isec
Politécnico de Coimbra

Deception Technology

28/06/2022
Engenharia Informática e Sistemas
José Maria Antunes 2018014484
Miguel Pirré 2020127309

Cadeira de Segurança
Professor Luís Santos

Índice

Introdução

A tecnologia de deceção é um conceito de segurança cibernética que consiste em defender-se contra um ataque estabelecendo com isso, um alvo falso e altamente controlado.
A tecnologia de deceção visa evitar que um cibercriminoso que conseguiu penetrar em uma rede cause grandes danos, oferecendo assim uma deteção mais precisa e rápida de invasores, não criando falsos positivos.

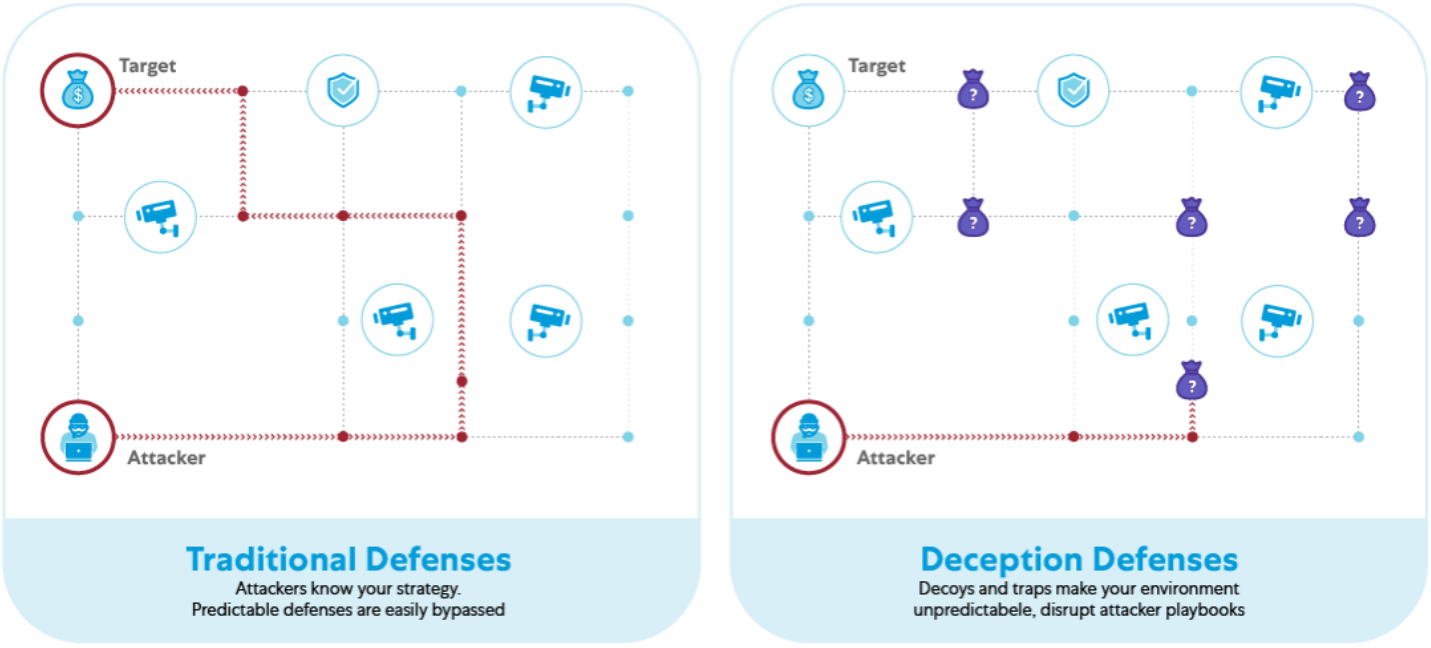


Figura 1 - Comparação do uso de técnicas de mitigação convencionais em comparação com a tecnologia de deceção)

O nosso projeto consiste em apresentar e experimentar um exemplo da tecnologia de deceção e um exemplo sem qualquer tipo de tecnologia de deceção. Para o sucesso da realização, usamos o GNS3 e o Wireshark, montando duas redes:

- ➔ Uma com a tecnologia de deceção;
- ➔ E uma outra sem qualquer tecnologia de deceção;

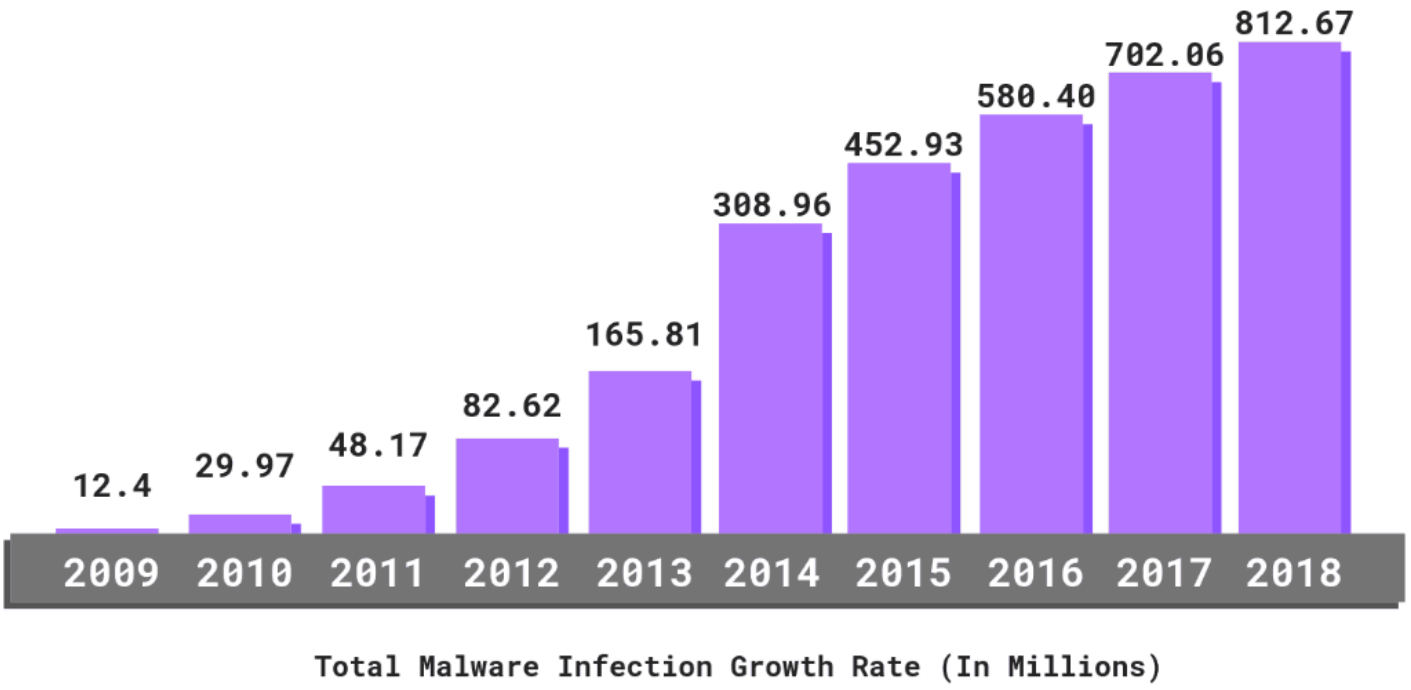
Como tal, foram usadas quatro máquinas virtuais, duas vítimas (Linux/Windows) e dois atacantes (Kali), sendo que cada exemplo terá uma vítima e um atacante, respetivamente.
Para concluir com este trabalhado que nos foi proposto, pretendemos mostrar o uso teórico e prático de uma tecnologia que não será abordada nas aulas e que é cada vez mais relevante no campo da Cyber-segurança.

A Cyber Segurança no mundo atual

Atualmente devido à Pandemia Mundial de Covid-19, registou-se um aumento de 600% de Cyber Crime. Pelo ano de 2025, prevê-se que o custo do Cyber Crime seja de 10,5 Bilhões de dólares, com um já custo anual de 6 Bilhões de dólares fazendo com que os Cyber Ataques acabem por valer 1% de todo o PIB a nível mundial.
Uma empresa em média perde cerca de 2,5 milhões de dólares cada vez que um ataque seja executado com sucesso, colocando muitas vezes em causa a viabilidade da empresa.
Nos dias de hoje, temos também um aumento da <<agressividade>> dos diversos malwares, por exemplo comparativamente a 2015, os *Ransomwares* foram cerca de 57 vezes mais destrutivos dos que os usados nesse ano e anteriores anos.
Com isso tem se vindo a implementar várias medidas, uma delas que está neste momento a ganhar um maior uso são as Políticas "ZERO TRUST" que muitas vezes salvam em média cerca de 1,76 Milhões de dólares as empresas que as decidem usar como um dos métodos de mitigação.
Com isso, nos dias de hoje os principais ataques usados são:

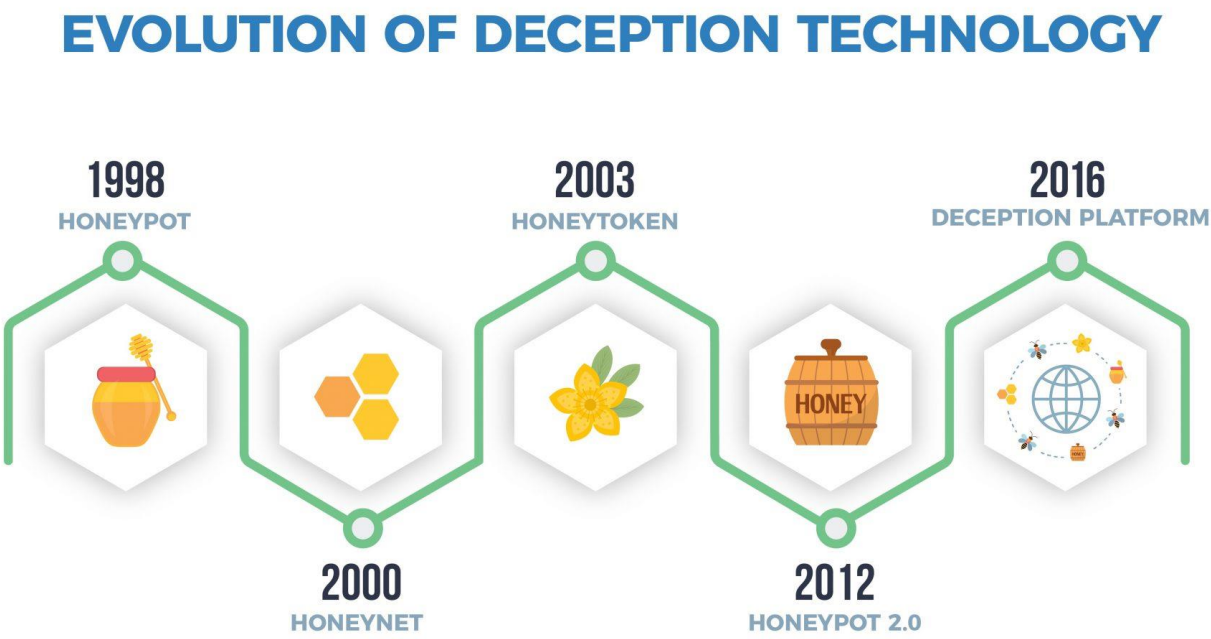
- ➔ Extorsão;
- ➔ Roubo de Identidade;
- ➔ Vazamentos de dados pessoais;
- ➔ Ataques "*Phishing*".

Concluindo, existe a necessidade de implementar medidas não só de vigiar ou de alertar as vítimas para possíveis ataques, mas também que deem para se defender e combater o próprio atacante durante o ataque realizado por ele. É daí que aparecem as técnicas de deceção.



Tecnologia HoneyPot

A tecnologia HoneyPot é uma precursora da Tecnologia de Deceção (Deception Tecnology) e que foi muito importante para o desenrolar da mesma no mercado atual da Cyber Segurança.



A tecnologia HoneyPot é um mecanismo de segurança que está configurado para detetar, desviar ou, de alguma maneira, neutralizar tentativas de uso não autorizado de sistemas de informação usando por isso, um ambiente falso de dados supostos como verdadeiros, mas que na realidade são falsos para ludificar o atacante a entrar num sistema falso, sendo assim capaz de neutralizar o atacante e de analisá-lo de seguida.

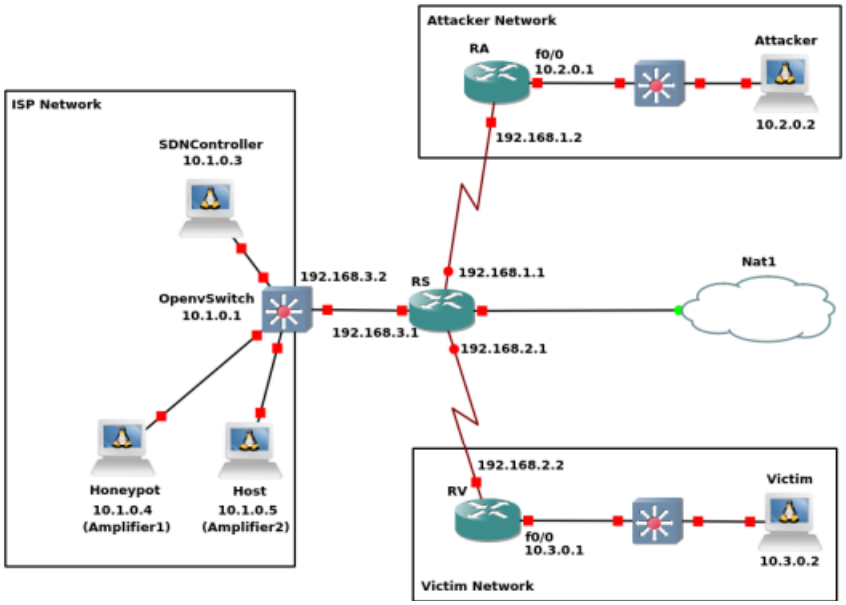
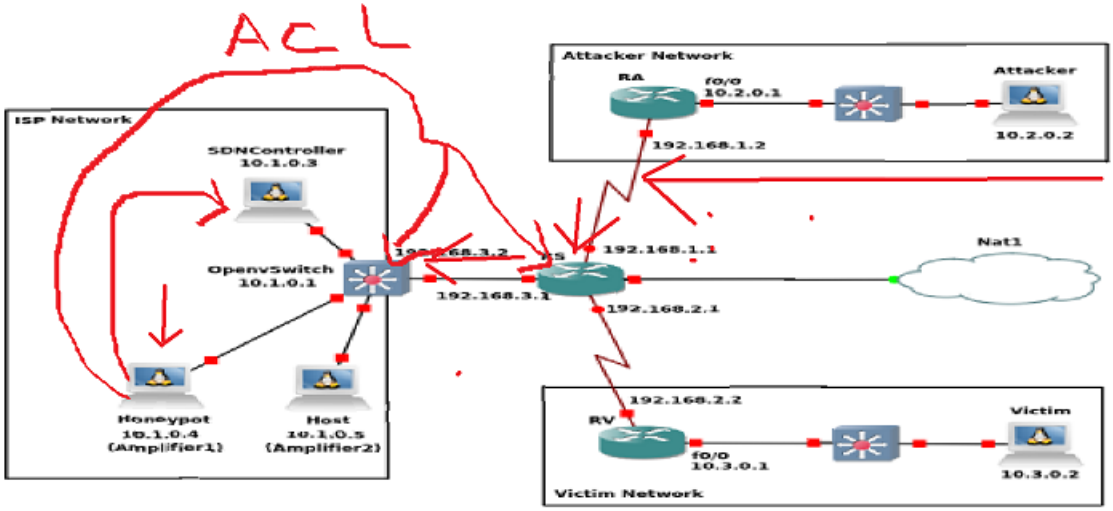


Figura 5 - Exemplo de implementação no GNS3 de um HoneyPot usando o AmpPot)

A figura 5 representa um snapshot exemplo de uma topologia implementada no GNS3 que faz uso ao recurso do HoneyPot(usando o AmpPot). O Router RS faz de ponte de ligação com os routers da rede ISP (10.1.0.0), com o router da rede do Atacante (10.2.0.0) e com o router da rede da Vítima (10.3.0.0). Neste caso, o switch faz o papel de dispositivo de ponta do ISP que guarda a rede onde os *amplifiers*(o "honeypot/isco" com o IP 10.1.0.4 e o host com a informação com o ip 10.1.0.5) estão localizados.
Usa-se o *AmpPot* como o Amplificador do HoneyPot/isco, que mimica um serviço vulnerável a Ataques de Amplificação (Smurf's attacks,Fraggle attacks…etc). Neste caso específico, o AmpPot corre com os serviços de DNS e NTP vulneráveis.
Após o atacante começar o ataque, o AmpPot consegue captar a informação sobre que tipo de ataque está a ser executado (ou a tentar ser executado) e o IP do atacante. Apartir daí, o gestor de redes pode adicionar várias funcionalidades no Switch e na Firewall do OpenvSwitch para criar uma Access-List para negar qualquer acesso à rede usando o ip do atacante/atacantes.
E assim é mitigado um ataque usando o HoneyPot.



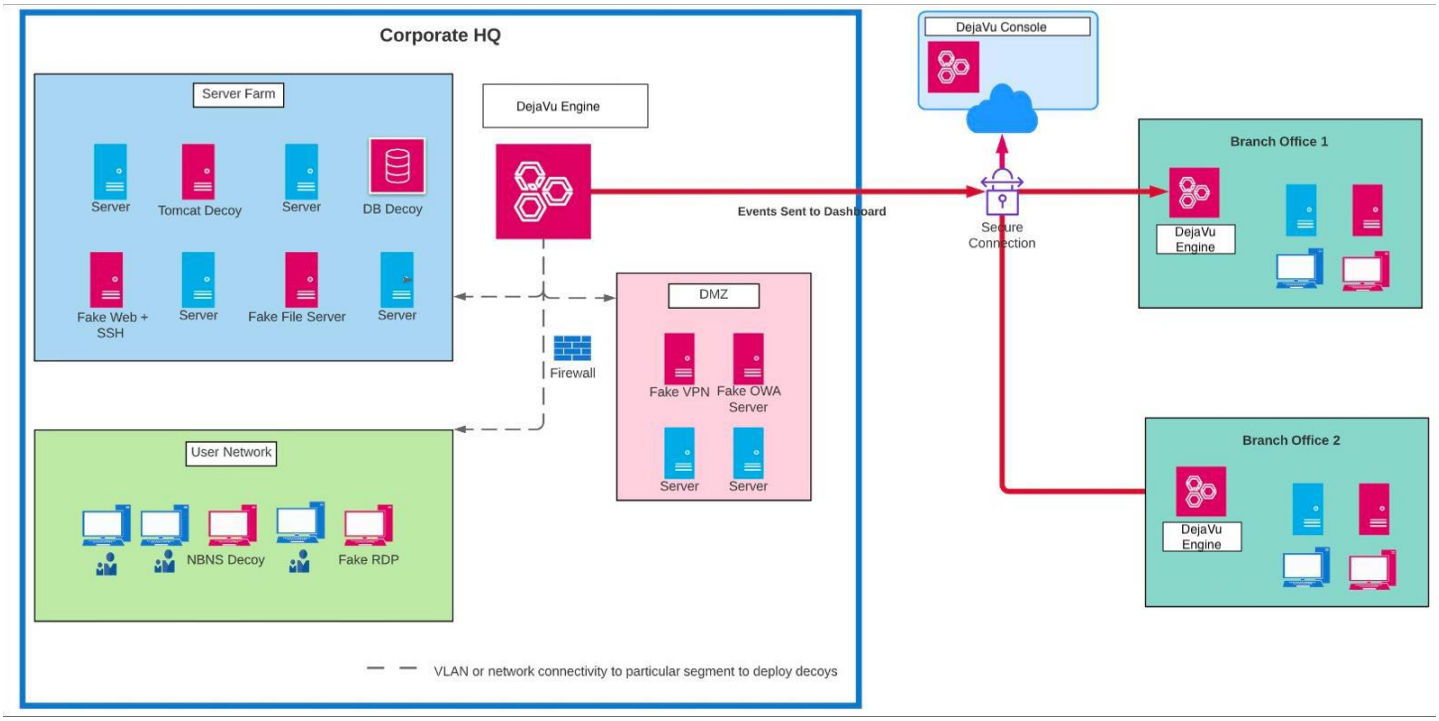
Deception Technology

Deception Technology ou Tecnologia de Deceção é uma categoria de defesas de segurança cibernética simples e eficazes que detetam ameaças antecipadamente e com impacto mínimo no desempenho da rede.

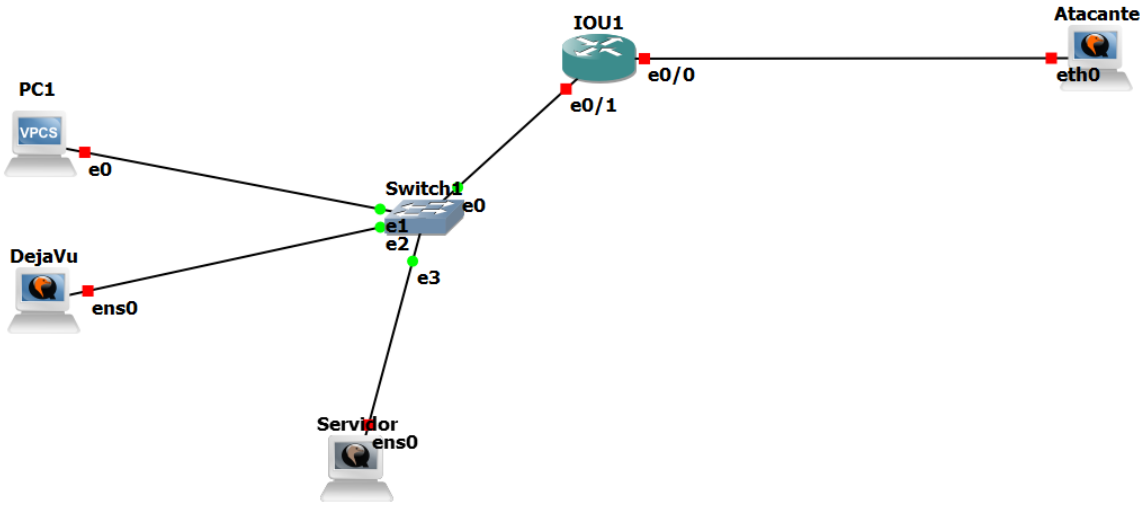
A tecnologia cria sistemas falsos, mas realistas (por exemplo, domínios, bancos de dados, diretórios ativos, servidores, aplicativos, arquivos, credenciais, *breadcrumbs*…) para serem colocados na rede juntamente com os sistemas reais para que os sistemas falsos atuem como iscos para os atacantes.

Os invasores que invadam a rede, não têm como diferenciar a informação falsa da real, e enquanto tentam diferenciar, um alarme silencioso é acionado nos sistemas chamariz fazendo com que esses sistemas comecem a recolher informações sobre as ações e intenções do invasor usando depois essa informação para gerar alertas de alta credibilidade. Diminuindo assim, o tempo de permanência do invasor e acelerando a resposta a incidentes.

A Tecnologia de Deceção, faz com que os atacantes percam tempo explorando sistemas "fantoche" e sem valor, atraindo-os para uma armadilha. Uma vez relevada a presença destes, obter-se-á um indicador antecipado do comportamento do atacante e suas informações que usar-se-ão contra eles.



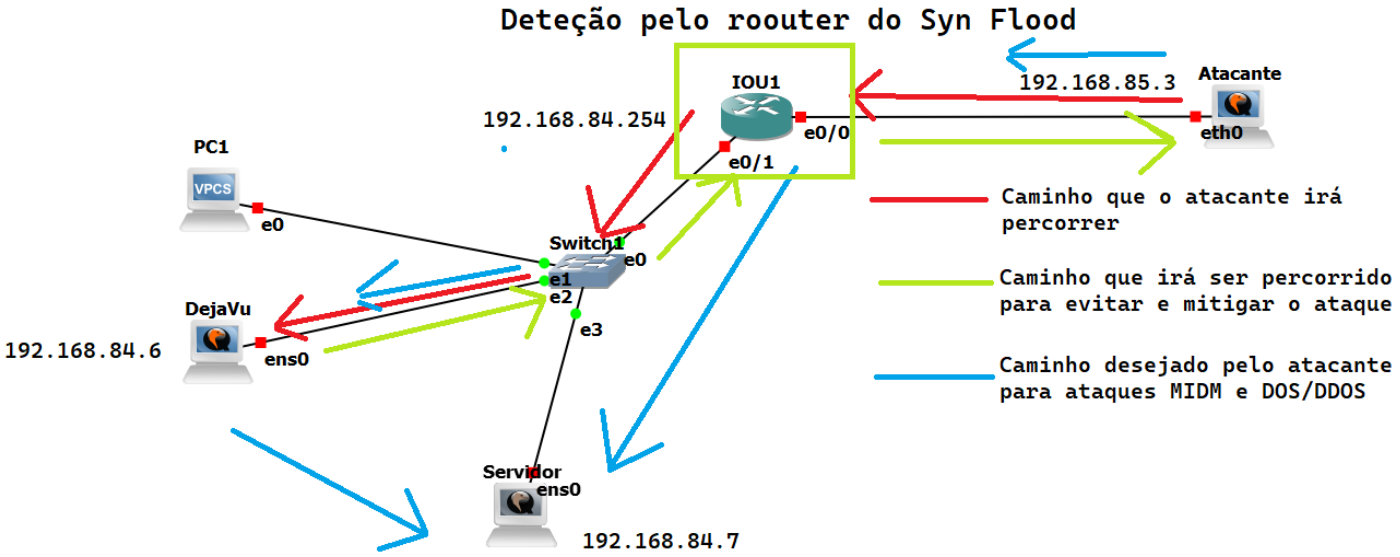
Experimentação usando o DejaVu



Nesta experimentação foram usados:
-> Um router;
-> Um Switch emulado;
-> Uma máquina com a VM do DejaVu a funcionar;
-> Um Servidor Ubuntu;
-> Um Host(PC1) que é VPCS(GNU);
-> Um atacante usando o Kali Linux.

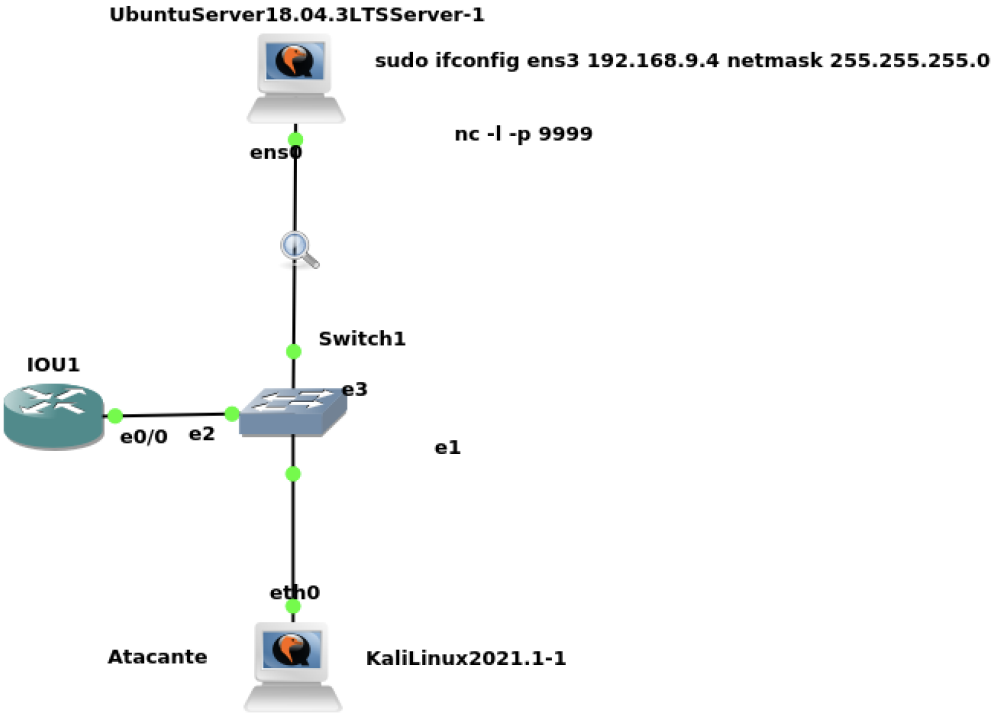
Com o uso do DejaVu , conseguimos colocar várias “armadilhas” que foram capturadas com sucesso pelo Wireshark. Desde ligações Telnet falsas que foram usadas para simular ligações desprotegidas de Telnet entre a vítima(Servidor) e o host(PC1), capturou com sucesso o ip do atacante e no Overall conseguiu-se fazer com que o atacante não só não tivesse sucesso a atacar, como deu para descobrir informação sobre o atacante que pode ajudar numa futura prevenção desse mesmo atacante conectar-se à rede, fazendo uma exceção na firewall para o negar o acesso daquele ip à rede.
Sendo assim, o DejaVu mostrou ser um programa capaz de complementar a segurança de uma rede.

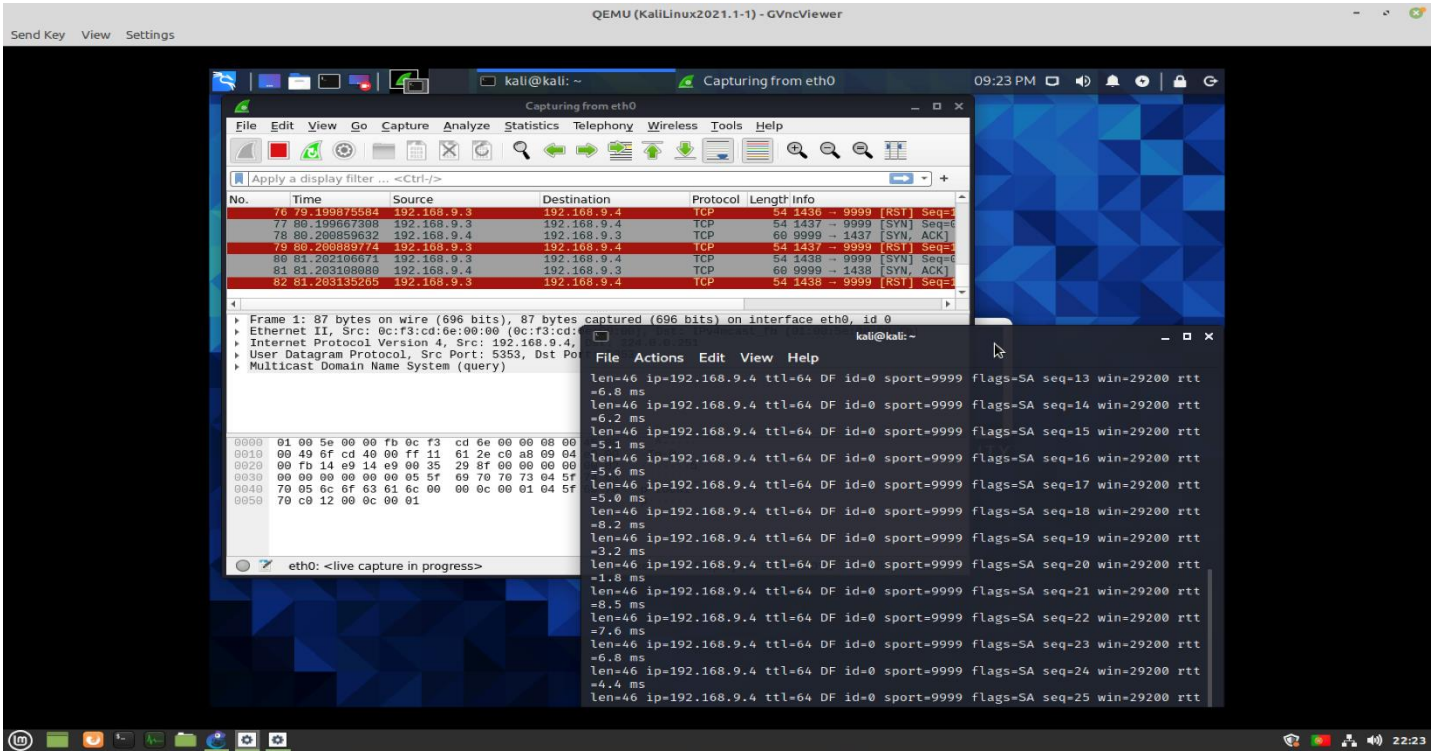
Modo de funcionamento:



O atacante (192.168.85.3) começa o ataque sabendo que o objetivo é atacar o Servidor (192.168.84.7) o router (192.168.84.254) com o auxílio do script SniffnReroute.py consegue detetar que estão a tentar fazer um Denial of Service e sabendo que estão a ser enviados vários pedidos para um dos ip's que está na lista de ip's protegidos e reencaminha o tráfego para o DejaVu que servirá nesse caso de HoneyPot. O DejaVu vendo isso vai reter o ip do atacante e informará o gestor de redes.
Depois, o gestor de redes poderá ou não implementar uma Access-list para negar o acesso daquele ip à rede.
Além disso, caso o atacante tente realizar ataques MIDM, já não será o router a detetar, mas sim o Dejavu(o nosso decoy) e enviará informações falsas.
Implementamos opcionalmente, vários scripts para melhorar o desempenho do DejaVu aumentando a sua eficácia na segurança e variedade de ataques suportados
Tentamos implementar opcionalmente, um sistema automático usando uma DRDoS Firewall, mas devido à elevada carga de trabalho não tivemos sucesso na sua completa realização e implementação.

Experimentação sem o uso do DejaVu





Decidimos comparar a segurança de um sistema usando Tecnologias de Deceção (páginas atrás) e sem o uso das mesmas:

Para realizar esta segunda experiência fizemos um ataque SYN flood a um servidor Ubuntu.

Um ataque SYN flood é um ataque que consiste em “inundar” a vítima com SYN requests sem responder aos SYN-ACKS que a vítima envia de volta. O facto de o atacante não responder aos SYN-ACKS faz com que o Three-way handshake não se realize, não havendo conclusão do mesmo. A vítima continua à espera de uma resposta que nunca chegará por parte do atacante e isso trará à vítima dificuldade e até mesmo incapacidade de responder a novos acessos. Este tipo de ataques é altamente prejudicial em grandes empresas pois cada segundo offline representa quantias enormes de dinheiro perdidas. Para não falar do perigoso que é um ataque destes ser feito por exemplo, num serviço de saúde, exemplo disso seria a falta de acesso à informação poderia causar mortes desnecessárias. A utilização de Deceptive Technology impediria que a vítima fosse afetada na sua maioria continuando a poder prestar os seus serviços enquanto o atacante se foca no honeypot sem perceber que este não é o alvo desejado e correndo o risco de ser intersetado.

Conclusão

Com este trabalho e experimentação conseguimos perceber que não existem 100% de segurança num sistema seja ele qual for que esteja ligado ao exterior, isto é, a algo para além de si mesmo.
Sendo assim, todas as técnicas de mitigação tem a sua percentagem de erro de não funcionar, principalmente se usadas poucas técnicas para a segurança de uma rede.
Percebemos assim, que a Tecnologia de Deceção será uma mais-valia para cobrir esse "buraco" que outrora já seria coberto pelos honeypot's mas agora de uma maneira mais inovadora e melhorada.
É de relembrar que mesmo assim, **quanto mais técnicas uma rede tiver de segurança, menor probabilidade de haver grandes dados derivados de um ataque informático.**