#### **Alfred**

### **Enumeration**

- # we find a jenkins server running on port 8080
- # PAssword spraying worked and logged in with admin:admin

REASON

Supported Methods: OPTIONS TRACE GET HEAD POST

# We can now use the groovy script build console to get code execution on the machine

**VERSION** 

syn-ack ttl 125 Microsoft IIS httpd 7.5

#### **PortScan**

80/tcp open http

| http-methods:

PORT

STATE SERVICE

Potentially risky methods: TRACE

| http-server-header: Microsoft-IIS/7.5 | http-title: Site doesn't have a title (text/html). 3389/tcp open ms-wbt-server? syn-ack ttl 125 | rdp-ntlm-info: Target Name: ALFRED NetBIOS Domain Name: ALFRED NetBIOS\_Computer\_Name: ALFRED DNS\_Domain\_Name: alfred DNS\_Computer\_Name: alfred Product Version: 6.1.7601 System Time: 2021-12-21T09:41:12+00:00 | ssl-cert: Subject: commonName=alfred | Issuer: commonName=alfred | Public Key type: rsa Public Key bits: 2048 Signature Algorithm: sha1WithRSAEncryption Not valid before: 2021-12-20T09:28:12 Not valid after: 2022-06-21T09:28:12 | MD5: 6ad1 1f76 7156 4387 3801 f755 0629 34db | SHA-1: 3892 55fd f061 7f12 dff4 2564 6b8b 4bbc 15b9 f3ec | ----BEGIN CERTIFICATE-----MIICODCCAbigAwIBAgIQLdswxtO0QK9G6/ekHt0j/TANBgkqhkiG9w0BAQUFADAR MQ8wDQYDVQQDEwZhbGZyZWQwHhcNMjExMjlwMDkyODEyWhcNMjlwNjlxMDkyODEy WjARMQ8wDQYDVQQDEwZhbGZyZWQwggEiMA0GCSqGSlb3DQEBAQUAA4IBDwAwggEK AolBAQCpnDzn6YMf56JmJjarll92SkuBNeYAPpj2b2JeG3u1QBEzde/QFpVgwdHk | 5t9pocO3dzVoER1w0rGDYzgXTzmgb/euYqrrB3th6OwoeY8EY0x1o4KeWEG4wl0v QZuxXUfPkUj8p4OilK9Rls9tWTwHLPMlL4yzEp5zXEU2FQtcXO00zHS0uU4Npooa U9cjlJ2ZyuLxXgVze9QUZDGO2I68qDH66ALk6GdynpUe5YO4DnVfp2i5Ir4u/P4P vu/0ndvBMMkDZUcQ2V8OF93kbMNE9kq7kif8szl0cEi0O7XAIAVX4/0gDmqVK9zx e0R4Fi6vPFEXeAmMg4skJLklHvWnAgMBAAGjJDAiMBMGA1UdJQQMMAoGCCsGAQUF BwMBMAsGA1UdDwQEAwIEMDANBqkqhkiG9w0BAQUFAAOCAQEATd5u3uK80LtrkqFk tliSnkByB1ug7rWQd6MD2vt63Dj9uV1VY0Po9C9YhSkVOT0oj3IYb3SLph3WONX7 K17bOlvHEMAuwRxXUoy43sJG6dKSy5p7HoCi6833nr/4IO3koc23Dd1dNPzWdhyL 6sFQrh/80HkbRqJZzaxxALwpJ61/7VXknj/R2zMwP58BuVWxA9C2oKG58vRZufRD | +bvCIVrHoJyUf6Ohm9222nwnCs/YWZJP5GMwPzXK6AjfvfMnwggLeP5J48IfB+su | 8hFB88dHIYxiMI3QWm8F5+iJhr4GreX3Y79U3klOITIqwKqFDHdBHDLgQonDGivc | 2+9ifQ== | ----END CERTIFICATE-----\_ssl-date: 2021-12-21T09:41:19+00:00; -1s from scanner time. 8080/tcp open http syn-ack ttl 125 Jetty 9.4.z-SNAPSHOT

http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1

| http-robots.txt: 1 disallowed entry

| /

|\_http-server-header: Jetty(9.4.z-SNAPSHOT)

| http-title: Site doesn't have a title (text/html;charset=utf-8).

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|phone|specialized

Running (JUST GUESSING): Microsoft Windows 2008/7/Phone/8.1/Vista (90%)

OS CPE: cpe:/o:microsoft:windows\_server\_2008:r2:sp1 cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows\_7::sp1 cpe:/o:microsoft:windows cpe:/o:microsoft:windows\_vista::sp1 cpe:/o:microsoft:windows\_7: cpe:/o:microsoft:windows\_7

OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (90%), Microsoft Windows Server 2008 R2 or Windows 8 (90%), Microsoft Windows 7 SP1 (90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 or 2008 Beta 3 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8.1 (89%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%)

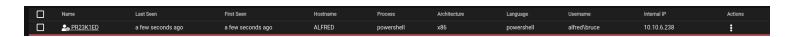
No exact OS matches for host (test conditions non-ideal).

### **Exploitation**

# We can use the jenkins groovy script build to get code execution



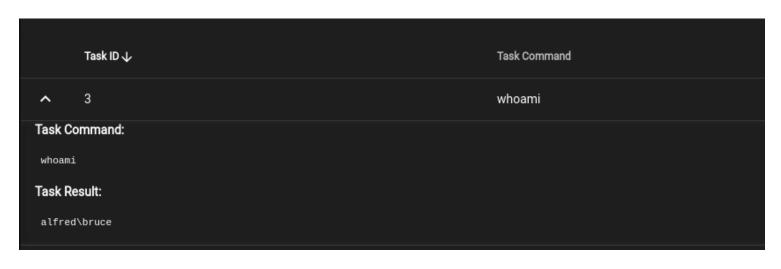
# we used empire launcher and listener to get a c2 infrastructure setup



# We got a agent back and now we can interact with the target machine

# **PostExploitation**

# we have interactive session with target



# we try to get a reverse shell because empire wasnt working stably

# whoami /priv showed that we can impersonate a user

SeManageVolumePrivilege	Perform volume maintenance		Disabled
GeImpersonatePrivilege GeCreateGlobalPrivilege	Impersonate a client after a Create global objects	autnentication	Enabled Enabled

# Got a msf session and impersonated administrator

#### Loot

### **Credentials**

# Flags

# user

79007a09481963edf2e1321abd9ae2a0

# System

dff0f748678f280250f25a45b8046b4a