PowerShell + DevOps Global Summit

Firewall Evasion and Remote Access with OpenSSH

Anthony E. Nocentino
Centino Systems

aen@centinosystems.com

@nocentino

Anthony E. Nocentino

Consultant and Trainer

Founder and President of Centino Systems

- Specialize in system architecture and performance
- Microsoft MVP - Data Platform - 2017-2018
- Linux Foundation Certified Engineer
- Microsoft Certified Professional

email: aen@centinosystems.com

Twitter: @nocentino

Blog: www.centinosystems.com/blog

Pluralsight Author: www.pluralsight.com

Agenda

- Background and SSH Basics
- Accessing Remote Resources
  - Proxying with Dynamic Port Forwarding
  - Tunneling with Local Port Forwarding
  - Tunneling with Remote Port Forwarding
  - SSH Based Multi-hop Jump Hosts
- Accessing Remote Networks
  - SSH Based VPNs
- Controlling and Preventing TCP Tunnelling

Background and Basics

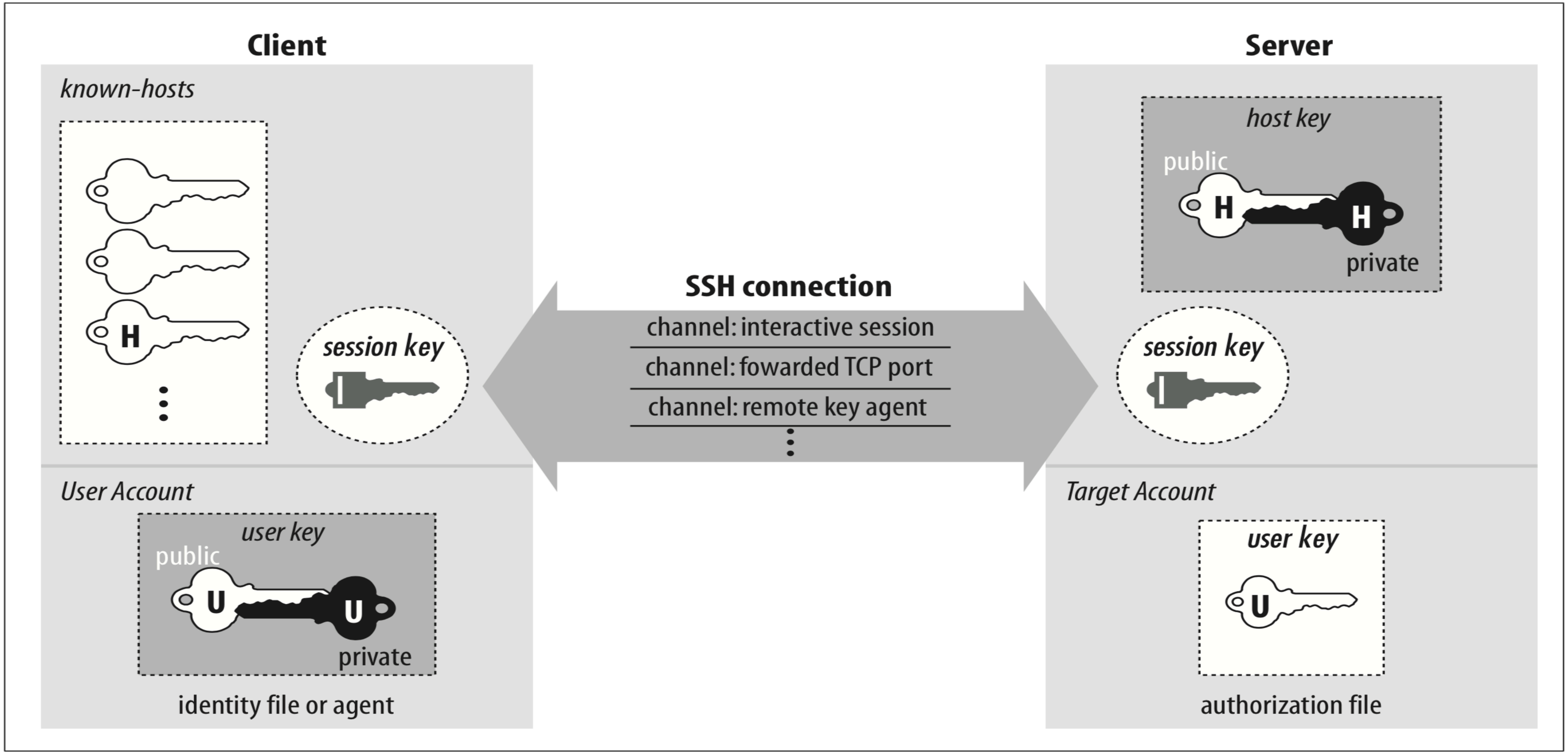
SSH is just for remote terminal access, right?

Key OpenSSH Functionality

- Secure client to server to communication
- Remote command execution
- Secure file copy
- **Tunneling of arbitrary TCP Services (firewall evasion)**
- Ensures remote system is who it says it is
- Message Integrity
- This is a transport layer for PowerShell Core Remoting!

OpenSSH Architecture

From: SSH, the Secure Shell
The Definitive Guide. O'Reily 2009



POWERSHELL + DEVOPS
GLOBAL SUMMIT

Accessing Remote Resources

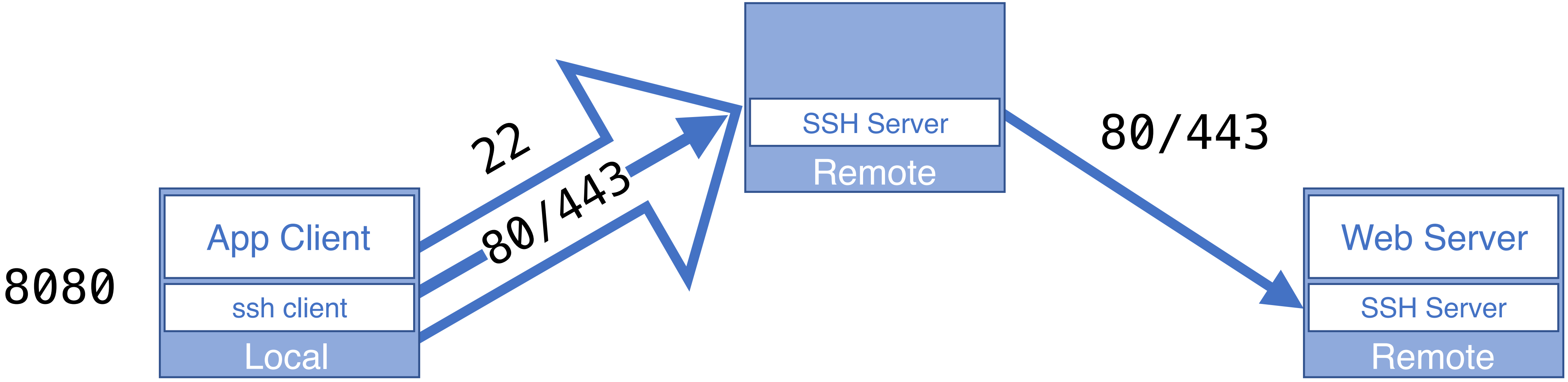
No one’s gonna suspect anything…

Proxying with Dynamic Port Forwarding

- Application level forwarding
- Uses SOCKS Protocol

Proxying with Dynamic Port Forwarding

- Local network doesn’t have Internet access
- Accessing Internet resources from trusted segments



```
ssh -D 8080 user@$REMOTE
```

DEMO

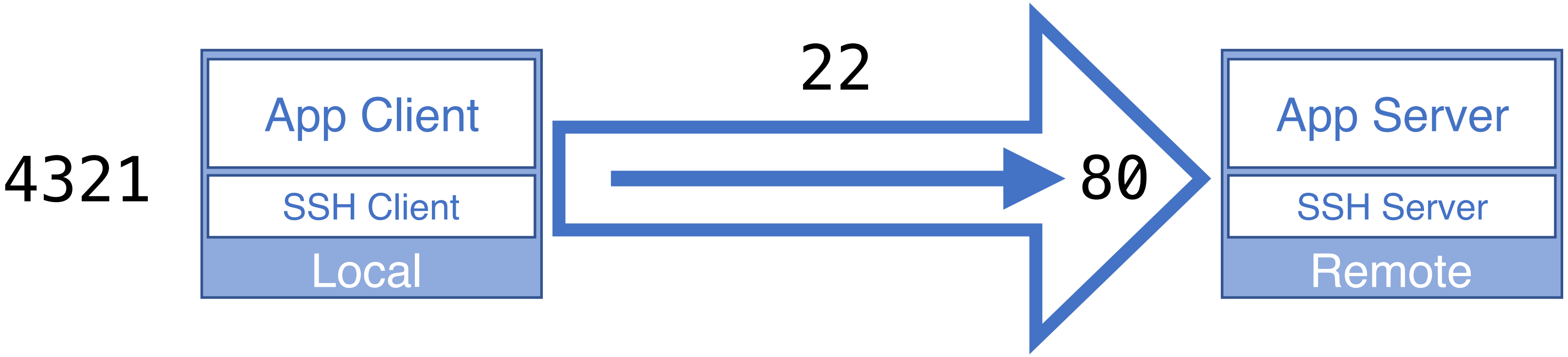
- Proxying with Dynamic Port Forwarding

Tunneling with Local Port Forwarding

- Local socket or port traffic is forwarded to a remote host
- Encapsulated in a secure SSH channel

Tunneling with Local Port Forwarding

- Accessing resources on trusted segments
- Accessing less secure applications
- Evading network and host based firewall rules
- Remote Port can be any TCP Port/UNIX Socket



```
ssh -L 4321:localhost:80 user@$REMOTE
```

DEMO

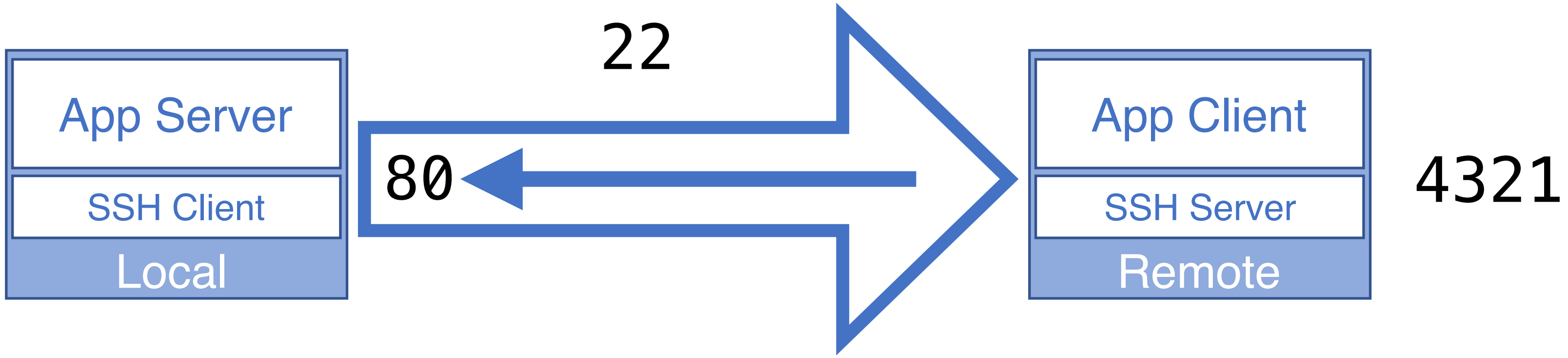
- Tunneling with Local Port Forwarding

Tunneling with Reverse Port Forwarding

- Remote socket or port with traffic is forwarded to the local host
- Encapsulated in a secure SSH channel

Tunneling with Reverse Port Forwarding

- Accessing local resources from a remote segment
- Evading network and host based firewall rules
- “Remote” Port can be any TCP Port/UNIX Socket



```
ssh -R localhost:4321:localhost:80 user@$REMOTE
```

DEMO

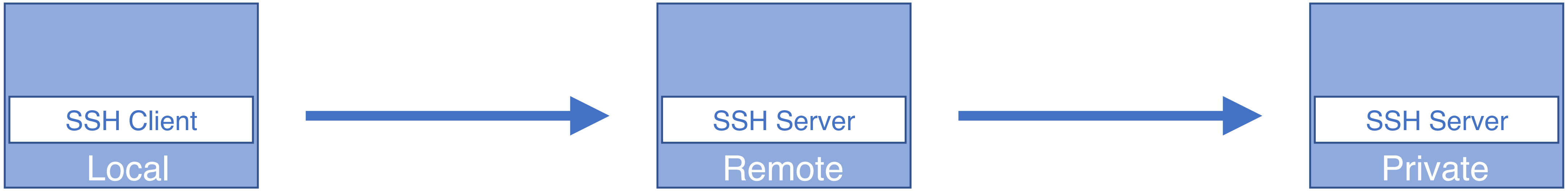
- Tunneling with Reverse Port Forwarding

SSH Based Multi-hop Jump Hosts

- Local SSH Connection passed through to a protected host

SSH Based Multi-hop Jump Hosts

- Accessing a protected host through a server
- Evading network and host based firewall rules
- Reaching not directly routable/reachable hosts



```
ssh -J aen@$REMOTE aen@$PRIVATE
```

DEMO

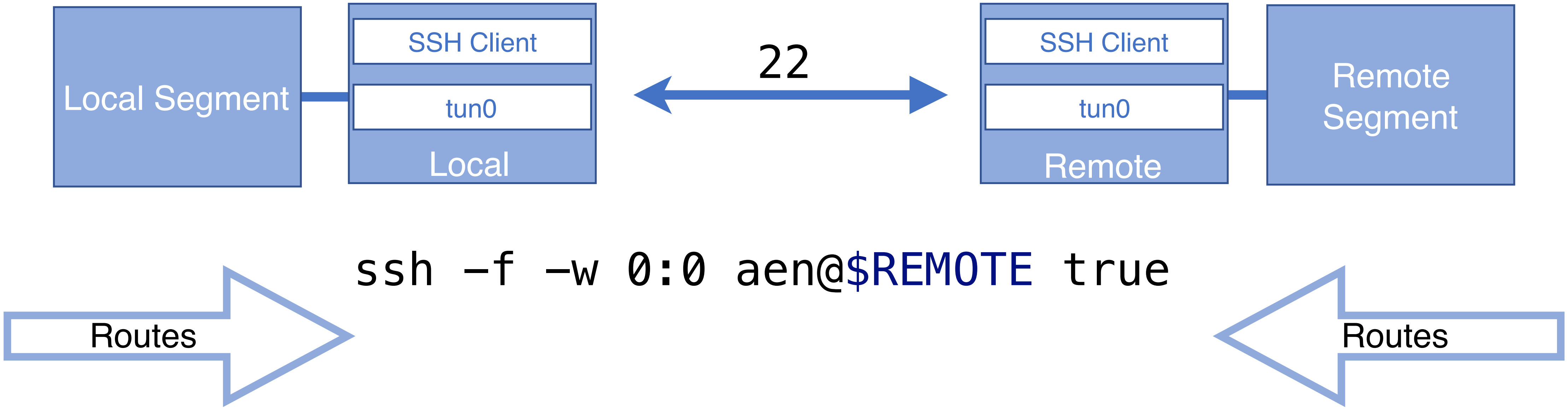
- SSH Based Multi-hop Jump Hosts

PowerShell + DevOps
GLOBAL SUMMIT

Accessing Remote Networks

Next level nerdiness…

SSH Based VPN



```
ssh -f -w 0:0 aen@$REMOTE true
```

DEMO

- SSH Based VPN

Controlling Tunneling and Forwarding

- `AllowTcpForwarding yes` - Is forwarding permitted?
- `GatewayPorts no` - Allow forwarded ports on interface IPs (or not)
- `PermitTunnel no` - Enable or disable ssh based VPN tunnels

-
  ```
  Match Group NoForwarding
    AllowTcpForwarding no
  ```

-
  ```
  Match User aen
    GatewayPorts Yes
  ```

Troubleshooting

- **Step 1 - make sure SSH works!**
  - **Client side debug with -v**
  - **Server side debug in sshd_config**
- User key mismatch
- Double hop key placement
- Host key mismatch
- Permissions on `authorized_keys` because of `StrictModes`

Review

- Background and SSH Basics
- Accessing Remote Resources
    - Proxying with Dynamic Port Forwarding
    - Tunneling with Local Port Forwarding
    - Tunneling with Reverse Port Forwarding
    - SSH Based Multi-hop Jump Hosts
- Accessing Remote Networks
    - SSH Based VPNs
- Controlling and Preventing TCP Tunnelling

More data?

- **Email:** aen@centinosystems.com
- **Twitter:** @nocentino
- **Blog:** www.centinosystems.com/blog

- **LFCE: Network and Host Security**
  - OpenSSH
  - Copying files, remote command execution and tunneling TCP
- **Understanding and Using Essential Tools for Enterprise Linux 7**
  - Installation, command execution, bash basics, file system and permissions
- **PowerShell Summit 2018 Videos on YouTube**

THANK YOU!

Please use the event app or Sched.com to submit a session rating!