Ex080 Submission

Gary Jones

Contents

Executive Summary **2**

Project Overview 2

Goals 2

Risk Ranking/Profile 2

Summary of Findings 2

Recommendation Summary 2

Technical Report **2**

Introduction 2

Finding: 2

Risk Rating and Vulnerability Description 2

Confirmation method 3

Mitigation or Resolution Strategy 3

Attack Narrative **3**

Executive Summary

Project Overview

Goals

The goal of this exercise is to exploit the infrastructure misconfigurations of www.artstailor.com to gain access into the system.

Risk Ranking/Profile

Due to the findings made during testing the risk ranking is critical.

Summary of Findings

By utilizing the sprayingtoolkit the tester was able to identify the username and password of an active user through https://mail.artstailor.com and then gain access to the remote desktop. In addition due to an open port on the innerouter the tester was able to gain access to the router settings and make modifications to the infrastructure configurations.

Recommendation Summary

Change the username and password for the pfsense homepage. It is through this that access was granted and modifications to the firewall was made.

Technical Report

Introduction

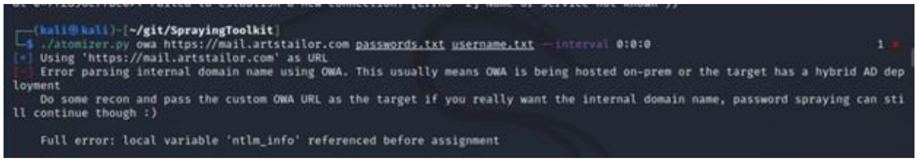
Finding:

Risk Rating and Vulnerability Description

The first risk is maintaining the default username and password on the pfsense login page. This allows external users to gain access to the system and change the settings on the firewall. Through this exploit testers did change the https configurations to RDP allowing remote desktop access. They also forwarded the connection from the innerouter to an unsecure port.

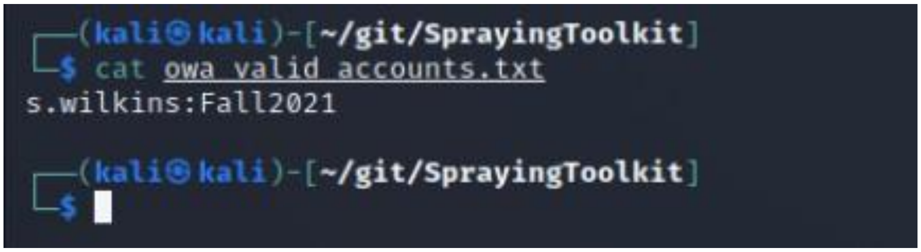
The second risk are the open ports on the artstailor.com router which were found to be 443 and 8443. These ports worked in conjunction with the firewall change above to allow remote access to the system.

The third risk are the simple usernames and passwords being used for credentials on the site. By utilizing atomizer.py from SprayingToolkit the testers were able to find active user credentials.



```
┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ ./atomizer.py owa https://mail.artstailor.com passwords.txt username.txt --interval 0:0:0          1 ✗
[*] Using 'https://mail.artstailor.com' as URL
[-] Error parsing internal domain name using OWA. This usually means OWA is being hosted on-prem or the target has a hybrid AD dep
loyment
    Do some recon and pass the custom OWA URL as the target if you really want the internal domain name, password spraying can sti
ll continue though :)

    Full error: local variable 'ntlm_info' referenced before assignment
```

Figure 1:



```
┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ cat owa_valid_accounts.txt
s.wilkins:Fall2021

┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ █
```

Figure 2:

Confirmation method

The methodologies used in this penetration test were confirmed utilizing rdesktop to the compromised system and utilizing the stolen credentials to gain access into the system.

Mitigation or Resolution Strategy

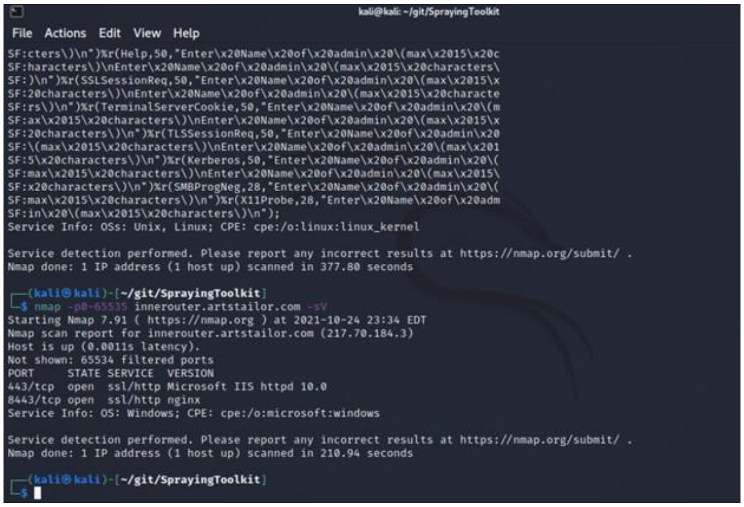
The first mitigation strategy is to not use the default credentials for pfsense. The second mitigation strategy is to force more complex username and passwords for users. Lastly, ports 443 and 8443 should be closed.

Attack Narrative

In order to begin valid credentials were sought for utilizing the SprayingToolkit through atomizer.py. Using this tool, and given the nature of the demographic involved, user names were predicated on the cast of Invincible which were saved in a username.txt file and with a series of simple passwords being saved in a passwords.txt file. This was run against https://mail.artstailor.com (see figure 1) and the credentials s.wilkins:Fall2021 was found to be valid (see figure 2).

Following this all open TCP ports were found with respect to the innerouter.artstailor.com domain thus identifying two potential openings into the system through port 443 and 8443 (see figure 3).

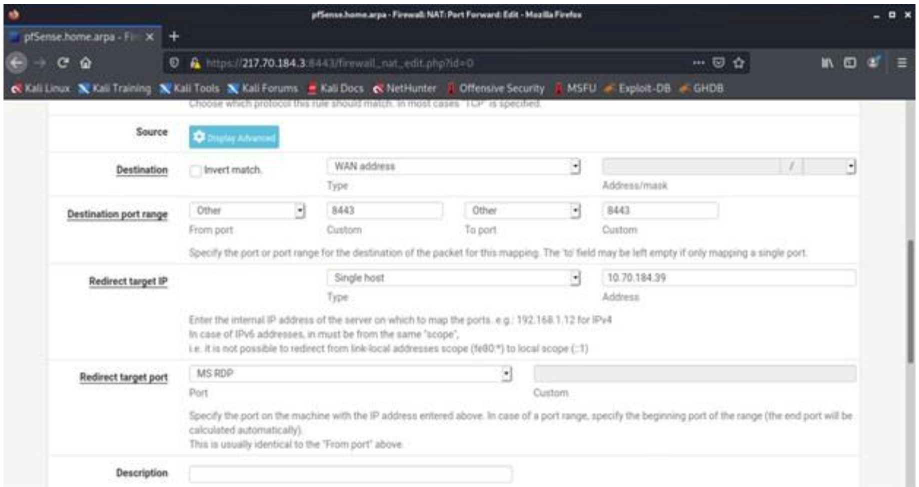
By going to the innerouter.artstailor.com IP on port 8443 the login to the firewall was accessed. By using the default username and password access was



```
SF:cters\)\n")%r(Help,50,"Enter\x20Name\x20of\x20admin\x20\(max\x2015\x20c
SF:haracters\)\nEnter\x20Name\x20of\x20admin\x20\(max\x2015\x20characters\
SF:)\n")%r(SSLSessionReq,50,"Enter\x20Name\x20of\x20admin\x20\(max\x2015\x
SF:20characters\)\nEnter\x20Name\x20of\x20admin\x20\(max\x2015\x20characte
SF:rs\)\n")%r(TerminalServerCookie,50,"Enter\x20Name\x20of\x20admin\x20\(m
SF:ax\x2015\x20characters\)\nEnter\x20Name\x20of\x20admin\x20\(max\x2015\x
SF:20characters\)\n")%r(TLSSessionReq,50,"Enter\x20Name\x20of\x20admin\x20
SF:\(max\x2015\x20characters\)\nEnter\x20Name\x20of\x20admin\x20\(max\x201
SF:5\x20characters\)\n")%r(Kerberos,50,"Enter\x20Name\x20of\x20admin\x20\(
SF:max\x2015\x20characters\)\nEnter\x20Name\x20of\x20admin\x20\(max\x2015\
SF:x20characters\)\n")%r(SMBProgNeg,28,"Enter\x20Name\x20of\x20admin\x20\(
SF:max\x2015\x20characters\)\n")%r(X11Probe,28,"Enter\x20Name\x20of\x20adm
SF:in\x20\(max\x2015\x20characters\)\n");
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 377.80 seconds

┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ nmap -p0-65535 innerouter.artstailor.com -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-24 23:34 EDT
Nmap scan report for innerouter.artstailor.com (217.70.184.3)
Host is up (0.0011s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE  VERSION
443/tcp  open  ssl/http Microsoft IIS httpd 10.0
8443/tcp open  ssl/http nginx
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.94 seconds

┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ 
```

Figure 3:

granted (see figure 5). From here the settings were changed from https to MS RDP to allow remote desktop access and a redirect target IP was implemented to IP address 10.70.184.39 (see figure 4) as hints suggested this domain enabled remote desktop access in the past. As a result of these changes, when a user performs the command rdesktop to the innerouter.artstailor.com IP address it gets redirected to the costumes.artstailor.com IP address thus allow user access into the system.



Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination ☐ Invert match. WAN address (Type) / (Address/mask)

Destination port range: Other (From port) 8443 (Custom) Other (To port) 8443 (Custom)

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP: Single host (Type) 10.70.184.39 (Address)

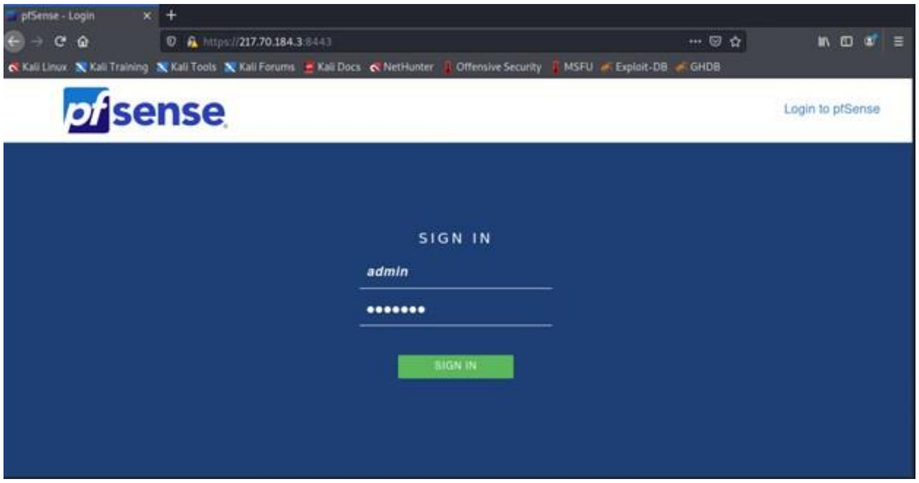
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port: MS RDP (Port) (Custom)

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

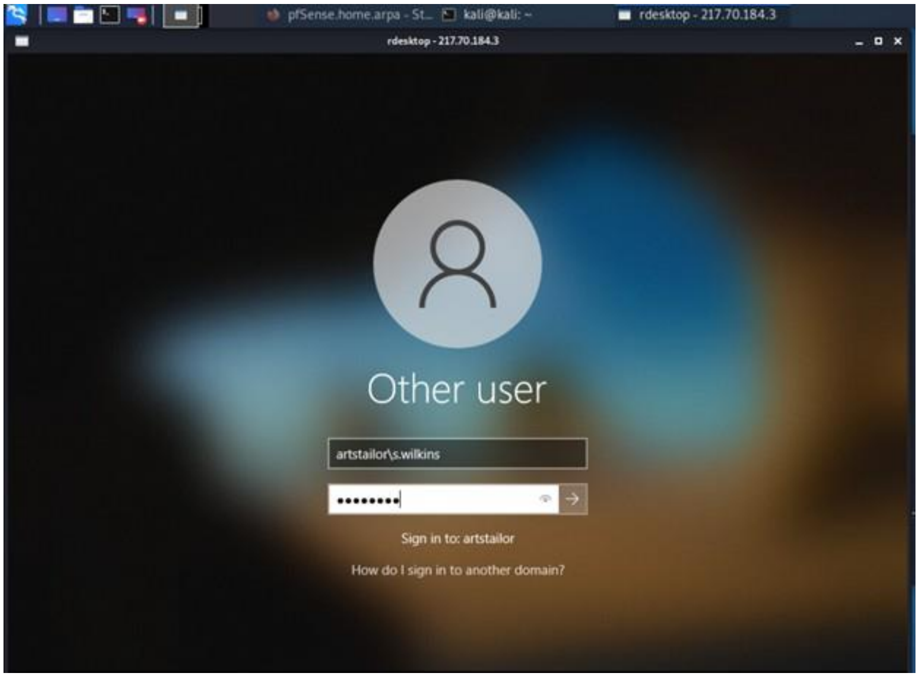
Description

Figure 4:



admin
•••••••

Figure 5:



Other user

artstailor\s.wilkins

••••••••

Sign in to: artstailor

How do I sign in to another domain?

Figure 6: