Ex080 Report

Benjamin Ruddy

2022-10-27

Contents

Goal 2

Technical Report **2**
Introduction 2
Finding: *Weak and easily guessable user account password* 2
Severity Rating: 6.0 2
Vulnerability Description 2
Confirmation method 2
Mitigation or Resolution Strategy 3
Finding: *Default credentials on pfSense router admin panel* 3
Severity Rating: 6.0 3
Vulnerability Description 3
Confirmation method 3
Mitigation or Resolution Strategy 3

Attack Narrative **3**
User list creation 3
Password list creation 4
Password spraying, gaining access to OWA 4
Nmap of artstailor.com router 5
Pfsense panel + misconfiguration 5
Port forwarding rule 5
SUGGESTION FOR REMAINDER OF PENETRATION TEST . . 5
MITRE ATT&CK Framework TTPs 5

Goal

The goal in this exercise was to employ password spraying and its adjacent OSINT techniques to ultimately exploit a router misconfiguration and get remote access to a Windows host through a custom port-forwarding rule

Technical Report

Introduction

Finding: *Weak and easily guessable user account password*

Severity Rating: 6.0

This vulnerability puts a user's business email at risk.
CVSS Base Severity Rating: 4.3 AV:A AC:L PR:N UI:N S:U C:L I:L A:N

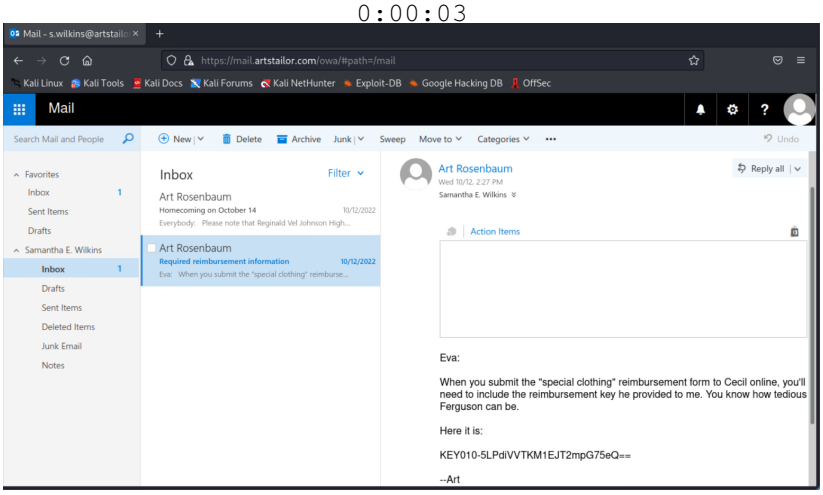
Vulnerability Description

On the `mail.artstailor.com` host, the user 's.wilkins' on the ARTSTAILOR domain has a password that is easily guessable and/or vulnerable to dictionary attacks using common wordlists. As a result, malicious actors may be able to gain access to their email account on the Microsoft OWA instance on the machine.

Confirmation method

Using `atomizer.py` from the *Password Spraying Toolkit*, one can create a password list combining seasons of the year along with year numbers to eventually spray arrive at valid credentials:

```
./atomizer.py <password_list> <user_list> --interval
                                0:00:03
```



Mitigation or Resolution Strategy

Prompt the user s.wilkins to change their password immediately to a more complex string, potentially with special characters and without common verb + year structure.

Finding: *Default credentials on pfSense router admin panel*

Severity Rating: 6.0

CVSS Base Severity Rating: 9.1 AV:A AC:L PR:N UI:N S:C C:H I:H A:N

Vulnerability Description

On the `innerouter.artstailor.com` host (public IP 217.70.184.3), the pfSense credentials for the admin account are unchanged from the default credentials of `admin:pfsense`. This is a crucial vulnerability because it allows attackers complete control over network traffic within the subnet, with attacks such as Man in the Middle and even logging in to unintended services such as RDP now being a possibility if an attacker finds the IP and port combination.

Confirmation method

Simply log on to 217.70.184.3 with the aforementioned credentials on a web browser, and you will now be in the administrator account for the router.

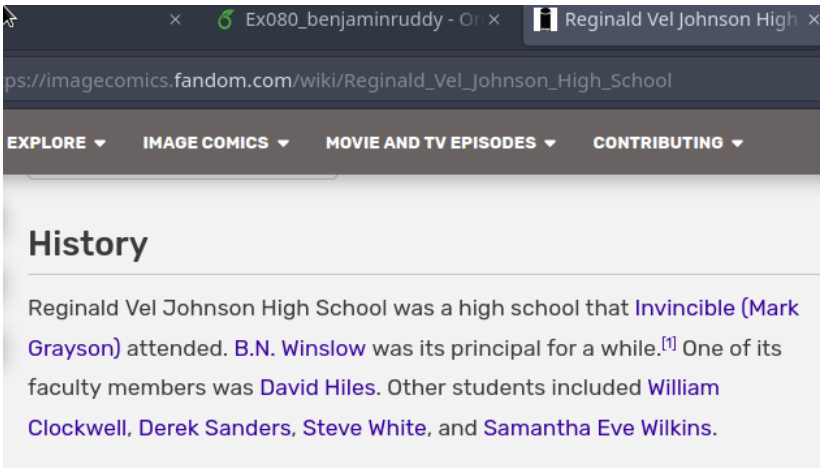
Mitigation or Resolution Strategy

Change the credentials for the administrator ASAP.

Attack Narrative

User list creation

With the OSINT gathered by Kory, we were able to arrive at the following list of students at Reginal Vel Johnson High School thanks to Google:



Knowing the likely format of the domain accounts (ARTSTAILOR first initial.last name), we compiled a list with the above names to use as a user list for password spraying.

Password list creation

To create the password list, some inspiration from the Password Spraying Toolkit GitHub repo was taken, in which they used a season of the year followed by the year number:

Password spraying, gaining access to OWA

With our user list and password list on hand, we launched the following command to spray against the OWA web application for Art's Tailor Shoppe:

```
./atomizer.py passwords.txt users.txt
https://mail.artstailor.com --interval 0:00:03
```

Nmap of artstailor.com router

Pfsense panel + misconfiguration

Port forwarding rule

SUGGESTION FOR REMAINDER OF PENETRATION TEST

MITRE ATT&CK Framework TTPs

TA0007: Discovery
- **T1046:** Network Service Discovery
  - **NA:** NA

TA0001: Initial Access
- **T1190:** Exploit Public-Facing Application
  - **NA:** NA