Precious Machine Hack The Box

Whoami-Ga Company
Security Assessment Findings Report

Business Confidential

Project: 2
Version 1.0

Table of Contents

Confidentiality Statement

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

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(4 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 Precious 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 Windows	Administrator Precious SRL	558-558-5581

Assessment Overview

From 10-03-2023 to May 14-04-2023 Whoami-GA engaged Precious 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
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.

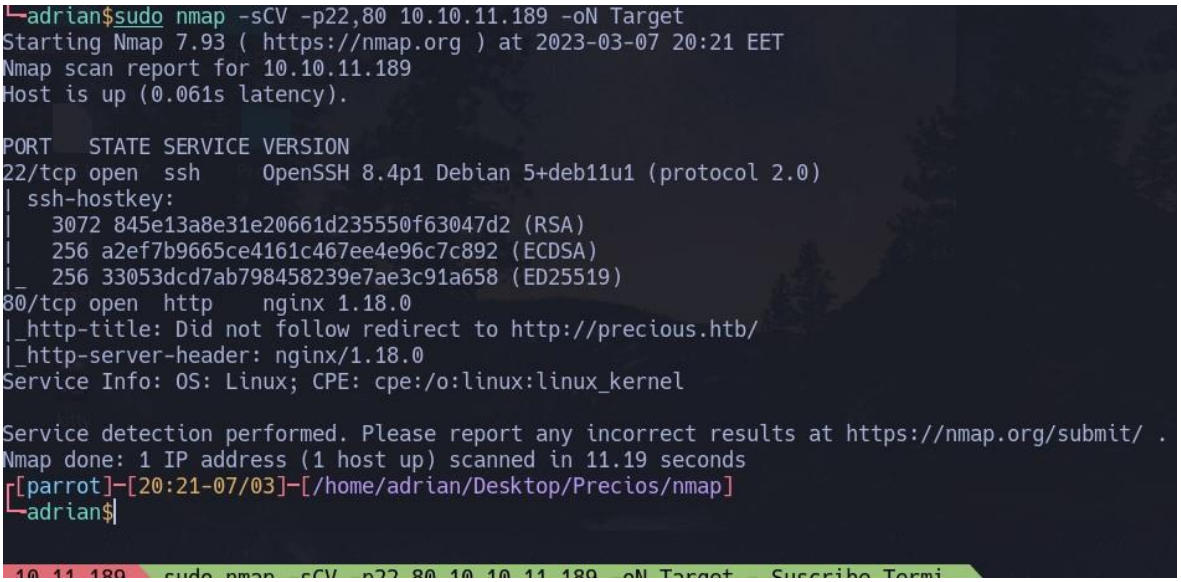
Scope

Assessment	Details
External Penetration Test	10.10.11.189

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

First contact

Precious.htb have active ports 22 fpt and 80 where a website is allocated.



1.0 External Penetration Test Findings

Description:	In your Website, you have the option to pass outsite any url into a pdf. we have chosen an example
Impact:	Critical
System:	10.10.11.198
References:	

Exploitation Proof of Concept

```
└─adrian$cat index.html
       File: index.html
   1   this is a test
┌[parrot]-[20:29-07/03]-[/home/adrian/Desktop/Precios/content]
└─adrian$sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.189 - - [07/Mar/2023 20:29:48] "GET /index.html HTTP/1.1" 200 -
```

Remediation

-

1.1 External Penetration Test Findings

Description:	We found that in your site generator you have a pdfkit v0.8.6 which is an older version. With CVE-2022-25765 pdfkit <0.8.6 command injection we were able to load an exploit to execute commands in your console.
Impact:	Critical
System:	10.10.11.198
References:	https://github.com/shamo0/PDFkit-CMD-Injection

Exploitation Proof of Concept

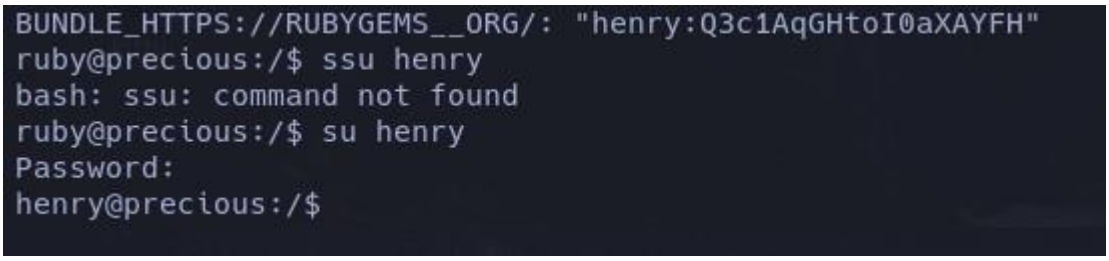
Remediation

Update the pdfkit and hide the metadata with a simple script.

1.2 External Penetration Test Findings

Description:	With a simple information leak we found a more privileged user (User Pivoting).
Impact:	Critical
System:	10.10.11.198
References:	RUBYGEMS

Exploitation Proof of Concept



Remediation

Never write your password into your computer or protect it with specially prepared programs such as keepass

1.3 External Penetration Test Findings

Description:	With a simple information leak we found a more privileged user (User Pivoting).
Impact:	Critical
System:	10.10.11.198
References:	

Exploitation Proof of Concept

Remediation

Never write your credentials into your computer or protect it with specially prepared programs such as keepas

1.4 External Penetration Test Findings(Privesc)

Description:	With a simple information leak we found a more privileged user (User Pivoting). With that we had greater control of the execution of commands like sudoers. which referenced a folder with no absolute destination folder which at the time we were root was modified to give us root access (chmod +s /bin/bash).

Impact:	Critical
System:	10.10.11.198
References:	Dependencies.yml

Exploitation Proof of Concept

```
User henry may run the following commands on precious:
    (root) NOPASSWD: /usr/bin/ruby /opt/update_dependencies.rb
henry@precious:/opt/sample$ cat /opt/update_dependencies.rb
# Compare installed dependencies with those specified in "dependencies.yml"
require "yaml"
require 'rubygems'

# TODO: update versions automatically
def update_gems()
end

def list_from_file
    YAML.load(File.read("dependencies.yml"))
end
```

```
/usr/lib/ruby/2.7.0/net/protocol.rb:458:in `system': no implicit conversion of nil into String (TypeError)
henry@precious:~$ bash -p
bash-5.1# whoami
root
bash-5.1#
```

Remediation

Every time you make a script, make sure you have an absolute path to the files to start and not a relative one.

Thank You ;)

Whoami-GA