CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO TECNÓLOGO EM
REDES DE COMPUTADORES

CAROLLYNE MARIA DE SOUZA CONCEIÇÃO
JACKSON AMARO DA SILVA FILHO

ATAQUES DDOS EM AMBIENTES CORPORATIVOS

RECIFE/2023

CAROLLYNE MARIA DE SOUZA CONCEIÇÃO
JACKSON AMARO DA SILVA FILHO

ATAQUES DDOS EM AMBIENTES CORPORATIVOS

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor(a) Orientador(a): Msc Camila

RECIFE/2023

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

C744a Conceição, Carollyne Maria de Souza.
Ataques DDOS em ambientes corporativos / Carollyne Maria de Souza Conceição; Jackson Amaro da Silva Filho. - Recife: O Autor, 2023.
9 p.

Orientador(a): MSc. Camila Bezerra Correia Neves.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro - UNIBRA. Tecnólogo em Redes de Computadores, 2023.

Inclui Referências.

1. Ataques. 2. Negação de serviço. 3. Redes de computadores. 4. Defender. I. Silva Filho, Jackson Amaro da. II. Centro Universitário Brasileiro. - UNIBRA. III. Título.

CDU: 004

Dedicamos esse trabalho a Deus, que é a nossa fortaleza todos os dias, e aos nossos familiares e amigos que nos apoiaram e sempre nos incentivaram a nunca desistir de concluir a nossa graduação.

AGRADECIMENTOS

Agradecemos primeiramente a Deus, o qual foi essencial em toda nossa trajetória até aqui, e esteve sempre conosco em todos os momentos.

Aos nossos familiares, que com muita compreensão e ajuda nos incentivaram e apoiaram a iniciar e concluir o curso.

A coordenação do curso ao qual deu todo apoio para nossa formação.

Agradecemos também à nossa orientadora por ter disponibilizado o seu tempo para nos ajudar e pelo incentivo à realização do nosso projeto de conclusão de curso.

Aos nossos professores desta graduação, que com muita dedicação e empenho nos ensinaram e foram extremamente importantes em todo aprendizado.

E principalmente, agradecemos um ao outro por conseguirmos concluir este projeto com muito empenho e muita luta dentro do que foi possível para nós.

“A persistência é o menor caminho do êxito”.

(Charles Chaplin)

RESUMO

Os ataques de negação de serviço dentro do contexto das redes de computadores vem crescendo e se aprimorando de acordo com o desenvolvimento de novas técnicas de combate aos mesmos. Esses ataques são de grande preocupação para as empresas atualmente, pois tem sido parte significativa da perda de lucros em situações onde a paralisação dos serviços ocorreram devido a estes tipos de ataques, pois eles agem sobrecarregando o tráfego de determinadas aplicações ou serviços de formas variadas visando a interrupção por sobrecarga. Neste trabalho são apresentados os conceitos básicos e o contexto em que esses ataques ocorrem, utilizando um exemplo real de uma ocorrência e que medidas podem ser tomadas para minimizar os riscos na hora de se defender destas tentativas de inundação de um servidor de redes que oferecem um serviço.

Palavras-chave: Ataques, Negação de serviço, Redes de computadores, Defender

ABSTRACT

Denial of service attacks within the context of computer networks have been growing and improving according to the development of new techniques to combat them. These attacks are of great concern to companies today, as they have been a significant part of the loss of profits in situations where service interruptions have occurred due to these types of attacks, as they act by overloading the traffic of certain applications or services in different ways, aiming overload interruption. This work presents the basic concepts and the context in which these attacks occur, using a real example of an occurrence and what measures can be taken to minimize the risks when defending against these attempts to flood a network server that offers a service.

Keywords: Attacks, Denial of service, Computer Network, Defend

SUMÁRIO

Lista de abreviaturas e Siglas

DDos	Distributed Denial of Service
DNS	Domain Name System
IoT	Internet of Things
OOB	Out of Band
BSoD	Blue Screen of Death
PE	Pernambuco

1 INTRODUÇÃO

Ao longo da história da tecnologia foram desenvolvidos vários tipos de sistemas e softwares visando facilitar o controle de informações, desenvolvimento e a otimização de operações das organizações. Com a rápida e crescente expansão da era tecnológica, começaram a ocorrer os crimes cibernéticos, que é uma atividade criminosa virtual que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede.(Kaspersky, 2022).

Na medida em que dados se tornaram commodities de alto valor, foi inevitável o surgimento dos crimes cibernéticos e a abordagem moderna de segurança contra essa prática. Qualquer coisa com valor pode ser comprada, vendida e, mais importante, roubada. As empresas tiveram que enfrentar a nova realidade: é preciso proteger as informações sigilosas contra cibercriminosos.(Avast, 2022).

Os crimes cibernéticos se dividem em diversas modalidades, como por exemplo, ataques DDOS, em que o invasor ataca várias máquinas através de um único computador. Dessa forma o hacker “derruba” servidores, redes privadas. No DDoS, um computador pode controlar diversos outros milhões de computadores, e assim coordenar um ataque em massa a uma rede em específico.(Márcio, 2022).

Um dos maiores ataques de negação de serviço distribuído(DDos), ocorreu em 2016 na empresa DYN que controlava grande parte da infraestrutura do sistema de nomes de domínio(DNS) da Internet. Os hackers utilizaram o DDoS para disparar ataques de negação de serviços contra servidores de nomes de domínios(DNS), que se originou de um malware botnet Mirai, e assim conseguiram derrubar sites como Twitter, Guardian, Netflix, e muitos outros na Europa e nos Estados Unidos. (CAO et al., 2017).

Diante das informações citadas, tendo em vista que o assunto abordado tem se tornado bastante comum, o objetivo desse trabalho de conclusão de curso é abordar o ataque DDoS, demonstrando a segurança da informação e segurança cibernética, com foco nos cuidados e prevenção que uma organização deve ter para se proteger de um ataque distribuído de negação de serviço.

2 REFERENCIAL TEÓRICO

Neste parágrafo será apresentado os principais conceitos para compreender o que é e como funciona um ataque de negação de serviço em uma empresa, bem como o que é e para que serve a segurança da informação e a segurança cibernética, como também um relato técnico feito de como se procedeu um ataque de negação de serviço de uma empresa do estado de Pernambuco.

2.1 ATAQUES DDoS

DDoS, ou negação de serviço distribuída, é um tipo de ataque cibernético que tenta indisponibilizar um website ou recurso de rede inundando-o com tráfego mal-intencionado e deixando-o incapaz de operar.(Akamai, 2022).

Existem numerosas formas deste ataque acontecer, nesse tipo de ataque o invasor infecta diversos dispositivos com malwares ou explora vulnerabilidades dos dispositivos alvos, cada dispositivo infectado é chamado de “bot”, cada bot possui a capacidade de infectar outros aparelhos fazendo com que eles façam parte da sua rede de bots, que por sua vez são chamados de “Botnet”. Depois da criação da botnet o atacante pode controlar todas as máquinas infectadas para atacar ao mesmo tempo o serviço da sua vítima.(Akamai, 2022).

Exploração de vulnerabilidade Esse tipo de ataque explora uma falha na implementação de um protocolo ou até mesmo o próprio protocolo. Podemos tomar como exemplo uma falha na implementação de como Windows NT lidava com pacotes Out of Band (OOB), que causava um Blue Screen of Death (BSoD) (Miranda, 2019, p.7).

Os ataques de negação de serviço volumétricos têm como objetivo saturar a largura de banda da vítima. Podem ser divididos em duas categorias: diretos e refletidos/amplificados. É indispensável para o atacante utilizar uma arquitetura distribuída para efetuar um ataque bem-sucedido nessa categoria de ataque (Miranda, 2019, p.7).

2.2 SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Segundo Zeferino (2020), a segurança da informação é um conjunto de boas práticas e ações que tem a finalidade de proteger um grupo de dados. Essas medidas de segurança podem ser executadas em todas as empresas que trabalham com dados, uma vez que a organização gera informações próprias. Ela é baseada em quatro pilares que sustentam as medidas tomadas para garantir a confidencialidade dos dados, que são: confidencialidade, autenticidade, disponibilidade e integridade

Confidencialidade:

Ela é necessária para que seja definida uma política de acesso de quem pode e quem não pode acessar determinados dados dentro de uma organização. Sendo assim assegurando a garantia de que dados privados e sensíveis só sejam acessados por usuários autorizados previamente. Um exemplo disto seria a criação de grupos de usuários para gerir o acesso aos dados de cada setor dentro de uma empresa, limitando as informações para que sejam acessadas somente as necessárias para o trabalho de determinado setor.

Autenticidade:

Este pilar é destinado a verificação da identidade do usuário. Através dessa validação é que se pode confirmar que o usuário que está fazendo o acesso é realmente o correto. Atualmente as estratégias de verificação em duas etapas através de um e-mail vinculado ou um número de celular para confirmação da identidade são os mais utilizados.

Integridade:

Diz respeito à capacidade de manter um dado ou informação sempre existente no sistema, mesmo que seja apagado ou modificado de forma intencional ou não. Esse dado pode ser mantido através de backups periódicos e/ou armazenamento de dados em outros servidores de suporte, sejam locais ou em nuvem. Outra forma de registrar movimentações é através de logs gerados no sistema para identificar modificações nos sistemas. É de extrema importância a conservação desses dados para que não haja prejuízos irreversíveis.

Disponibilidade

A disponibilidade é o foco principal dos ataques de negação de serviço. É a garantia de que um servidor ou aplicação estará sempre pronta para um uso fluido e estável para seu uso em qualquer momento. O monitoramento constante dos dados e do tráfego com estatísticas sólidas e uma base de uso definida são elementos cruciais para evitar surpresas neste quesito. Como também a atualização periódica de softwares e firmwares utilizados e ferramentas de proteção de dados em caso de tentativas de ataque.

A segurança cibernética é um braço da segurança da informação, nesse caso a segurança cibernética tem o objetivo de prevenir ataques realizados por sistemas que se aproveitam de falhas sistêmicas para assim invadir dispositivos, manipulando, roubando e tornando indisponível uma série de dados ou arquivos. (SCHULTZ, 2020).

2.3 RELATÓRIO TÉCNICO: INVASÃO DE FIREWALL E COMPROMETIMENTO DO VIRTUALIZADOR

Este relatório descreve um incidente de tentativa de invasão em nossa rede, que foi rapidamente detectado e mitigado por nosso sistema de firewall. Após a detecção, a conexão com os servidores foi imediatamente retirada para evitar que a intrusão continuasse. Ao retomar o acesso, descobriu-se que o virtualizador do firewall havia sido comprometido, tornando-o inacessível. Como resultado, o equipamento afetado precisou ser formatado para recuperar o acesso ao sistema de virtualização. Felizmente, nenhum acesso não autorizado foi feito além do virtualizador, garantindo a segurança de nossa rede interna. O virtualizador comprometido tornou-se inacessível se fazendo necessária a formatação do equipamento afetado para recuperar o acesso ao sistema de virtualização. O acesso à rede foi restabelecido após a implementação das medidas necessárias. Foi feita em seguida uma mitigação do ocorrido e os protocolos de segurança foram revistos e reforçados para evitar incidentes semelhantes no futuro. Logs do sistema e outros dados relevantes foram coletados para análise. O impacto desse incidente foi limitado ao comprometimento do firewall do virtualizador. Nenhum acesso não autorizado além do virtualizador foi detectado, protegendo nossa rede interna e sistemas críticos. A formatação dos equipamentos afetados garantiu a eliminação de possíveis ameaças ou modificações não autorizadas. A rápida detecção da tentativa de invasão e o subsequente isolamento de nossos servidores se mostraram eficazes na prevenção de novos comprometimentos. Embora o virtualizador do firewall tenha sido comprometido, nenhum acesso não autorizado foi feito à nossa rede além da barreira inicial. A necessária formatação dos equipamentos restaurou com sucesso o acesso ao sistema de virtualização, garantindo a segurança contínua de nossa infraestrutura. Para evitar futuros incidentes, recomenda-se monitoramento contínuo da segurança, atualizações regulares e fortalecimento dos protocolos de segurança. Investigações adicionais serão conduzidas para identificar a origem e a natureza da tentativa de invasão e reforçar as defesas de nossa rede.

3 METODOLOGIA

O trabalho desenvolvido é delineado por meio da pesquisa bibliográfica, baseado em websites de empresas reconhecidas com conteúdos confiáveis e artigos científicos já publicados, buscados e encontrados no Google Scholar, com critérios aplicados do ano de 2017 até o presente momento, e string de busca: “Ataques DDos”, “Ataques DDos em ambientes corporativos”, “segurança da informação em ataques ddos”, com intuito de encontrar os artigos com maior qualidade e informações necessárias para seu acréscimo em nesse trabalho de conclusão de curso. Como também, foi feito um relatório técnico de uma tentativa de ataque DDos que ocorreu em uma empresa, ao qual com muita cautela nos foi registrado para acrescentar em nosso trabalho, e relatar um acontecimento real vivenciado pela mesma..

A pesquisa bibliográfica é uma etapa fundamental em todo trabalho científico que influenciará todas as etapas de uma pesquisa, na medida em que der o embasamento teórico em que se baseará o trabalho. Consistem no levantamento, seleção, fichamento e arquivamento de informações relacionadas à pesquisa.(AMARAL, 2007, p. 5).

De acordo com Boccato (2006), a pesquisa bibliográfica busca o levantamento e análise crítica dos documentos publicados sobre o tema a ser pesquisado com intuito de atualizar, desenvolver o conhecimento e contribuir com a realização da pesquisa.

4 RESULTADOS

Visto como funcionam os Ataques DDos, e também de acordo com o relatório feito de um ataque tratando de uma tentativa de invasão na rede de uma empresa onde se encontra no tópico 2.3, nos parágrafos abaixo serão abordados e expostos algumas prevenções e defesas que podem ser tomadas diante da tentativa de invasão do relatório exposto e de ataque de negação de serviço em geral, tendo em vista que esses ataques que tem crescido cada vez mais.

Detecção Rápida e Isolamento: A tentativa de invasão foi rapidamente detectada pelo sistema de firewall. E a conexão com os servidores foi imediatamente retirada para evitar a continuidade da intrusão.

Mitigação e Recuperação: Após a detecção, o acesso aos servidores foi retomado, mas descobriu-se que o virtualizador do firewall foi comprometido. O equipamento afetado foi formatado para recuperar o acesso ao sistema de virtualização. A formatação do equipamento garantiu a eliminação de possíveis ameaças ou modificações não autorizadas.

Análise de Logs e Coleta de Dados: Logs do sistema e outros dados relevantes foram coletados para análise. Essa análise pode ser crucial para entender a natureza da tentativa de invasão e identificar possíveis melhorias nos protocolos de segurança.

Revisão e Reforço dos Protocolos de Segurança: Após o incidente, os protocolos de segurança foram revisados e reforçados para evitar incidentes semelhantes no futuro. Investigações adicionais serão conduzidas para identificar a origem e a natureza da tentativa de invasão, contribuindo para melhorias contínuas na segurança.

Restabelecimento do Acesso e Continuidade da Segurança: O acesso à rede foi restabelecido após a implementação das medidas necessárias. A rápida detecção, isolamento e formatação bem-sucedida garantiram a segurança contínua da infraestrutura.

Defesa de Origem e Extremidade: essa abordagem pode ser implementada no computador do usuário, limitando e otimizando o envio e recebimento dos pacotes de rede, assegurando um maior controle entre a conexão (Nascimento, 2021, p.33).

Defesa Intermediária da Rede: são os mecanismos intermediários dentro da infraestrutura e do ambiente, como os IDS e os IPS, que oferecem diferentes meios de proteção à infraestrutura e ao serviço (Nascimento, 2021, p.33).

Defesa Baseada no Hospedeiro: é um método de defesa sem adição de ativos no caminho do tráfego. Nela, o próprio hospedeiro é responsável por sua defesa, que pode ser a prevenção, detecção e mitigação de ameaças. O hospedeiro é capaz de realizar por si só contramedidas de proteção (Nascimento, 2021, p.33) .

5 CONSIDERAÇÕES FINAIS

Este trabalho de conclusão de curso buscou desenvolver e mostrar o que é e como são feitos os ataques DDos, mostrando ataques já efetuados e comprovando o quanto a segurança de uma rede é um ponto essencial na defesa desse tipo de tentativa de interrupção de serviço. Foi realizado um relatório técnico real para mostrar de forma prática como funciona uma das diversas maneiras de se defender de um ataque desse tipo. Com base em todas as informações descritas, no capítulo 4 trata-se sobre os resultados e abordam as prevenções, cuidados e defesas que um ambiente corporativo deve ter para evitar sofrer com um ataque de negação de serviço e assim crescer e se desenvolver nesse meio tecnológico que tem crescido cada vez mais.

REFERÊNCIAS

[1] AKAMAI. Significado de ataque de DDoS, 2022. Disponível em: <https://www.akamai.com/pt/our-thinking/ddos>

[2] AMARAL, J. J. F. Como fazer uma pesquisa bibliográfica. Fortaleza, CE: Universidade Federal do Ceará, 2007. Disponível em: <http://200.17.137.109:8081/xiscanoe/courses1/mentoring/tutoring/Como%20fazer%20pesquisa%20bibliografica.pdf>

[3] AVAST. Qual a história e o futuro da segurança de rede?. 2022. Disponível em: <https://www.avast.com/pt-br/business/resources/future-of-network-security#pc>

[4] BOCCATO, V. R. C. Metodologia da pesquisa bibliográfica na área odontológica e o artigo científico como forma de comunicação. Rev. Odontol. Univ. Cidade de São Paulo, São Paulo, v. 18, n. 3, p. 265-274, 2006.Disponível em: <A pesquisa bibliográfica Cadernos da Fucamp, v.20, n.43, p.64-83/2021 https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/1896>

[5] CAO, C. *et al*.Hey, you, keep away from my device: remotely implanting a virus expeller to defeat Mirai on IoT devices. p. 1–15, 2017. Disponível em: <https://arxiv.org/pdf/1706.05779.pdf> Citado na página 2

[6] KASPERSKY. O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos. 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>

[7] MARCIO. Ascensão dos crimes virtuais, suas legislações e os principais métodos de prevenção, em 2022. Disponível em: <https://cepein.femanet.com.br/BDigital/arqTccs/1811401408.pdf>

[8] MIRANDA. Ataque De Negação De Serviço Por Reflexão Amplificada explorando Memcached. 2019 Disponível em: <https://bdm.unb.br/bitstream/10483/25262/1/2019_IgorFernanesMiranda_tcc.pdf>

[9] NASCIMENTO. Uma Metodologia para Selecionar Contadores de Desempenho de Hardware para dar Suporte ao Diagnóstico não Invasivo a Classificação Ataques DDoS de Inundação Servidores Web. 2021. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/42414/1/DISSERTAÇÃO%20Pablo%20Philipe%20Pessoa%20do%20Nascimento%20%281%29.pdf>

[10] SCHULTZ, Felix. Segurança Cibernética: o que é e como ser um especialista no assunto. Disponível em: <https://blog.milvus.com.br/seguranca-cibernetica-o-que-e/>

[11] ZEFERINO, Denis. O que é Segurança da Informação e qual sua importância?. Disponível em: <https://www.certifiquei.com.br/seguranca-informacao/>