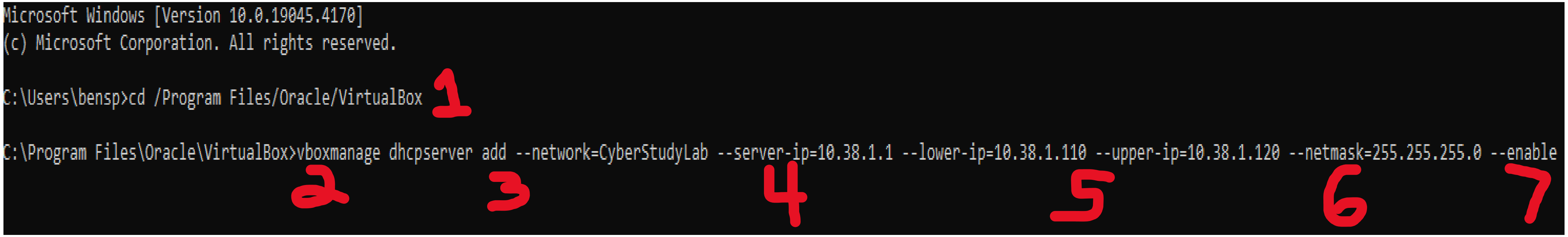
Creating a Splunk Alert From a Simulated Brute Force Attack

By: Ben Spidle

Technical Background

- Interested in Blue Teaming, more specifically being a Cybersecurity Analyst
- Concepts applied: Networking, Pentesting, SIEMs
- Steps: Installed two different VMs on Virtual Box, created a DHCP server for their internal network, opened port 22 on the victim machine, created a new user on the victim machine, ran a scan against the victim machine IP, applied the new user's username to the tool "hydra" and ran the attack, collected the logs on the victim machine, uploaded the logs to Splunk, analyzed the logs, created an alert.

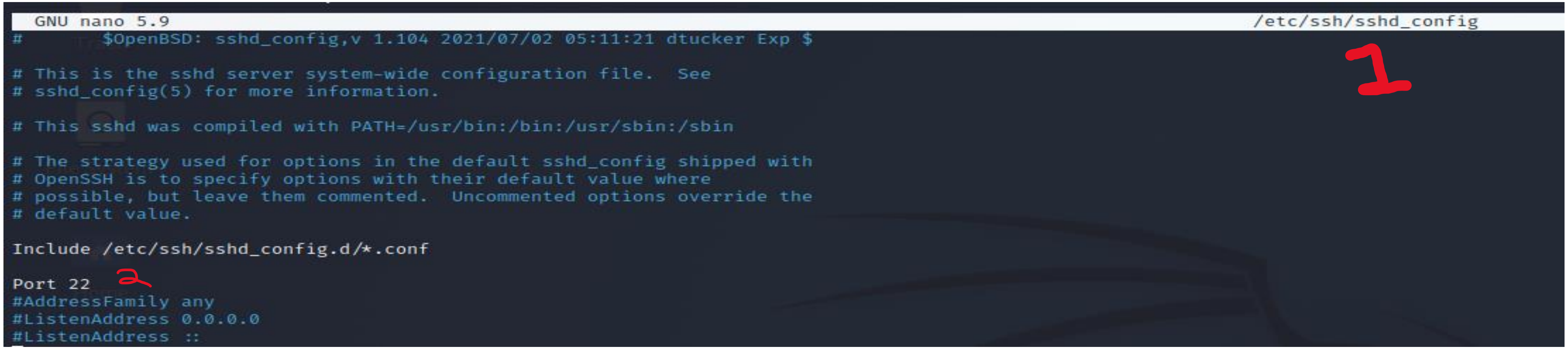
Reference to Lab Setup: DHCP Server



```
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bensp>cd /Program Files/Oracle/VirtualBox

C:\Program Files\Oracle\VirtualBox>vboxmanage dhcpserver add --network=CyberStudyLab --server-ip=10.38.1.1 --lower-ip=10.38.1.110 --upper-ip=10.38.1.120 --netmask=255.255.255.0 --enable
```

1) Navigate to the folder that contains "Virtual Box"
2) Virtual Box specific configuration command
3) Adding a DHCP server to the network "CyberStudyLab"
4) Creating the server IP
5) Network IP range
6) Netmask; divides an IP address into subnets and specifies the network's available hosts
7) Enables the DHCP server

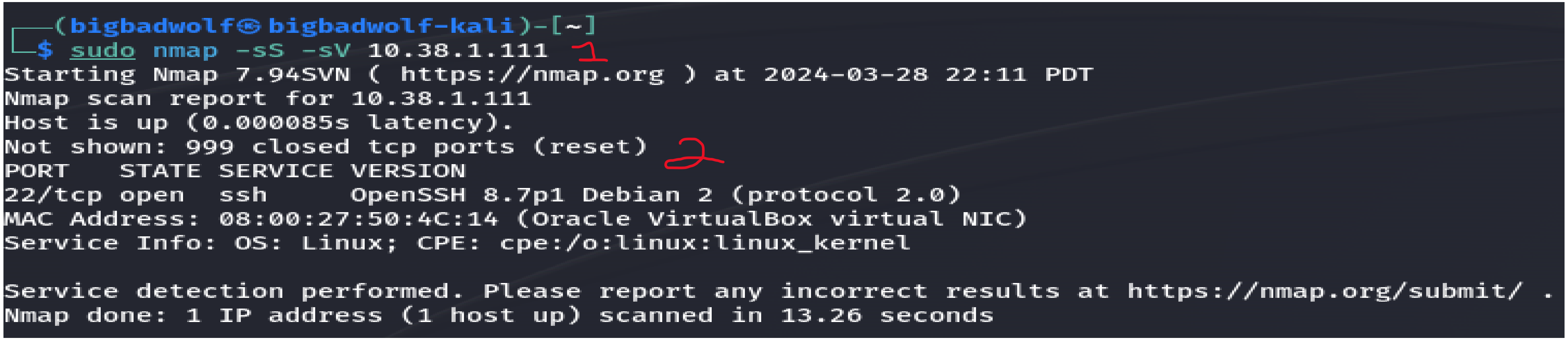
Reference to Lab Setup: SSH Config



```
  GNU nano 5.9                                                                                  /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

1) File to configure SSH
2) Line uncommented to enable port 22

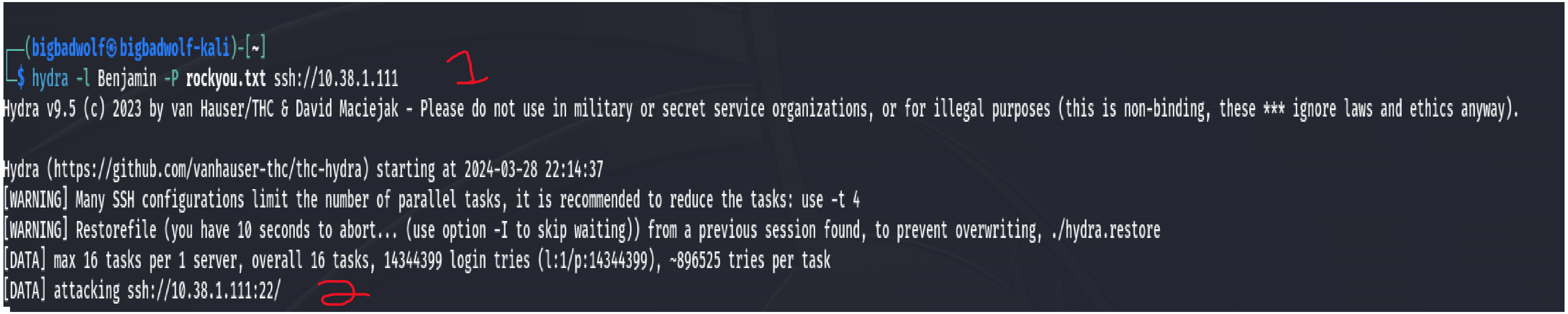
Screenshot of Command Ran: nmap



```
┌──(bigbadwolf㉿bigbadwolf-kali)-[~]
└─$ sudo nmap -sS -sV 10.38.1.111  1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-28 22:11 PDT
Nmap scan report for 10.38.1.111
Host is up (0.000085s latency).
Not shown: 999 closed tcp ports (reset)  2
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.7p1 Debian 2 (protocol 2.0)
MAC Address: 08:00:27:50:4C:14 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

1) Command ran; SYN Scan and Version Scan ran against target IP
2) Open ports, services, and version of services on target host discovered

Screenshot of Command Ran: Hydra



```
┌──(bigbadwolf㉿bigbadwolf-kali)-[~]
└─$ hydra -l Benjamin -P rockyou.txt ssh://10.38.1.111
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-28 22:14:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.38.1.111:22/
```

1) Command ran; user "Benjamin" listed and given a password list "rockyou.txt" ran against SSH on victim host IP
2) Confirmation of attack on designated port and host

In The Following Demonstration:

1) I will act as the "script kiddie" portraying his journey in the attack, from network scan, to brute force attack.
2) I will then act as the company's cybersecurity analyst by taking the logs and uploading them to Splunk for further analysis, and create an alert.

gBadWolf [Running] - Oracle VM VirtualBox
Machine
View
Input
Devices
Help
Applications
Places
Mar 3 19:24
KALI LINUX
"the quieter you become, the more you are able to hear"

Demonstration Summary

- Simulated a very loud brute force attack
- Collected the authentication logs
- Uploaded the logs to Splunk
- Analyzed the logs
- Created an alert

Mitigation

- Close Port 22
- SSH Keys
- Strong passwords
- Do not leave credentials online
- Allow Splunk to manually monitor logs