black hat
WEBCASTS

Now is the time for cyber deception

March 21, 2019

Sponsored by
Carbon Black.

@BlackHatEvents / #BlackHatWebcasts

Speakers

Featured Presenter:

John Strand, @strandjs

Owner,

Black Hills Information Security and Active Countermeasures

Sponsor Presenter, @network232

David Balcar,

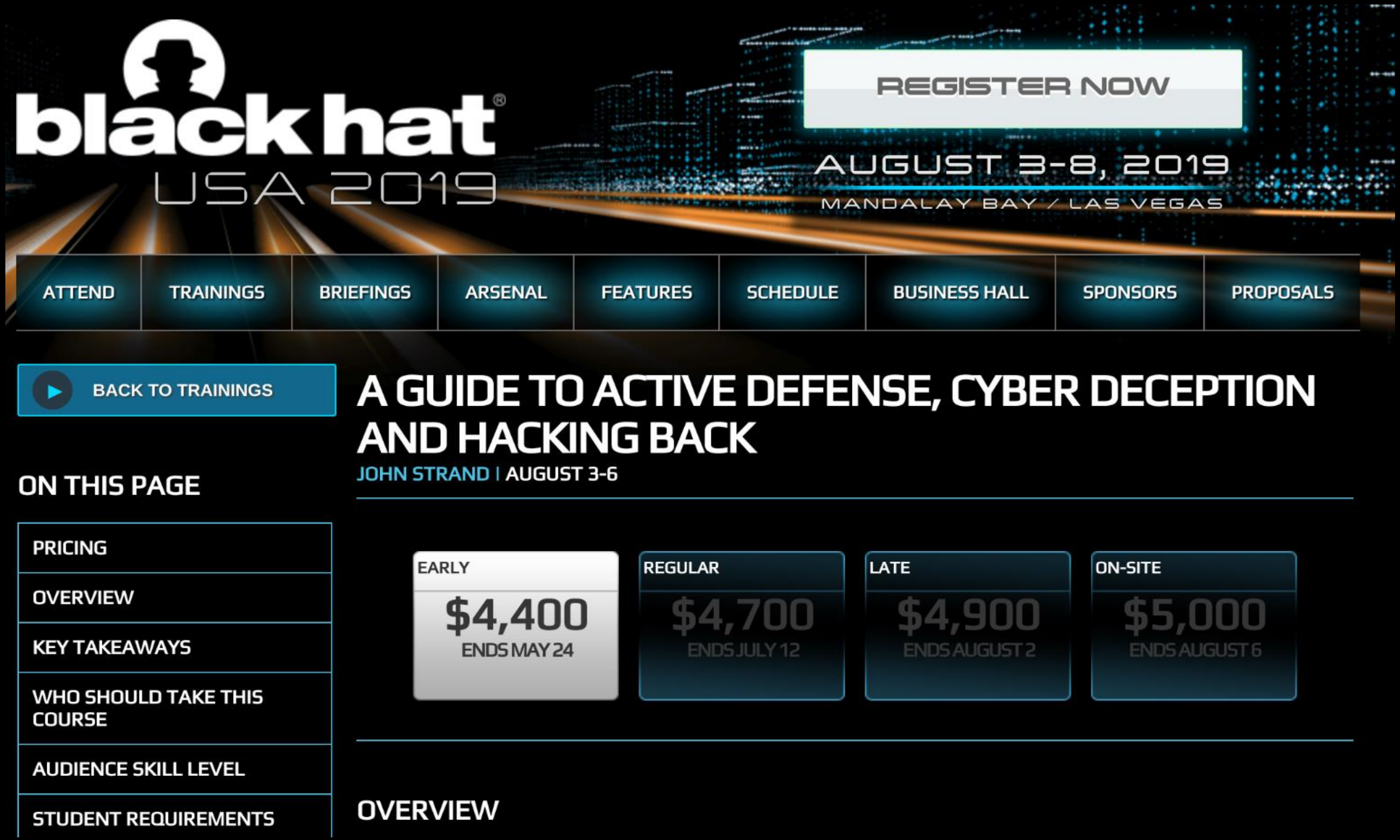
Security Strategist,

Carbon Black

Sponsored by

Carbon Black.

Brought To You By!



A GUIDE TO ACTIVE DEFENSE, CYBER DECEPTION AND HACKING BACK

JOHN STRAND | AUGUST 3-6

EARLY	REGULAR	LATE	ON-SITE
$4,400 ENDS MAY 24	$4,700 ENDS JULY 12	$4,900 ENDS AUGUST 2	$5,000 ENDS AUGUST 6

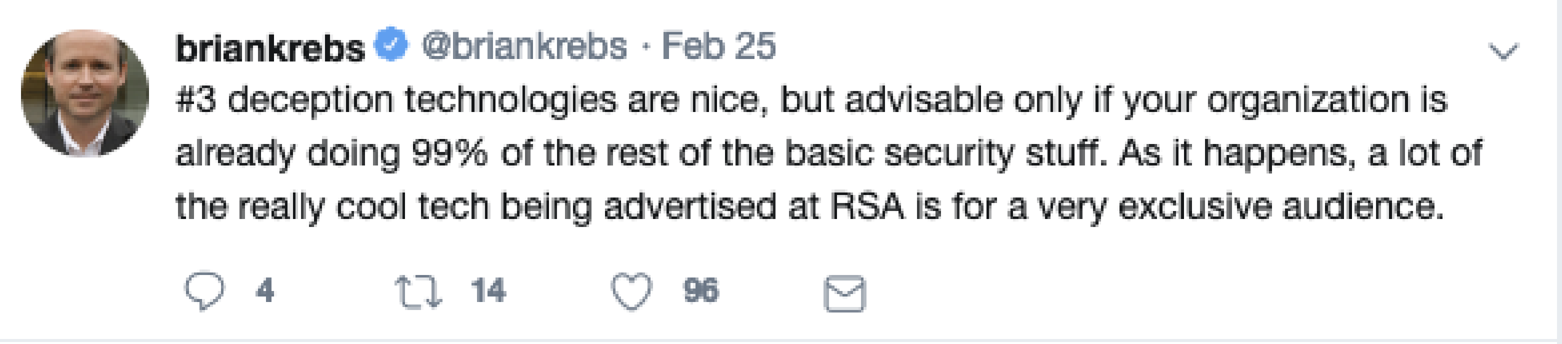
ON THIS PAGE

- PRICING
- OVERVIEW
- KEY TAKEAWAYS
- WHO SHOULD TAKE THIS COURSE
- AUDIENCE SKILL LEVEL
- STUDENT REQUIREMENTS

OVERVIEW

http://bit.ly/BlackHatDeception

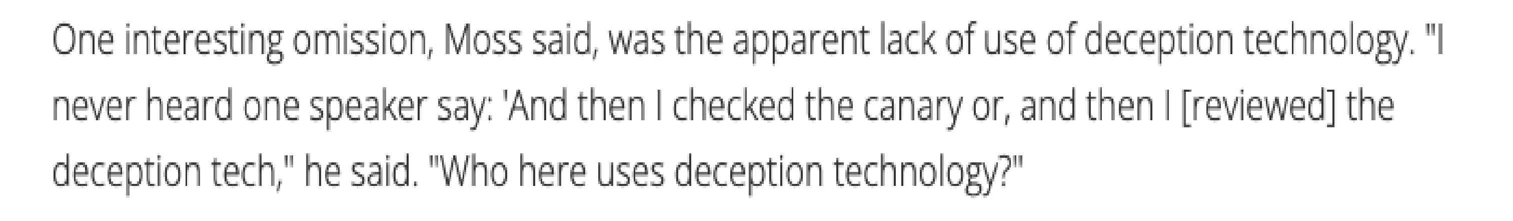
Conversation



briankrebs @briankrebs · Feb 25

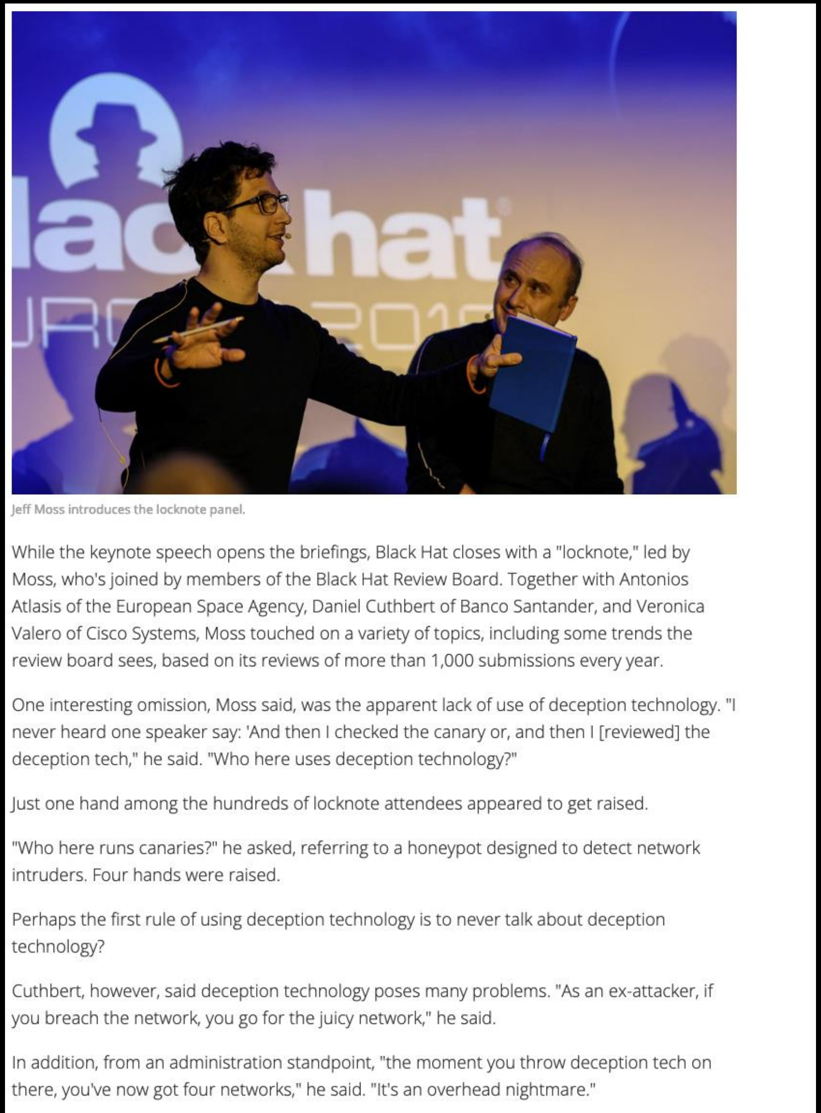
#3 deception technologies are nice, but advisable only if your organization is already doing 99% of the rest of the basic security stuff. As it happens, a lot of the really cool tech being advertised at RSA is for a very exclusive audience.

4 14 96



One interesting omission, Moss said, was the apparent lack of use of deception technology. "I never heard one speaker say: 'And then I checked the canary or, and then I [reviewed] the deception tech," he said. "Who here uses deception technology?"

Let’s Change that



Jeff Moss introduces the locknote panel.

While the keynote speech opens the briefings, Black Hat closes with a "locknote," led by Moss, who's joined by members of the Black Hat Review Board. Together with Antonios Atlasis of the European Space Agency, Daniel Cuthbert of Banco Santander, and Veronica Valero of Cisco Systems, Moss touched on a variety of topics, including some trends the review board sees, based on its reviews of more than 1,000 submissions every year.

One interesting omission, Moss said, was the apparent lack of use of deception technology. "I never heard one speaker say: 'And then I checked the canary or, and then I [reviewed] the deception tech," he said. "Who here uses deception technology?"

Just one hand among the hundreds of locknote attendees appeared to get raised.

"Who here runs canaries?" he asked, referring to a honeypot designed to detect network intruders. Four hands were raised.

Perhaps the first rule of using deception technology is to never talk about deception technology?

Cuthbert, however, said deception technology poses many problems. "As an ex-attacker, if you breach the network, you go for the juicy network," he said.

In addition, from an administration standpoint, "the moment you throw deception tech on there, you've now got four networks," he said. "It's an overhead nightmare."

Why?

- Another useless rant on Threat Intelligence Feeds
- But there is value in understanding attackers
- How about attackers that are attacking you right now?
- What if we (as an industry) got better tracking attackers?
- Broken Windows

ADHD

https://www.activecountermeasures.com/free-tools/

What Is Cyber Deception?

- Cyber deception is the deliberate and calculated process of deceiving attackers in an effort to wage a better defense
  - Slow them down, confuse them, deceive them … make them work harder
  - Serves to significantly increase your chances of detection
  - Designed to make **D**etection$_t$ + **R**eaction$_t$ < **A**ttack$_t$ **($D_t + R_t < A_t$)**
- Cyber deception does not replace other efforts or layers of defense
- It should complement and feed the other layers
- Militaries have employed deception strategies since the beginning of time. Why don't we?

Advanced Persistent Thieves (APTs)

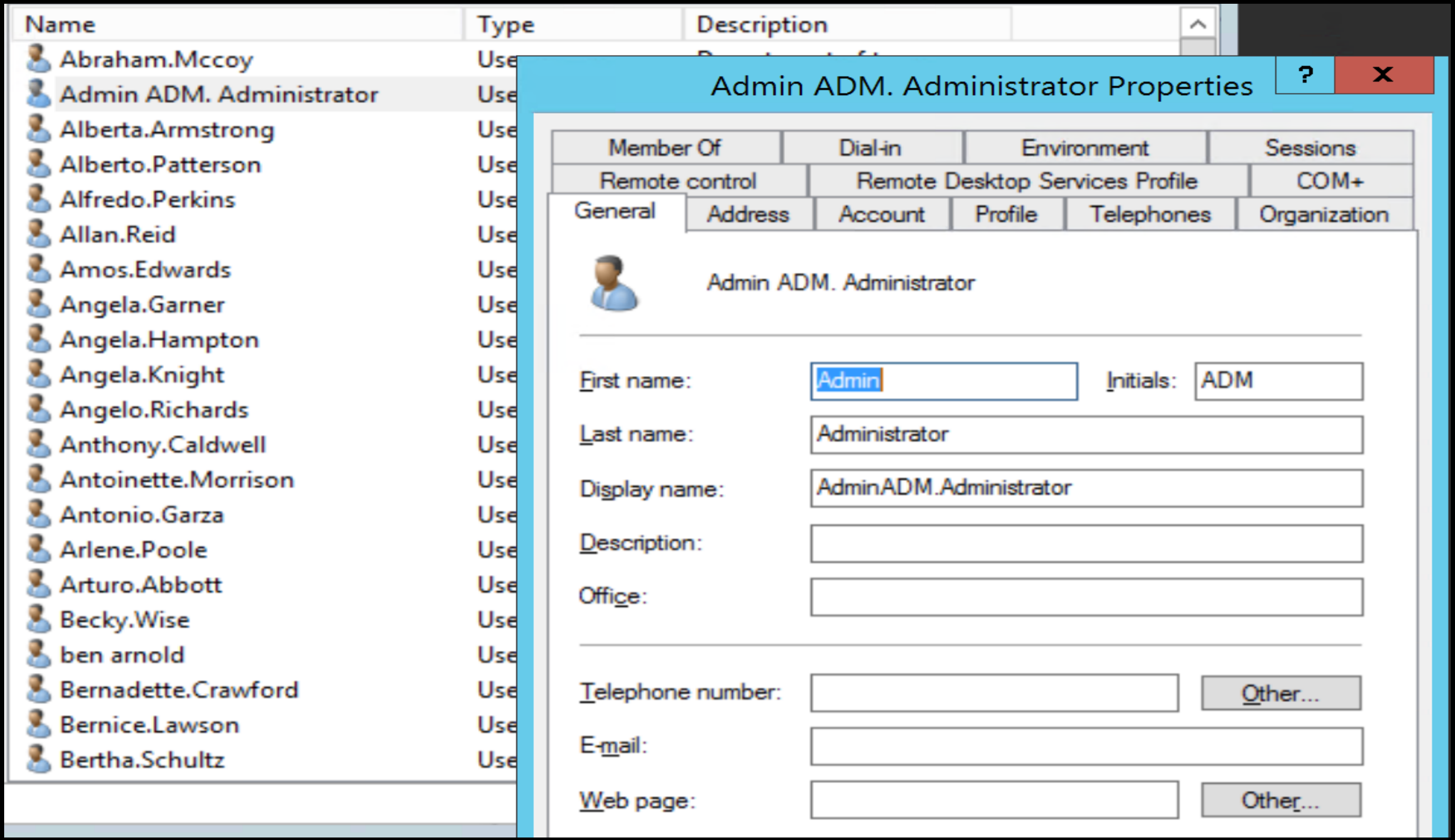
- So who's after your electrons?
  - China?
  - Russia?
  - The Five Eyes?
  - Other nation-states?
  - Organized crime?
  - Insiders?
  - **All of the above!?**

Susan v. Absolute

- Substitute teacher buys a stolen laptop
- The laptop has tracking software and software to “spy” on the potential “thief”
- Embarrassing pictures are taken
  - "It is one thing to cause a stolen computer to report its IP address or its geographical location in an effort to track it down," Rice wrote in his decision. "It is something entirely different to violate federal wiretapping laws by intercepting the electronic communications of the person using the stolen laptop.“ –Judge Walter Rice
- Absolute settled out of court
- Just because they do something bad to you, it does not give you the right to violate their rights

Active Directory HoneyAdmin

Go on.. Be obvious!



Name	Type	Description
Abraham.Mccoy	Use	
Admin ADM. Administrator	Use	
Alberta.Armstrong	Use	
Alberto.Patterson	Use	
Alfredo.Perkins	Use	
Allan.Reid	Use	
Amos.Edwards	Use	
Angela.Garner	Use	
Angela.Hampton	Use	
Angela.Knight	Use	
Angelo.Richards	Use	
Anthony.Caldwell	Use	
Antoinette.Morrison	Use	
Antonio.Garza	Use	
Arlene.Poole	Use	
Arturo.Abbott	Use	
Becky.Wise	Use	
ben arnold	Use	
Bernadette.Crawford	Use	
Bernice.Lawson	Use	
Bertha.Schultz	Use	

Admin ADM. Administrator Properties

Admin ADM. Administrator

First name: Admin

Initials: ADM

Last name: Administrator

Display name: AdminADM.Administrator

Description:

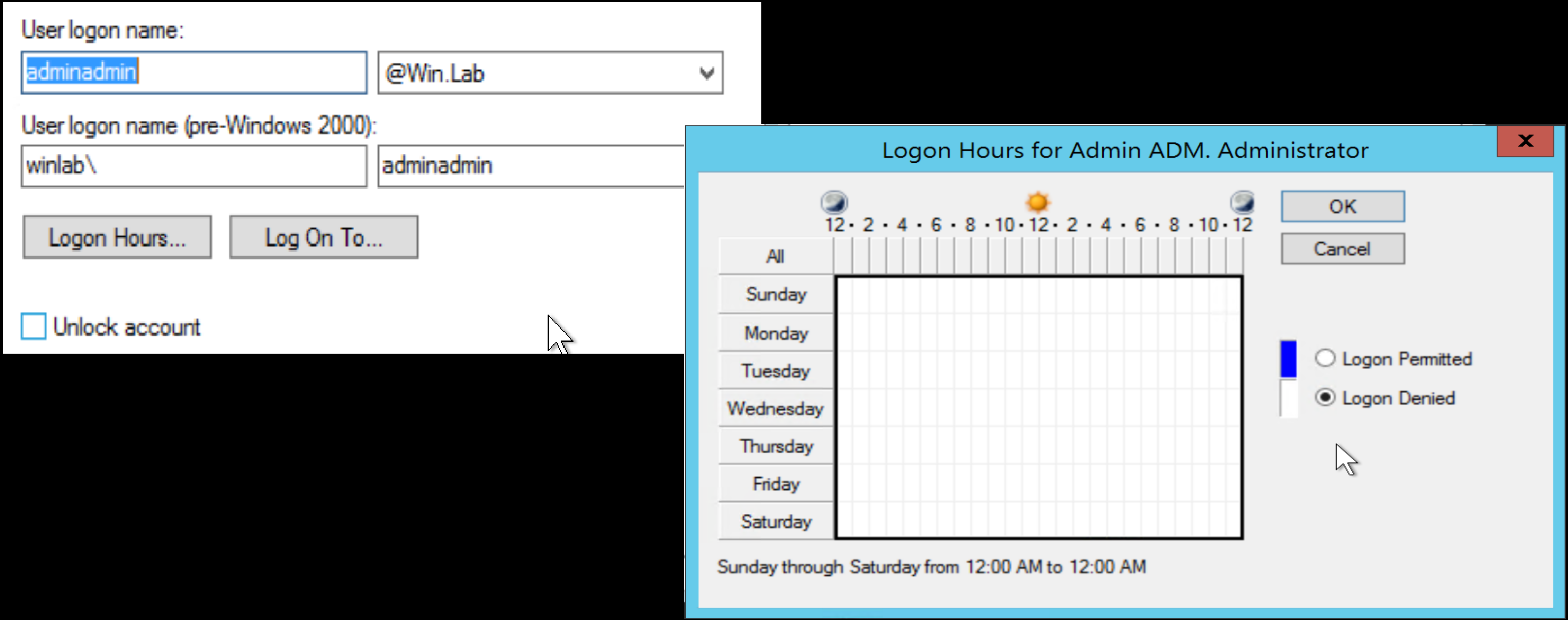
Office:

Telephone number:

E-mail:

Web page:

Disable Logon Hours



User logon name:

adminadmin @Win.Lab

User logon name (pre-Windows 2000):

winlab\ adminadmin

Logon Hours... Log On To...

□ Unlock account

Logon Hours for Admin ADM. Administrator

12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12

All

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

OK

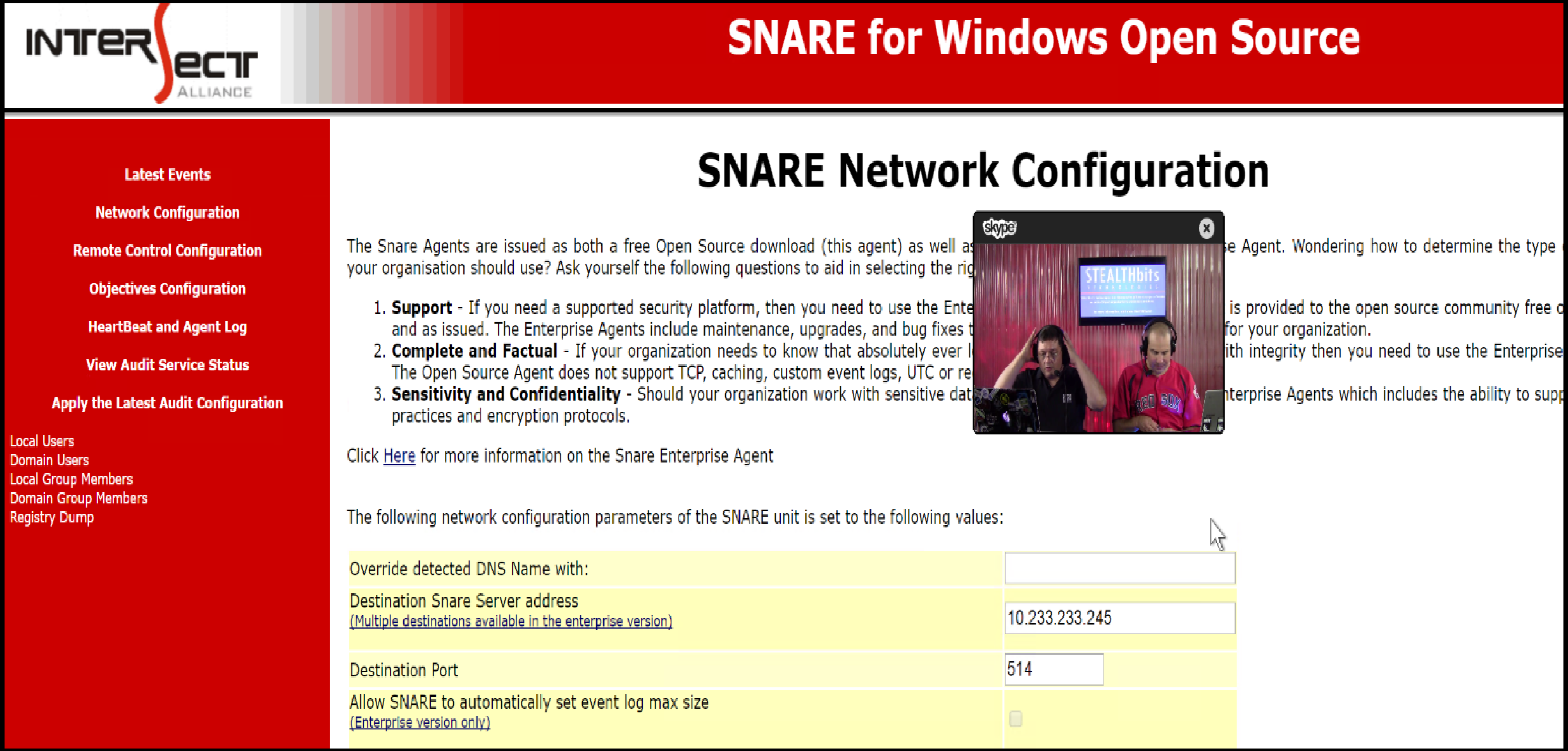
Cancel

○ Logon Permitted

● Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

Set up Snare



SNARE for Windows Open Source

SNARE Network Configuration

The Snare Agents are issued as both a free Open Source download (this agent) as well as … e Agent. Wondering how to determine the type … your organisation should use? Ask yourself the following questions to aid in selecting the rig…

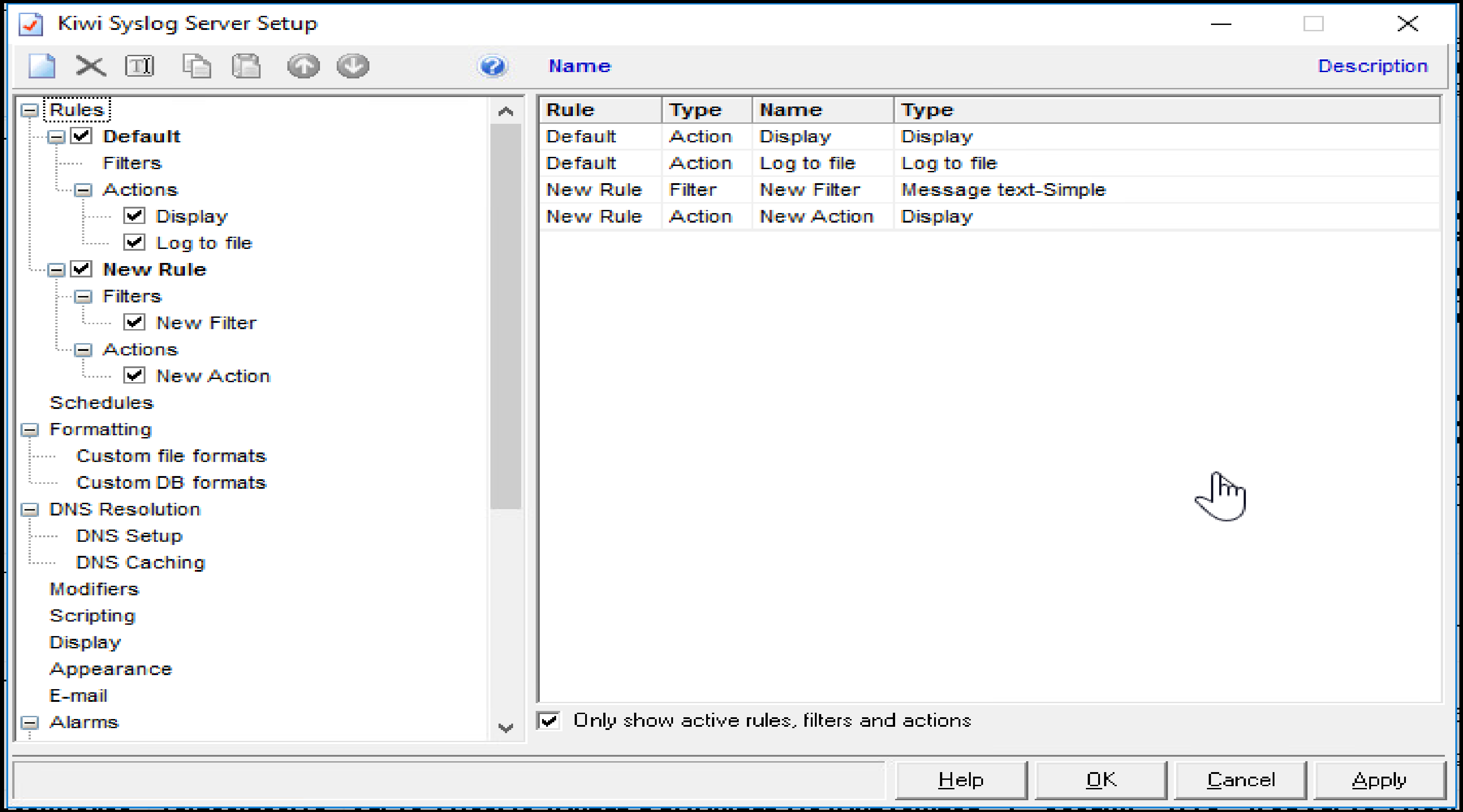
1. **Support** - If you need a supported security platform, then you need to use the Ente… is provided to the open source community free o… and as issued. The Enterprise Agents include maintenance, upgrades, and bug fixes t… for your organization.
2. **Complete and Factual** - If your organization needs to know that absolutely ever… ith integrity then you need to use the Enterprise… The Open Source Agent does not support TCP, caching, custom event logs, UTC or re…
3. **Sensitivity and Confidentiality** - Should your organization work with sensitive dat… nterprise Agents which includes the ability to supp… practices and encryption protocols.

Click Here for more information on the Snare Enterprise Agent

The following network configuration parameters of the SNARE unit is set to the following values:

Override detected DNS Name with:	
Destination Snare Server address (Multiple destinations available in the enterprise version)	10.233.233.245
Destination Port	514
Allow SNARE to automatically set event log max size (Enterprise version only)	□

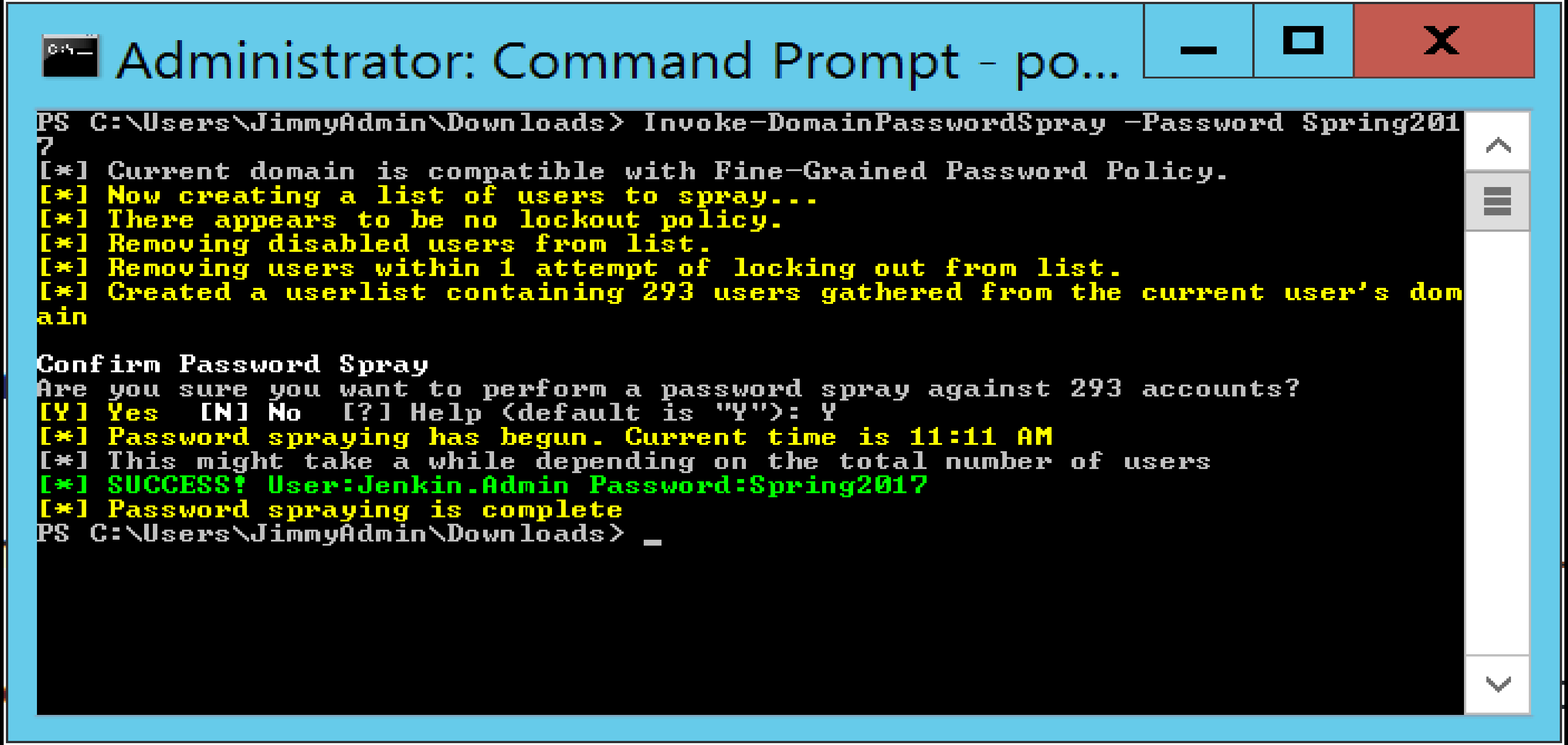
Set up Kiwi



Rule	Type	Name	Type
Default	Action	Display	Display
Default	Action	Log to file	Log to file
New Rule	Filter	New Filter	Message text-Simple
New Rule	Action	New Action	Display

☑ Only show active rules, filters and actions

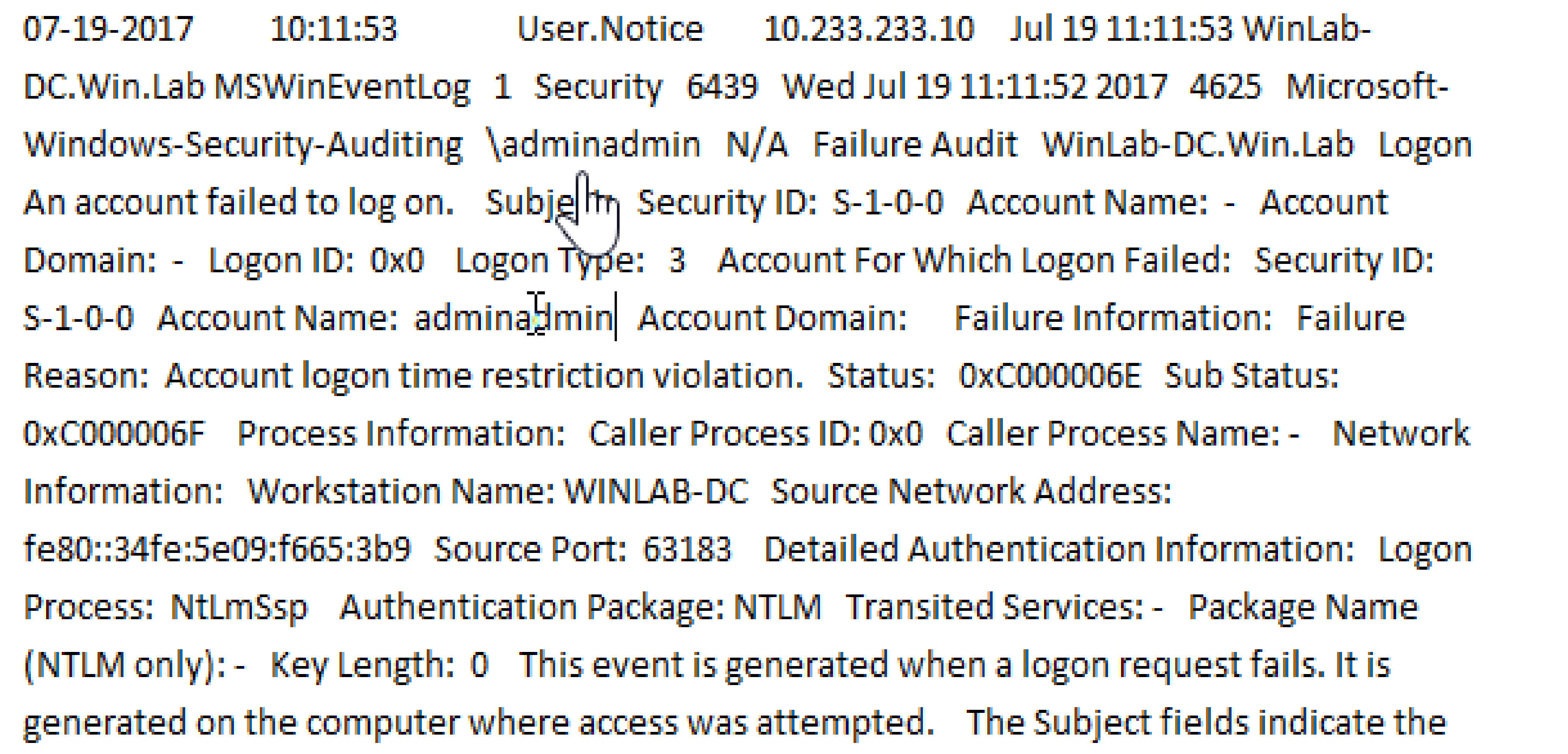
Password Spray



```
PS C:\Users\JimmyAdmin\Downloads> Invoke-DomainPasswordSpray -Password Spring201
7
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] There appears to be no lockout policy.
[*] Removing disabled users from list.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 293 users gathered from the current user's dom
ain

Confirm Password Spray
Are you sure you want to perform a password spray against 293 accounts?
[Y] Yes  [N] No  [?] Help (default is "Y"): Y
[*] Password spraying has begun. Current time is 11:11 AM
[*] This might take a while depending on the total number of users
[*] SUCCESS! User:Jenkin.Admin Password:Spring2017
[*] Password spraying is complete
PS C:\Users\JimmyAdmin\Downloads> _
```

Alerts!

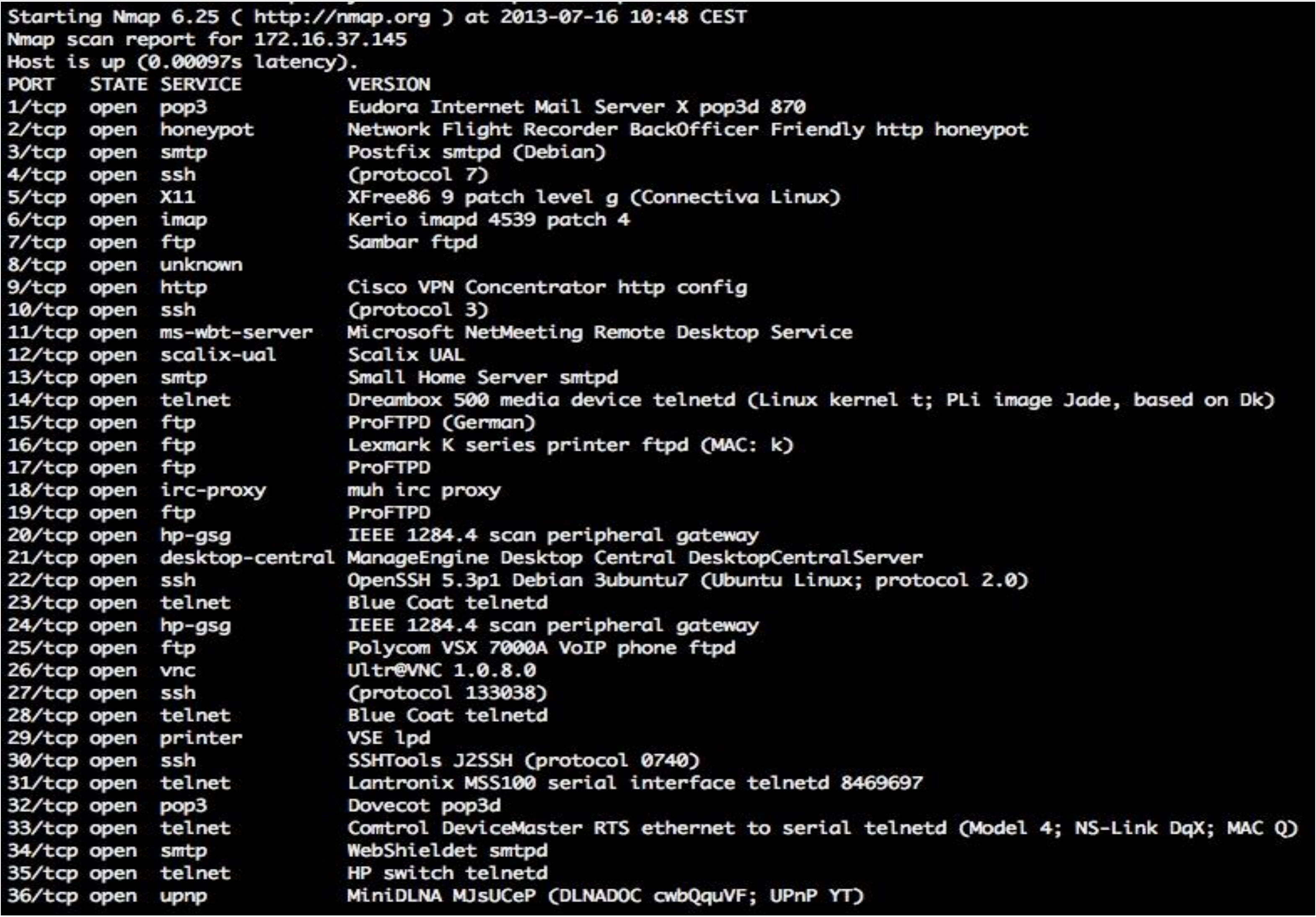


```
07-19-2017      10:11:53        User.Notice     10.233.233.10   Jul 19 11:11:53 WinLab-
DC.Win.Lab MSWinEventLog  1  Security  6439  Wed Jul 19 11:11:52 2017  4625  Microsoft-
Windows-Security-Auditing  \adminadmin  N/A  Failure Audit  WinLab-DC.Win.Lab  Logon
An account failed to log on.  Subject:  Security ID:  S-1-0-0  Account Name:  -   Account
Domain:  -   Logon ID:  0x0   Logon Type:  3   Account For Which Logon Failed:  Security ID:
S-1-0-0  Account Name:  adminadmin  Account Domain:     Failure Information:  Failure
Reason:  Account logon time restriction violation.  Status:  0xC000006E  Sub Status:
0xC000006F   Process Information:  Caller Process ID: 0x0  Caller Process Name: -   Network
Information:  Workstation Name: WINLAB-DC  Source Network Address:
fe80::34fe:5e09:f665:3b9  Source Port:  63183   Detailed Authentication Information:  Logon
Process:  NtLmSsp   Authentication Package: NTLM  Transited Services: -   Package Name
(NTLM only): -   Key Length:  0   This event is generated when a logon request fails. It is
generated on the computer where access was attempted.   The Subject fields indicate the
```

Evil Honeyports: Portspoof

- In addition to our “tripwires,” why not create white noise and chaff as well?
- Portspoof does this
- It generates random responses to service identification requests
- Basically, the ports that get scanned never come back the same
- It can take hours to run a simple service identification scan

Portspoof in Action



```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-07-16 10:48 CEST
Nmap scan report for 172.16.37.145
Host is up (0.00097s latency).
PORT   STATE SERVICE         VERSION
1/tcp  open  pop3            Eudora Internet Mail Server X pop3d 870
2/tcp  open  honeypot        Network Flight Recorder BackOfficer Friendly http honeypot
3/tcp  open  smtp            Postfix smtpd (Debian)
4/tcp  open  ssh             (protocol 7)
5/tcp  open  X11             XFree86 9 patch level g (Connectiva Linux)
6/tcp  open  imap            Kerio imapd 4539 patch 4
7/tcp  open  ftp             Sambar ftpd
8/tcp  open  unknown
9/tcp  open  http            Cisco VPN Concentrator http config
10/tcp open  ssh             (protocol 3)
11/tcp open  ms-wbt-server   Microsoft NetMeeting Remote Desktop Service
12/tcp open  scalix-ual      Scalix UAL
13/tcp open  smtp            Small Home Server smtpd
14/tcp open  telnet          Dreambox 500 media device telnetd (Linux kernel t; PLi image Jade, based on Dk)
15/tcp open  ftp             ProFTPD (German)
16/tcp open  ftp             Lexmark K series printer ftpd (MAC: k)
17/tcp open  ftp             ProFTPD
18/tcp open  irc-proxy       muh irc proxy
19/tcp open  ftp             ProFTPD
20/tcp open  hp-gsg          IEEE 1284.4 scan peripheral gateway
21/tcp open  desktop-central ManageEngine Desktop Central DesktopCentralServer
22/tcp open  ssh             OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet          Blue Coat telnetd
24/tcp open  hp-gsg          IEEE 1284.4 scan peripheral gateway
25/tcp open  ftp             Polycom VSX 7000A VoIP phone ftpd
26/tcp open  vnc             Ultr@VNC 1.0.8.0
27/tcp open  ssh             (protocol 133038)
28/tcp open  telnet          Blue Coat telnetd
29/tcp open  printer         VSE lpd
30/tcp open  ssh             SSHTools J2SSH (protocol 0740)
31/tcp open  telnet          Lantronix MSS100 serial interface telnetd 8469697
32/tcp open  pop3            Dovecot pop3d
33/tcp open  telnet          Comtrol DeviceMaster RTS ethernet to serial telnetd (Model 4; NS-Link DqX; MAC Q)
34/tcp open  smtp            WebShieldet smtpd
35/tcp open  telnet          HP switch telnetd
36/tcp open  upnp            MiniDLNA MJsUCeP (DLNADOC cwbQquVF; UPnP YT)
```

Kippo

- Kippo is different from a simple honeypot because it allows the attacker to interact with a fake SSH service
- Kippo is an outstanding SSH honeypot
- It allows you to intercept and capture logins and activity by attackers
- It is useful for capturing the passwords an attacker has, or at least what he thinks he has
- It can be used for both annoyance and for attribution

Questions & Answers

Featured Presenter:

John Strand, @strandjs

Owner,

Black Hills Information Security

Active Countermeasures

Sponsor Presenter:

David Balcar,

Security Strategist,

Carbon Black

- **To join the Black Hat mailing list, email BH LIST to:** feedback@blackhat.com
- **To join our LinkedIn Group:** http://www.linkedin.com/groups?gid=37658&trk=hb_side_g
- **To follow Black Hat on Twitter:** https://twitter.com/Blackhatevents
- **Black Hat's Facebook Fan Page:** http://www.facebook.com/blackhat
- **Find out more at www.blackhat.com**
- **Next Webcast: April 18, 2019**

Sponsored by

Carbon Black.

black hat®
WEBCASTS

Thank You!

@BlackHatEvents / #BlackHatWebcasts