

Penetration Test Ex08

Esteban Calvo

2023-10-27

Contents

1	Technical Report	2
1.1	Finding: <i>User Credentials</i>	2
2	Attack Narrative	2
2.1	OSInt	2
2.2	Using Credentials to find Key	3
2.3	Port Forwarding	3
2.4	MITRE ATT&CK Framework TTPs	4
2.5	Temporary Internal Access to Artstailor	5

1 Technical Report

1.1 Finding: *User Credentials*

Severity Rating

High Risk: CVSS Base Severity Rating: 7.1 AV:L AC:L PR:N UI:R S:U C:H I:H A:N

Vulnerability Description

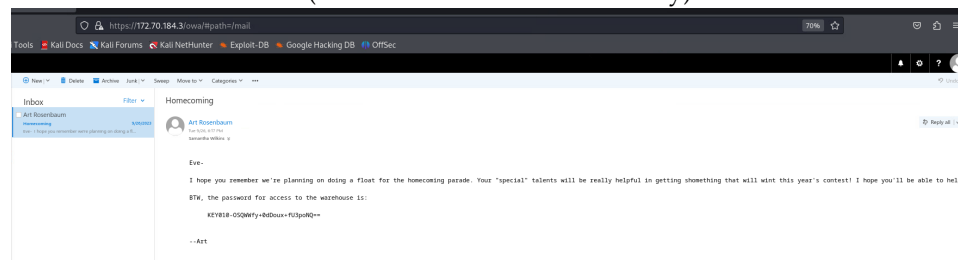
A password spraying method was used to find a list of possible user credentials for the internal email address. With a list of common passwords and some OSInt, I was able to access user emails and log on to the company email of one employee.

Confirmation method

Open port 443 in the browser with the following name

`https://172.70.184.3:443`

and enter the credentials (not included for confidentiality)



Mitigation or Resolution Strategy

Have all employees change their passwords and have some sort of company program to check passwords against list of commonly used hashes and other forms of password validation. If it is too easy for attackers to guess the password, it will be inevitable that an attack can access sensitive user information. The use of MFA could also be enforced to ensure an attacker would need more than just one attack vector.

2 Attack Narrative

2.1 OSInt

To get a list of usernames, Google was used to find some possible credentials for some internal emails. Googling "Arts Tailor Shoppe" revealed a wiki with

a list of superheroes and real names of some of the people Art makes costumes for. We are given the email "w.clockwell@artstailor.com", so I used this general structure with the list of superheros to compile a list of names that could be used. To generate the list of passwords, cewl as well as some generic commonly used passwords was used. The last step was putting it together and running the atomizer.py script as follows

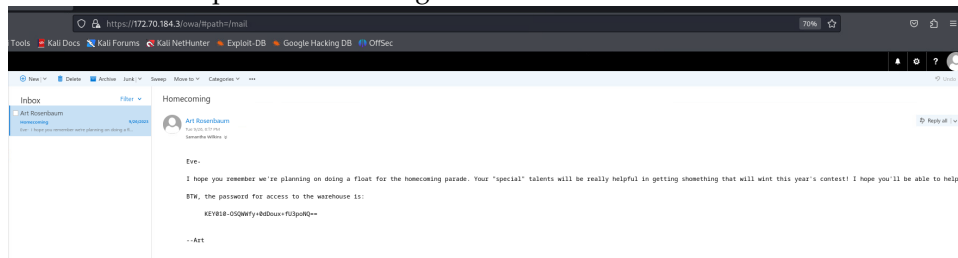
```
./atomizer.py owa https://mail.artstailor.com/owa/ passwords.txt users.txt --int
```

which revealed the credentials:

```
user: artstailor\s.wilkins
password: Spring2023
```

2.2 Using Credentials to find Key

After using nmap on mail.artstailor.com, we found that there were 2 different ports open, 443 and 8443 as well as the innerrouter IP of 172.70.184.3. Opening port 443 on the browser using the mail IP address, we were able to login to Samantha Wilkins email account. Once inside the email, I was able to see that there was only one email and this email as shown earlier included key 10. Once here, we also have access to send emails and monitor new emails on her account until the password is changed.



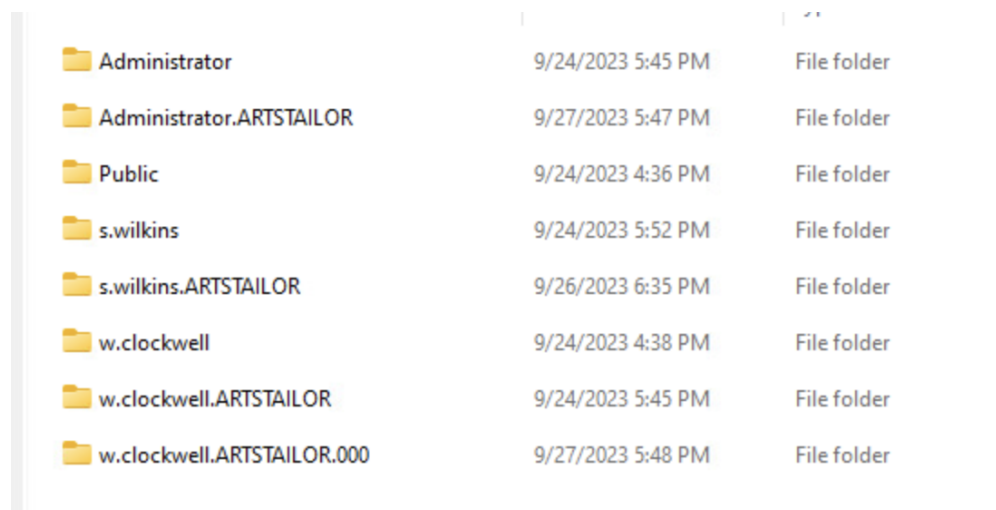
2.3 Port Forwarding









We are now able to open the other port we found available which was port 8443. On this port, we were able to access opnsense for artstailor innerrouter. The default credentials still seemed to work so using username root and password opnsense gave me access to write a new port forward for the network. Going to Firewall → NAT → Port Forwarding allowed me to forward the traffic coming in to innerrouter to the RDP port in the machine 10.70.184.0/24. In one of the earlier assignments, we found some of IPs on this network that were open and in particular the instructions mention costumes as being important so the router corresponding to costumes was used as follows:

<input type="checkbox"/>	WAN	TCP	*	WAN address	3389 (MS RDP)	10.70.184.39	3389 (MS RDP)
--------------------------	-----	-----	---	-------------	---------------	--------------	---------------

From here, using the following command gave me access to a remote desktop on the RDP port and using the credentials found earlier gave me access Samantha's desktop

```
rdesktop mail.artstailor.com
```



 Administrator	9/24/2023 5:45 PM	File folder
 Administrator.ARTSTAILOR	9/27/2023 5:47 PM	File folder
 Public	9/24/2023 4:36 PM	File folder
 s.wilkins	9/24/2023 5:52 PM	File folder
 s.wilkins.ARTSTAILOR	9/26/2023 6:35 PM	File folder
 w.clockwell	9/24/2023 4:38 PM	File folder
 w.clockwell.ARTSTAILOR	9/24/2023 5:45 PM	File folder
 w.clockwell.ARTSTAILOR.000	9/27/2023 5:48 PM	File folder

2.4 MITRE ATT&CK Framework TTPs

TA0043: Reconnaissance

T1593: Search Open Websites/Domains

.002: Search Engine

TA0006: Credential Access

T1110: Brute Force

.003: Password Spraying

TA0109: Lateral Movement

T0812: Default Credentials

TA0011: Command and Control
T1572: Protocol Tunneling

2.5 Temporary Internal Access to Artstailor

For the remainder of Penetration Testing, I would like access to the innerrouter network. I feel it is important to gain access to the router for several reasons. I believe it is important for configuration review to make sure client facing ports such as seen with the buffer overflow incident are better guarded against. I also think it is important I can conduct more internal vulnerability scanning and access to internal services. Lastly, I want more ability to monitor router traffic and make sure that all people on the router have adequate credentials. To make sure my access is secure, ensure that there is strong authentication such as MFA and also make it to where users on this router must be on the internal network or using a VPN.