BTRSys v1

Status	complete

+ Add a Property

Add a comment...

Figuring out the machine IP address

```bash
sudo netdiscover -r 192.168.99.0/24 -i eth1
```

Bash

Nmap Scanning on the IP address

```bash
nmap -Pn -e eth1 -oN nmap 192.168.99.105 nmap -Pn -p- -e
eth1 -oN nmap-all 192.168.99.105 nmap -A -sC -sV -p
21,22,80 -e eth1 -oN nmap-detailed 192.168.99.105
```

Bash

nmap-all 0.4KB

nmap-detailed 1.4KB

nmap 0.3KB

Possible network attack vectors and explanations

Name	Status	Reason
80 HTTP	exploited	Enumerated to get login.php and bypassed client side validations to use SQLi to get login and then use file upload to get reverse shell by bypassing the image upload limitations and then got passwords from mysql and SSHed into the server.

+ New

COUNT 1