PENTESTING AND PENTESTING ON WINDOWS

13.03.2023

Grigoraș Ana-Maria

Application Security and Pentesting ILV mcr22

Dr. Gerald Emerick

INTRODUCTION

Over the years, the demand for penetration testing has grown significantly as organizations have recognized the need to protect against internal or external threats.

What is a penetration test?

A penetration test (or, for short, pentest) involves conducting an attack on a system in a controlled environment, with the sole intention of discovering security weaknesses and exploiting them safely, using them to access system data and its functionality. Thus, it can help determine a system's vulnerabilities, whether protection systems are adequate, and what defenses (if any) may have been bypassed by the pentest.

CONTENTS

Security issues discovered through penetration testing are reported to the system owner. These penetration test reports can also assess the potential impact on the company and come up with recommendations to mitigate the risks.

Thus, there is a specialized team of specialists in the field that tests the security of an IT infrastructure, having an approach similar to that of cybercriminals (hackers).

It is very important to test the security of an infrastructure, whether it is a website, an application, an online service, or an entire network of servers, services, and applications. The process involves identifying the target systems and the objective, then reviewing the available information and determining the means available to achieve the objective.

Obviously, there are several types of Penetration Testing, this one taking one of the following forms:

- **White Box** – when the specialists have inside information about what is in that network and where all the information related to the context and system is provided;

• **Black Box** – when the specialists attack the infrastructure starting from the minimum necessary information (in most cases only the IPs of the network) to be able to carry out the tests so that the information provided is basic or even not at all, except for the company name;

• **Gray Box** – a mix between the two, both white box and black box tests are performed.

Thus, usually, information security professionals use their ethical hacking expertise to detect weak points in the infrastructure configuration, defects in operating systems, services and applications used throughout the company, improper configurations, risky behaviors of users in the company, logic errors in application processes, weak login credentials that attackers can use for malicious purposes or Hijacking and many other details.

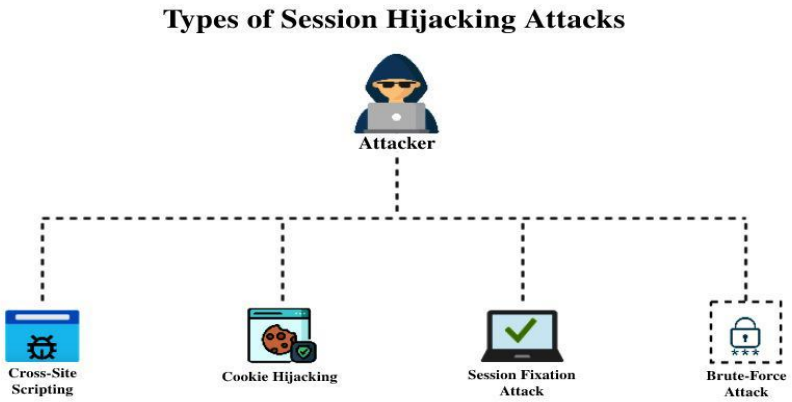


Figure 1 *Hijacking Attacks*

Note: Types of Sessions Hijacking Attacks. From **What are Types of Session Hijacking?** [Geeks for geeks], 31 August 2022,(https://www.geeksforgeeks.org/what-are-types-of-session-hijacking/)

Most of the time, those who do Penetration Testing, use various Open Source/Licensed tools that help to carry out complete tests more efficiently, plus the value being brought by the human interpretations and the subsequent tests that are done, based on the results obtained after the automatic analyses that are made.

Unfortunately, these applications, most of the time (especially if they are Open Source) are not compatible with the Windows operating system, Linux being the favorite OS to work within such scenarios. However, many people still use Windows. Therefore, one way to do Penetration Testing on Windows is with the help of ***Pentest Box***.

Pentest Box is a kind of *Kali Linux*, but exclusively for Windows. It manages to organize almost 100 Open Source applications and tools, which until now were mostly available only for Linux users, in categories such as web vulnerability scanners, web proxy, web crawling, tools used for information gathering, exploitation tools, wireless attacks, etc.

Advantages of Pentest Box

Pentest Box has several important advantages that make it even more attractive, namely: it can be used directly on the physical machine, without the presence of a virtual machine, can run on freshly installed Windows, has no special dependencies, can be customized, it also has an auto-updater and, most important, due to the lack of a virtual machine, it consumes only about 20 MB of RAM at launch and obviously, much less space on the Hard Disk, being able to be permanently available on a simple USB stick.

CONCLUSION

In conclusion, penetration testing represents one or a series of cyber attacks on a system with the aim of identifying its vulnerabilities and being useful for the following reasons:

- Determining the feasibility of a given set of attack vectors;
- Identify higher-risk vulnerabilities that result from a series of lower-risk vulnerabilities exploited in a certain order;
- Identifying vulnerabilities that may be difficult or impossible to detect using an automated network or application vulnerability scanning software;

• Evaluation of the potential impact on the business from an operational point of view in the event of attacks;

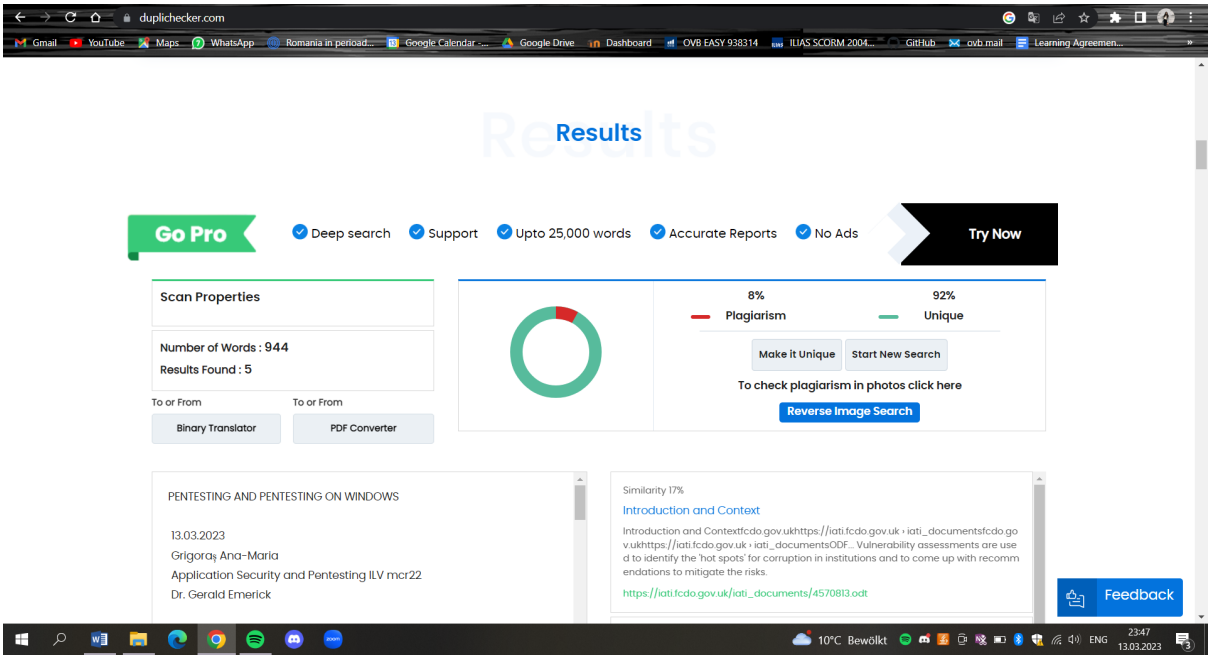
• Testing the ability of network protection measures to successfully detect and react to attacks;

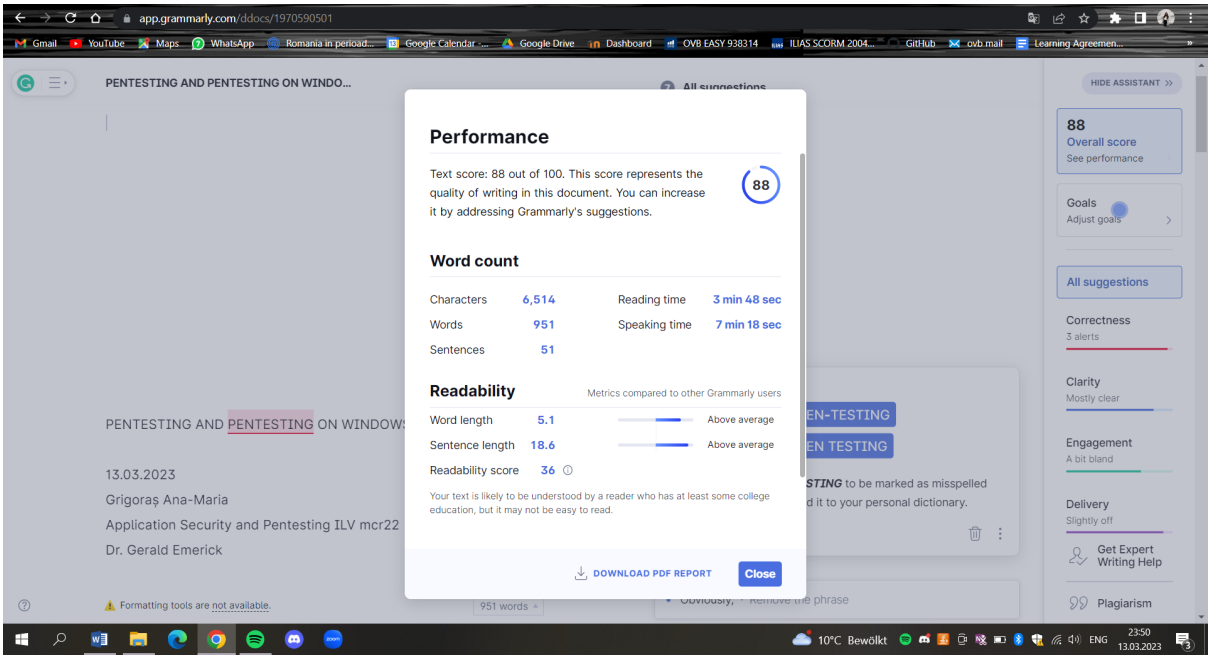
• Reporting system issues that provide arguments to support the decision to make increased investments in security personnel and technology.

Obviously, this does not change the fact that the one who uses this suite of IT security tools independently, must be a specialist in the field, master the advantages and way of working of these tools and, at the same time, his work must be legal. However, we should not forget that there are large companies that do IT security tests, and not only that, daily and their experience is welcome.

SOURCES

1. Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking.
2. Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.
3. Bit Sentinel. (n.d.). Ce Este Un Test De Penetration Testing? Retrieved from https://bit-sentinel.com/ro/ce-este-un-test-de-penetration-testing%E2%80%8B/
4. Avădănei, A. (2015, June 24). Cum poți face teste de securitate IT (Penetration Testing) folosind Windows? [Blog post]. WORLDIT.INFO. https://www.worldit.info/noutati/securitate-noutati/cum-poti-face-teste-de-securitate-it-penetration-testing-folosind-windows/
5. KPMG. (n.d.). Teste de penetrare şi protecţie cibernetică. Retrieved from https://kpmg.com/ro/ro/home/servicii/consultanta-afaceri/consultanta/securitate-cibernetica/teste-penetrare-securitate-cibernetica.html


duplichecker.com
Results
Go Pro
Deep search
Support
Upto 25,000 words
Accurate Reports
No Ads
Try Now
Scan Properties
Number of Words : 944
Results Found : 5
To or From
Binary Translator
To or From
PDF Converter
8%
Plagiarism
92%
Unique
Make it Unique
Start New Search
To check plagiarism in photos click here
Reverse Image Search
PENTESTING AND PENTESTING ON WINDOWS
13.03.2023
Grigoraș Ana-Maria
Application Security and Pentesting ILV mcr22
Dr. Gerald Emerick
Similarity 17%
Introduction and Context
Introduction and Contextfcdo.gov.ukhttps://iati.fcdo.gov.uk › iati_documentsfcdo.gov.ukhttps://iati.fcdo.gov.uk › iati_documentsODF... Vulnerability assessments are used to identify the 'hot spots' for corruption in institutions and to come up with recommendations to mitigate the risks.
https://iati.fcdo.gov.uk/iati_documents/4570813.odt
Feedback


app.grammarly.com/ddocs/1970590501
PENTESTING AND PENTESTING ON WINDO...
Performance
Text score: 88 out of 100. This score represents the quality of writing in this document. You can increase it by addressing Grammarly's suggestions.
88
Word count
Characters 6,514
Words 951
Sentences 51
Reading time 3 min 48 sec
Speaking time 7 min 18 sec
Readability
Metrics compared to other Grammarly users
Word length 5.1 Above average
Sentence length 18.6 Above average
Readability score 36
Your text is likely to be understood by a reader who has at least some college education, but it may not be easy to read.
DOWNLOAD PDF REPORT
Close
HIDE ASSISTANT
88
Overall score
See performance
Goals
Adjust goals
All suggestions
Correctness
3 alerts
Clarity
Mostly clear
Engagement
A bit bland
Delivery
Slightly off
Get Expert Writing Help
Plagiarism
PENTESTING AND PENTESTING ON WINDOWS
13.03.2023
Grigoraș Ana-Maria
Application Security and Pentesting ILV mcr22
Dr. Gerald Emerick
Formatting tools are not available.
951 words