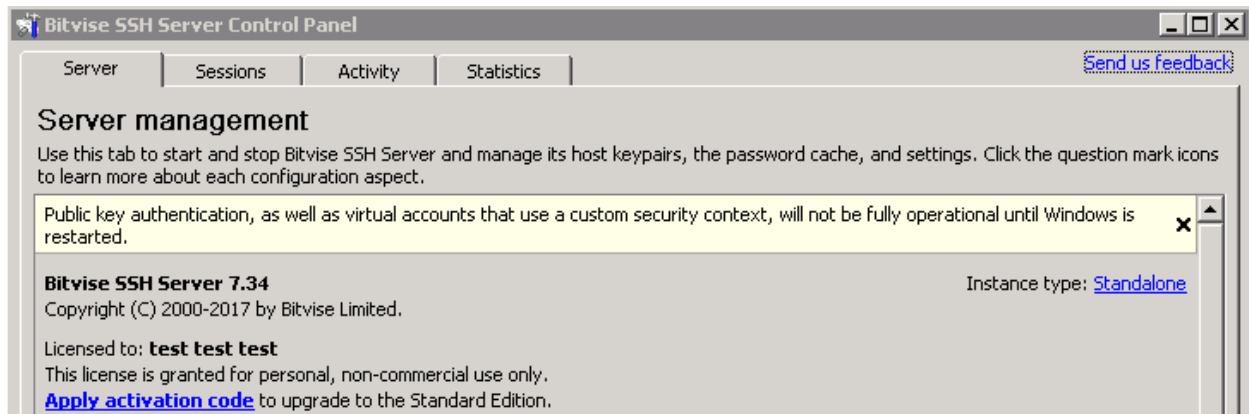


Proxychains with Windows machine

This document is walkthrough of how you go about setting up Proxychains via Windows box. This setup will eliminate the need to install your attacking tools on the remote Windows machine, instead you'll use your attacking machine (Kali Linux) tools locally and proxy all of your traffic via the Windows machine (pivot box). The following is step-by step guide:

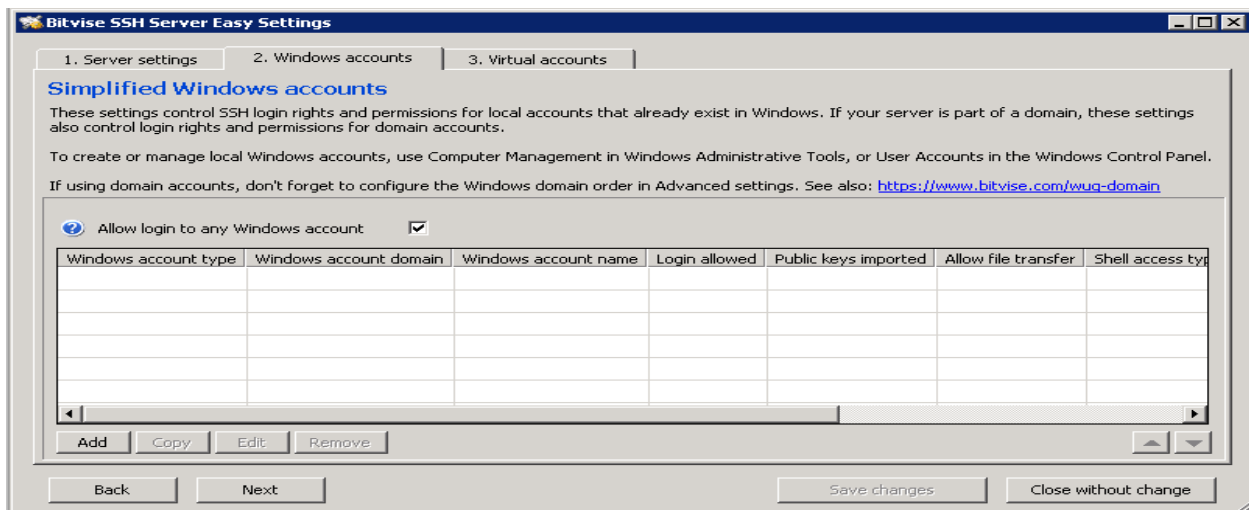
- Check if compromised Windows machine (pivot box) have SSH server up and running, if not go ahead and install [Bitvise](#) SSH Server (use default settings).



- Start Bitvise SSH Server service.



- Make sure you can SSH to that Windows box (In some cases you'd have to setup port forwarding).



- Setup SSH Dynamic on attacking machine that will listen on local port and forward traffic to the remote Windows box.

```
ssh -D <local_port> <remote_username>@<remote_IP>
```

- Setup Proxychains **“/etc/proxychains.conf”** on attacking machine to use local port from previous SSH Dynamic command.

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 <local_port>
```

- Now use can use Proxychains to run commands on Kali Linux that will automatically go through Windows box (pivot box). Here's couple of examples

```
proxychains nmap -p- -A -r -n --open -sT -Pn <IP_address>
```

```
proxychains nikto -h http://<IP_address>/
```

```
Proxychains dirb http://<IP_address>/ /usr/share/wordlists/dirb/big.txt
```