Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

IDP

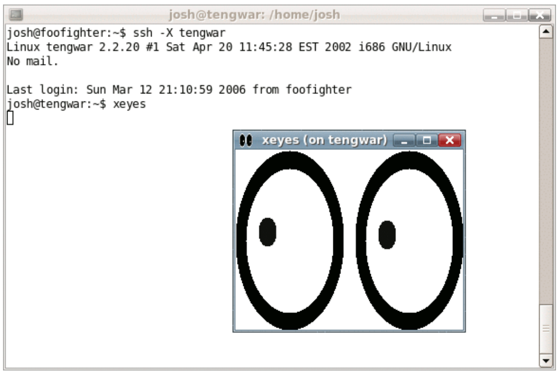
Revisiting SSH Security in the IPv{4,6} Internet

Motivation

Servers in the Internet are mostly administrated via the Secure Shell (SSH) protocol. The protocol allows to open a shell on a remote system, copy files securely and create encrypted tunnels. Therefore, the security of SSH is paramount to guarantee the correct working of server administration.

In 2014 two studies [a] [b] discovered wide-spread duplicate SSH server key usage due to low entropy and factory default keys. Additionally they found that servers were still vulnerable to Debian-weak and coprime-weak keys. The cryptographic properties of the servers was imperfect as well: SSH servers offer short keys, weak ciphers and broken hash algorithms.

The goal of this thesis is to conduct SSH scans to revisit the previously found security issues. Previous scans were performed using a combination of nmap and openssh. For performance reasons we want to move to ZMap and a module for goscanner which will be extended in the course of this thesis. Furthermore a service should be implemented to conduct these scans regularly.



```
josh@foofighter:~$ ssh -X tengwar
Linux tengwar 2.2.20 #1 Sat Apr 20 11:45:28 EST 2002 i686 GNU/Linux
No mail.

Last login: Sun Mar 12 21:10:59 2006 from foofighter
josh@tengwar:~$ xeyes
▯
```

CC BY-SA: https://commons.wikimedia.org/wiki/File:X11_ssh_tunnelling.png

[a] Gasser et al.: *A deeper understanding of SSH: results from Internet-wide scans.* NOMS 2014.

[b] Heninger et al.: *Mining your Ps and Qs: Detection of widespread weak keys in network devices.* USENIX Security 2014.

Your Task

- Research previous work on SSH scans and security evaluation
- Extend SSH feature in scanning framework written in Go
- Conduct scans, evaluate the results and compare with results from 2014
- Set up regular scanning service

Contact

Oliver Gasser gasser@net.in.tum.de

http://go.tum.de/306574