threats has become paramount. This document discusses the critical importance of integrating infrastructure penetration testing and risk assessment as a comprehensive strategy to fortify defences against data breaches. Infrastructure penetration testing involves evaluating the security of an organization's network, systems, and devices by simulating cyberattacks. Conversely, risk assessment aims to identify vulnerabilities, evaluate their potential impact, and prioritize them based on their significance to the organization.

What is Penetration testing

Penetration testing, in its various forms such as infrastructure, cloud, network, web, API, and mobile, aims to expose vulnerabilities in systems. Infrastructure penetration testing, also known as network penetration testing, systematically assesses an organization's network and IT infrastructure. Its purpose is to identify security weaknesses that malicious actors could exploit. This testing simulates real-world cyberattacks to evaluate security measures and pinpoint areas needing improvement. Ultimately, it enhances an organization's IT infrastructure security, reducing risks like unauthorized access, data breaches, and cyber threats.

How to establish Penetration testing

When developing an infrastructure penetration testing checklist, it is critical to design testing efforts around identifying as many security gaps as possible. For maximum ROI on penetration testing, infrastructure pentest checklists should attempt to simulate the worst possible attack scenarios. To that effect, **there are two primary kinds of pentest to consider when planning**:

1. **Internal penetration testing:** Internal penetration testing involves simulating an attack from an insider.
2. **External penetration testing:** designed to discover and exploit vulnerabilities in hosts accessible via the Internet.

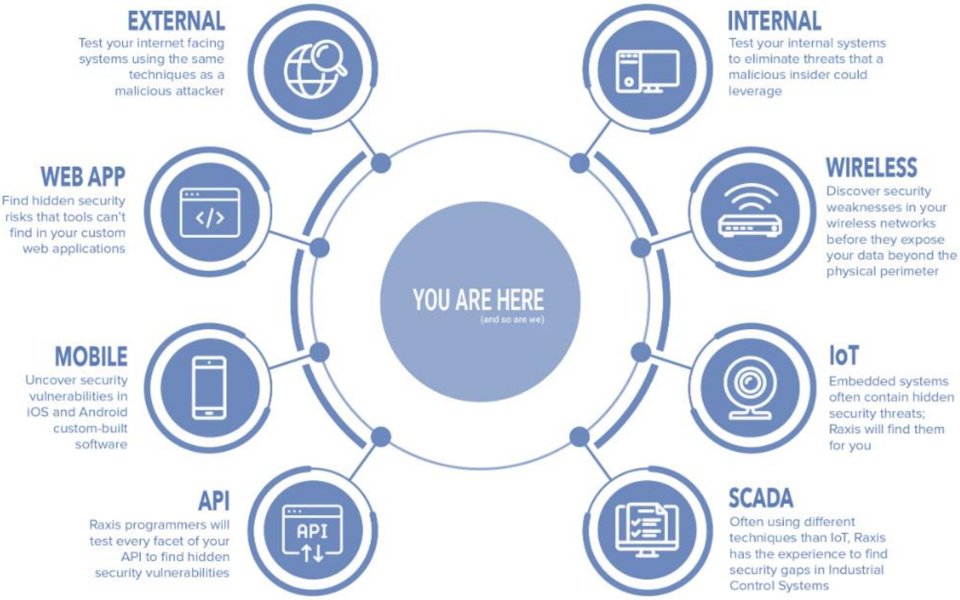
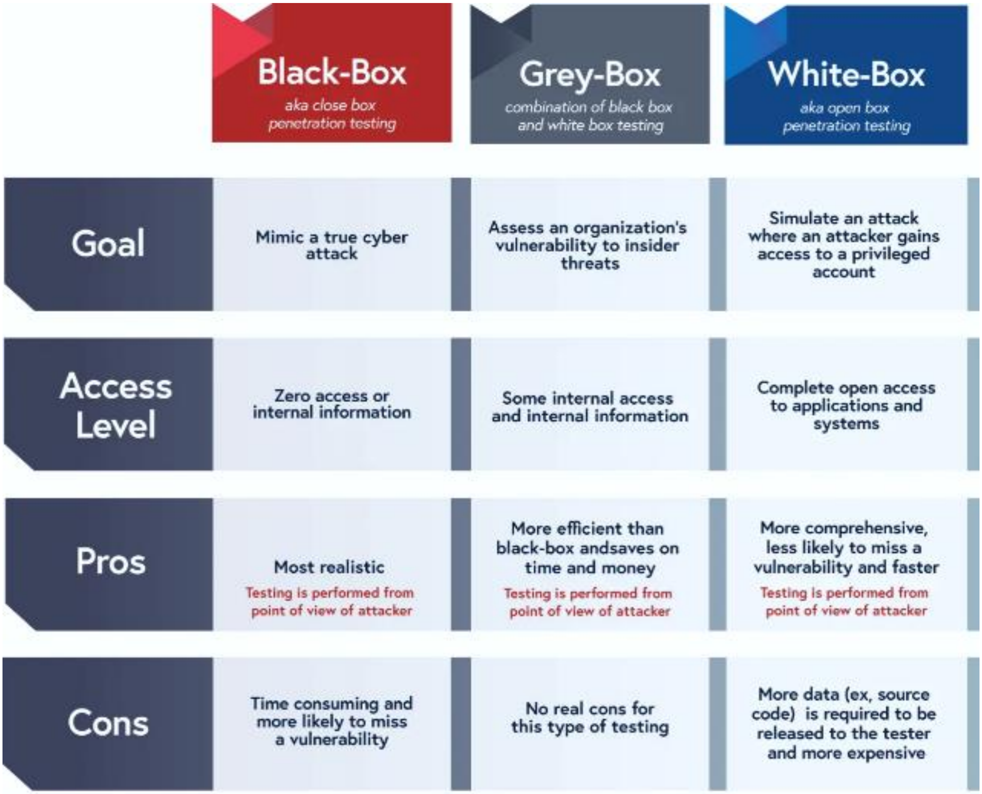

EXTERNAL
Test your internet facing systems using the same techniques as a malicious attacker
INTERNAL
Test your internal systems to eliminate threats that a malicious insider could leverage
WEB APP
Find hidden security risks that tools can't find in your custom web applications
WIRELESS
Discover security weaknesses in your wireless networks before they expose your data beyond the physical perimeter
YOU ARE HERE
(and so are we)
MOBILE
Uncover security vulnerabilities in iOS and Android custom-built software
IoT
Embedded systems often contain hidden security threats; Raxis will find them for you
API
Raxis programmers will test every facet of your API to find hidden security vulnerabilities
SCADA
Often using different techniques than IoT, Raxis has the experience to find security gaps in Industrial Control Systems

Figure 1 Types of Penetration testing

Types of testing method



	Black-Box aka close box penetration testing	Grey-Box combination of black box and white box testing	White-Box aka open box penetration testing
Goal	Mimic a true cyber attack	Assess an organization's vulnerability to insider threats	Simulate an attack where an attacker gains access to a privileged account
Access Level	Zero access or internal information	Some internal access and internal information	Complete open access to applications and systems
Pros	Most realistic Testing is performed from point of view of attacker	More efficient than black-box andsaves on time and money Testing is performed from point of view of attacker	More comprehensive, less likely to miss a vulnerability and faster Testing is performed from point of view of attacker
Cons	Time consuming and more likely to miss a vulnerability	No real cons for this type of testing	More data (ex, source code) is required to be released to the tester and more expensive

Figure 2 Types of testing method

The Penetration testing engagement process

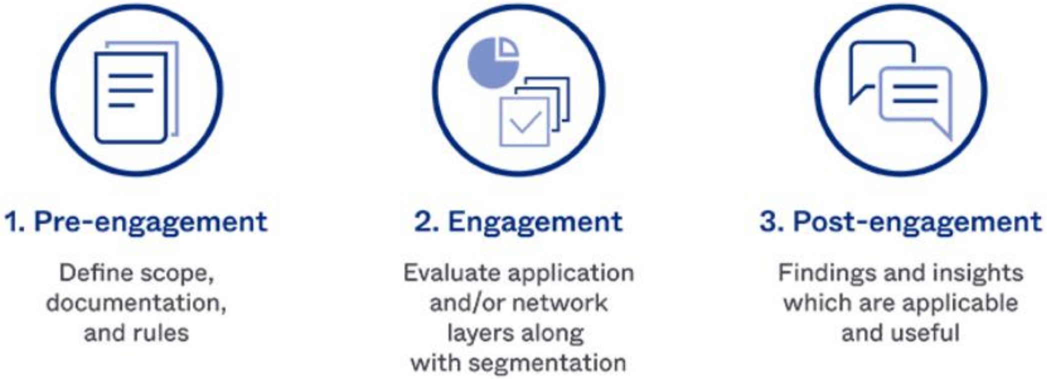

1. Pre-engagement
Define scope, documentation, and rules
2. Engagement
Evaluate application and/or network layers along with segmentation
3. Post-engagement
Findings and insights which are applicable and useful

Figure 3 Engagement process of Penetration testing

Scenario

Adding a penetration testing team to our risk assessment process for "Malek.com" is a smart move. Malek.com insists that their server is always up-to-date, claiming 100% certainty about it. While we appreciate their confidence, we know that sometimes things may not be as they seem. That's why it's crucial to bring in a penetration testing team that can dig deep into the website's security. These experts will use both manual and automated methods to give us an unbiased view of the server's condition. This way, our risk assessment will rely on solid, trustworthy information, helping us make firmed decisions about Malek.com's security. This step shows our dedication to thoroughness and ensuring the accuracy of our evaluations as a risk assessment decision maker.

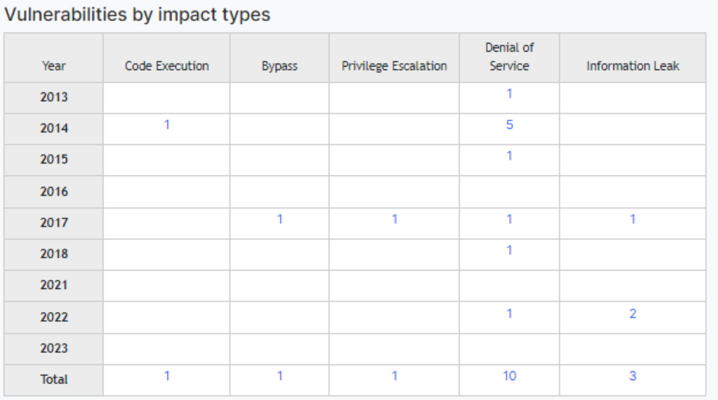
Penetration testing report

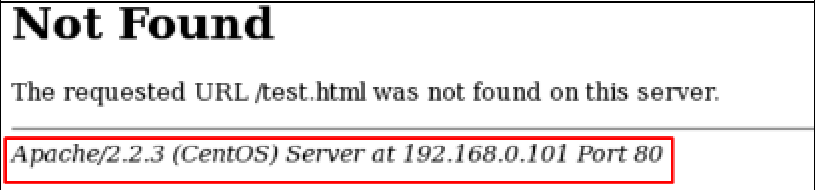
The scope details.

scope	Malek.com
deadline	30th of August
notes	if there any critical vulnerabilities don’t exploit it

Findings

Unpatched server has critical CVE’s.

<table>
<tr><td>Name</td><td>Unpatched server has critical CVE’s</td></tr>
<tr><td>Url</td><td>Malek.com/test.html</td></tr>
<tr><td>Impact</td><td>The unpatched server has several CVE’s which are an available source of exploitation that could harm the server and launch several attacks, such as DDoS, Auth by pass ..

Vulnerabilities by impact types
<table>
<tr><th>Year</th><th>Code Execution</th><th>Bypass</th><th>Privilege Escalation</th><th>Denial of Service</th><th>Information Leak</th></tr>
<tr><td>2013</td><td></td><td></td><td></td><td>1</td><td></td></tr>
<tr><td>2014</td><td>1</td><td></td><td></td><td>5</td><td></td></tr>
<tr><td>2015</td><td></td><td></td><td></td><td>1</td><td></td></tr>
<tr><td>2016</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2017</td><td></td><td>1</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>2018</td><td></td><td></td><td></td><td>1</td><td></td></tr>
<tr><td>2021</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2022</td><td></td><td></td><td></td><td>1</td><td>2</td></tr>
<tr><td>2023</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Total</td><td>1</td><td>1</td><td>1</td><td>10</td><td>3</td></tr>
</table>
</td></tr>
</table>

Steps to reproduce	1. Visit Malek.com/test.html 2. The unpatched version will be appeared
Remediation	Upgrade to the latest version
Screenshot	 Not Found The requested URL /test.html was not found on this server. Apache/2.2.3 (CentOS) Server at 192.168.0.101 Port 80
References	https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-403262/Apache-Http-Server-2.2.3.html

Risk Assessment integration

Risk assessment will be provided, and the Finding report will be demonstrated it by the penetration testing team. Risk assessment report a document that identifies and evaluates the potential hazards and threats that could affect a project, a process, or an organization in managerial level. Consistently conducting risk analysis also diminishes the exposure of the business to unforeseen circumstances. It contains several general steps to be followed:

How the risk assessment assesses the penetration testing?

After the Penetration testing is conducted and the vulnerabilities has been exposed in a **clear report on details.**

REF ID NO.	SUBMITTED BY	DATE SUBMITTED
1	Malek Althubiany	6th of September

RISK TYPE *select one*

	Financial	
	Legal / Contractual	
	Reputation / Customer Relations	
☒	Resources	
☒	Operational	
	Other:	

RISK DESCRIPTION

An unpatched server poses a significant and imminent threat to data security, as it could potentially pave the way for a data breach through an authentication bypass process. This vulnerability opens the door for cybercriminals to gain unauthorized access to sensitive systems and information, putting both clients and customers at risk.

SOURCE OF RISK

Apache server

PERSON(S) IMPACTED *check all that apply*

☒	Customers / Clients
	Employees
☒	Contractors
	Public

RISK IMPACT select *one*

	IMPACT LEVEL	DESCRIPTION
	NOT SIGNIFICANT	Negligible injuries not needing medical treatment
	MINOR	Minor injuries causing temporary impairment needing medical treatment
	MODERATE	Illness and/or injury requiring hospitalization
☒	MAJOR	Illness and/or injury resulting in permanent impairment
	SEVERE	Fatality

RISK PROBABILITY *select one*

	PROBABILITY LEVEL	DESCRIPTION
	HIGHLY UNLIKELY	Rare chance of an occurrence
	UNLIKELY	Not likely to occur under normal circumstances
	POSSIBLE	May occur at some point under normal circumstances
☒	LIKELY	Expected to occur at some point in time
	HIGHLY LIKELY	Expected to occur regularly under normal circumstances

RISK SEVERITY MATRIX *based on Impact and Probability Levels*

IMPACT x PROBABILITY	**NOT SIGNIFICANT**	**MINOR**	**MODERATE**	**MAJOR**	**SEVERE**
HIGHLY UNLIKELY	LOW	LOW	LOW / MED	MEDIUM	MEDIUM
UNLIKELY	LOW	LOW / MED	LOW / MED	MEDIUM	MED / HIGH
POSSIBLE	LOW	LOW / MED	MEDIUM	MED / HIGH	MED / HIGH
LIKELY	LOW	LOW / MED	MEDIUM	MED / HIGH	HIGH
HIGHLY LIKELY	LOW / MED	MEDIUM	MED / HIGH	HIGH	HIGH

RISK SEVERITY LEVEL *select corresponding Severity Level from matrix above based upon Impact and Probability Levels*

	SEVERITY LEVEL
	LOW
	LOW / MED
	MEDIUM
☒	MED / HIGH
	HIGH

CURRENT CONTROL MEASURES

Based on the existing policies controls within the corporate

FURTHER ACTION NEEDED? *select one*

☒	YES
	NO

ACTIONS TO IMPLEMENT if *applicable*

ACTION	ASSIGNED TO	DUE DATE	STATUS
UPDATE THE SERVER within certain amount of time (2 weeks)	Malek	15th of September	Pending

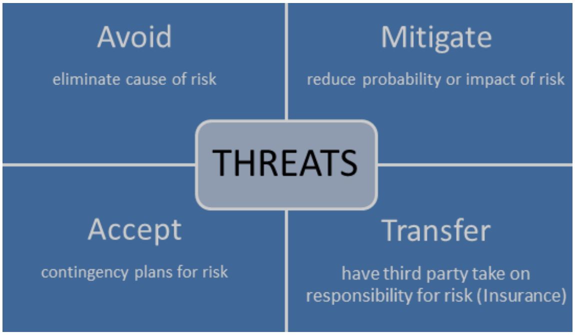

Avoid
eliminate cause of risk
Mitigate
reduce probability or impact of risk
THREATS
Accept
contingency plans for risk
Transfer
have third party take on responsibility for risk (Insurance)

Figure 3 Risk assessment response

The risk assessment report concludes respond that the mitigation action should be taken place to **risk owner.**

Conclusion

The integration of penetration testing into the risk assessment process is crucial for two main reasons: validating client statements and preventing data breaches. This integration combines **technical and managerial aspects**, with penetration testing uncovering vulnerabilities and risk assessment determining how to address them. This harmonization of technical expertise and strategic decision-making forms a strong defense mechanism for validating client claims and protecting valuable data assets.

References

- *Peraton Labs. Enterprise Risk Assessment (ERA) Process. Retrieved from https://www.peratonlabs.com/uploads/1/3/4/9/134979869/1222_360_enterprise_risk_assessment.pdf*

- *TechTarget. How to perform a cybersecurity risk assessment: Step-by-step. Retrieved from https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step*

- *RSI Security. Your Infrastructure Penetration Testing Checklist. Retrieved from https://blog.rsisecurity.com/your-infrastructure-penetration-testing-checklist/*

- *Raxis. Penetration Testing. Retrieved from https://raxis.com/pentest/*

- *Black-Box vs Grey-Box vs White-Box Penetration Testing from https://www.packetlabs.net/posts/types-of-penetration-testing/*