TÉCNICAS DE INVASÃO E PROTECÇÃO CIBERNÉTICA NO SEIO DOS TRABALHADORES E ESTUDANTES DA FET EM 2024

Nunes Tchimúa Mucuata Rafael

https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime

Namibe, 2024

[1]Nunes Tchimúa Mucuata Rafael
Faculdade de Engenharia e Tecnologia da UNINBE

TÉCNICAS DE INVASÃO E PROTECÇÃO CIBERNÉTICA NO SEIO DOS TRABALHADORES E ESTUDANTES DA FET EM 2024

Namibe, 2024

Resumo

O presente trabalho intitulado *"Técnicas de invasão e protecção cibernética no seio dos funcionários e estudantes da FET 2024"*, é um instrumento que aborda as técnicas de invasão de sistemas, com intuito de conhecê-las e traçar estratégias de protecção contra invasores de sistemas. É constituído por 3 capítulos, o primeiro aborda as referências bibliográficas, cujas conclusões serviram de base para a pesquisa, o segundo fala sobre os materiais e métodos utilizados durante a pesquisa e o último tem que ver com os resultados obtidos, fruto dos dados recolhidos e da proposta de protecção de senhas implementada e executada na linguagem de programação python. No final da abordagem do trabalho notou que há insuficiências em termos do conhecimento dos modus operantes de invasores e foi possível elaborar um plano estratégico visa aumentar a segurança nas comunicações.

Palavras- chaves: Segurança, Cibersegurança, invasão, protecção, internet.

Abstract

The present work entitled "Invasion techniques and cyber protection among employees and students of FET 2024", is an instrument that addresses system invasion techniques, with the aim of understanding them and devising protection strategies against system intruders. It consists of 3 chapters, the first addresses the bibliographic references, whose conclusions served as the basis for the research, the second talks about the materials and methods used during the research and the last has to do with the results obtained, as a result of the data collected and of the password protection proposal implemented and executed in the python programming language. At the end of the work approach, it was noted that there are insufficiencies in terms of knowledge of the modus operandi of attackers and it was possible to develop a strategic plan aimed at increasing security in communications.

Keywords: Security, Cybersecurity, invasion, protection, internet.

ÍNDICE

INTRODUÇÃO 4
1. FUNDAMENTAÇÃO TEÓRICA 10
1.1. Conceitos gerais 10
1.2. Principais tipos de ciberataques 11
1.3. Técnicas de protecção contra invasões 15
1.4. Partilha de senhas 19
1.4.1. Polinômio interpolador de Lagrange 20
1.4.2. Esquema de partilha Shamir 23
1.4.3. Boas práticas de usuários da internet 25
2. MATERIAIS E MÉTODOS 27
2.1. Materiais utilizados 27
2.2. População e amostra 27
2.2.1. Detalhes dos elementos da amostra 28
2.3. Métodos 28
2.3.1. Instrumentos de recolha de dados 29
2.4. Técnica de protecção cibernética “proposta” 29
2.4.1. Segurança da técnica proposta para o armazenamento de senhas 30
3. RESULTADOS E DISCUSSÃO 32
3.1. Resultados da técnica de protecção cibernética proposta 32
3.1.1. Discussão dos resultados da proposta 33
3.2. Resultado do inquérito aplicado à amostra 35
3.2.1. Discussão dos resultados dos inquéritos 36
3.3. Plano estratégico em Cibersegurança para a FET 37
Conclusão 40
Recomendações 41
Referências bibliográficas 42

INTRODUÇÃO

O presente trabalho, intitulado: *"Técnicas de invasão e protecção cibernética no seio dos funcionários e estudantes da FET em 2024*", é resultado de uma pesquisa que teve como objectivo de elaborar um plano de estratégico baseado ao ensino de Cibersegurança e investimento em ferramentas de segurança para o conhecimento e aplicação das técnicas de invasão e protecção contra ataques Cibernéticos no seio dos funcionários e estudantes da FET. O trabalho baseou-se em diversas referências bibliográficas, cujas conclusões permitiram fundamentar a nossa abordagem. Aplicou-se diversos métodos, desde os que visaram a identificação do problema, recolha, representação de dados e a interpretação dos mesmos para o alcance dos objectivos preconizados e assim, chegar às conclusões acerca do tema. Portanto como resultado propôs-se um plano estratégico em Cibersegurança, uma técnica de protecção de dados baseada no armazenamento seguro de senhas, deixou-se também algumas recomendações às entidades de tutela e académicos em geral.

i. Contextualização

A Cibersegurança tem sido um assunto que despertado interesse e curiosidades não só às pessoas, empresas, mas também para os governos de vários países com um acentuado nível de desenvolvimento tecnológico.

Com a extensão do acesso à internet por parte das populações em geral, as vulnerabilidades existes em softwares começaram a ser exploradas por agentes maliciosos, que a princípio desenvolviam ataques sem propósitos de causar danos aos usuários, mas, às vezes realizavam por diversão. Um destes ataques realizado com propósito de ver a eficiência do vírus, foi o vírus Morris, um dos primeiros a afectar o mundo das tecnologias, executado em 1988 por Robert Tapan Morris, estudante de Pós- graduação na altura. Por detrás dos ataques cibernéticos pode ter várias motivações: económicas, sociais, políticas, por exemplo. O ataque que ficou conhecido como Stuxnet, realizado em 2010, contra o sistema de segurança do Irão com motivações políticas, tendo sido projectado à arquitetura de controlo de sistemas que controlava todas reservas nucleares, visando atingir o sistema nuclear do país. Os ataques cibernéticos actualmente, atingiram níveis alarmantes, chegando a alcançar cidades mais desenvolvidas por exemplo, em sistemas de distribuição de rede eléctrica, abastecimento de água e até em alguns casos, serviços de transportes públicos (Faria, 2022).

Em geral, os governos de vários países, têm implementado mecanismos de segurança, visando aumentar a resiliência das infraestruturas digitais de seus países e preparar as sociedades para o futuro. Em Angola, dados fornecidos em 2021 pelo Instituto Nacional de Estatística (INE), mostraram que dos 17.274.534 de jovens inqueridos, com idades maiores de 15 anos, 21% tem acesso à internet e 33% possui um computador, telemóvel ou tablet. 23% dos usuários têm o antivírus como o único meio de protecção contra malware (software malicioso). 22% dos inqueridos já ouviu falar sobre Cibersegurança. 6% dos entrevistados sofreram algum ataque cibernético e 18% deles já acessaram links de entidades desconhecidas ou forneceram informações sigilosas pela internet (INE, 2021).

Em Fevereiro de 2017, o Governo Angolano publicou em Diário da República, a Lei de protecção das redes e sistemas informáticos, aplicável no ciberespaço angolano. O documento apresenta a partir do artigo 12º, os requisitos a serem cumpridas pelas entidades detentoras de plataformas servidoras de serviços pela internet, e o não cumprimento desses

requisitos a lei a partir do artigo 42º, multas que variam de 1.000.000 a 150.000.000 (um a cento e cinquenta milhões) de kwanzas a Cibersegurança tem dado sinais positivos (Diário da República, 2017).

Dados divulgados no relatório da FILDA 2022 nas áreas das tecnologias pela agência Angola Cables, mostram que Angola é o segundo país em ataques cibernéticos a nível da África, o que gerado um prejuízo económico às empresas e não só, aproximadamente na ordem de 2.000.000.000 (dois mil milhões) de dólares (*https://www.jornaldeangola.ao/ao/noticias/pais-e-o-segundo-em-ataques-ciberneticos-no-continente/*).

Portanto, a Cibersegurança em Angola tem dados sinais positivos, e estado no centro das atenções das entidades governamentais. Facto que tem sido motivado pelo progresso tecnológico que o país tem experimentado nos últimos anos. Mas, acreditamos que muito ainda tem que ser feito, e está é uma das principais razões dessa pesquisa, contribuir no conhecimento, divulgação da cultura da segurança na internet e estimular entidades a adoptarem medidas que visam a implementação extensiva da cibersegurança em Angola.

ii. Identificação do problema

A segurança de informações que circulam através da internet, tem sido um assunto da actualidade a nível mundial, e constantemente ouve-se grito de pessoas e empresas que foram vítimas de ataque cibernético. Por outra, tenho notado pouco(a) interesse (preocupação) dos gestores públicos em Moçâmedes, quanto às questões de segurança, com excepção das empresas que seus modos operantes é quase 100% através da internet, concretamente os bancos.

Numa auscultação feita em alguns familiares e amigos, para saber se as empresas onde trabalham têm mantido um procedimento de cibersegurança, ou se têm uma secção de cibersegurança com um técnico formado na área a responder por estes serviços, todos foram unânimes em afirmar não haver, e na sua maioria mostraram um forte desconhecimento do assunto.

Outrossim, a nível da UNINBE, temos servidores de internet a funcionar em todas unidades orgânicas, mas não existem secções de segurança de informação, segundo dados fornecidos pelo departamento de tecnologia da UNINBE, o que na minha maneira de ver, considero uma atitude arriscada para a segurança de informações geridos e transacionados.

Não obstante a isso, também tenho notado a nível da Faculdade de Engenharia e Tecnologia, pouco investimento ou organização na área de Cibersegurança. E o que considero agravante é o facto de termos o sistema Infordocente como uma ferramenta de gestão de dados sigilosos e fundamentais para o êxito do processo de Ensino e Aprendizagem. Porém, a meu ver o mesmo está sujeito às acções de criminosos.

Todavia, actualmente a internet tem servido de um meio de comunicação das empresas para o exercícios de suas funções, quer seja para gestão de dados pessoais, processamento de dados financeiros, e entre tantos outros serviços. A grande problemática reside no facto da internet ser um meio de comunicação inseguro, razão pela qual, nesta era das TIC's, instituições que ignoram ou pouco investem em Cibersegurança para o bem da organização, carecem de um incentivo de alguém com conhecimento na área. Contudo, formulou-se o problema da investigação da seguinte forma:

Como contribuir na implementação dos princípios de Cibersegurança na FET, a fim de tornar seguras as comunicações realizadas através da internet no seio dos trabalhadores e estudantes?

iii. Hipótese da investigação

Temos como hipótese da investigação, a seguinte:

Se for implementado um plano de estratégico baseado ao ensino de Cibersegurança e investimento em ferramentas de segurança, aumentará a segurança das comunicações realizadas através da internet na FET

iv. Variáveis de investigação

Variável independente: plano de estratégico baseado ao ensino de Cibersegurança e investimento em ferramentas de segurança.

Variável dependente: Segurança das comunicações.

v. Objectivos

Objectivo geral:

Elaborar um plano de estratégico baseado no ensino de Cibersegurança e investimento em ferramentas de segurança para o conhecimento e aplicação das técnicas de invasão e protecção contra ataques Cibernéticos no seio dos trabalhadores e estudantes da FET.

Objectivos específicos:

- Revisar a bibliografia existente para o conhecimento das conclusões de outros autores.
- Fundamentar o tema para dar sustentabilidade das abordagens.
- Medir o nível de conhecimento sobre o tema aos funcionários e estudantes da FET.
- Elaborar um plano de estratégico baseado ao ensino de Cibersegurança e investimento em ferramentas de segurança.

vi. Objecto de estudo

O objecto de estudo da investigação é a gestão da informação.

vii. Campo de acção

O campo de acção (actuação) é a segurança da informação.

viii. Tipo de investigação

A presente investigação é descritiva. Pois, fez-se a descrição do fenómeno conforme ele ocorre e consequentemente foram traçadas medidas que visam contribuir para o melhor desenrolar do fenómeno, isto é, no que diz respeito ao domínio das técnicas de invasão e protecção contra ataques cibernéticos na FET.

ix. Justificativa

O estudo da Cibersegurança desempenha um papel muito importante na garantia da segurança da informação, na medida que opostamente ao funcionamento de um sistema informático, existem agentes maliciosos com propósito de perverter a segurança de um sistema, através de ataques. Um ataque bem- sucedido pode gerar inúmeras consequências económico-sociais aos usuários, visto que nem sempre é possível detectar a tempo, a ocorrência de um determinado ataque cibernético. Por outra, os criptoanalistas (hackers) têm desenvolvido cada vez mais as suas técnicas de invasão, o que tem dificultado a manutenção de segurança cibernética em sistemas informáticos. A Cibersegurança tem conquistado seu espaço na tecnologia, ao desenvolver técnicas de segurança que visam inibir ou contrapor as

acções maliciosas dos atacantes, bem como também, na disseminação da educação cibernética aos usuários. Sendo a FET, a única Faculdade estatal no Namibe, responsável pela formação de Engenheiros, é importante desenvolver e aplicar a cultura de Cibersegurança, para gradualmente evoluir em outras facetas, que tem a ver com a formação de quadros na área. Com esta investigação, pretende-se incentivar os responsáveis da instituição, a olharem para a implementação dos princípios de Cibersegurança e a formação de quadros na área, como um desafio inovador da era da tecnologia.

Portanto, estas são as razões que me motivaram a desenvolver esta investigação.

1. FUNDAMENTAÇÃO TEÓRICA

1.1. Conceitos gerais

Apresentamos de seguida, as definições de alguns conceitos que serviram de base para a abordagem feita no trabalho (Sousa, 2013):

Cibersegurança: é a área da informática, cuja arte é proteger redes, dispositivos e dados contra acesso não autorizado ou uso não autorizado, e a práctica de garantir a confidencialidade, integridade e disponibilidade da informação no ciberespaço.

O conceito estende-se para a segurança das redes de computadores, das aplicações de softwares e dos sistemas operativos. Bem como, medidas de recuperação de incidentes de cibersegurança e de educação dos usuários.

Ciberataque: é o ataque realizado através da internet com propósito de causar danos, obter informações sigilosas ou alterar o funcionamento de um sistema informático.

Ciberespaço: é o conjunto de tecnologias, informações e serviços da internet.

Cibercrime: é o crime cometido com recurso aos sistemas informáticos.

Ciberdefesa: é o conjunto de acções de monitorização, prevenção e respostas às ameaças através da internet, que colocam em risco o sistema de segurança de uma organização, região ou país.

Hacker: é um indivíduo que possui capacidade e aptidão computacional de criar ou alterar hardwares ou softwares sem intenção de causar qualquer tipo de danos.

Cracker: diferentemente do hacker, um craker é aquele que desenvolve suas acções com propósito de causar danos a uma entidade ou empresa.

Hacking: são actividades que consistem em comprometer dispositivos ou sistemas informáticos.

Bot de internet: são aplicações autônomas que realizam tarefas através da internet.

IP (Protocolo de internet): é o conjunto de números que permitem a identificação e a comunicação consiste entre de uma rede, mediante a plataforma de internet.

Software: é um conjunto de programas e dados que instruem a um computador como executar determinadas tarefas.

Hardware: é a parte física de computadores e outros sistemas.

1.2. Principais tipos de ciberataques

Para invadir sistemas, os invasores de sistemas executam as seguintes técnicas (ataques) (Oliveira, 2021):

a) Daniel-of-service (DoS/ DDoS): é um ataque que consiste em dificultar o acesso a uma máquina ou rede, tornando-a inacessível aos utilizadores, através da inundação (sobrecarga) do sistema alvo com tráfego excessivo.

No DoS por exemplo, um único computador cria simultaneamente vários pedidos para um site ou sistema.

Portanto, num ataque DoS, o atacante faz várias solicitações em simultâneo, com um único computador. É um ataque fácil de detectar e bloquear, pois o trafego é emitido a partir de um único endereço IP.

Já no DDos são usadas várias fontes de proveniência para atacar um sistema. Igualmente, o atacante inunda o sistema com vários pedidos simultâneos para tornar o sistema indisponível para outros usuários. Seu propósito também consiste em denegrir a prestação de serviço de um servidor (sistema), em benefício de um outro servidor, ou apenas para prejudicar a vítima.

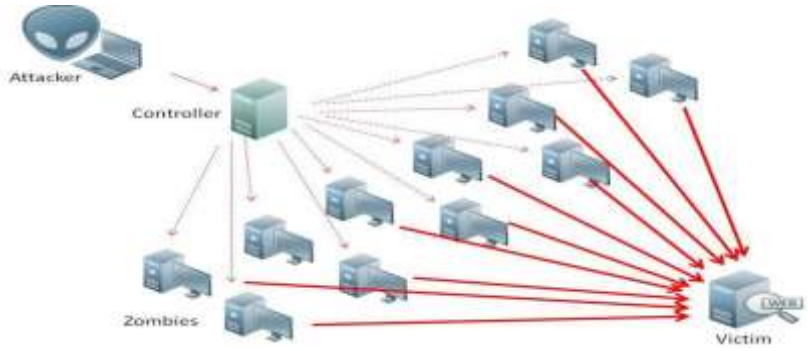

***Fig. 1**. Ataque DDoS*
***Fonte**: https://pt.m.wikipedia.org/wiki/Ficheiro:Ddos-attack-ex.png*

Da figura que ilustra o ataque DDoS, o atacante não tem acesso aos vários computadores, para a execussão do ataque. Ele utiliza bots de internet, que repetidamente emitem as solicitações à ao servidor ou vítima. Cada bot tem seu IP, assim, o trafego em DDos vem de vários endereços IP, o que torna difícil identificar ou bloquear um ataque DDoS.

b) Malware: é qualquer programa ou código malicioso que seja prejudicial para os sistemas. Exemplos de malwares:

- Cavalo de tróia (trojan): um cavalo de tróia, de forma a enganar o utilizador, parece que algo é útil, mas quando entra no sistema, consegue obter acesso não autorizado ao sistema em causa, e roubar informações ou instalar ameaças.

- Ransomware: é um software malicioso desenvolvido com intuito bloquear (negar) o acesso a um dispositivo (ficheiros), a fim de obter benefícios, e causar danos a outrem.

c) Man-in-the-minddle: é um ataque que permite o atacante interromper a comunicar (transferência de dados), atingindo os participantes legítimos, acedendo informações confidenciais, enviando links maliciosos para os dois agentes da comunicação.

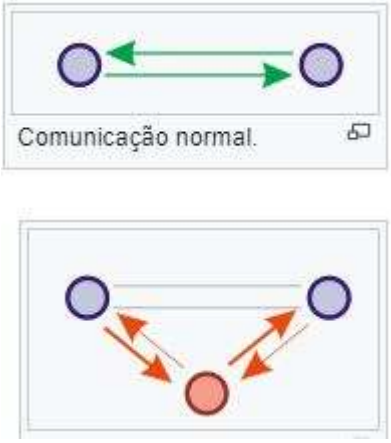

Fig. 2. *Ataque Man-in-the-mindlle*
Fonte: *https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack*

d) Phishing: deriva da palavra inglesa "fishing" que significa pescar. Consiste em levar utilizadores a revelar seus dados confidenciais, ao responderem com dados secretos uma mensagem aparentemente inofensiva, inserir credenciais para aceder uma página, ou carregar um link malicioso.

Fig. 3. *Ataque fishing*
Fonte: *https://www.shutterstock.com/pt/search/phishing*

Como ilustra a figura, a vítima é aliciada com propostas aparentemente benéficas, até que aceda ao anzol, e desta o atacante pesca os dados sigilosos deste. O objectivo deste ataque é

conduzir os usuários à uma página falsa, idêntica à verdadeira, e daí recolher dados secretos das vítimas.

e) SQL injection: é uma falha de segurança do sistema (vulnerabilidade), que pode ser aproveitada pelo atacante para consultar a base de dados de uma determinada aplicação, podendo modificar ou apaga-los, causando alterações no conteúdo ou comportamento da aplicação.

f) Spoofing: Spoofing tem origem do verbo inglês "to spoof", que significa em português fingir ou imitir. É um tipo de crime que direcionado para clientes ou servidores de serviços de internet.

O ataque ocorre quando um agente (atacante) malicioso durante a comunicação, se faz passar de alguém fidedigno. O ataque também pode ser executado via chamada telefónica, quando o individuo recebe por exemplo, uma ligação com seu próprio número. Neste caso, o objectivo é clonar o telemóvel da vítima, e aceder os dados confidenciais.

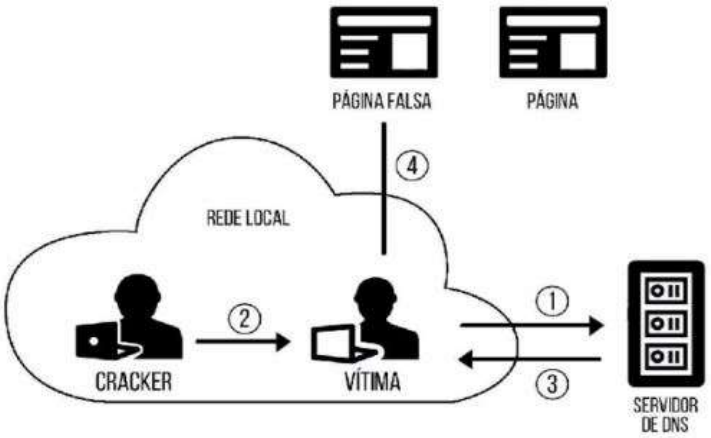

Fig. 4. *Ataque Spoofing*
Fonte: *https://networksimulationtools.com/spoofing-attack-network-projects/*

A figura apresentado, faz menção de um ataque Spoofing por DNS, que consiste em manipular as conexões de rede. O objectivo é desviar os usuários para sites falsos. Para tal, o atacante aproveita-se de alguma vulnerabilidade em servidores para fraudar nomes de domínio e efectivar o desvio.

O ataque Spoofing também pode ser executado para atacar uma rede, enviando um IP falso ou disfarçado. O atacante finge que é usuário da mesma rede e solicita que o acesso seja concedido. Para isso usa o IP de um usuário legítmo. Ao ter sucesso, o atacante consegue sequeatrar um navegador e desviar os usuários de um site legal para um falso, de aparência semelhante.

Em geral, num ataque Spoofing, os criminosos fazem-se passar por outras pessoas mascando seu endereço ao das entidades de confiança da vítima, para enganá-las, acabando por convence-las a fornecer seus dados singilosos. Para além da mensagem de email, pode-se usar outros meios para concretizá-lo, tais como, Sms e Watshapp.

O ataque quando é emitido por email, a fraude envolve links, solicitação de dados pessoais ou financeiros. Também às vezes o email contém anexos maliciosos, contendo algum software malicioso , que pode activar vulnerabilidades, que servem de porta de acesso dos criminosos.

Quando é feito por ligação ou sms, realiza-se a clonagem ou falsificação de identificador de chamadas para ocultar a origem da verdadeira ligação, para tal o criminoso utiliza números próximos ou aparentemente familiares à vítima.

g) Cross-site-scripting: Conhecido por XSS, é um tipo de malware que é injetado em sites, e desta forma os usuários ao executá-lo, permitem que os atacantes acedam seus dados confidenciais.

Fig. 5. *Ataque Cross- site- scripting*

Fonte: *https://www.researchgate.net/figure/Cross-site-scripting-XSS-attack-Source-Coursera-80_fig4_353195865*

Nota-se na figura que, o atacante visa inicialmente atingir o servidor, aproveitando alguma vulnerabilidade existente, acabando por injectar um malware. A vítima ao se comunicar com o servidor e recebe um malware que o conecta com o intruso (atacante), acabando por dá-lo permissões.

h) Zero-day-exploit: é um método usado para atacar sistemas através de uma vulnerabilidade que ainda não foi identificada pelos fornecedores do sistema. Como a vítima não sabia da existência dessa vulnerabilidade, eles têm zero dias para desenvolverem um método de resolução, permitindo ataques bem-sucedidos.

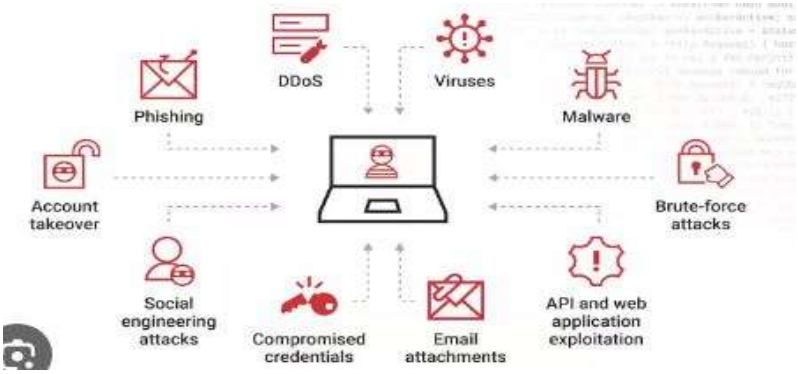

***Fig. 6**. Ataque zero-day-exploit*

***Fonte**: https://www.imperva.com/learn/application-security/zero-day-exploit/*

Como se observa na figura, o atacante pode aproveitar-se de prováveis vulnerabilidades não corrigidas, para emitir qualquer tipo de ataque. Pois, em geral, vulnerabilidades tornam débil a imunidade do sistema.

i) Força bruta: consiste em realizar diversas tentativas até quebrar a chave de cifração ou decifração (senhas de login) do sistema criptográfico (informático).

1.3. Técnicas de protecção contra invasões

Existem softwares que protegem sistemas contra ataques (Assunção, s.d):

1) Caixa virtual: uma caixa virtual, virtual box em Inglês, é um software que funciona como um computador virtual, que permite a instalação de vários sistemas operativos. Dentro da caixa virtual, o IP do usuário permanece oculto, reduzindo as chances de ser localizado ou alcançado pelos atacantes. Caso haver uma tentativa de ataque através do IP, é atingido apenas as funcionalidades que estejam fora da caixa virtual.

Temos na figura abaixo, uma caixa virtual a funcionar no Windows:

Fig. 7. *Ícone de uma máquina virtual (virtual box) no Windows*
***Fonte**: Autor*

A figura apresenta o ambiente de trabalho com o ícone da caixa virtual, e abri-la, pode instalar outros softwares e usufruir de suas funcionalidades.

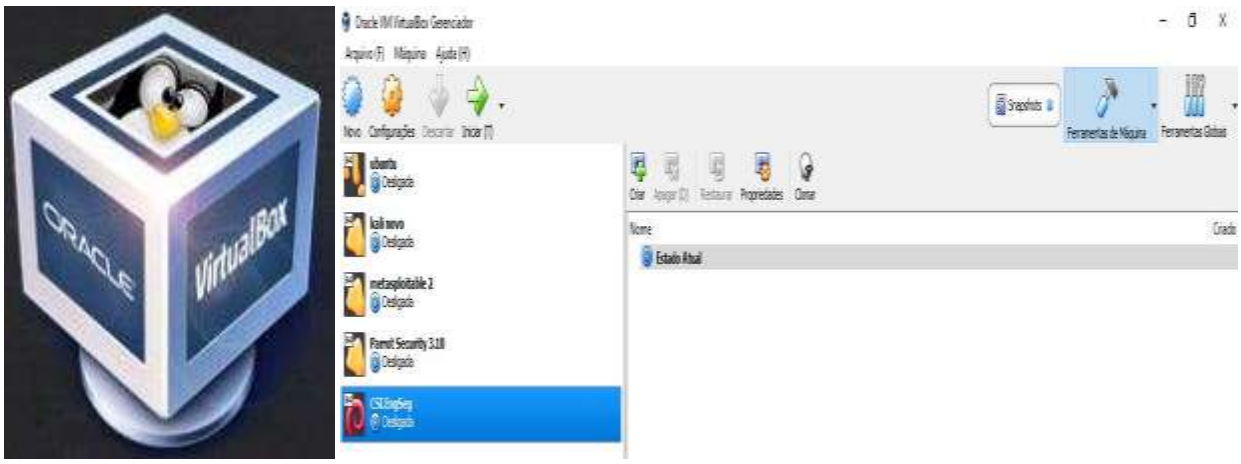

***Fig. 7**. Máquina virtual com 5 sistemas operativos*
***Fonte**: Autor*

Temos instalado na caixa virtual, três versões do sistema operativo Linux, que são: ***Ubuntu, Kali linux e o Parrot***. De igual modo, temos dois softwares de análise de vulnerabilidades: ***Metasploitable 2 e CSI.EngSeg***.

2) Backup: é uma técnica que garante a solução da problemática da perda de conteúdos informáticos. Isto é, a aplicação do Backup assegura ao usuário a recuperação de dados perdidos ou roubados.

Essa técnica consiste em realizar cópias de segurança de dados informáticos em um dispositivo, a fim de recuperá-los em caso de perdas ou falhas de sistema. As cópias de segurança são armazenadas em um sistema Backup em nuvem.

Um Backup funciona armazenando cópias de ficheiros de um dispositivos em outro destino, podendo ser acessado noutros dispositivos conectados à internet. Pois, os dados ficam disponíveis aos usuários devidamente autorizados.

Portanto, os computados ou outros dispositivos, estão sujeitos a avarias ou ataques cibernéticos, e o procedimento Backup actua ma prevenção contra incidentes ou acções maliciosas que façam desaparecer os ficheiros. A técnica se parece com o armazenamento de cópias de ficheiros feitos em dispositivos físicos (Discos, Pendrive), diferenciando no facto do Backup poder ser acessado em qualquer momento, local ou dispositivo conectado à internet, tornando-se mais seguro que o armazenamento físico.

3) VPN (Virtual Private Net): é um software que consiste em tornar segura a privacidade do usuário durante o trafego na internet. A VPN torna anónimo o tráfego e a localização do usuário.

A questão cinge-se no facto dos sites usarem o IP dos usuários de internet para determinar a localização dos usuários, e quando alguém se conecta a um servidor VPN, o seu endereço IP permanece oculto. Todavia, algumas VPN bloqueiam acções maliciosas, sites que contém malwares, proibindo o acesso à tais sites para evitar infecções e causarem danos.

Uma VPN aplica a Criptografia ponta-a-ponta para proteger o usuário. Isto é, ninguém poderá ver o que o usuário está fazendo através da internet, nem mesmo o provedor da internet ou do fornecedor dos serviços. Desta forma é cortada a possibilidade aos criminosos acederem os dados confidenciais dos usuários.

Com a aplicação VPN, os dados circulam através da internet criptografados (cifrados), e ainda que alguém os intersecte, não poderá decifrá-los.

Uma VPN funciona com intuito de velar pela privacidade do usuário, tornando indetectável por terceiros. Pois, Quando alguém, a partir de um lugar (servidor A) se conecta à outro servidor B, o trafego é enviado criptografado do servidor A para o B pelo servidor VPN. Desta forma o provedor do dos serviços do servidor A não conseguirá rastrear o trafego, nem o

provedor dos serviços do servidor B. Durante o tráfego o site será o servidor VPN como a origem do tráfego, em vez do dispositivo do usuário. Isto é, estará disponível no site, o IP do servidor VPN, ocultando o IP do usuário.

Em geral, as VPN's usam milhares de servidores e actualizam seus endereços IP's regularmente, para que sites não tenham tempo suficiente para bloqueá-los, garantindo dessa forma, a funcionalidade e privacidade dos usuários.

4) Firewall (Parede de fogo): é um sistema de segurança baseado em hardware ou software que serve de barreira de defesa, cuja missão é bloquear o trafego de dados maliciosos e liberar acessos legítimos.

Uma Firewall pode impedir várias acções maliciosas: um malware que possa comprometer o sistema de segurança do computador, ou a integridade do dispositivo; uma tentativa de acesso a partir de computadores externos não autorizados, por exemplo.

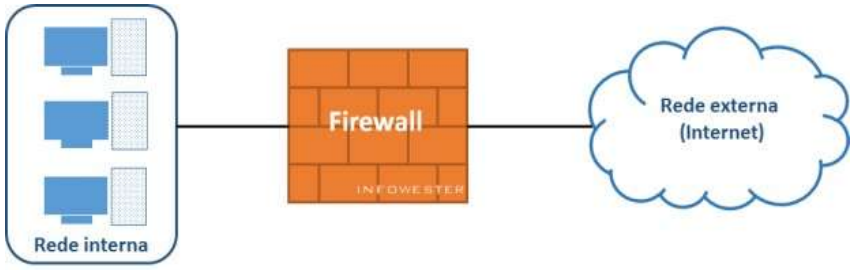

Fig. 8. *Ilustração de um Firewall.*
Fonte: *https://stock.adobe.com/search?k=firewall*

Conforme a imagem, o sistema Firewall está posicionado entre a rede interna e a externa, servindo de filtro do tráfego, liberando ou bloqueando acessos. Portanto, o Firewall legitima o acesso, quando o agente é devidamente reconhecido como legal, o inverso implica o bloqueamento da solicitação.

5) Gerenciador de senhas:

De acordo o artigo científico intitulado "Gestão de senhas, políticas e o mundo conectado: desafios e soluções", de Carvalho Peixinho (s.d, pg. 7), existem 5 formas de tornar as senhas mais seguras:

- Trocar as senhas a cada 3 meses;
- Criar senhas com 8 ou mais caracteres;
- Criar símbolos, letras e números;

- Não anotar a senha;
- Memorizar a senha.

No caso de senhas de elevado tamanho (números de dígitos ou caracteres), o usuário pode esquecer e para minimizar este problema, a internet permite a gestão de senhas através do gerenciador de senhas e também é possível armazenar senhas através da técnica de armazenamento em nuvens “Backup”.

Quer uma, quer outra técnica, não resolve o problema. Pois, as duas técnicas são inseguras. O Backup é importante pois permite o armazenamento de cópias de nossos dados em nuvem, podendo prevenir a perca de informações valiosas em caso de avaria do dispositivo, ou inacessibilidade ao dispositivo por causa de vírus ou um outro tipo de ataque. Pois, a técnica permite-nos aceder aos dados a partir de outros dispositivos e em qualquer lugar.

Do mesmo jeito, existe o gerenciador de senhas, que vem resolver o problema de memorização de senhas, pois o armazenamento em qualquer lugar ou em meio acessíveis, constitui um perigo para um sistema tecnológico. Também resolve o problema de ter que memorizar ou armazenar várias senhas diferentes.

Mas, essas duas técnicas geram outros problemas ou fragilidade, porque o Backup por exemplo, precisa de credenciais para aceder as informações perdidas ou inacessível a partir do dispositivo habitual, noutros dispositivos. E, o caso do gerenciador de senhas, precisa de uma senha mestra, que também carece de uma protecção segura. Daí que e conforme a publicação da academia de tecnologia CISCO Academy (s.d, pg. 2): “*Se o usuário optar por usar um gerenciador de senhas, a primeira característica de uma senha forte pode ser descartada porque o usuário tem acesso ao gerenciador de senha a qualquer momento. Alguns usuários só confiam em suas memórias para guardar suas senhas. Gerenciadores de senha, locais ou remotos, precisam ter um armazenamento de senhas e podem ser comprometidos. O armazenamento de senha do gerenciador de senha deve ser fortemente criptografado e o acesso a ele deve ser rigidamente controlado.”*

Desta forma, decidi propor uma outra técnica de armazenamento seguro de senhas, mediante a implementação computacional da proposta na linguagem de programação “python”, implementação resultante da combinação entre os algoritmos do polinómio interpolador de Lagrange e do esquema de partilha de segredos de Shamir.

1.4. Partilha de senhas

1.4.1. Polinômio interpolador de Lagrange

Sejam $(x_0,\ y_0), (x_1,\ y_1), \dots, (x_{n-1},\ y_{n-1}),\ (x_n,\ y_n)$ conjunto de pares ordenados, o problema da interpolação consiste na determinação de uma função polinomial f, designada por polinômio interpolador, onde $f(x_i) = y_i$ e $i = 1, 2, \dots, n$ (Giacomelli, 2014).

As abcissas $x_0, x_1, \dots, x_{n-1}, x_n$ são designadas por nós da interpolação, tal que: $i \neq j \Longrightarrow x_i \neq x_j$, isto é, devem ser todos diferentes e as ordenadas $y_0, y_1, \dots, y_{n-1}, y_n$ designam-se por valores modais.

Definição (unicidade do polinômio interpolador): sejam $P(x)$ e $Q(x)$ polinômios de graus menores ou iguais a n, que assumem os mesmos valores num conjunto de nós $x_0, x_1, \dots, x_{n-1}, x_n$ distintos, então estes polinômios são iguais.

Definição: sejam os nós distintos $x_0, x_1, \dots, x_{n-1}, x_n$, os polinômios definidos pela expressão:

$$l_j(x) = \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{x\ -\ x_i}{x_j\ -\ x_i}, \quad j = 0,1, \dots, n$$

são designados por polinômios de Lagrange relativos aos nós $x_0, x_1, \dots, x_{n-1}, x_n$.

O **polinômio interpolador de Lagrange** é obtido como combinação linear dos polinómios de Lagrange relativos aos nós. Os coeficientes desta combinação linear são os valores modais a interpolar.

Definição: o polinômio $P(x)$ de grau menor ou igual a n, que interpola o conjunto de valores $y_0, y_1, \dots, y_{n-1}, y_n$ nos nós correspondentes, é dado por:

$$P(x) = \sum_{j=0}^{n} y_j l_j(x)$$

Vejamos que $P(x)$ é a soma de polinômios de grau n ou nulos, conclui-se que o grau de $P(x)$ é menor ou igual a n. Por outra, para cada nó x_i tem-se:

$$P(x_i) = \sum_{j=0}^{n} y_j l_j(x_i) = y_i$$

Pelo que $P(x)$ interpola valores modais.

Notemos que, para os pares ordenados $(x_0,\ y_0), (, (x_1,\ y_1), (x_2,\ y_2)$, o polinômio interpolador de Lagrange seria:

$$l_0(x) = \frac{(x - x_1)}{(x_0 - x_1)} . \frac{(x - x_2)}{(x_0 - x_2)}$$

$$l_1(x) = \frac{(x - x_0)}{(x_1 - x_0)} . \frac{(x - x_2)}{(x_1 - x_2)}$$

$$l_2(x) = \frac{(x - x_0)}{(x_2 - x_0)} . \frac{(x - x_1)}{(x_2 - x_1)}$$

$$P(x) = \sum_{j=0}^{n} y_j\ l_j(x)$$

$$P(x) = y_0\ l_0(x) + y_1 l_1(x) + y_2 l_2(x)$$

$$P(x) = y_0 . \frac{(x - x_1)}{(x_0 - x_1)} . \frac{(x - x_2)}{(x_0 - x_2)} + y_1 . \frac{(x - x_0)}{(x_1 - x_0)} . \frac{(x - x_2)}{(x_1 - x_2)} + y_2 . \frac{(x - x_0)}{(x_2 - x_0)} . \frac{(x - x_1)}{(x_2 - x_1)}$$

Exemplo: Determinemos o polinômio interpolador de Lagrange para os seguintes pontos:

$$(x_0;\ y_0) = (1\ ;1)$$

$$(x_1;\ y_1) = (2;\ 8)$$

$$(x_2;\ y_2) = (3;\ 27)$$

$$(x_3;\ y_3) = (4;\ 81)$$

Calculando os polinómios de Lagrange $l_j(x)$:

$$l_j(x) = \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{x\ -\ x_i}{x_j\ -\ x_i}$$

$$l_0(x) = \frac{(x - x_1)(x - x_2)(x - x_3)}{(x_0 - x_1)(x_0 - x_2)(x_0 - x_3)}$$

$$l_0(x) = \frac{(x - 2)(x - 3)(x - 4)}{1 - 2)(1 - 3)(1 - 4)}$$

$$l_0(x) = \frac{(x^2 - 5x + 6)(x - 4)}{-6}$$

$$l_0(x) = \frac{x^3 - 9x^2 + 26x - 24}{-6}$$

$$\boxed{l_0(x) = -\frac{1}{6}x^3 + \frac{3}{2}x^2 + \frac{13}{3}x + 4}$$

$$l_1(x) = \frac{(x - x_0)(x - x_2)(x - x_3)}{(x_1 - x_0)(x_1 - x_2)(x_1 - x_3)}$$

$$l_1(x) = \frac{(x - 1)(x - 3)(x - 4)}{(2 - 1)(2 - 3)(2 - 4)}$$

$$l_1(x) = \frac{(x^2 - 4x + 3)(x - 4)}{2}$$

$$l_1(x) = \frac{x^3 - 8x^2 + 19x - 12}{2}$$

$$\boxed{l_1(x) = \frac{1}{2}x^3 + 4x^2 + \frac{19}{2}x - 6}$$

$$l_2(x) = \frac{(x - x_0)(x - x_1)(x - x_3)}{(x_2 - x_0)(x_2 - x_1)(x_2 - x_3)}$$

$$l_2(x) = \frac{(x - 1)(x - 2)(x - 4)}{(3 - 1)(3 - 2)(3 - 4)}$$

$$l_2(x) = \frac{(x^2 - 3x + 2)(x - 4)}{-2}$$

$$l_2(x) = \frac{x^3 - 7x^2 + 14x - 8}{-2}$$

$$\boxed{l_2(x) = -\frac{1}{2}x^3 + \frac{7}{2}x^2 - 7x + 4}$$

$$l_3(x) = \frac{(x - x_0)(x - x_1)(x - x_2)}{(x_3 - x_0)(x_3 - x_1)(x_3 - x_2)}$$

$$l_3(x) = \frac{(x - 1)(x - 2)(x - 3)}{(4 - 1)(4 - 2)(4 - 3)}$$

$$l_3(x) = \frac{(x^2 - 3x + 2)(x - 3)}{6}$$

$$l_3(x) = \frac{x^3 - 6x^2 + 11x - 6}{6}$$

$$\boxed{l_3(x) = \frac{1}{6}x^3 - x^2 + \frac{11}{6}x - 1}$$

Então, o polinómio interpolador resultante é:

$$P(x) = \sum_{j=0}^{n} y_j \, l_j(x)$$

$$P(x) = y_0 \, l_0(x) + y_1 \, l_1(x) + y_2 \, l_2(x) + y_3 \, l_3(x)$$

$$P(x) = \frac{1}{6}x^3 + \frac{3}{2}x^2 + \frac{13}{3}x + 4 + 4x^3 + 32x^2 + 76x - 48 - \frac{27}{2}x^3 + \frac{189}{2}x^2 - 189x + 81 \; + \frac{27}{2}x^3 - 81x^2 + \frac{297}{2}x - 81$$

$$P(x) = (\frac{1}{6} + 4)x^3 + (\frac{3}{2} + 32 + \frac{189}{2} - 81)x^2 + (\frac{13}{3} + 76 - 189 + \frac{297}{2})x + 4 - 48 + 81 \; - 81$$

$$P(x) = \frac{25}{6}x^3 + \frac{93}{2}x^2 + 42x - 44$$

1.4.2. Esquema de partilha Shamir

O esquema de partilha utilizado para a nossa proposta de armazenamento de senha, baseou-se no esquema de Shamir, que é um algoritmo em criptografia criado por Adi Shamir, nascido no ano de 1952, em Israel, (Mortensen, 2007).

Definição: o esquema de Shamir, consiste em dividir um segredo $\boldsymbol{S}$ em n pedaços de dados $S_1, \ldots, S_n$, de modo que:

- O segredo $\boldsymbol{S}$ pode ser reconstruído a partir de qualquer combinação de k partes do segredo.

- O segredo $\boldsymbol{S}$ não pode ser reconstruido com menos de k partes de dados. O esquema representa-se como $(\boldsymbol{k}, \boldsymbol{n})$, onde:

$\boldsymbol{n}$ – Número total de participantes;

$\boldsymbol{k}$ – Número de partes secretas (pedaços de dados) necessárias para reconstruir $\boldsymbol{S}$.

Esta é uma forma de compartilhamento secreto , onde um segredo é dividido em partes, distribuído a cada participante uma parte única. Se $k = n$, então é necessário reunir todas as partes secretas de $\boldsymbol{S}$ para reconstruí-lo (Shoenmakers, 2018).

Logo, o segredo só pode ser reconstruído (recuperado quando um número k menor ou igual a n reunirem seus segredos. Qualquer subconjunto menor que k ,isto é, $k - 1$ (ou menos) segredos combinados, torna-se inviável a reconstrução do segredo.

A escolha de k permite construir um polinômio de grau $k-1$, polinômio este, que permitirá obter as n partes secretas a serem partilhadas. Mas, se ao invés de k, for usado maliciosamente $k-1$ (exigiria num polinômio de grau $k-2$ para reconstruir o segredo). E uma vez que inicialmente determinou-se ser necessário a junção de k partes secretas para a reconstrução do segredo, e com $k' \neq k$ partes secretas não permite reconstrui-lo.

Portanto, podemos notar que cada subconjunto de n participantes tomados para reconstruir o segredo, corresponde à um único polinómio interpolador, facto sustentado pela unicidade do polinômio interpolador.

Sejam $n, k\ e\ \boldsymbol{S}$, conhecidos de antemão, a definição matemática do esquema de partilha da chave secreta de Shamir é a seguinte:

Seja $\mathbb{G} = \mathbb{Z}_p^*$, grupo cíclico de ordem p primo. Onde $g \in \mathbb{G}$ é gerador do grupo.

Seja $Q(x) = P(x) = S + \sum_{i=1}^{k-1} a_i x^i$, o polinômio interpolador de Lagrange, com $a_i \in \mathbb{G}$, $i = 1, 2, \ldots, k-1$. Suponhamos que, usando (k, n) queremos compartilhar um segredo $\boldsymbol{S}$, onde, $1 < k \leq n$ (k é igual a 2 ou mais).

1. Escolhe-se aleatoriamente $k-1$ números inteiros a_i tal que: $i = 1, 2, \ldots, k-1$, isto é, $a_1, \ldots, a_{k-1}$, onde $a_0 = \boldsymbol{S}$. Os valores de a_i serão os coeficientes do polinómio interpolador de Lagrange P$(x) = Q(x)$ de grau $k-1$.

2. Constrói-se $Q(x)$, tal que:

$$Q(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$$

3. Faz-se a correspondência dos n valores de $t = 1, 2, \ldots, n$ na função polinomial $Q(x)$, isto é, calculam-se as partes secretas $D_{(t-1)} = (t,\ Q(t))$.

4. A partilha é feita distribuindo a cada participante a sua parte secreta $D_{(t-1)}$ correspondente.

5. A reconstrução do segredo é feita a partir da reunião de $k \leq n$ partes secretas, calculando o polinómio que interpola as k partes secretas. Quer dizer, os k pares ordenados $(x_0,\ y_0), (, (x_1,\ y_1), \ldots, (x_{k-1},\ y_{k-1})$ escolhidos entre os n (total de partes partilhadas).

Portanto, esta é uma das melhores formas de armazenamento de senhas. Pois, um agente de confiança partilha a senha, sem que cada participante (por si só) tenha informações sobre a senha, para além da senha que lhe foi atribuída. A recuperação da senha, pressupõe um acordo mútuo dos participantes. Que é o número de pares ordenados necessários para reconstruir o polinómio. Os pares ordenados, que são as raízes do polinómio, basta serem mais de um pare ordenado, pois, pela unicidade do polinómio interpolador de Lagrange, segundo a qual, um polinómio que interpola pelo menos dois pontos é único.

Mas, para a presente proposta, e para aumentar o grau segurança da senha, para a recuperação da senha, serão necessário todas as partes partilhadas. Assim, um intruso para a concretização de uma acção maliciosa, teria a necessidade de reunir todas as porções partilhadas. O que torna incompatível esta acção, porque um dos envolvidos na partilha é o responsável da partilha ou o dono da senha.

Esta técnica pode ser usada em várias aplicações, por exemplo, no armazenamento da senha de uma urna electrónica de um sistema eleitoral electrónico. Neste caso, basta partilhar a senha com os concorrentes do processo eleitoral. Logo, seria quase impossível entre eles, juntarem suas partes da senha e tentarem acede-la, por terem propósitos diferentes.

1.4.3. Boas práticas de usuários da internet

Para minimizar as manobras dos atacantes os usuários devem tomar atitudes que aumentam a sua segurança na internet (Oliveira, 2021):

- ✓ Crie senhas seguras, aquelas que possuem um comprimento mínimo de 16 caracteres, que preservam a aleatoriedade (imprevisível) e singularidade (única).
- ✓ Troque as senhas periodicamente.
- ✓ Evite um malware. Esteja seguro da fonte do link, ou não clique em links vindos de fontes desconhecidas. Não insira ou forneça dados confidenciais à qualquer agente. Instale aplicativos só depois provar sua segurança.
- ✓ Desconfie de mensagens ou ligações suspeitas.
- ✓ Mantenha seus dispositivos actualizados, ou active actualização automática.
- ✓ Não ignore o perigo dos dispositivos USB apresentam para seus dispositivos ou rede.
- ✓ Mantenha atitudes correctas para proteger a sua rede wifi. Use senhas fortes; Garanta apenas o acesso autorizado; treine regularmente sua equipe sobre aspectos de segurança

web; Tenha um agente de segurança para monitorar a sua rede e corrigir vulnerabilidades; Use ferramentas de monitoramento fidedignas.

✓ Previna-se dos ataques internos ou externos contra a sua rede, monitorando periodicamente seu sistema, ou supervisionando as acções dos elementos da equipa.

Vejamos por exemplo, a tentativa de um ataque "Spoofing," excutado via via Watshapp, no dia 22 de Maio de 2024.

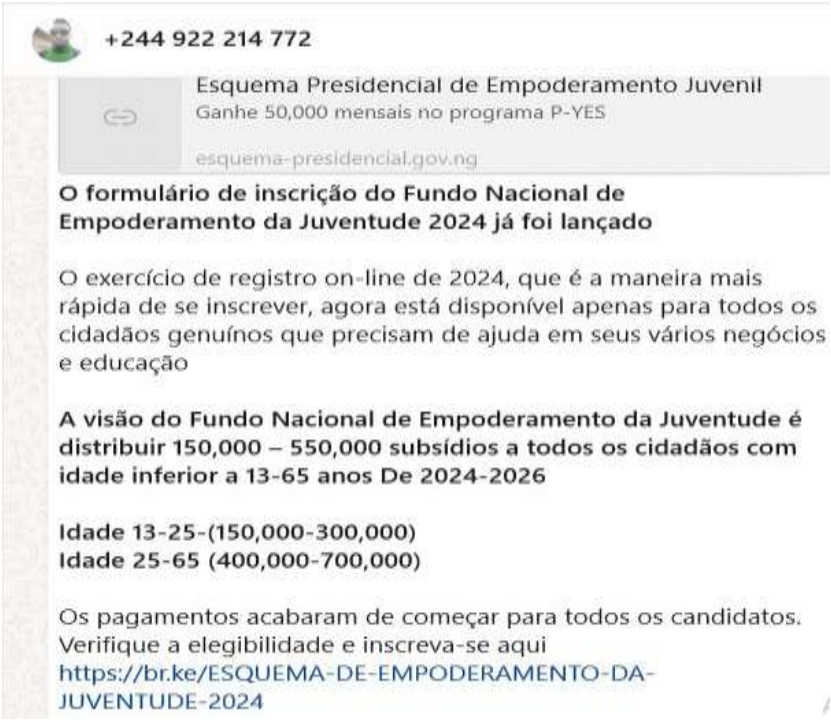

Fig. 9: *Tentativa de ataque Spoofing*
Fonte*: Autor*

O conteúdo parece ser benéfico, o endereço (*esquema-presidencial.gov.ng*) do site proposto pelo link: *https://br.ke/esquema-de-emponderamento-da-juventude-2024*, com o domínio "*gov*", é uma estratégia dos invasores para convencer a vítima que, a fonte da mensagem é fidedigna, quando na verdade se trata de tentativa de uma acção maliciosa.

O propósito era de levar-me a clicar no link, e conduzir-me à uma página falsa, e desta forma, concretizar seus intentos criminosos.

2. MATERIAIS E MÉTODOS

2.1. Materiais utilizados

Para a realização deste trabalho utilizou-se os seguintes materiais:

- **Computador**
- **Impressora**
- **2 Resmas de papel**
- **Placa de internet**

Computador:

Este material serviu para a redigir o conteúdo da pesquisa, construção e implementação do código da abordagem proposta no trabalho, versada em uma técnica para armazenamento de senhas, como forma de protecção contra invasão cibernética.

Não obstante a isso, também foi utilizado para o processo de escrita e impressão dos inquéritos aplicados à amostra da investigação.

Impressora:

É o meio utilizado para imprimir o trabalho, bem como a impressão dos planos de aula relacionado ao tema do trabalho.

Resma de papel:

O papel, foi posto na impressora, usado para imprimir os documentos.

Placa de internet:

A internet foi o meio através do qual, as bibliografias inerentes à pesquisas foram descarregadas. Por outra os inquéritos foram elaborados e aplicados via internet, com recurso ao "*Microsoft forms"*.

2.2. População e amostra

De acordo os dados fornecidos pela área académica e pelos humanos da FET, a população da investigação foi constituída por 190 trabalhadores e 803 estudantes que confirmaram a matricula no segundo semestre do corrente ano académico, perfazendo um total de 993

elementos da população. Dos 190 trabalhadores, 94 são docentes e 96 são funcionários não docentes. De realçar que, no início do ano académico os estudantes matriculados, foram no total 1354, a redução dos alunos para 803, a área académica justificou que os 501 não matriculados para o segundo semestre, corresponde aos estudantes do 5º Ano que defenderam no primeiro semestre, aos reprovados e outros desistidos por razões socioeconómicas.

A amostra foi não probabilística pelo facto de se ter usado a recolha de dados por meio da internet, e os factores: disponibilidade e acessibilidade, tiveram influência na selecção da amostra, na medida que as condições de acesso à internet e a disponibilidade dos inqueridos não favoreceram a composição de uma amostra probabilística.

2.2.1. Detalhes dos elementos da amostra

A amostra foi constituída por 200 elementos, sendo 24 docentes, 159 estudantes e 17 funcionários administrativos. Isto é, 112% da amostra foi constituída por docentes, 79,5% por estudantes e 8,5% por funcionários administrativos.

2.3. Métodos

Durante a investigação aplicou-se os seguintes métodos:

Qualitativo:

O método aplicado no é o método qualitativo, cujos resultados são dados não numéricos. Fez-se a análise a análise bibliográfica sobre o tema e buscou-se opiniões sobre o fenómeno: Invasão e protecção contra ataques cibernéticos, tendo em conta o caso dos funcionários e estudantes.

Empírico:

O método foi aplicado baseando-se nas experiências vividas e contadas por pessoas próximas e na observação da maneira como o assunto se processa no seio da sociedade académica da FET e da sociedade em geral. Com este método foi capaz identificar, descrever e formular o problema da investigação.

Estatístico:

Com este método, foi possível organizar, representar os dados recolhidos através da aplicação dos inquéritos em tabelas de frequências e gráficos, bem como a interpretação dos mesmos, o permitiu tirar conclusões acerca do tema.

2.3.1. Instrumentos de recolha de dados

Para a recolha de dados, aplicou-se um inquérito à amostra. O inquérito esteve composto por 3 perguntas. A primeira questão: *O que entendes por Cibersegurança*? Tinha o objectivo de medir a noção que os inqueridos tinham sobre Cibersegurança. Pois, é importante estar seguro da noção que os elementos da amostra têm, para melhor aplicar as estratégias preconizadas.

Na segunda questão: *Já foi alvo de um ataque cibernético*? Tinha o objectivo de medir o nível de impacto do problema de investigação no seio dos estudantes, docentes e funcionários administrativos da FET. Facto que permitiu a consolidação da descrição e a identificação do problema.

E, na última questão: *Quais dos nomes (Nuvem rompida, Hacking, Crakernet, Folder break, Nenhum) são de um ataque cibernético*? Tinha o objectivo de medir o nível de conhecimento que se tem sobre as técnicas de invasão cibernética. O que nos permitiu elaborar um plano de capacitação actuante e consistente dirigido aos docentes, estudantes e funcionários administrativos da Instituição.

Portanto, as questões constantes no inquérito, todas são do tipo escolhas múltiplas, e para a recolhas de dados foi aplicado faseadamente. Primeiro aos docentes, a seguir aos estudantes e por último aos funcionários administrativos.

2.4. Técnica de protecção cibernética "proposta"

A proposta que visa a proteção de dados através do armazenamento sigiloso de senha, é uma técnica que consiste na determinação da senha como termo independente de um polinómio real $P(x)$, onde são determinados pares ordenados resultantes da aplicação dos números $1,2,\dots,n$ a $P(x)$, que a posterior são partilhados, tal que a recuperação da senha é feita mediante a reconstrução do polinómio que interpola os referidos pares ordenados.

Algoritmo

Suponhamos que, usando (b,n) queremos partilhar uma senha S, onde $k=n$, onde:

b- É o número total de coeficientes do polinómio;

$(b-1)$- Grau do polinómio a construir;

n- Total de agentes participantes na partilha das partes;

k- Total de partes necessárias para reconstruir o polinómio.

A técnica de protecção cibernética proposta tem o seguinte algoritmo, seja $G = \mathbb{Z}_p^*$, um grupo cíclico de ordem $(p-1)$, tendo $g \in G$ como seu gerador, a técnica de protecção cibernética proposta tem o seguinte algoritmo:

1) Escolhe-se $(b-1)$ coeficientes do polinómio $a_i \in G$ tais que $i = 1,2,\ldots,(b-1)$ são os coeficientes do polinómio, em seguida escolhe-se também $a_0 = S$.

2) Constrói e fixa-se o polinómio:

$$P(x) = S + \sum_{i=1}^{b-1} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_{b-1} x^{b-1}$$

3) Calcula-se os pares ordenados ou pontos de $P(x)$, resultantes da aplicação de $t = 1,2,\ldots,n$ em $P(x)$, isto é:

$$(t,\ P(t)_i), \text{ com } i = 1,2,\ldots,n$$

A partilha é feita distribuindo a cada participante o pare ordenado correspondente.

4) A reconstrução do polinómio é feita mediante o cálculo do polinómio que interpola as $k = n$ partes, pares ordenados partilhados, e em seguida determina-se o número da senha $a_0 = S$, que se pretende reaver.

O algoritmo foi implementado computacionalmente na linguagem de programação "python," com intuito de verificar a sua funcionalidade e a execução de tarefas, conforme o programado. Os resultados das execuções demostraram a eficiência computacional da proposta. Portanto, os mesmos foram capturados e guardados e discutidos no capítulo a seguir.

2.4.1. Segurança da técnica proposta para o armazenamento de senhas

A proposta de armazenamento de senhas é segura, na medida que não necessita de credenciais para ser acedida, pois ela não é armazenada a bruto. Mas, funciona como se tivesse que destruir o polinómio em vários fragmentos. Podendo a senha ser reavida com a reconstrução do polinómio tendo as partes da destruição. Apenas a entidade responsável pela partilha, ao executar a acção de recuperação da senha, tem acesso à mesma, sem necessidade de partilhar a senha ou solicitar um gerenciador (servidor). Visto que, solicitam-se as partes partilhadas e não a senha no seu todo, diferentemente das demais técnicas de

armazenamento de senhas que existem actualmente. Assim, a partilha das partes da senha (polinómio), pode ser pública, mas a recuperação da senha é secreta (confidencial). Só é possível uma entidade ter acesso a senha. Porque ainda que haja um plano malicioso para aceder a senha de forma ilegal a partir dos participantes, precisariam do fragmento da entidade principal (responsável) pela partilha e recuperação da senha, que por sua vez, esta entidade pode ser o proprietário do sistema ou da organização que usufrui os serviços. Isto quer dizer que, a proposta é resistente à ataques internos, assim como de ataques externos, pois os ataques externos necessitam de encontrar o conteúdo alvo, armazenado ou em circulação, o que não acontece com esta proposta. Pois, não se armazena nem se partilha a senha, mas os fragmentos que podem dar acesso à senha.

Outrossim, os fragmentos não dão nenhuma pista da senha, nem o atacante consegue ter uma noção ou certeza em identificar a localização dessas partes, nem associá-las com exactidão, porque elas não são armazenadas em nuvem, mas o código em si, destrói o polinómio que contém a senha, e quando for preciso, executa a construção.

Em organizações com vários proprietários, ou participantes com interesses diferentes, como é o caso de empresas com vários accionistas, ou no caso de um sistema de eleição electrónico por exemplo, basta partilhar com todos accionistas ou políticos concorrentes.

Portanto, no caso da FET, para supervisionar o sistema e garantir a segurança de informações, o Decano deve fazer parte das partilhas de todas as senhas que comprometem os dados sigilosos, ou o sistema da Instituição. Assim, a obtenção da senha seria só pela permissão do Decano, ou se pelo menos autorizar alguém. Mas, fica salvaguarda a propriedade segundo a qual, o acesso à senha permanece secreto.

3. RESULTADOS E DISCUSSÃO

3.1. Resultados da técnica de protecção cibernética proposta

Depois de construído e implementado o algoritmo da proposta, obteve-se no seguinte código:

```
def main(bits):
    p= random_prime(2**bits)
    Zp= IntegerModRing(p)
    g=Zp.multiplicative_generator()
    a0=input("Digite a SENHA:")
    n=input("Quantos participantes terá o esquema de PARTILHA?")
    while n<=1:
        n=input("Número rejeitado.Insira um número maior que 1:")
    k=n
    return (n, k, g, p, a0)
def Coeficientes(p, a0, n, k):

    Zp= IntegerModRing(p)
    t=k-1
    coef = [a0]
    for r in range (1, t+1):
        a = Zp.random_element()
        coef.append(a)
    return coef

# Construção do polinómio
def polinomio(coef):
    Zp=coef[0].parent()
    Pol.<x> = PolynomialRing(Zp)
    polinomio=Pol(coef)
    return polinomio
def shared(n, polinomio):
    pares=[]
    for x in range (1, n+1):
        pares.append([x, polinomio(x)])
    return pares
def pol_rec(coef, pares):
    Zp=coef[0].parent()
    Pol.<x> = PolynomialRing(Zp)
    k = len(coef)
    pol = Pol(0)
    for j in range(k):
        lj = Pol(Zp(1))
        for i in range(k):
            if j!=i:
                lj = lj * ((x-pares[i][0])/(pares[j][0] - pares[i][0]))
        pol = pol + lj * pares[j][1]
    return pol
```

Fig. 10. *Implementação computacional do armazenamento seguro de senhas*

3.1.1. Discussão dos resultados da proposta

O código da implementação da proposta, é constituído por 5 funções:

1) **Função *"main"*:** Esta função que inicializa o processo, recebe o número de bits como parâmetro de entrada para determinar o tamanho da chave. Gera aleatoriamente um número primo "p", o grupo cíclico "Z_p" e o gerador "g" do grupo. De seguida solicita ao usuário a sua senha e ao responsável pela partilha, solicita a definição do número de participantes pela partilha, que deve ser maior que 1, caso não for, a solicitação repete-se até que se satisfaça a condição do sistema. Feito isto, o sistema confirma que a inicialização foi feita com sucesso, exibindo uma mensagem que indica o tamanho da chave da Criptografia aplicada. Portanto, a execussão dos resultados da função é feita invocando:

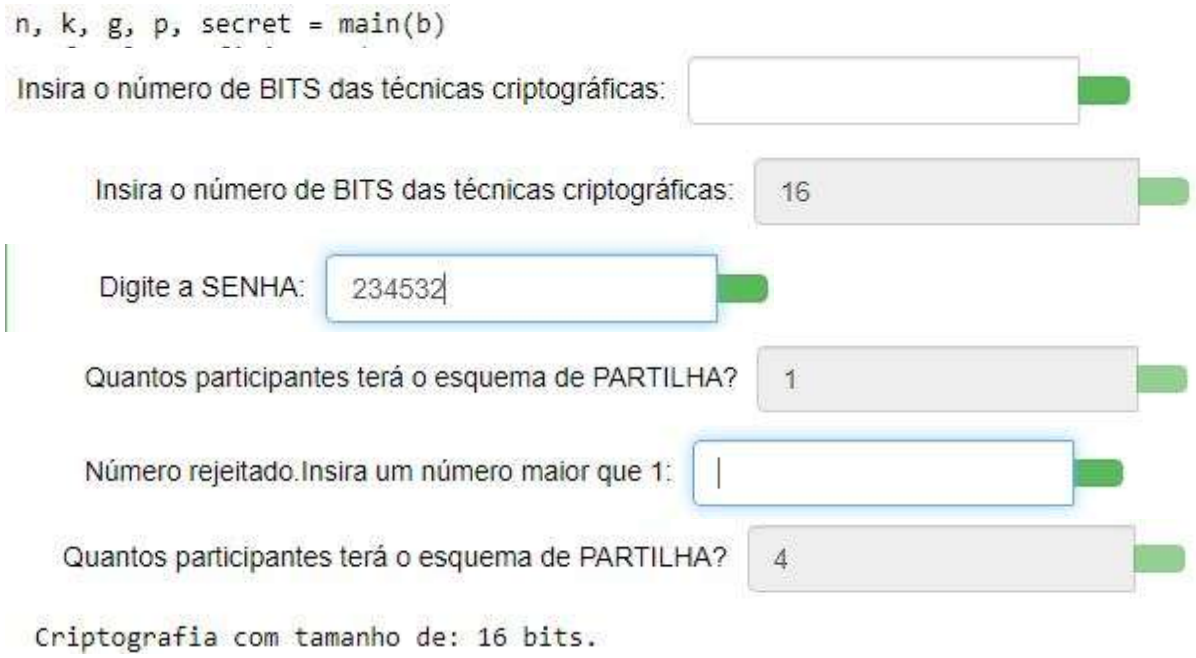

Fig. 11. *Invocação da função que inicializa o sistema*

2) **Função "*Coeficientes*"**: Esta função gera os coeficientes aleatórios do polinómio, seus parâmetros de entrada são, a senha, o número primo, o total de participantes e o número total de elementos necessários para recuperar a senha. Define-se a variável equivalente à senha como o termo independente do polinómio.
3) **Função "*polinómio*"**: É a função que constrói o polinómio, a fim de permitir o cálculo dos pares ordenados do polinómio, para posteriormente serem partilhados. Recebe os coeficientes gerados anteriormente como parâmetros de entrada.

Invocando a função que gera o polinómio temos:

```
coef_pol= Coeficientes(p, secret, n, k)
pol_const= polinomio (coef_pol)
22040*x^3 + 9134*x^2 + 27614*x + 234532
```

***Fig. 12**. Geração dos coeficientes e do polinómio*

Notemos que, como antes definimos que o números de participantes é igual a 4, o sistema constrói um polinómio de grau 3 com a parte do código "Pol.<x> = PolynomialRing(Zp)", cuja independente é o "x". Todavia o polinómio terá sempre um grau igual ao número total dos participantes na partilha menos a unidade.

4) **Função "*Shared*"**: Tendo o polinómio e o número total de participantes como parâmetros de entrada, o sistema calcula os pares ordenados com a parte do código "for x in range (1, n+1)", atribuindo valores à variável independente valores percorrendo uma lista, e em calcula as respectivas imagens com a parte do código "pares.append([x, polinomio(x)])" e consequente formação dos 4 pares ordenados.

Para a função exibir os resultados, invoca-se:

```
partes= shared(n, pol_const)
SENHA PARTILHADA EM 4 PADAÇOS: [[1, 293320], [2, 502616], [3, 994660], [4, 1901692]]
```

***Fig.13.** Partilha da senha em várias partes*

Para cada par ordenado, a abcissa indica a ordem ou posição do participante e a ordenado indicado o pedaço partilhado.

5) **Função** "***Pol_rec***": É a função que recebe as partes partilhadas e os coeficientes, para reconstruir o polinómio interpolador de Lagrange que passa pelos 4 pontos calculados. A parte do código responsável pela aplicação da definição polinómio de Lagrange é a seguinte:

```
for j in range(k):
    lj = Pol(Zp(1))
    for i in range(k):
        if j!=i:
            lj = lj * ((x-pares[i][0])/(pares[j][0] - pares[i][0]))
    pol = pol + lj * pares[j][1]
```

***Fig. 14.** Invocação do polinómio interpolador de Lagrange*

O polinómio é reconstruido invocando:

```
pol_reconst= pol_rec(coef_pol, partes)
POLINÓMIO RECUPERADO: 15699*x^3 + 21313*x^2 + 29018*x + 243652

A TUA SENHA FOI RECUPERADA: 243652
```

***Fig. 15**. Invocação da reconstrução do polinómio e apresentação da senha.*

E por fim, necessitando de usufruir da sua credencial, o usuário recebe a informação da sua senha, informando-o que a senha foi recuperada e indicando o respectivo número. Portanto, a senha tanto no polinómio inicial quanto no final, figura dentro polinómio como termo independente.

3.2. Resultado do inquérito aplicado à amostra

Resultados da 1ª questão

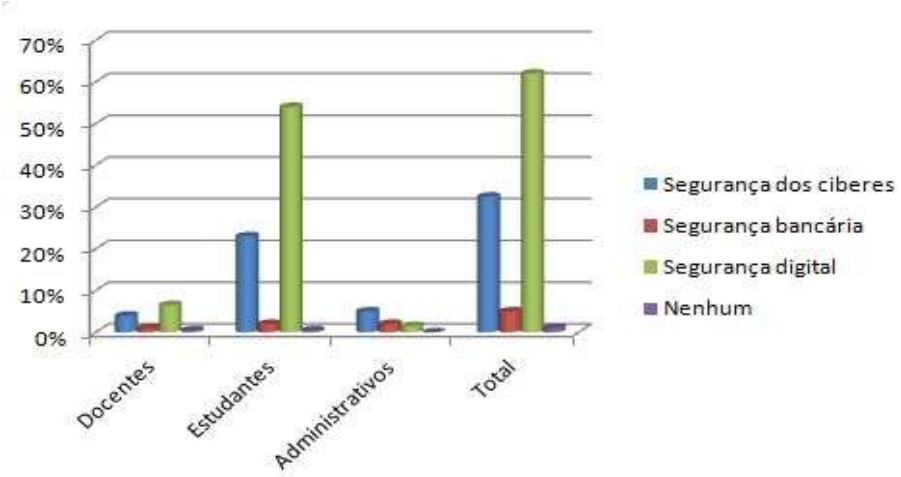

***Grafico 1.** Representação da primeira questão do inquérito*

Resultados da 2ª questão

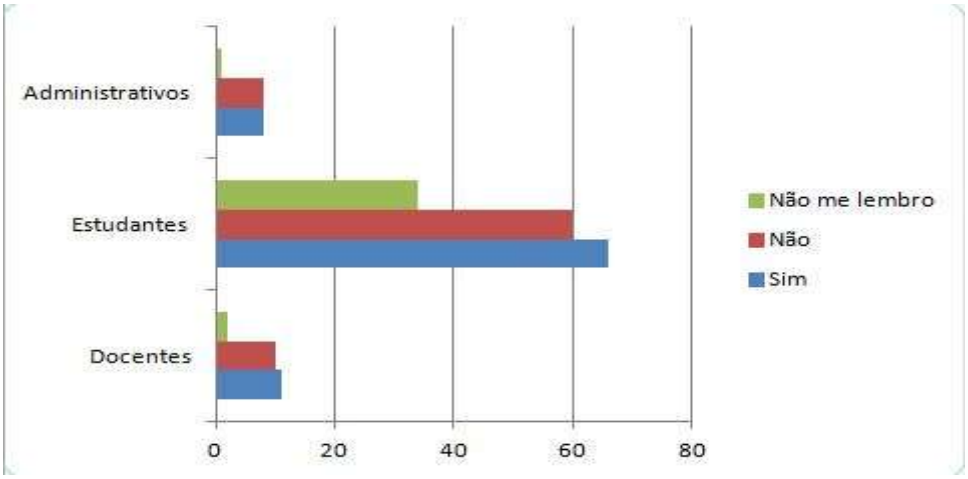

***Gráfico 2**. Representação dos resultados da 2ª questão do inquérito*

Resultado da 3ª questão

Amostra	Quais destes nomes são de um tipo de ataque?									
	Nuvem rompida		Hacking		Crakernet		Folder break		Nenhum	
	F	*P*	*F*	*P*	*F*	*P*	*F*	*P*	*F*	*P*
Docentes	1	0,5%	20	10%	1	0,5%			2	1%
Estudantes	15	7,5%	101	50,5%	29	14,5%	3	1,5%	11	5,5%
Administrativos	4	2%	5	2,5%	7	3,5%	1	0,5%		
Total	20	10%	126	63%	37	18,5%	4	2%	13	6,5%

***Tabela 1**. Resultados da questão sobre tipos de ataques*

3.2.1. Discussão dos resultados dos inquéritos

Para a 1ª questão:

No total foram inqueridos 200 indivíduos, onde os estudantes tiveram a maior representação com 159 deles correspondendo a 79,5%. Quanto a primeira questão, com 4 alternativas, 8 docentes afirmaram que a Cibersegurança é a segurança dos ciberes o que perfaz 4% da amostra, do mesmo modo, 46 estudantes e 10 funcionários administrativos, com 23% e 5 % do total, respectivamente. 10 Pessoas inqueridas afirmaram que a Cibersegurança é a segurança bancária, destas 1% foram docentes, 8% repartidos equitativamente foram estudantes e funcionários administrativos, respectivamente. 124 Do total afirmaram que é a segurança digital, isto é, 62% da amostra demonstrou ter noção sobre Cibersegurança, respondendo acertadamente, onde 13 foram docentes, 108 estudantes e 3 funcionários administrativos. Apenas 2 pessoas disseram que nenhuma alternativa corresponde ao conceito Cibersegurança.

Fazendo uma análise horizontal dos dados, Dos 24 docentes inqueridos, 33% afirmaram que a Cibersegurança é a segurança dos ciberes, 8% dizem ser a segurança bancária, 55 % demonstraram terem noção sobre o assunto, afirmando que é a segurança digital, e apenas 1 afirmou que nenhuma alternativa define a Cibersegurança.

Quanto as estudantes, 68% afirmou ser a segurança digital, para 28% deles disseram que é a segurança dos ciberes, 3% escolheram de opção segurança bancária e 1% disse que nenhuma alternativa é verdadeira.

No quesito funcionário administrativo, num total de 17, 59% afirmou que a Cibersegurança é a segurança dos ciberes, 24% diz ser segurança bancária e 17% foram os que afirmaram que é segurança digital.

Para a 2ª questão:

De modo geral, 42,5% dos inqueridos já sofreram algum tipo de ataque cibernético, onde 66 foram os estudantes, 11 docentes e 8 funcionários administrativos. 39% nunca sofreram algum ataque cibernético, sendo 59 estudantes, 10 docentes e 9 funcionários administrativo e 18,5% não se lembravam se já foram alvo de algum tipo de ataque cibernético.

Entre os estudantes, 42,5% já sofreram ataque, 37% e 21% não se lembravam. Entre os docentes, 46% já sofrem ataque cibernético, 41% nunca sofreram ataque e 13% não se lembravam se já sofreram ataque. No leque dos 18 funcionários administrativos 47% já sofreram ataques cibernéticos, outros 47% nunca sofreram e 6% não se lembravam.

Para a 3ª questão:

10% Dos 200 inqueridos consideram que nuvem rompida é um tipo de ataque cibernético, sendo 1 docente, 15 estudantes e 4 funcionários administrativos. 63% Afirmaram que Hacking é um tipo de ataque, onde 20 são docentes, 101 estudantes e 5 funcionários administrativos. 18,5% Optaram em Crakernet, onde 1 era docente, 29 estudantes e 7 funcionários administrativos. 2% Escolheram a opção Folder break e 13% tinham conhecimentos sobre técnicas de invasão cibernética, sendo 2 docentes, 11 estudantes e nenhum funcionário administrativo.

Portanto, entre os docentes, 8% têm conhecimento sobre técnicas de invasão cibernética e 7% dos estudantes é o número dos têm conhecimento sobre técnicas de invasão cibernética. Isto revela um baixo nível de conhecimento s obre o assunto em estudo.

3.3. Plano estratégico em Cibersegurança para a FET

Propomos de seguida o seguinte plano estratégico de Cibersegurança:

1) Inserir a Cibersegurança como uma unidade extracurricular em todos cursos a partir do 3º Ano.

2) Realizar seminários de capacitação ou refrescamento semestralmente.

3) Aplicar as ferramentas de protecção de dados no sistema de internet da Faculdade.

4) Realizar o diagnóstico de prováveis vulnerabilidades do sistema de internet da Faculdade mensalmente, a fim de permitir a correção das mesmas.

5) Supervisionar as operações e as condições de trabalho dos colaboradores para prevenir ataques internos, aqueles que são sugeridos pela fragilidade existente no dispositivo de um usuário devidamente autorizado.

6) Realizar palestras aos estudantes, docentes ou funcionários da Faculdade, sempre que as condições exigirem.

A inserção da Cibersegurança como uma unidade extracurricular da grelhar curricular dos cursos da Faculdade de Engenharia e Tecnologia (FET) a partir do 3º Ano, é uma estratégia que pode impulsionar a formação de quadros que correspondam aos desafios do século XXI, uma época que as tarefas profissionais são na sua maioria digitalizadas.

Os seminários periódicos dirigidos aos funcionários, é muito importante porque no exercício de funções lidam com meios tecnológicos, cujas comunicações são realizadas através da internet e nem todos são formados não área, ou têm domínio aceitável em Cibersegurança. Logo, os seminários permitirão capacitá-los para melhor desempenharem suas funções e se defendam de acções maliciosas.

Não obstante capacitar o homem, é necessário também fazer um investimento em temos de softwares e hardwares que visam aumentar a segurança de informações para o bem da Instituição.

Assim como os automóveis são feitos manutenções periódicas para diagnosticar prováveis anomalias, ou renovar os acessórios para o bom funcionamento do meio automóvel, também os sistemas de segurança são diagnosticados e actualizados constantemente para a organização se manter resistente às novas manobras maliciosas dos atacantes.

É necessário supervisionar e estar ciente dos estados dos dispositivos utilizados, os tipos de softwares instalados e avaliar se os mesmos ainda satisfazem aos requisitos de segurança recomendados universalmente. Caso não satisfaçam, ou abram brechas para

a intrusão de ataques que podem afetar a Instituição toda, deve-se fazer um upgrade (actualização) ou substituição dos mesmos.

As palestras vêm para responder as situações imergentes, para não se esperar apenas aos encontros ordinários de capacitação, havendo necessidades para contrapor défices vividos por um determinado grupo, deve-se organizar uma palestra para a instrução do que lida com meios tecnológicos capazes de beneficiar e prejudicar uma organização ou no mais agravante, prejudicar uma nação.

Conclusão

Portanto, face a abordagem feita e de acordo aos resultados obtidos, podemos concluir o seguinte:

1) As técnicas de protecção contra ataques e as boas práticas dos usuários da internet, resumem-se em investimento do aumento de segurança, actualização periódica de sistemas, capacitação dos usuários e monitoramento do sistema para prevenir ataques e efectuar correções de vulnerabilidades.

2) A aplicação de um plano estratégico versado na capacitação dos funcionários e estudantes, investimento em ferramentas de segurança e observação dos princípios de Cibersegurança, é uma medida para o aumento da robustez de sistemas digitais.

3) É necessário investir em ferramentas de Cibersegurança, para contrapor as manobras de invasores de sistemas, que constantemente têm aprimorado suas técnicas de técnicas de invasão.

4) O baixo grau de conhecimento em Cibersegurança, denuncia a necessidade de formação de quadros em Cibersegurança para salvaguardar o futuro da segurança de dados de modo geral.

5) É possível aumentar o nível de segurança de uma senha através do armazenamento resultante da aplicação de polinómios.

6) O armazenamento de senhas proposto, abordado e cujos resultados da execução foram é seguro em todas suas fases, na medida que, quer seja na fase da partilha e recuperação de senha, é preservado o acesso privado à mesma.

Recomendações

De modo a minimizar e prevenir impacto negativo do problema, bem como de acordo a necessidade de acompanhar o desenvolvimento tecnológico na segurança de dados, recomenda-se:

1. A proposta do armazenamento de senhas baseada na aplicação de polinómios, limita-se à senhas numéricas. Deve-se incluir no código da proposta uma instrução que converte o conteúdo das senhas ou password's em caracteres ou inteiros, para construir uma proposta que abrange credenciais alfanuméricas.
2. A Direcção da Faculdade deve velar pela criação de uma secção de Cibersegurança, que possa responsabilizar-se pela segurança cibernética da Instituição, a fim de precaver-se de futuros danos que possam advir de prováveis ataques.
3. O trabalho está aberto a melhorias, no que diz respeito a elaboração do plano curricular de capacitação, implementação do plano e avaliação do impacto para análises e implementações futuras.

Referências bibliográficas

Assunção, A. F. M. (s.d). O Guia Hacker Brasileiro.

CISCO Academy (s.d). Laboratório: Criar e Armazenar Senhas fortes. Networking.

Diário da República de Angola (2017). Lei sobre protecção das Redes e Sistemas Informáticos. I Série- Nº 27.

Faria, C. N. (2022). Estratégia de Cibersegurança. Uminho: Portugal.

Giacomelli, I. (2014). Verifiable Secret-Sharing Shemes. AARHUS UNIVERSITY: Aalborg.

Instituto Nacional de Estatística (INE). (2021). Relatório sobre Cibersegurança e Serviços Digitais. Mescti.gov.ao. Luanda: Angola.

Mortensen, M. (2007). Secret Sharing and Secure Multy-Party Computation. N-5020 Bergen.

National Democratic Institute (NDI) (s.d). Manual de segurança cibernética para partidos políticos: Um guia prático para partidos políticos que desejam implantar um plano de segurança cibernética.

Oliveira, Q. M. F. A. (2021). Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação. IMS. Lisboa: Portugal.

Peixinho, C. I. (s.d). Gestão de senhas, políticas e o mundo conectado: desafios e soluções. CTI. MJ.

Shoenmakers, B. (2018). Lecture Notes Cryptographic Protocols. Eindhoven: Netherlands.

Sousa, G. D. (2013). A ética hacker na era do sigilo da informação. Rio de Janeiro: Brasil.