Using SSH Keys

Beth Lancaster
IT Security Office, Virginia Tech
blancast@vt.edu
GNFA, GCED, GCFA, GPYC, GCDA, GASF, GDSA

ITSO SOC

- IT Security Analyst
  - Network monitoring for malware
  - Vulnerability scanning
  - Forensics
  - Training / Education / Outreach
  - KnowledgeBase Articles
    - 4help.vt.edu search “ssh keys”
    - https://4help.vt.edu/sp?id=kb_article&sysparm_article=KB0012516
    - https://4help.vt.edu/sp?id=kb_article&sysparm_article=KB0012527

DEMO Details

- MacOS Version 10.15.7 (Catalina)
- VirtualBox Version 6.1.36
  - VBoxGuestAdditions
  - NAT Network
- Four VMs with Ubuntu 20.04.1
  - Local (192.169.80.9) – White background
  - Remote (192.168.80.10) – Cream background
  - BadActor (192.168.80.8) – Yellow background
  - Jump (192.168.80.11) – Blue background
- “util”

Connecting to a remote host

- Telnet
  - HTTP
  - High utility
  - Low (No) security
    - Network traffic in clear text
  - User credentials available from intercepted traffic

SSH
(Secure Shell)

- Created by Tatu Ylonen
- SSH1 1995
- SSH2 1998

SSH or Secure Shell

- Login credentials sent after a secure channel is established
  - ssh –Q KexAlgorithms
  - ssh –Q kex (MacOS)
- Network traffic is encrypted

SSH or Secure Shell

- Vulnerable to brute-force password guessing
- Password complexity rules may not be enforced
- Recovered user / password credentials
  - training:training
  - leo:leo
  - up:up

Using SSH Keys

- Public Key Authentication
- Asynchronous key pair
  - Private key on local host
  - Public key on remote host
- Algorithm options:
  - DSA: Older, not recommended
  - RSA with a key size of at least 4096 bits
  - ECDSA: *Maybe* not recommended
  - ED25519 / EdDSA

SSH Key Creation

- RSA: ssh-keygen –t rsa –b 4096
- ED25519: ssh-keygen –t ed25519
- Use a Passphrase when creating the key pair
- VT Password Complexity Ruleshttps://4help.vt.edu/sp?id=kb_article&sysparm_article=KB0010084
- ssh-copy-id –i ~/.ssh/ed_25519.pub

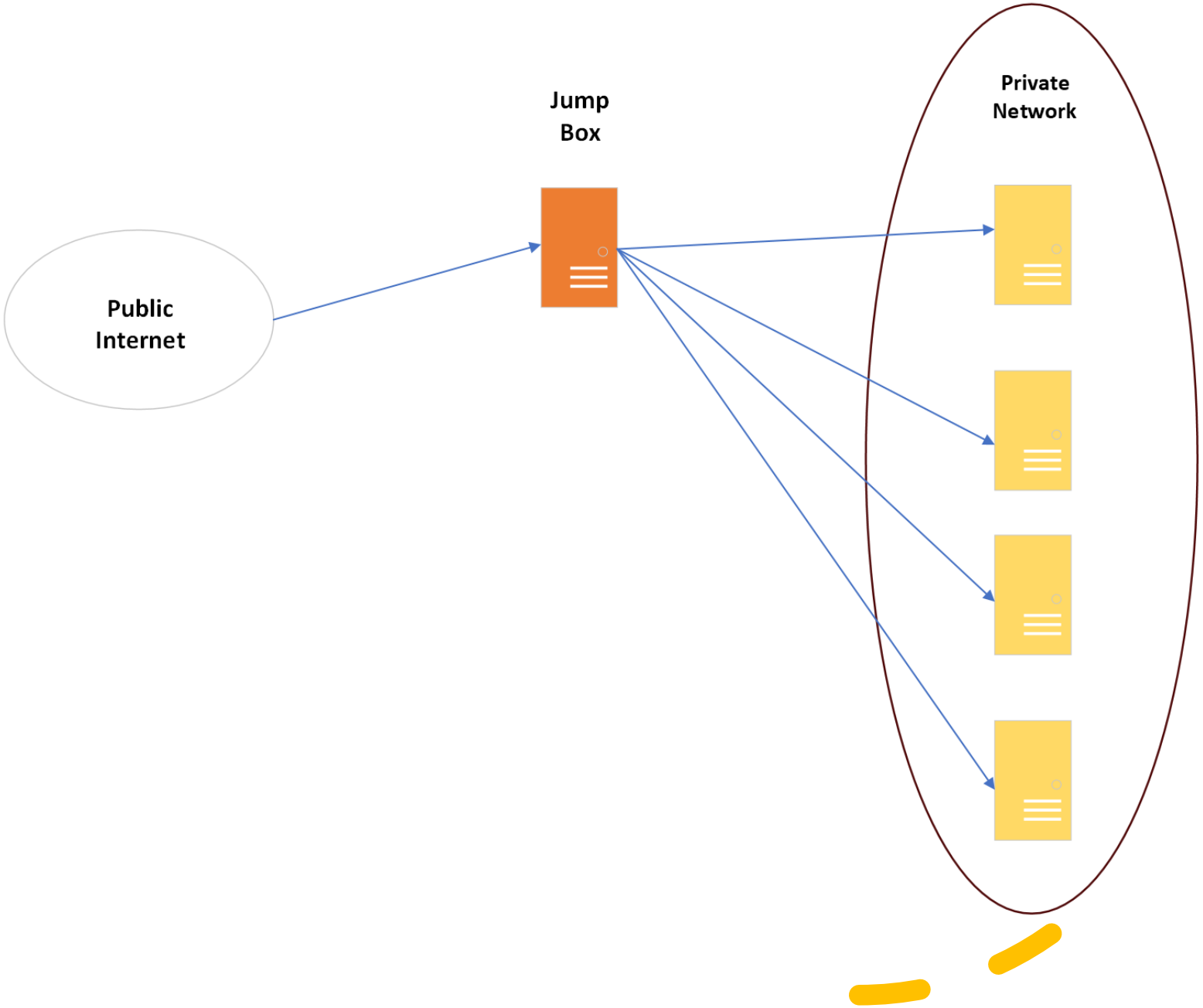
SSHD Config

- StrictModes yes
- PubkeyAuthentication yes
- ChallengeResponseAuthentication no
- PermitRootLogin no
- Banner /etc/ssh/sshd_banner
- TEST!
- PasswordAuthentication no
- TEST!
  - ssh -o PubkeyAuthentication=no

Benefits of Using SSH Keys

- Turn off PasswordAuthentication
- Fewer logs

Jump Box



Jump Box Config

- ~/.ssh/config

```
Host jump
    User hokie
    HostName 192.168.80.11
    PubkeyAuthentication yes
    IdentityFile ~/.ssh/id_25519

Host remote
    User hokie
    HostName 192.168.80.10
    ProxyJump jump
```

- ssh remote

SSHD_Config ED25519

- HostKey /etc/ssh/ssh_host_ed25519_key
- HostKeyAlgorithms ssh-ed25519-cert-v01@openssh.com,ssh-ed25519
- KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org
- Ciphers chacha20-poly1305@openssh.com
- MACs hmac-sha2-512-etm@openssh.com
- PubkeyAcceptedKeyTypes ssh-ed25519,sk-ssh-ed25519@openssh.com
- HostbasedAcceptedKeyTypes ssh-ed25519,sk-ssh-ed25519@openssh.com

Questions?

Beth Lancaster

IT Security Office, Virginia Tech

blancast@vt.edu

GNFA, GCED, GCFA, GPYC, GCDA, GASF, GDSA