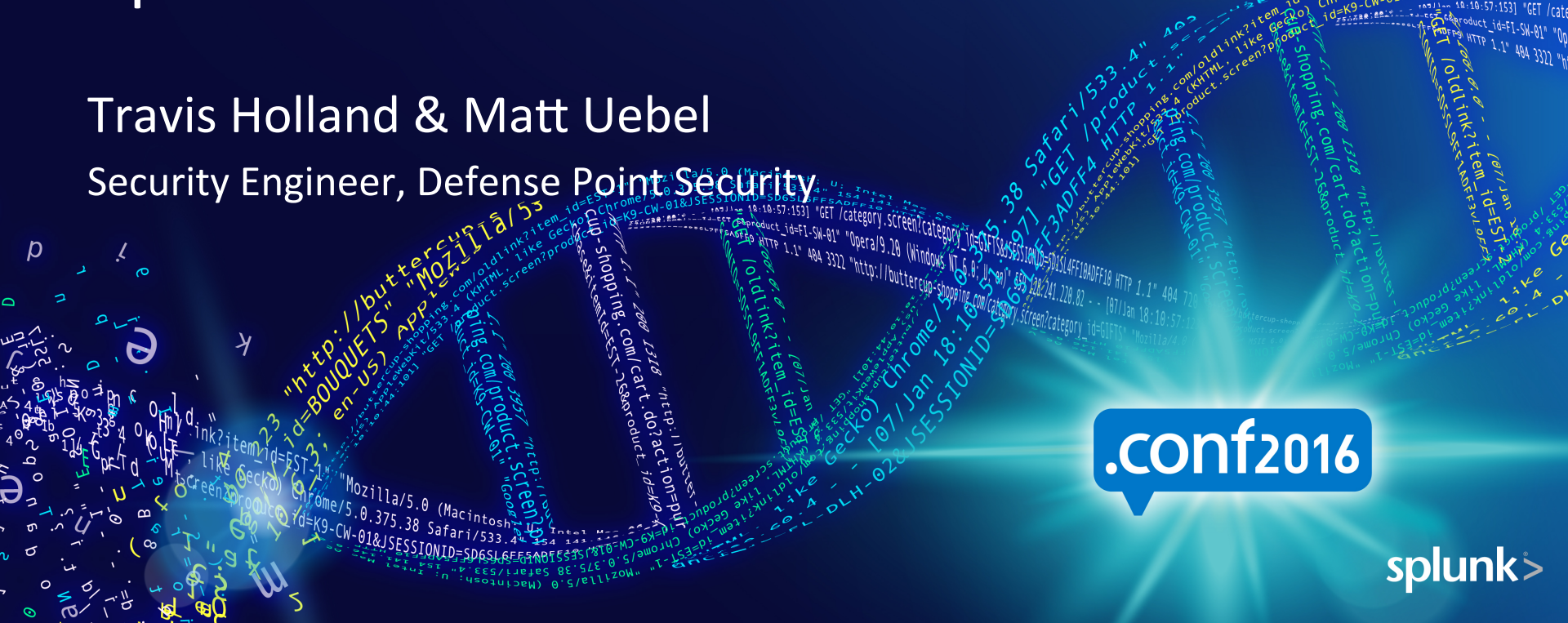
Universal Forwarder Security: Don’t Input More Than Data Into Your Splunk Environment

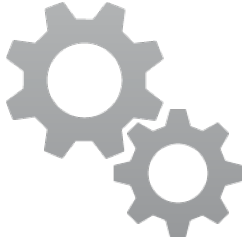
Travis Holland & Matt Uebel

Security Engineer, Defense Point Security



Matt Uebel

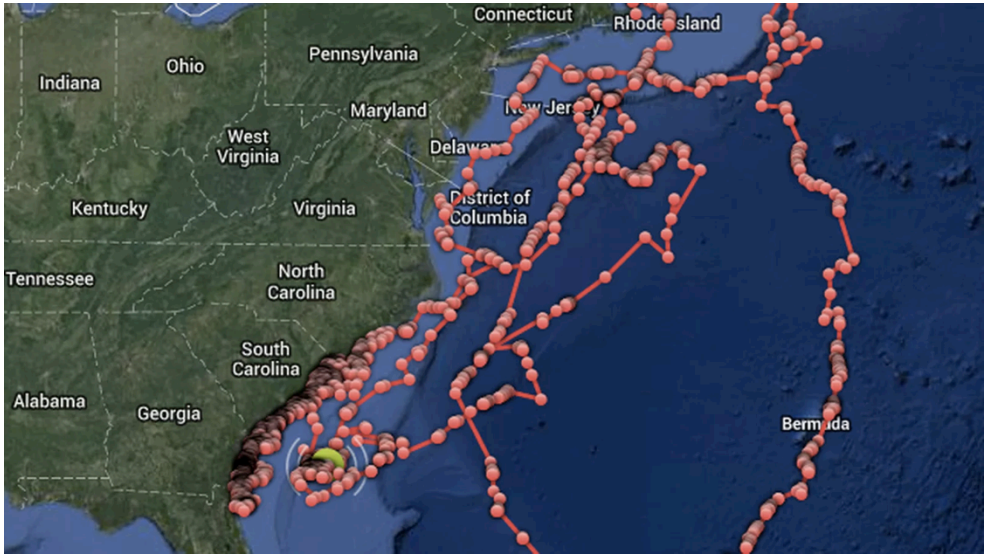
DEFENSE POINT
SECURITY



splunk> .conf2016

Travis Holland

DEFENSE POINT SECURITY



splunk> .conf2016

Who is DPS?

DPS is one of the largest privately owned, small businesses exclusively providing cyber security services and solutions to the federal government and commercial corporations.

- CYBER DEFENSE
- SECURITY ENGINEERING & ARCHITECTURE
- INFORMATION SECURITY
- CYBER OFFENSE
- CYBER SECURITY TRAINING & EDUCATION
- RESEARCH & DEVELOPMENT
- DPS SHIELD™ MANAGED SECURITY SERVICES

splunk>

- **Splunk** *Professional Service Public Sector Partner of the Year* 2015
- 20+ **Splunk** Certified Architects on Staff
- We use **Splunk** to achieve many of the expertise domains above

Agenda

- Deployment of the Universal Forwarder
- Discuss common vulnerabilities of a default Universal Forwarder installation
- Solutions to the problem
- Automation scripts and snippets

splunk> .conf2016

Introduction

- Is it enough to harden just your Splunk Enterprise servers?
- Do you understand the default configuration of a Universal Forwarder?
- What are the dangers of a misconfigured Universal Forwarder?
- What can Deployment Server credentials really do?
- Are your Splunk admins more than Splunk admins?

splunk> .conf2016

Exploitation - Universal Forwarder

Defense Point pentester successfully escalated from non-root credentials to root leveraging a misconfigured Universal forwarder

- User credentials to server obtained
- Engages with DPS Community

Exploitation - Universal Forwarder

Escalation from non-root to root via the Universal Forwarder

1. Create rogue deployment server
2. Change the deployment server of the universal forwarder
3. Restart the Universal Forwarder
4. Create exploitation App

5. Deploy App - Reap the rewards

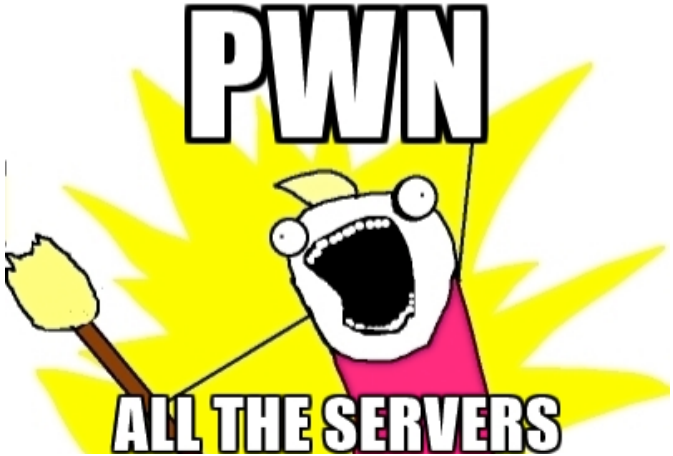
splunk> .conf2016

Exploitation - Bonus Scenario

- Universal Forwarders Managed by Deployment Server
- Legitimate Splunk admin credentials obtained
- Mass Deployment of exploitation app to entire environment

Compensating Control:

- Lockdown the Deployment Server
- Configure forwarders appropriately



The UF Deployment Plan

- Usually simply “yum/apt-get install splunkforwarder” all the things
- Much more can be done

The Issues

User Account	✗
Admin Credentials	✗
Management Port	✗
Deployment Server	✗
Firewall Rules	✗
SSL Certificates	✗

splunk> .conf2016

Run as non-root

- Setup init script specifying some user (splunk user is default)

```
/opt/splunkforwarder/bin/splunk enable boot-start -user splunk
chown -R splunk:splunk /opt/splunkforwarder
```

- Lockdown splunk-launch.conf, which contains runas user config

```
chown root:splunk /opt/splunk/etc/splunk-launch.conf
chmod 644 /opt/splunk/etc/splunk-launch.conf
```


splunk> .conf2016

Reading Files as non-root

- Create a “log reading” group and add the spunk user to it, or simply change group ownership to splunk

```
groupadd syslog
chown -R :syslog /var/log
chmod -R g+s /var/log
usermod -a -G syslog splunk
```


splunk> .conf2016

Reading Files as non-root cont.

- Usual defaults have /var/log unreadable by non-root user

```
setfacl -Rm u:splunk:r-x,d:u:splunk:r-x /var/log
```

- Auditd represents special case, requires modification to /etc/audit/auditd.conf

```
log_group = splunk
```

- Additionally modify permission set on audit directory

```
chgrp -R splunk /var/log/audit
chmod 0750 /var/log/audit
chmod 0640 /var/log/audit/*
```

Windows Low-privilege Mode

- Suitable for typical windows system
- You will need to specify a local or domain user

```
msiexec.exe /i splunkforwarder.msi AGREETOLICENSE=Yes
  LOGON_USERNAME="$env:computername\splunk"
  LOGON_PASSWORD="$password" SET_ADMIN_USER=0
  LAUNCHSPLUNK=0 /qn
```

The Issues

User Account	✓
Admin Credentials	✗
Management Port	✗
Deployment Server	✗
Firewall Rules	✗
SSL Certificates	✗

splunk> .conf2016

Change Admin Password (nix)

- Bash script to set admin password to random string

```
$SPLUNK_HOME/bin/splunk edit user admin -password `head -c 500 /dev/
    urandom | sha256sum | base64 | head -c 16 ; echo` -auth admin:changeme
```

GOTCHA: What if you need to issue a command?
SOLUTION: Remove $SPLUNK_HOME/etc/passwd, restart splunk

splunk> .conf2016

Change Admin Password (win)

- Generate the random password.

```
do {
        $password = (-join ((48..57) + (65..90) + (97..122) | Get-Random -Count 14 | % {[char]$_}))
} until ($password -match "[0-9]" -and $password -match "[a-z]" -and $password -match "[A-Z]")
```

- Set that password for admin user

```
& "$env:programfiles\splunkuniversalforwarder\bin\splunk.exe" edit user admin -password ($password) -auth
admin:changeme | out-null
```

splunk> .conf2016

The Issues

User Account	✓
Admin Credentials	✓
Management Port	✗
Deployment Server	✗
Firewall Rules	✗
SSL Certificates	✗

splunk> .conf2016

Disable Management Port (nix)

- Create app directory

```
mkdir -p /opt/splunkforwarder/etc/apps/UF-TA-killrest/local
```

- Generate server.conf containing config to disable management interface

```
echo '[httpServer]
disableDefaultPort = true' > /opt/splunkforwarder/etc/apps/UF-TA-killrest/local/server.conf
```


splunk> .conf2016

Disable Management Port (win)

- Create app directory

```
new-item -path "$env:programfiles\splunkuniversalforwarder\etc\apps\UF-TA-killrest
\local" -ItemType "Directory" -force | out-null
```

- Generate server.conf containing config to disable management interface

```
"[httpServer]`r`ndisableDefaultPort = true" | out-file "$env:programfiles
\splunkuniversalforwarder\etc\apps\UF-TA-killrest\local\server.conf" -force | out-null
```

The Issues

User Account	✓
Admin Credentials	✓
Management Port	✓
Deployment Server	✗
Firewall Rules	✗
SSL Certificates	✗

splunk> .conf2016

The Deployment Server

Splunk's configuration control system, can potentially run arbitrary commands on systems through scripted inputs.

This and a Universal Forwarder running as root/system can easily take over an environment

splunk> .conf2016

Watch for Rogue DS

- This will need adjusted based on your environment

```
index=_internal sourcetype=splunkd DeployedApplication
  Downloaded url!=your-ds-server*
```

splunk> .conf2016

Who Has Access to DS?

- Careful consideration for auth config
- Default user role doesn't allow interaction with DS interface
- How many users in admin role?

splunk> .conf2016

Monitor Deploy Capable Users

- While in known good state, make lookup

```
| rest splunk_server=local /services/authentication/users | search capabilities=edit_deployment* OR capabilities=list_deployment* | eval username=title | eval permitted="True" | table username permitted | outputlookup deploy_capable_users.csv
```


splunk> .conf2016

Monitor Deploy Capable Users cont.

- On some schedule, search to find any users not in lookup

```
| rest splunk_server=local /services/authentication/users | search capabilities=edit_deployment* OR capabilities=list_deployment* | eval username=title | table username | lookup deploy_capable_users.csv username OUTPUTNEW permitted | search NOT permitted=*
```


splunk> .conf2016

Watching Audit Log for Bundle Reloads

- Useful in particular for off hours events

```
index=_audit action=list_deployment_server info=granted
object="_reload" operation="_reload"
```


splunk> .conf2016

Gather Bash History

- DS App modification require some interaction with the file system
- Can add a layer of protection by gathering bash commands
- See repo for more details

splunk> .conf2016

The Issues

User Account	✓
Admin Credentials	✓
Management Port	✓
Deployment Server	✓
Firewall Rules	✗
SSL Certificates	✗

splunk> .conf2016

SSL Certificates and Firewall Rules

Control the flow of communication

- Splunk SSL Configuration
  SSLippery Slope - George and Duane's SSL Talk

- Network or Host based Firewall
- Rules will vary across organizations

The Issues

User Account	✓
Admin Credentials	✓
Management Port	✓
Deployment Server	✓
Firewall Rules	✓
SSL Certificates	✓

splunk> .conf2016

What Now?

- Keeping the Junk Out of Splunk
- Worst Practices… and How to Fix Them
- Shop Smart at the KV Store: Best Value Tricks from the Splunk KV Store and REST API
- Lesser Known Search Commands
- Fields, Indexed Tokens and You

splunk> .conf2016

Links

- Code Repository for Scripts related to this talk
- Great answers post on the topic of reading logs as non-root user
- Skip's change admin password app
- Splunk Answers
- Splunk Community Slack (Nebraska User Group setup this form)
- Splunk IRC - #splunk on EFNet

splunk> .conf2016

THANK YOU

splunk>