Linderhof: uma ferramenta para avaliação de sistemas de mitigação de ataques reflexivos volumétricos (DDoS)

Amanda Lopes Dantas[1], **Matheus de Oliveira Vieira**[1],
Alan Tamer Vasques[2], **João José Costa Gondim**[1,2]

[1]Departamento de Ciência da Computação – Universidade de Brasília (UnB)
Brasília – DF – Brasil

[2]Programa de Pós-Graduação Profissional em Engenharia Elétrica - PPEE
Departamento de Engenharia Elétrica – Universidade de Brasília (UnB)
Brasília – DF – Brasil

amandadantas19@gmail.com,{matheus.vieira,alan.tamer}@aluno.unb.br,gondim@unb.br

Abstract. *Denial of service attacks aim to disrupt legitimate users from accessing a particular service. Its amplified and reflected version is more commonly used and has become an increasing threat to the Internet stability. The Linderhof tool was created for the study of reflective and volumetric attacks mitigation systems. It enables the evaluation of the CoAP, DNS, Memcached, NTP, SSDP, SNMP protocols and is extensible to other protocols. In this paper the tool and its use will be presented in more detail.*

Resumo. *Os ataques de negação de serviço têm como objetivo interromper o acesso de usuários legítimos a um determinado serviço. A versão amplificada e refletida desse tipo de ataque é mais comumente utilizada e têm se tornado uma ameaça crescente à estabilidade da Internet. A ferramenta Linderhof foi criada para o estudo de sistemas de mitigação de ataques reflexivos volumétricos. Ela possibilita a avaliação dos protocolos CoAP, DNS, Memcached, NTP, SSDP, SNMP e é extensível a outros protocolos. Nesse artigo a ferramenta e seu uso serão apresentadas em mais detalhes.*

1. Introdução

Um ataque de Negação de Serviço (DoS, *Denial of Service*) tem como objetivo impedir o acesso de usuários legítimos aos serviços fornecidos pela vítima [Riza et al. 2019]. Existem vários contextos onde um ataque DoS pode ocorrer, como em sistemas operacionais e serviços baseados em rede. Um ataque DoS por reflexão/amplificação tem o objetivo de mascarar a fonte do ataque, usando terceiros para repassar tráfego ilegítimo para a vítima. Esses terceiros são denominados refletores [Peng et al. 2007]. O atacante manda para o refletor pacotes com o endereço de origem igual ao IP da vítima. Assim, quando o refletor responder aos pacotes, ele direciona o tráfego de resposta à vítima. Nesse ataque, geralmente são usados protocolos onde o pacote de *reply* é maior que o pacote de *request*, assim, o ataque também gera um efeito de amplificação [Paxson 2001]. O uso de refletores dificulta o rastreamento da origem do ataque [Rossow 2014].

Um ataque Distribuído de Negação de Serviço (DDoS, *Distributed Denial of Service*) ocorre quando vários dispositivos coordenados atacam uma ou mais vítimas, com o

intuito de exaurir os recursos de processamento ou conectividade dessas vítimas. Assim, os ataques Distribuídos de Negação de Serviço por Reflexão Amplificada (AR-DDoS, *Amplified Reflection Distributed Denial of Service*) são ataques de negação de serviço distribuídos, refletidos e amplificados.

O volume do tráfego dos ataques DDoS têm crescido nos últimos anos [Mahjabin et al. 2017]. Um exemplo desse crescimento é o ataque ao provedor DNS Dyn [Hilton 2016], que ocorreu em 2016, e afetou empresas como Amazon, Spotify, Netflix, Twitter e Github. Esse ataque chegou a magnitude de 1.2 Tbps, causando horas de indisponibilidade e perdas financeiras para as empresas afetadas, além da perda de clientes.

Visando a melhoria das formas de mitigação, o estudo desses ataques motivou a necessidade de implementações de referência. Entre outros requisitos, foram considerados: implementação do ataque sobre diferentes protocolos; controle de condução do ataque no que diz respeito à sua dinâmica; instrumentação e *logging*.

Esse trabalho apresenta a ferramenta Linderhof, que foi desenvolvida para servir de apoio em pesquisas relacionadas à mitigação de ataques AR-DDoS. Ela implementa ataques AR-DDoS abusando vários protocolos com a finalidade de estudar a dinâmica desses ataques em um ambiente controlado e acadêmico para que técnicas de defesa e de controle de danos sejam propostas e estudadas.

Nesse contexto, a ferramenta também suporta a avaliação de soluções de mitigação para tais ataques. [Gondim and Albuquerque 2019], [Gondim et al. 2020], [Gondim et al. 2016] e [Vasques and Gondim 2019] utilizaram versões iniciais que implementavam isoladamente os ataques para diversos protocolos compartilhando um *core* de geração de pacotes. Estas várias versões foram unificadas levando à versão apresentada nesse trabalho, que foi utilizada em [Vasques and Gondim 2020]. Nesses trabalhos, a ferramenta foi usada para a caracterização do comportamento de saturação de refletores sobre diversos protocolos. A ferramenta também tem sido utilizada no desenvolvimento de técnicas de detecção e identificação de refletores, além de avaliação de capacidade de sistemas de mitigação.

O restante desse artigo está organizado da seguinte forma: a Seção 2 apresenta a arquitetura e os detalhes de implementação do Linderhof, a Seção 3 explica como a demonstração será feita no salão, assim como informa onde o código-fonte e o vídeo estão disponíveis, a Seção 4 analisa o desempenho da ferramenta em um caso específico e, por fim, na Seção 5, as conclusões são expostas.

2. Ferramenta Linderhof

Linderhof é o nome de um palácio real alemão, construído por Ludwig II no século XIX, no sudoeste da região da Baviera. A ferramenta, desenvolvida em C, possui esse nome em alusão à Galeria de Espelhos (*Hall of Mirrors*) do palácio, cujos espelhos refletiam e amplificavam a luz das velas dos candelabros que ali existiam, de forma similar ao que ocorre com os pacotes nos ataques AR-DDoS. Nesse sentido, cada protocolo implementado na ferramenta representa um espelho (*mirror*) diferente da sua galeria.

A versão da ferramenta apresentada nesse artigo é a 1.0.0. Ela implementa o ataque AR-DDoS para os seguintes protocolos: CoAP, DNS, Memcached, NTP, SNMP e SSDP. A ferramenta gera os *probes* que são enviados aos refletores, que por sua vez

os amplificam e enviam ao alvo. No Linderhof, para um dado protocolo, além de suas características específicas, controla-se a taxa de geração de *probes*, a duração dos ataques, a evolução temporal da intensidade do ataque, a quantidade de refletores utilizados e seu regime de emprego. A ferramenta relata a quantidade de *probes* efetivamente enviados e os volumes de bytes transmitidos.

2.1. Arquitetura

A ferramenta é composta por quatro módulos principais (Fig. 1) descritos a seguir:

- ***Interface*:** é responsável pela interação com o usuário, recebendo como entrada os parâmetros do ataque e devolvendo na saída um resumo dos pacotes gerados e enviados;
- ***Commander*:** é o módulo onde ocorre o planejamento do ataque, de acordo com o protocolo (espelho) selecionado e os parâmetros escolhidos pelo usuário;
- ***Hall of Mirrors*:** é encarregado pela geração dos pacotes e pela iniciação dos ataques. Também é onde os espelhos são adicionados à ferramenta;
- ***Injector*:** é onde o ataque de fato ocorre, realizando o envio dos pacotes para o(s) refletor(es) e a geração de um resumo dos pacotes gerados e enviados. Esse módulo também regula a quantidade e a taxa de injeção de pacotes.

Entre as principais funcionalidades estão a possibilidade de enviar tráfego a múltiplos refletores, personalização dos parâmetros do ataque, como portas e opções específicas dos protocolos implementados e o suporte ao protocolo IPv6.

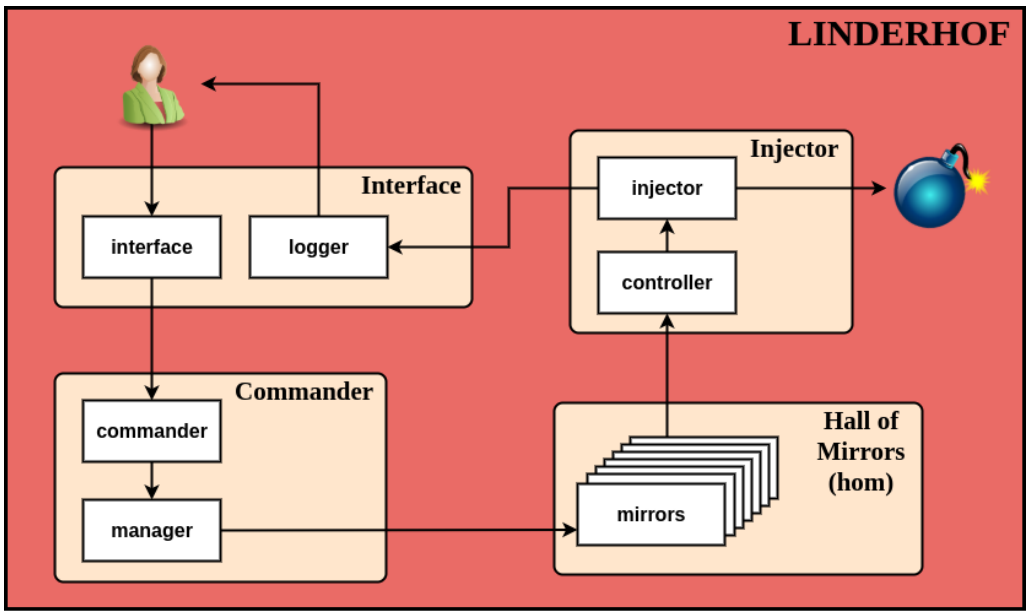

Figura 1. Arquitetura do Linderhof

2.2. Modos de Ataque

A ferramenta disponibiliza quatro modos de ataques que diferem no processo de injeção de pacotes. A injeção de pacotes segue níveis de intensidade, baseados em potência de 10.

O Linderhof possui 10 níveis disponíveis (1 a 10) e cada um possui uma intensidade diferente, que vai crescendo de forma exponencial, conforme a Eq. 1 (PpS significa Pacotes por Segundo):

$$PpS = 10^{\text{nível-1}} \tag{1}$$

Assim, por padrão, é gerado um número fixo de pacotes, distribuídos igualmente entre cada refletor, por nível. Já no modo de ataque incremental, a ferramenta aumenta o nível do ataque de acordo com a frequência passada pelo usuário. O modo agressivo, por sua vez, extrapola o nível do ataque para os refletores. Ou seja, cada refletor recebe a quantidade total de pacotes desejada para aquele nível. E, por fim, para o modo *flood* a ferramenta envia o máximo de pacotes possível para todos os refletores.

2.3. Implementação

A ferramenta foi desenvolvida em linguagem C com uma preocupação de deixá-la o mais modular possível, para que sua expansão acontecesse de forma simplificada. Desse modo, além dos seis protocolos atualmente suportados (CoAP, DNS, NTP, Memcached, SSDP e SNMP), é possível a implementação de outros protocolos sem que seja necessária uma modificação na estrutura já existente da ferramenta.

Os parâmetros e argumentos para inicialização da ferramenta e preparo do ataque podem ser passados via linha de comando ou via arquivo de configuração. A tabela 1 contém uma lista com todos os parâmetros globais do Linderhof, ou seja, os que podem ser utilizados com qualquer espelho, enquanto que a tabela 2 possui a lista de parâmetros específicos para cada espelho implementado na ferramenta, ambos para utilização via linha de comando.

3. Demonstração

A demonstração no Salão de Ferramentas será realizada utilizando um conjunto de máquinas reais e/ou virtuais, e seguirá o roteiro idêntico ao do vídeo enviado. Ao todo são necessárias pelo menos três máquinas: um atacante, um refletor e uma vítima, sendo que o Linderhof precisa ser instalado apenas na máquina do atacante. Em caso de serem utilizadas três máquinas físicas, elas serão interligadas por um *switch* e cabos. Essa rede poderá ser expandida com mais máquinas para demonstrar o uso de múltiplos refletores. Dependendo das máquinas envolvidas, será demonstrado o custo do ataque e sua consequente vantagem.

Serão explorados os diferentes protocolos e modos de ataques disponibilizados pela ferramenta e o resultado da demostração será exemplificado pelos logs da ferramenta e por análise do trafego de rede nas máquinas envolvidas. A demonstração poderá ser realizada *in loco* ou acessando o CyberSecLab via Internet.

O código-fonte da ferramenta foi disponibilizado na URL **https://cyberseclab.gigacandanga.net.br/CyberSecLab/linderhof-sbrc2020** e, para acessar o repositório, tanto o usuário quanto a senha são "**sbrc2020**". A documentação da ferramenta se encontra na pasta **docs** e na Wiki disponível no repositório. O vídeo de demonstração do Linderhof está disponível na URL **https://www.youtube.com/watch?v=M0ss3MAIRo8**, onde a instalação e as funcionalidades da ferramenta são detalhadas.

Tabela 1. Parâmetros globais do Linderhof

Parâmetro Curto	Parâmetro Longo	Parâmetro Obrigatório	Argumento Obrigatório	Argumento Padrão	Descrição
-m	--mirror	Sim	Sim	Nenhum	Espelho a ser utilizado
-t	--target	Sim	Sim	Nenhum	Endereço IP da vítima
-r	--reflector	Sim	Sim	Nenhum	Endereço IP do refletor ou arquivo com refletores
-g	--targport	Não	Sim	Aleatório (40000-60000)	Porta de origem da requisição
-p	--reflecport	Não	Sim	Padrão do Espelho	Porta de destino da requisição
-l	--level	Não	Sim	1	Nível do ataque
-d	--timer	Não	Sim	Ilimitado	Duração do ataque (em segundos)
-i	--inc	Não	Sim	Ilimitado	Duração de cada nível (em segundos)
-c	--config	Não	Sim	linderhof.conf	Arquivo de configuração
-a	--aggressive	Não	Não	-----	Modo agressivo
-f	--flood	Não	Não	-----	Modo *flooding*
-h	--help	Não	Não	-----	Ajuda

Tabela 2. Parâmetros dos espelhos do Linderhof

Parâmetro Curto	Parâmetro Longo	Parâmetro Obrigatório	Argumento Obrigatório	Argumento Padrão	Descrição
-D	--domain-name	Não	Sim	ddos.dns.com	DNS - Nome de domínio
-V	--upnp-version	Não	Sim	1.0	SSDP - Versão do UPnP
-U	--unicast	Não	Não	-----	SSDP - M-SEARCH no formato unicast
-C	--community-string	Não	Sim	public	SNMP - Comunidade
-R	--max-repetitions	Não	Sim	2000	SNMP - Campo max-repetitions
-Z	--szx	Não	Sim	6	CoAP - Campo SZX
-P	--uri-path	Não	Sim	/.well-known/core	CoAP - Caminho da URI

4. Caso de uso

Para demonstrar um caso real de utilização do Linderhof, foi utilizado um computador pessoal com as seguintes configurações, que atuou como um atacante, gerando tráfego a um determinado refletor:

- **Processador:** Intel Core i9-9900KS @ 4.00GHz;
- **Memória:** 32GB DDR4 @ 2666MHz RAM;
- **Interface de rede:** GigabitEthernet Intel I219-V;
- **Sistema Operacional**: Ubuntu 18.04 LTS x64.

Foram gerados ataques utilizando os seis protocolos disponíveis na ferramenta, nos seus 10 níveis, sendo 5 segundos para cada nível, com destino aos endereços IPv4 e IPv6 do refletor. Foi utilizado o comando abaixo, variando-se apenas as opções ”mirror”, ”ip-vitima”e ”ip-refletor”:

linderhof-sbrc2020$ bin/lhf -m *mirror* -t *ip-vitima* -r *ip-refletor* -d 50 -i 5 -l 1

Com o auxílio do *tcpdump*, foram analisadas as quantidades de tráfego e pacotes gerados pela ferramenta em cada um dos protocolos testados, tanto IPv4 quanto IPv6, e o resultado está exibido nas figuras 2, 3, 4 e 5.

Nota-se que a quantidade de pacotes gerados via IPv6, a partir do nível 5, é ligeiramente menor. Isso se deve ao tamanho do cabeçalho IPv6, que é de 40 bytes, contra 20 bytes do cabeçalho padrão do IPv4. Essa sobrecarga de 20 bytes em cada um dos pacotes faz com que nos níveis mais altos, onde uma grande quantidade de pacotes é gerada, o computador e o meio de comunicação não comporte todos os pacotes daqueles níveis.

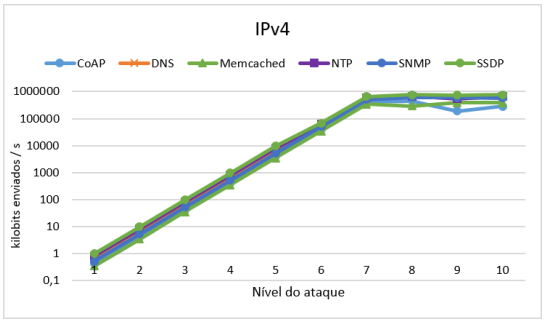

Figura 2. Kbps gerados - IPv4

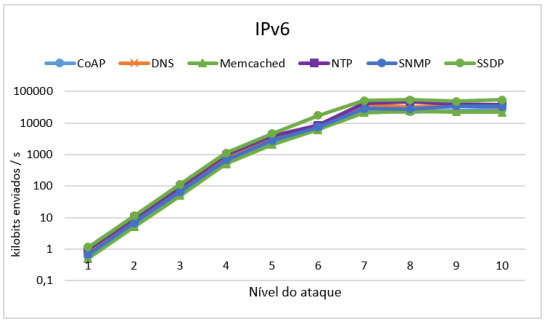

Figura 3. Kbps gerados - IPv6

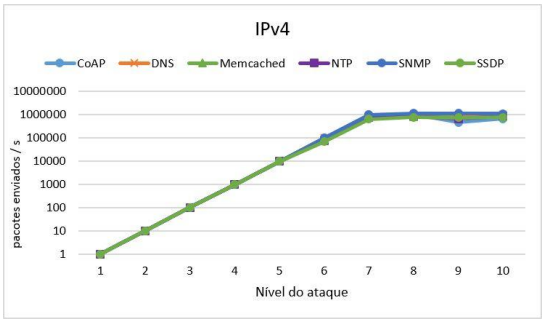

Figura 4. pkt/s gerados - IPv4

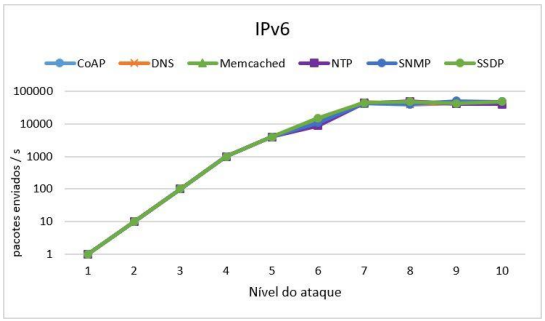

Figura 5. pkt/s gerados - IPv6

Também é possível notar, que a partir do nível 7, não foi possível gerar a quantidade máxima de pacotes destes níveis. Uma possível explicação é que a capacidade máxima do barramento do computador foi atingida. Dessa forma, a ferramenta se mostra eficiente utilizando ao máximo a capacidade oferecida pelo hardware hospedeiro.

5. Conclusão

A incidência de ataques DDoS no cenário atual da tecnologia têm crescido exponencialmente. Assim, o estudo da mitigação e controle de danos desse tipo de ataque é essencial. A ferramenta Linderhof não só representa uma boa alternativa para o estudo dessa mitigação, como também é uma boa alternativa para o estudo da natureza de ataques DDoS podendo ajudar, assim, a expandir as técnicas de detecção desse tipo de ataque.

Como trabalhos futuros, espera-se a inclusão de diferentes táticas de ataque como *carpet bombing* e *pulse attack*, além do avanço da ferramenta com a elaboração de uma interface gráfica e a inclusão de novos protocolos. Também espera-se criar um *scanner* de refletores, o que tornaria a ferramenta mais próxima do contexto de ataques DDoS reais. Já está sendo desenvolvido um *fork* para DDoS por *flooding*.

Agradecimentos

Os autores agradecem a Igor Miranda, Alexander Vieira, Rodrigo Saldanha e Pedro Henrique Pereira por colaborarem nas versões iniciais da ferramenta, e à GigaCandanga REDECOMEP-DF por seu suporte tecnológico.

Referências

Gondim, J. and Albuquerque, R. d. O. (2019). Mirror saturation in amplified reflection ddos. Actas de las V Jornadas Nacionales de Ciberseguridad; Junio 5-7, 2019, Cáceres,

España. Ed. Caro Lindo, Andrés and García Villalba, Luis Javier and Sandoval Orozco, Ana Lucila, Universidad de Extremadura, Servicio de Publicaciones.

Gondim, J. J. C., de Oliveira Albuquerque, R., Clayton Alves Nascimento, A., García Villalba, L., and Kim, T. H. (2016). A methodological approach for assessing amplified reflection distributed denial of service on the internet of things. *Sensors*, 16(11):1855.

Gondim, J. J. C., de Oliveira Albuquerque, R., and Sandoval, O. A. L. (2020). Mirror saturation in amplified reflection distributed denial of service: A case of study using snmp, ssdp, ntp and dns protocols. `https//doi.org/10.1016/j.future.2020.01.024`. Future Generation Computer Systems.

Hilton, S. (2016). Dyn analysis summary of friday october 21 attack. `https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/`. visitado em: 08/04/2020.

Mahjabin, T., Xiao, Y., Sun, G., and Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, 13(12):1550147717741463.

Paxson, V. (2001). An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review*, 31(3):38–47.

Peng, T., Leckie, C., and Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the dos and ddos problems. *ACM Comput. Surv.*, 39(1).

Riza, A., Yusof, R., Udzir, N., and Selamat, A. (2019). Systematic literature review and taxonomy for ddos attack detection and prediction. *International Journal of Digital Enterprise Technology*, 1:292.

Rossow, C. (2014). Amplification hell: Revisiting network protocols for ddos abuse. In *21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014*.

Vasques, A. T. and Gondim, J. J. C. (2019). Amplified reflection ddos attacks over iot mirrors: A saturation analysis. 2019 Workshop on Communication Networks and Power Systems (WCNPS). IEEE.

Vasques, A. T. and Gondim, J. J. C. (2020). Ataques ddos por reflexão amplificada sobre refletor iot rodando coap. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). Submetido e Aceito.