

Funbox: Script Kiddies

domingo, 1 de agosto de 2021 23:43

Este é o relatório de teste de invasão (write-up) da máquina "Funbox: Script Kiddie".
Essa VM é um desafio de nível "fácil", então tentei explorar outras formas de invasão além das mais correlativas a esse tipo de desafio.

Segue abaixo o ataque de modo detalhados, inclusive os passos que não deram certo.

```
root@pentester: /home/jbf/funbox11 x root@pentester: /home/jbf/funbox11 x root@pentester: /home/jbf/funbox11 x
Currently scanning: Finished! | Screen View: Unique Hosts
906 Captured ARP Req/Rep packets, from 6 hosts. Total size: 54360

IP          At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.0.1  [REDACTED]         53     3180 HUMAX Co., Ltd.
192.168.0.41 [REDACTED]         8      480  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.120 [REDACTED]        9      540  Hon Hai Precision Ind. Co.,Ltd.
192.168.0.200 [REDACTED]        3      180  Unknown vendor
192.168.0.68  [REDACTED]        82     49260 Arcadyan Corporation
192.168.0.232 08:00:27:36:62:db 12      720  PCS Systemtechnik GmbH
```

Como o alvo é uma máquina dentro de minha rede local, utilizei a ferramenta "netdiscover", para identificar o endereço ip do alvo.

```
(root@pentester) - [ /home/jbf/funbox11 ]
# cat hosts.txt | grep "Up"
Host: 192.168.0.1 ( ) Status: Up
Host: 192.168.0.41 ( ) Status: Up
Host: 192.168.0.68 ( ) Status: Up
Host: 192.168.0.120 ( ) Status: Up
Host: 192.168.0.200 ( ) Status: Up
Host: 192.168.0.232 ( ) Status: Up
Host: 192.168.0.210 ( ) Status: Up
```

Para validação, utilizei o "nmap".

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.3c
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 a6:0e:30:35:3b:ef:43:44:f5:1c:d7:c6:58:64:09:92 (RSA)
  256 c2:d8:bd:62:bf:13:89:28:f8:61:e0:a6:c4:f7:a5:bf (ECDSA)
  256 12:60:6e:58:ee:f2:bd:9c:ff:b0:35:05:83:08:71:b8 (ED25519)
25/tcp    open  smtp         Postfix smtpd
smtp-comands: funbox11, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN,
ssl-cert: Subject: commonName=funbox11
Issuer: commonName=funbox11
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2021-07-19T16:52:14
Not valid after: 2031-07-17T16:52:14
MD5: a87d b2f7 11b8 5f43 8716 517e 4445 7ed1
SHA-1: 72cb ba50 cfff 9e5d 5537 3ae8 7648 34df f84b 714d
ssl-date: TLS randomness does not represent time
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
http-generator: WordPress 5.7.2
http-methods:
  Supported Methods: GET HEAD POST OPTIONS
http-server-header: Apache/2.4.18 (Ubuntu)
http-title: Funbox: Scriptkiddie
110/tcp   open  pop3         Dovecot pop3d
pop3-capabilities: CAPA TOP RESP-CODES PIPELINING UIDL AUTH-RESP-CODE SASL
139/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
imap-capabilities: capabilities SASL-IR more post-login listed LITERAL+ LOGIN-REFERRALS Pre-login ID OK ENABLE IDLE LOGINDISABLEDA0001 IMAP4rev1 have
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:36:62:DB (Oracle VirtualBox virtual NIC)
Service Info: Hosts: funbox11, FUNBOX11; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Executado o "nmap" e identificado diversas portas de serviço em status "open", as que mais se destacaram foram as porta 21/tcp, 80/tcp e 445/tcp.

```
# gobuster dir -e -u http://funbox11/ -w /usr/share/wordlists/dirb/big.txt -x "php,txt"

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://funbox11/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php,txt
[+] Expanded: true
[+] Timeout: 10s

2021/08/01 23:28:56 Starting gobuster in directory enumeration mode

http://funbox11/.htaccess (Status: 403) [Size: 273]
http://funbox11/.htaccess.php (Status: 403) [Size: 273]
http://funbox11/.htpasswd (Status: 403) [Size: 273]
http://funbox11/.htpasswd.txt (Status: 403) [Size: 273]
http://funbox11/.htpasswd.php (Status: 403) [Size: 273]
http://funbox11/.htpasswd.txt (Status: 403) [Size: 273]
http://funbox11/index.php (Status: 301) [Size: 0] [→ http://funbox11/]
http://funbox11/license.txt (Status: 200) [Size: 19915]
http://funbox11/server-status (Status: 403) [Size: 273]
http://funbox11/wp-content (Status: 301) [Size: 309] [→ http://funbox11/wp-content/]
http://funbox11/wp-admin (Status: 301) [Size: 307] [→ http://funbox11/wp-admin/]
http://funbox11/wp-includes (Status: 301) [Size: 310] [→ http://funbox11/wp-includes/]
http://funbox11/wp-config.php (Status: 200) [Size: 0]
http://funbox11/wp-trackback.php (Status: 200) [Size: 135]
http://funbox11/wp-login.php (Status: 200) [Size: 6180]
http://funbox11/xmlrpc.php (Status: 405) [Size: 42]
```

Executado a ferramenta "gobuster" e identificado ao retornar arquivos e diretórios de que se trata de um servidor com wordpress.

```
[+] astra
Location: http://funbox11/wp-content/themes/astra/
Last Updated: 2021-07-29T00:00:00.000Z
Readme: http://funbox11/wp-content/themes/astra/readme.txt
[!] The version is out of date, the latest version is 3.6.7
Style URL: http://funbox11/wp-content/themes/astra/style.css
Style Name: Astra
Style URI: https://wpastra.com/
Description: Astra is fast, fully customizable & beautiful WordPress theme suitable for blog, personal portfolio, ...
Author: Brainstorm Force
Author URI: https://wpastra.com/about/

Found By: Known Locations (Aggressive Detection)
- http://funbox11/wp-content/themes/astra/, status: 200

Version: 3.6.5 (80% confidence)
Found By: Style (Passive Detection)
- http://funbox11/wp-content/themes/astra/style.css, Match: 'Version: 3.6.5'

[+] block-lite
Location: http://funbox11/wp-content/themes/block-lite/
Latest Version: 1.2.2 (up to date)
Last Updated: 2020-08-18T00:00:00.000Z
Readme: http://funbox11/wp-content/themes/block-lite/README.txt
Style URL: http://funbox11/wp-content/themes/block-lite/style.css
Style Name: Block Lite
Style URI: https://organicthemes.com/theme/block-lite/
Description: The Block Lite theme features a modern and responsive design with a block style layout for blog post ...
Author: Organic Themes
Author URI: https://organicthemes.com

Found By: Urls In Homepage (Passive Detection)
Confirmed By: Known Locations (Aggressive Detection)
- http://funbox11/wp-content/themes/block-lite/, status: 500

Version: 1.2.2 (80% confidence)
Found By: Style (Passive Detection)
- http://funbox11/wp-content/themes/block-lite/style.css, Match: 'Version: 1.2.2'
```

Foi executado o "wpscan" e foi encontrado dois plugins (Astra e Block-lite), mas nenhum deles possui exploit públicos disponíveis.

```
[+] admin
Found By: Rss Generator (Passive Detection)
Confirmed By:
Wp Json Api (Aggressive Detection)
- http://funbox11/index.php/wp-json/wp/v2/users/?per_page=100&page=1
Author Id Brute Forcing - Author Pattern (Aggressive Detection)
Login Error Messages (Aggressive Detection)
```

Com o "wpscan" executado a enumeração de usuário e foi localizado o usuário "admin".
A aplicação está vulnerável a ataques de enumeração de usuários e a ataques de brute force.

Tentei enumerar outros usuários de forma manual, mas sem sucesso.
Foi tentando fazer um ataque de brute-force com o usuário "admin" e a wordlist rockyou, para senhas, mas sem sucesso.

```
(root@pentester)~/home/jbf
# smbclient -L \\funbox11 -N

Sharename      Type            Comment
-----
print$         Disk            Printer Drivers
IPC$           IPC             IPC Service (funbox11 server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

Como o alvo tem a porta 445/tcp, que é do serviço de compartilhamento SMB aberto, foi feito a enumeração da porta.
A porta está vulnerável a ataques "login anonymous", então foi feito a exploração, mas não tem nenhum diretório compartilhado.

```
(root@pentester)~/home/jbf/funbox11
# searchsploit "dovecot"

Exploit Title | Path
-----
Dovecot 1.1.x - Invalid Message Address Parsing Denial of Service | linux/dos/32551.txt
Dovecot IMAP 1.0.10 < 1.1rc2 - Remote Email Disclosure | multiple/remote/5257.py
Dovecot with Exim - 'sender_address' Remote Command Execution | linux/remote/25297.txt

Shellcodes: No Results

(root@pentester)~/home/jbf/funbox11
# searchsploit -m multiple/remote/5257.py
Exploit: Dovecot IMAP 1.0.10 < 1.1rc2 - Remote Email Disclosure
URL: https://www.exploit-db.com/exploits/5257
Path: /usr/share/exploitdb/exploits/multiple/remote/5257.py
File Type: ASCII text, with CRLF line terminators
Copied to: /home/jbf/funbox11/5257.py

(root@pentester)~/home/jbf/funbox11
# python 5257.py
Dovecot IMAP [1.0.10 -> 1.1rc2] Exploit
Prints out all E-Mails for any account if special configuration option is set
Exploit written by kingcope

usage: 5257.py <hostname/ip address> <account> [-nossll]
```

Voltei uma passo atrás e verifiquei se havia possibilidade de exploração da porta 143/TCP que é do IMAP.
Foi encontrado uma exploit para ele, mas ao executar o mesmo, solicita uma conta de e-mail para uso da aplicação, informação essa que não temos disponível.

