ANÁLISE DE SEGURANÇA DA INFORMAÇÃO EM AMBIENTE PÚBLICO

Marlene Tonel Lopes Jordão*
Msc. Elias de Souza Gonçalves**

RESUMO

A tecnologia se tornou mais presente em nossas vidas, principalmente na pandemia causada pela Covid-19, onde muita coisa foi automatizada, incluindo aulas e outras atividades educacionais. Informação é a moeda de muita empresa e de cibercriminosos, que muitas das vezes sequestram tais dados e exigem dinheiro em troca. No caso de um órgão público, informações e dados pessoais não é a moeda do governo, mas são de cibercriminosos, que vendem para a *Dark Web*. Este trabalho teve como objetivo analisar a segurança da informação de um ambiente público de pequeno porte, analisando desde sua estrutura à segurança direta das máquinas com o mínimo de interferência pessoal. É demonstrado as vulnerabilidades encontradas, o que foi adquirido e o perigo que poderia ocorrer se as informações adquiridas caíssem em mãos erradas. O foco do trabalho foi na vulnerabilidade Eternalblue (CVE-2017-0146).

Palavras-chave: Segurança da informação. Órgão público. Vulnerabilidade.

ABSTRACT

Technology has become more present in our lives, especially in the Covid-19 pandemic, where a lot has been automated, including classes and other educational activities. Information is the currency of many companies and cybercriminals, who often hijack such data and demand money in return. In the case of a public agency, personal information and data is not the currency of the government, but are of cybercriminals, who sell to the Dark Web. This work aimed to analyze the security of information in a small public environment, analyzing from its structure to the direct safety of the machines with minimal personal interference. It demonstrates the vulnerabilities found, what was acquired, and the danger that could occur if the acquired information fell into the wrong hands. The focus of the work was on the Eternalblue vulnerability (CVE-2017-0146).

Keywords: Information security. Public agency. Vulnerability.

* Rede de Ensino Doctum – Unidade Caratinga – marlenetonel@gmail.com – graduando em Ciência da Computação
** Rede de Ensino Doctum – Unidade Caratinga – prof.elias.goncalves@doctum.edu.br. (orientador do trabalho).

1 INTRODUÇÃO

A informação hoje se tornou o bem mais precioso para as empresas conforme a competição se torna mais acirrada. Através disso, a inovação e crescimento no mercado depende muito da tecnologia, e com ela, vem a segurança delas. Com isso, vem o perigo de ataques cibernéticos, correndo risco da organização ter suas informações roubadas, sequestradas ou até mesmo intencionalmente deletadas por completo.

Mesmo com o fácil acesso à informações sobre segurança e o perigo de ataques cibernéticos, há empresas (geralmente de pequeno e médio porte) que ainda usam *softwares* e sistemas operacionais já defasados, que são uma brecha fácil para cibercriminosos. A responsabilidade do profissional de TI é evitar que isto ocorra e alertar os diretores da organização sobre os perigos, mostrando a melhor solução possível.

O estudo se deve demonstrar a importância da segurança de um ambiente público, onde dados pessoais dos cidadãos e informações delicadas estão em constante movimento. Saber que tais informações estão seguras ou não, é de extrema importância da população nos dias de hoje, não importando o método usado, como a caixa preta[1] (*black box*), caixa cinza (*grey box*) e caixa branca (*white box*).

Testar a segurança é necessário para prevenir futuros ataques ou acidentes como nos recentes ocorridos do Sistema Único de Saúde (SUS) e universidades federais. Apesar da diferença entre um ambiente público municipal e um federal ser grande, o estudo tem como seu objetivo demonstrar o quão é necessário melhorar a segurança ou se está de acordo com as normas da ISO/IEC 27002 e seus funcionários atentos à Política de Segurança da Informação, se houver uma.

Geralmente, essas informações são dados pessoais ou assuntos importantes da gestão, e por conta disso, há uma constante necessidade de se comunicar com os servidores governamentais. Dados pessoais são valiosos para criminosos, principalmente golpistas, que usam esse tipo de informação para enganar a vítima e tirar o máximo de dinheiro que pode dela.

Analisar e testar a segurança é um investimento para não ter prejuízos futuros com ataques cibernéticos ou até mesmo de engenharia social. A área da segurança da informação sempre tem que estar em constante investigação, e se não for estudada ou no

---

[1] *Black box* é a definição utilizada para o estilo de teste usado no *penetration testing*. Nele, o *pen tester* não tem informações sobre o alvo, sendo o cenário mais autêntico. Há outros tipos de estilo de testes: *white box* e *grey box*. O *white box* é onde o *tester* tem acesso a muita coisa, incluindo credenciais. O *grey box* é onde o *tester* tem acesso limitado. O *black box* é o mais caro entre eles.

mínimo analisada, há grandes riscos de brechas, ataques cibernéticos, roubos e sequestros de dados, infestação de malwares, e entre outros, podendo levar até mesmo à falência uma organização privada. No caso de órgãos públicos, pode gerar desconfiança na gestão, pois o objetivo do mesmo é mostrar confiança e estabilidade.

2 REFERENCIAL TEÓRICO

2.1 Segurança da Informação

De acordo com Fontes (2006, p. 11), a segurança da informação é “o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada”. A ISO/IEC 27002, define a segurança da informação em sua seção introdutória como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Vai atuar com o intuito de melhorar a gestão de segurança da informação apontando quais são as formas mais adequadas para se garantir a integridade do sistema.

De acordo com Fontes (2006, p. 11)

> A segurança da informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometem o seu funcionamento e o retorno de investimento dos acionistas.

Vale-se observar como dito por Fontes (2006) que a segurança da informação vai além do funcionamento da organização, podendo comprometer também a qualidade do serviço, afetando diretamente o setor financeiro e *marketing*, dando uma imagem ruim do mesmo.

Segundo os padrões da ISO/IEC 27002, os atributos básicos da segurança da informação são:

- **Confidencialidade:** limita o acesso à informação apenas às pessoas autorizadas.
- **Integridade:** a informação deve-se manter correta, verdadeira e não corrompida.
- **Disponibilidade:** garante que a informação deve estar acessível para o alcance de seus objetivos.
- **Autenticidade:** a informação deve estar garantida da fonte anunciada e que não foi alvo de alterações ao longo do processo.

Na segurança da informação deve-se proporcionar meios eficientes para evitar possíveis riscos ao ambiente das organizações. Fontes (2006) reforça que é essencial implementar a solução ideal e mais adequada para a situação para proteger a informação, onde é a adequada com o risco e possível impacto que pode sofrer caso a proteção contra ameaças possam ser quebradas.

Segundo Resende e Barbosa (2013), “Para que as empresas tenham a garantia de segurança de suas informações, são necessários profissionais para atuarem nos setores de informática, que estejam preparados e atualizados”, reforçando que é de extrema importância funcionários qualificados para manter as informações da organização seguras.

2.2 Política de Segurança da Informação

De acordo com a ISO/IEC 27002, o objetivo principal da política de segurança da informação é “prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes”.

Conforme Antunes e Moreira (2015, p. 117)

> A Política de Segurança da Informação é basicamente um manual de procedimentos que descreve como os recursos de que manipulam as informações da empresa devem ser protegidos e utilizados, e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos.

Andrade (2017) explica a importância de se estabelecer a política de segurança, pois através dela é que se define as regras, normas e procedimentos que visam a utilização de recursos de forma confiável dentro da organização.

Machado (2014) destaca que a política de segurança é projetada para garantir que a tríade de segurança (integridade, confidencialidade e disponibilidade) sejam mantidas. O autor explica que “Na política de segurança de uma empresa, a gestão estabelece como um programa de segurança será criado e as metas deste programa, atribui as responsabilidades, mostra o valor estratégico e tático da segurança e descreve como a aplicação desta política deve ser realizada”. Ele ainda reforça que o objetivo da política de segurança é prever as bases da garantia da segurança de informação da organização.

Em Antunes e Moreira (2015, p. 118) “uma política de segurança da informação implantada com sucesso torna a empresa assegurada do mau uso de seus dados e faz com que os seus colaboradores mais propícios a terem um melhor rendimento no trabalho”. O autor completa explicando que o sucesso da elaboração e implementação depende do envolvimento da alta administração e gerências superiores.

A ISO/IEC 27002 ressalta que a “estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização”. Nela, a direção responsável pela organização terá que aprovar a política de segurança da informação, atribuir as funções de segurança, coordenar e analisar de forma crítica a implementação da segurança da informação.

Ainda na ISO/IEC 27002, a política de segurança da informação deve-se ter um gestor capaz de ter responsabilidade aprovada para desenvolvimento, análise crítica e avaliação da política de segurança da informação.

2.3 Vulnerabilidades

Para Machado (2014) “Vulnerabilidade pode ser um software, hardware ou falha de um processo que pode fornecer a um atacante uma porta aberta que ele está à procura, para entrar em um computador ou rede e ter acesso não autorizado aos recursos dentro deste ambiente”. Ainda de acordo com o autor, as vulnerabilidades são brechas que, ao serem exploradas por invasores mal-intencionados, afeta a confidencialidade, disponibilidade e integridade das informações de uma pessoa ou organização.

De acordo com Assunção (2014, p. 29), há seis tipos de falta de segurança: 1) configurações malfeitas; 2) softwares com falhas; 3) redes desprotegidas; 4) proteções ineficazes; 5) falta de atualizações e 6) fator humano.

1. **Configurações malfeitas:** É o primeiro motivo da falta de segurança, como senhas fracas, pastas e arquivos importantes expostos à rede do ambiente, computadores que podem ser acessadas por qualquer pessoa, *switchs* e roteadores com contas de usuário padrão, etc.
2. ***Software* com falhas:** Podem serem usados para se infiltrar ou atrapalhar a pessoa que utiliza tal programa falho. Muitos programas hoje atualizam sozinhos, mas alguns usuários esquecem de ativar a atualização automática ou simplesmente usam um computador antigo que não tem suporte a novas versões de tal *software*.
3. **Redes desprotegidas:** Envolve vários tipos de vulnerabilidades, sendo as principais mencionadas por Assunção (2014, p. 30): falta de criptografia, que envolve utilizar HTTPS em vez de HTTP; redirecionamento de tráfego, que de acordo com Assunção (2014, p. 30), é onde as máquinas da rede podem ser alvos de *ARP POISONING*, *DHCP SPOOFING*, *ICMP REDIRECT* ou *PORT STEALING*; e *spoofing*.
4. **Proteções ineficazes:** São ferramentas como antivírus, *proxys* e filtros, mas que sofrem muitos problemas de segurança. Um exemplo mencionado por Assunção

(2014, p. 31) sobre filtro de pacotes é “mesmo negando o acesso a todas as portas no tráfego de entrada da rede, um atacante ainda poderia acessar uma máquina realizando uma conexão reversa com tunelamento por http ou ICMP”.

5. **Falta de atualizações:** Ele abre vários fatores para grandes riscos à segurança. Assunção (2014, p. 31) exemplifica do porque isso acontece, mencionando que “muitos usuários têm resistência a baixar e instalar *patches* por contra própria”. Em alguns casos, os próprios *patches* podem abrir novas brechas, causando os famosos *zero-day exploits*. *Softwares* muito antigos, como *Windows* XP e 7, já foram abandonados por *Microsoft*, logo, não há mais *patches* de correção a esses sistemas operacionais, sendo um risco enorme ao usuário.
6. **Fator humano:** Segundo Assunção (2014, p. 31), o fator humano é o mais frágil deles.

> Através de técnicas de Engenharia Social, a manipulação do fator humano causa enormes desastres como: fazer um usuário rodar um cavalo de troia sem saber, conseguir informações privilegiadas sobre a empresa, obter especificações de um novo produto, etc.

Um exemplo recente sobre a falta de atualizações é o Eternalblue*, exploit* descoberto pelo grupo *Shadow Brokers* no ano de 2017, se espalhou pelo mundo inteiro atacando sistemas operacionais como Windows 7, Windows Server 2008, Windows XP e até mesmo Windows 10 na porta 445 (como demonstrado na Figura 2). Conforme SentinelOne (2019), havia em torno de 1 milhão de máquinas vulneráveis para o Eternalblue no mundo, sendo 400 mil nos Estados Unidos da América (como demonstrado na Figura 1), mesmo após a correção estar disponível há mais de 2 anos para os sistemas vulneráveis.

Figura 1 – Resultado das máquinas vulneráveis ao Eternalblue

Fonte: SentinelOne, 2019

Figura 2 – Resultado detalhado dos sistemas operacionais vulneráveis ao Eternalblue

Fonte: SentinelOne, 2019

2.4 Um investimento essencial

Vazamentos de dados e senhas têm sido mais comum nos últimos anos. O mais recente e preocupante foi o vazamento de dados de mais de 223 milhões de brasileiros, sendo que há em média 221 milhões no país. A possibilidade é que muitos desses dados são de pessoas já mortas. De acordo com Rohr (2021), as informações vazadas incluem CPF, data de nascimento, dados de escolaridade, benefício do INSS e programas sociais, renda e score de crédito. Esses dados foram colocados à venda na *web* por criminosos.

Segundo Arimathea et al. (2021), menciona “(…) especialistas de empresas, de universidades e do terceiro setor mostram que há por aqui um terreno fértil para ação de cibercriminosos e incidentes de cibersegurança”. No Índice Global de Cibersegurança,

publicado em 2019, o Brasil ocupa a 70.ª posição, e isso reflete no número de ataques e roubos de dados nos últimos anos. Mesmo com a Lei Geral de Proteção de Dados (LGPD), que foi aprovada em 2018, ainda não pode multar os responsáveis pelos vazamentos, pois a Autoridade Nacional de Proteção de Dados (ANPD) é quem fiscalizará e aplicará as devidas multas, mas só terá vigência a partir de agosto de 2021 (ARIMATHEA et al., 2021).

A administração pública brasileira é a quarta mais afetada em todo o mundo sobre vazamento de senhas de e-mail, sendo 3,2 bilhões no total em todo o mundo, ocorrido em fevereiro de 2021 (ARIMATHEA et al., 2021). Nesse vazamento, 68.535 eram senhas de e-mails hospedados em endereços “gov.br”, usados na administração pública brasileira, e outras 4.589 dos domínios “jus.br”, usados pelo Judiciário. Entretanto, não se sabe se as senhas expostas são antigas, pois se trata de informações com origens distintas, podendo conter dados antigos e inválidos nos dias de hoje.

Na publicação de Cruz e Baptista (2021), a rede do Ministério da Saúde foi invadida em janeiro de 2021 por um hacker, mas não houve vazamentos de dados. O invasor deixou uma mensagem na rede do FormSUS, uma plataforma que serve para agrupar dados coletados de pacientes atendidos pela rede pública. O hacker deixou um recado na mensagem de alerta da plataforma dizendo que qualquer um que tenha habilidade mínima de invasão poderia invadir a rede, e finalizou deixando uma solução para o problema.

A preocupação com a segurança da informação não é só nos setores públicos. Arimathea et al. (2021) menciona que empresas privadas no Brasil investem pouco na segurança, com isso, receberam incentivo a mais da parte dos criminosos. O especialista Alexandre Bonatti menciona que somente 2% do orçamento total das companhias brasileiras é dedicado à cibersegurança, sendo que a média mundial é 10%, mas melhorou um pouco de 2% para 5% na pandemia do Covid-19. O tipo mais comum de ataque contra empresas é *ransomware*, deixando o Brasil sendo o segundo maior alvo no mundo, ficando atrás dos Estados Unidos. Mesmo quando as empresas querem contratar um profissional de cibersegurança, o mesmo não se encontra facilmente no mercado, pois há uma baixa formação nas universidades, e quando se encontra, estes saem do Brasil (ARIMATHEA et al., 2021).

Um exemplo de megavazamento por empresa privada nos últimos meses mostrado por Arimathea et al. (2021) é da operadora Vivo, onde teve mais de 100 milhões de celulares expostos na rede, sendo que no ano de 2019 a mesma admitiu que uma falha expôs dados de mais de 24 milhões de clientes. Essas mesmas informações podem ter voltado a circular no ano de 2021 por conta da alta de ataques na pandemia.

Em junho de 2021, mostrado pelo site BBC, um ataque cibernético deixou uma grande empresa brasileira de processamento de carnes, a JBS, inativa em 3 países, podendo ter sérias causas de atrasos nas entregas e aumento nos preços dos produtos. O ataque por *ransomware* fez com que operações na Austrália, Canadá e Estados Unidos fossem temporariamente fechadas, afetando milhares de trabalhadores. De acordo com o site G1 (2021), 7 dias após o ataque, a empresa JBS pagou US$ 11 milhões aos invasores, tendo o objetivo de reduzir problemas relacionados à invasão e evitar vazamento de dados, mesmo o governo dos Estados Unidos recomendando que as empresas não pagassem os criminosos por ataques de *ransomware*.

2.5 O cibercrime não escolhe tamanho

Não são só os órgãos públicos federais e estaduais que são alvos de ataque. Na redação do site Monitor Mercantil (2021), o diretor de Professional Services da Scunna, Ricardo Dastis, disse que as prefeituras são os órgãos mais expostos aos ataques. Nos últimos 2 anos, os ataques ocorriam e nada era feito para os gestores aumentarem a segurança. Isso se trata de um assunto muito grave, pois ocorre roubo de dados e até recursos.

Segundo na redação (2021), em abril de 2021, uma prefeitura no interior do Rio Grande do Sul, Piratini, sofreu um ataque causando um prejuízo de R$ 528 mil. No fim de 2020, outra prefeitura, Candiota, também no Rio Grande do Sul, teve quatro sistemas invadidos que eram usados pela mesma, tendo dados sequestrados e um *ransomware*. Ainda em 2021, o Sistema Digital de Fiscalização da Prefeitura de Belo Horizonte foi invadido, onde os invasores haviam deixado mensagens que atacavam diretamente o prefeito. A prefeitura de Santa Cruz do Sul, interior do Rio Grande do Sul, teve o site invadido. O mais alarmante das mencionadas na redação da invasões nas prefeituras é o que ocorreu em março de 2020, em Imbuia de Santa Catarina, com apenas 6.200 habitantes, onde os invasores invadiram 10 contas bancárias da prefeitura e roubaram cerca de R$ 2 milhões.

De acordo com o site Monitor Mercantil (2021), na pesquisa de *Cyberattacks Targeting Latin America*, entre fevereiro e abril de 2021, o Brasil ocupa a sétima posição mundial como principal fonte de tráfego contaminado, com 7 milhões de *malwares*. Segundo o levantamento da Fortinet na redação, na pandemia, os ataques têm sido alarmantes, ultrapassando a marca de 8,4 bilhões em 2020, representando um crescimento de mais de 350% no Brasil. Isso se dá por conta da falta de investimento em estrutura

tecnológica e do cenário causado pela Covid-19, onde muitas coisas foram automatizadas e dependentes de servidores.

Ainda na redação do site Monitor Mercantil (2021) “Dados da McAfee apontam que os prejuízos gerados por cibercriminosos somaram mais de US$ 1 trilhão. Comparado ao último levantamento da companhia de 2018, o aumento dessa cifra foi maior que 50% em dois anos”. A preocupação com a segurança digital despertou interesse nas empresas em investir após a Lei Geral de Proteção de Dados (LGPD) estar entrando em vigor.

3 METODOLOGIA

O objetivo deste trabalho é analisar a segurança da informação no ambiente público, especificamente de pequeno porte. Para isso, foram utilizados métodos das pesquisas bibliográficas para conhecer melhor as estruturas básicas e recomendadas da segurança da informação de uma organização. Os métodos para invasões e como fazê-las foram de acordo com vídeo-aulas lecionadas por Zaid Sabih[2] e Aleksa Tamburkovski[3] na plataforma Udemy. A classificação dos testes é a caixa preta (*black box*) onde não se tem nenhum conhecimento e acesso da organização.

As ferramentas escolhidas foram de acordo com a necessidade dos testes, utilizando de algumas as recomendadas por Assunção (2014), Zaid Sabih e Aleksa Tamburkovski em cada situação. Também nas pesquisas bibliográficas, foi possível saber quais os tipos mais comuns de vulnerabilidades e erros cometidos. O foco é a vulnerabilidade do código CVE-2017-0146, conhecido também como Eternalblue.

3.1 Ferramentas

O aircrack-ng é uma ferramenta gratuita e de código aberto para detectar redes, sniffer de pacote, aplicativo de quebra de WEP e ferramenta de análise para redes locais sem fios 802.11. Seu funcionamento com placas de rede que suportam o modo de monitoramento podem capturar e analisar tráfegos 802.11a, 802.11b e 802.11g. A ferramenta vem com um pacote de aplicações separadas, cada um com propósitos diferentes, mas todos envolvendo a aplicação na rede. Foi utilizado configuração padrão na ferramenta. As aplicações utilizadas no trabalho foram:

- aircrack-ng: Quebra de chaves WEP e WPA/WPA2-PSK.

[2]Disponível em: <https://www.udemy.com/course/learn-ethical-hacking-from-scratch/>. Acesso em: 4 de março de 2021.

[3]Disponível em: <https://www.udemy.com/course/complete-ethical-hacking-bootcamp-zero-to-mastery/>. Acesso em: 6 de março de 2021.

- aireplay-ng: Injeção de pacotes, sendo um deles podendo causar desautenticação na rede para pegar o WPA *handshake*, agilizando a captura do mesmo.
- airodump-ng: Usado para capturar o tráfego da rede em um arquivo .cap, mostrando as informações da rede.

O hashcat é uma ferramenta gratuita e de código aberto para recuperação de senha, suportando 5 modos únicos de ataque, mas foram utilizados apenas dois deles: direto e força bruta. O ataque direto tenta todas as palavras de uma lista (ou *wordlist*). O ataque de força bruta e de máscara (ou *mask*) tenta todos os caracteres usados no *charsets* disponíveis na ferramenta. Nele é possível fazer o uso de placa de vídeo para as quebras de senhas, agilizando muito o processo. A placa de vídeo usada nos testes é a NVIDIA GeForce GTX 970 e foi utilizado configuração padrão da ferramenta.

Nmap (*Network Mapper*) é uma ferramenta gratuita e de código aberto, sendo utilizado para descobrir serviços e servidores em uma rede de computadores, avaliar a segurança e escanear as portas. Sua utilidade é vasta e pode até mesmo escanear vulnerabilidades das máquinas na rede, incluindo ver a versão do sistema operacional e *firewall* usados. Sua utilização foi constante durante os testes, pois os IP's mudavam, indicando que alguns computadores utilizavam a aquisição de IP de forma aleatória. Foi utilizado configuração padrão da ferramenta.

Para analisar se a rede tem proteção contra ataques *man-in-the-middle*, foi utilizado a ferramenta Bettercap. Nele, o invasor pode ver todo o tráfego de rede, analisando o que cada máquina conecta e possíveis informações sensíveis caso a vítima esteja navegando em sites com o protocolo HTTP. Foi utilizado um pequeno *script* para agilizar o processo de ligar os módulos necessários para o ataque. Os seguintes comandos eram:

- set arp.spoof.fullduplex true
- set arp.spoof.targets 192.168.25.1/24
- arp.spoof on
- set net.sniff.local true
- net.sniff on

Para executar o Bettercap juntamente com o *script*, foi utilizado o seguinte comando:

- sudo bettercap -iface wlp2s0 -caplet spoof.cap

Nexpose é uma ferramenta paga criada pela Rapid7, com 1 mês de teste grátis, e código fechado, sendo utilizado para escaneamento de vulnerabilidades. A escolha da ferramenta se dá ao teste de 1 mês grátis, dando total controle ao usuário sem interrupções ou limites de escaneamentos. Com Nexpose foi possível fazer um escaneamento de toda a rede em busca por vulnerabilidades, dando um gráfico intuitivo e uma lista de gravidade de cada uma delas. Seu banco de dados sobre as vulnerabilidades é vasta. Foi utilizado configuração padrão da ferramenta.

Metasploit é uma ferramenta gratuita (contendo versão paga) e de código aberto, sendo utilizado para facilitar os testes de penetração, permitindo que o usuário escreva, teste e execute o código de *exploit*. A ferramente é pertencente a empresa Rapid7. Ele contém uma extensa lista de ferramentas mais utilizadas para testes de segurança. Com ele, foi possível explorar as máquinas vulneráveis ao Eternalblue. Foi utilizado um módulo modificado, demonstrado na Figura 3.

O Arch foi a distribuição Linux escolhida para os testes. Apesar de existirem distribuições mais voltadas para o *Penetration Test*, como o Kali Linux e Parrot OS, a preferência pela escolha pelo Arch se deu pela experiência pessoal da autora e pelo fato da distribuição ser *rolling release*, fazendo com que as ferramentas estejam sempre com as versões mais recentes.

3.2 Reconhecimento do local

Os testes foram realizados na prefeitura de Tarumirim - MG, entre os meses de abril e maio do ano de 2021, finalizando alguns detalhes em setembro. Foi autorizado pelo Chefe de Informática e Sistema que os testes poderiam ser feitas, mas não foi permitido perturbar, impedir e prejudicar os funcionários de seu trabalho. A autorização se encontra no Anexo A. Os dados sensíveis e pessoais adquiridos serão demonstrados no trabalho de forma anônima e nunca compartilhados. Após o término dos testes, os dados foram excluídos.

Em média, haviam 3 computadores em cada sala, dando um total aproximado de 60, sendo 2 deles usados como servidor: um para e-sus e outro para o sistema integrado. Cada funcionário é responsável por apenas um computador, mas era trocado caso houvesse necessidade de mudança ou manutenção. Boa parte das máquinas ainda executam o sistema operacional Windows 7, que parou de receber suporte da Microsoft em janeiro de 2020. Haviam também várias conexões Wi-Fi, todas com senhas.

Todos os computadores, incluindo dispositivos móveis, conectam-se em uma única rede local. A configuração da rede é de forma básica, sem nenhum tipo de monitoramento

ou fixação dos IP's em cada dispositivo. Este tipo de configuração facilita quando há mudanças o tempo todo, mas também ajuda o invasor a utilizar de ataques como spoofing e redirecionamento de tráfego sem ser interrompido em momento algum. Os computadores são conectados via cabo de rede, todos organizados e longe de possíveis acessos externos. O *backbone* da rede do prédio, onde os cabos de rede dos computadores conectam na internet, estava trancada e longe do alcance de pessoas não autorizadas.

3.3 Varredura

Para a aquisição dos *handshakes*, foi utilizado um adaptador USB Wi-Fi da TP-Link TL-WN821N, pois ele possui o modo de monitoramento, permitindo que ele monitore todo o tráfego recebido das redes *wireless* do local. Após a aquisição da senha de um dos Wi-Fi do local, foi feito um escaneamento por vulnerabilidades utilizando a ferramenta Nexpose. Antes de iniciar os testes dentro da rede, foi feito uma análise e observação no acesso FTP do sistema integrado da prefeitura. Nele foi possível adquirir algumas informações com dados pessoais de alguns cidadãos como mostrado na Figura 8.

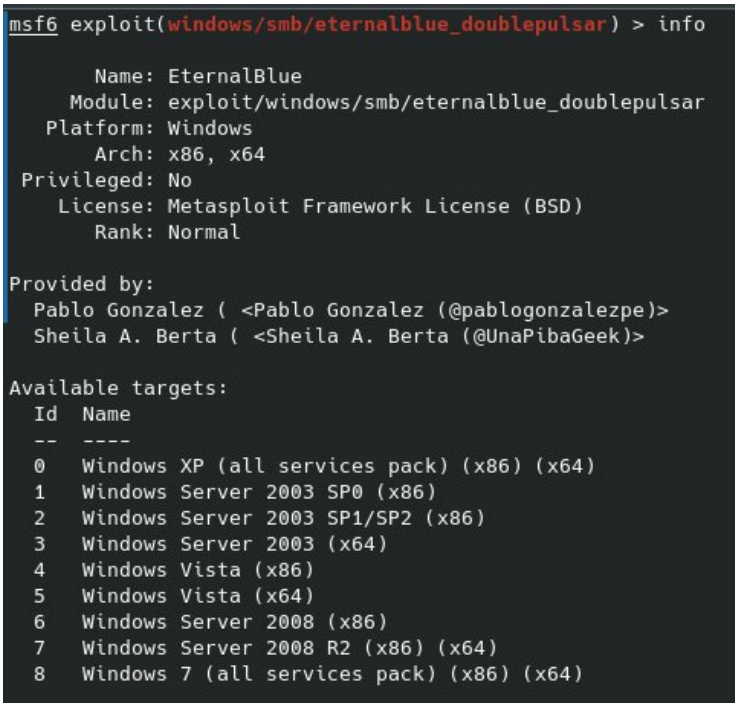
O teste feito na rede foi utilizando o tipo de ataque *ARP spoofing*, que faz com que o invasor envia mensagens de um Protocolo de Resolução de Endereços na área da rede local. O invasor associa o endereço MAC dele com o endereço IP do hospedeiro. Com o ataque sendo executado, o invasor pode interceptar os quadros de dados da rede invadida, modificar o tráfego ou interromper o tráfego, mostrado na Figura 9. Este tipo de ataque é geralmente usado para negação de serviço, ou DoS (*Denial of Service*), e *man-in-the-middle*. Não foi possível utilizar o ataque DoS por conta do acordo feito com a prefeitura de não prejudicar o funcionamento da mesma durante os testes.

3.4 Exploração da vulnerabilidade Eternalblue

Para invadir as máquinas vulneráveis ao Eternalblue, foi usado um módulo[4] modificado do Metasploit para melhores resultados. Os testes foram feitos entre os meses de abril e maio.

[4]Disponível em: <https://github.com/Telefonica/Eternalblue-Doublepulsar-Metasploit>. Acesso em: 17 de abril de 2021.

Figura 3 – Informação básica do módulo e dos sistemas operacionais que afeta



Fonte: Captura de tela obtido pela autora

Com o acesso ao computador através da vulnerabilidade, é possível baixar os documentos salvos, verificar o que tem instalado, fechar e abrir programas, e podendo enviar e executar outros *softwares* sem a necessidade do usuário fazê-lo. O invasor tem total controle sobre o computador, incluindo escanear o teclado da vítima como demonstrado na Figura 13, onde é possível adquirir em forma de texto o que a vítima digita e até mesmo tirar captura de tela, mostrado na Figura 12.

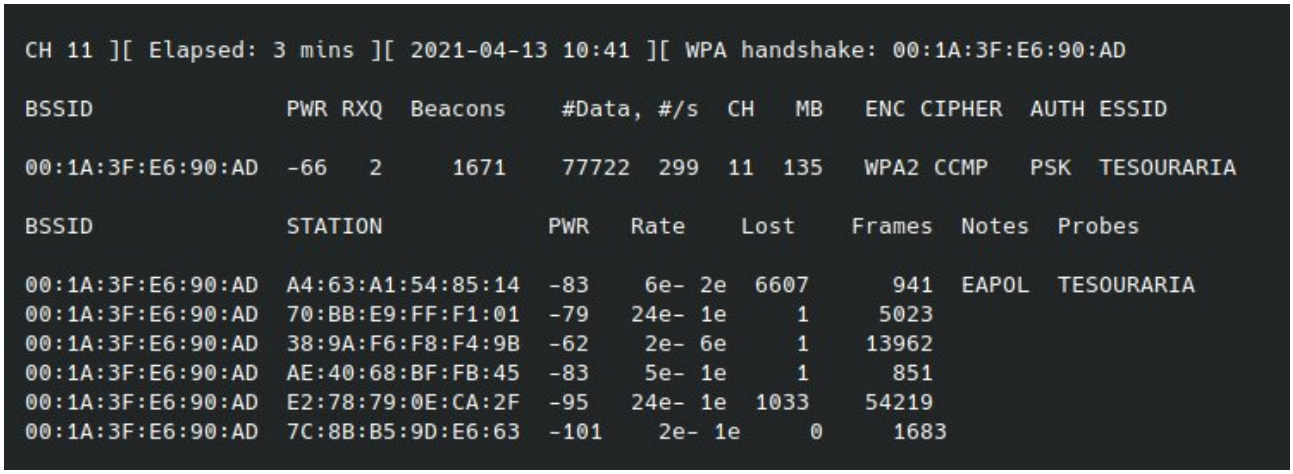
4 RESULTADOS

Esta seção apresenta informações obtidas após a execução dos testes no ambiente da prefeitura. Nela estão todas as vulnerabilidades mais relevantes e perceptíveis. Os resultados obtidos são apresentados por nível de perigo das vulnerabilidades de acordo com a lista feita pelo Nexpose, começando pelo menos crítico.

4.1 Acesso a rede

Para fazer os testes, é necessário ter acesso a rede da prefeitura. Haviam vários sinais Wi-Fi no local, e de acordo com a análise do airodump-ng, 5 deles eram bem movimentados: CHEFE DE GABINETE, CPD2, INFORMATICA, TESOURARIA e GABINETE. Foi possível adquirir o *handshake* de todos eles, um exemplo é apresentado na Figura 4.

Figura 4 – Aquisição do WPA *handshake* do Wi-Fi com nome de TESOURARIA



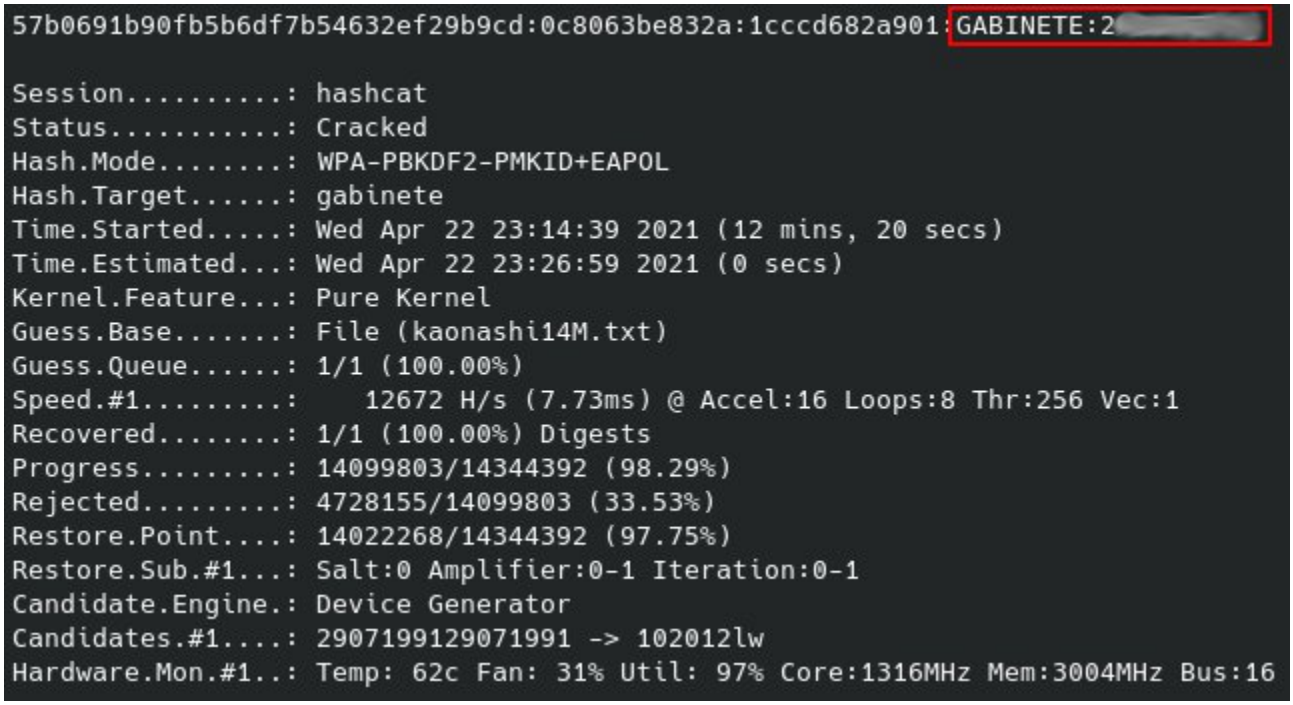
Fonte: Captura de tela obtido pela autora

Meses após a aquisição dos *handshakes*, foram removidos os Wi-Fi do último andar do prédio, sendo eles o TESOURARIA e INFORMATICA, sobrando apenas os CPD2, CHEFE DE GABINETE e GABINETE.

Para a quebra de senha dos Wi-Fi, foi escolhido a tentativa de uso de *wordlist*, uma lista de palavras, números e caracteres especiais aleatórios. Para isso, foi usado a ferramenta hashcat para a quebra de senha utilizando várias *wordlists* de tamanho médio adquiridas no site Weakpass[5], entre 100MB à 700MB. Apenas o Wi-Fi GABINETE teve sucesso e a quebra de senha durou apenas 12 minutos e 20 segundos, conforme pode ser visto na Figura 5.

[5]Disponível em: <https://weakpass.com/>. Acesso em: 19 de abril de 2021.

Figura 5 – Quebra de senha do Wi-Fi GABINETE



Fonte: Captura de tela obtido pela autora

Após a senha adquirida, foi possível entrar na rede sem problemas e fazer um escaneamento com a ferramenta nmap para uma rápida análise de quantos dispositivos estavam conectados na rede. Haviam 63 dispositivos conectados no momento da análise, indicando que a rede local do prédio é consideravelmente movimentada.

4.2 Escaneamento e FTP

Utilizando a ferramenta Nexpose, foi possível fazer um escaneamento preciso de cada dispositivo na rede em busca por vulnerabilidades com os gráficos intuitivos e informações em cada uma delas. Após o escaneamento, foi possível ver que 8 computadores estavam vulneráveis ao Eternalblue (CVE-2017-0146). Todos os vulneráveis pelo Eternalblue são do sistema operacional Windows 7, conforme mostram as Figuras 6 e 7.

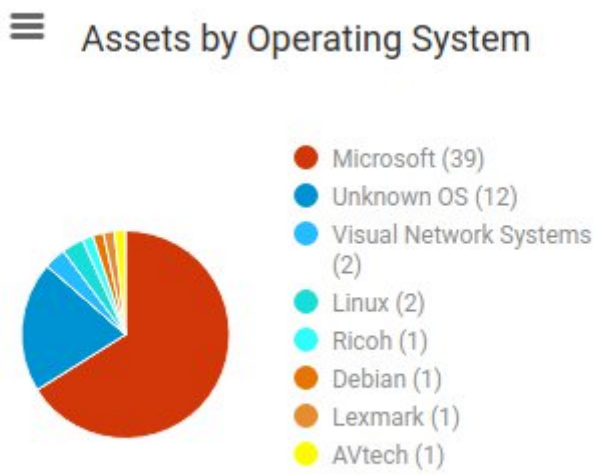
Figura 6 – Lista de vulnerabilidades com o maior risco de acordo com Nexpose

Title			CVSS	CVSSv3	Risk	Published On	Modified On	Severity	Instances
Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability			9.3	8.1	919	Tue Mar 14 2017	Fri Aug 23 2019	Critical	8
Default or Guessable SNMP community names: public			10		916	Wed Jan 01 1997	Wed Dec 04 2013	Critical	2
FTP access with administrator/null credentials			7.5		907	Fri Jan 01 1999	Thu Sep 27 2012	Critical	1
FTP access with admin/password credentials			7.5		907	Fri Jan 01 1999	Thu Sep 27 2012	Critical	1
FTP access with admin/passwd credentials			7.5		907	Fri Jan 01 1999	Thu Sep 27 2012	Critical	1
FTP access with administrator/password credentials			7.5		907	Fri Jan 01 1999	Thu Sep 27 2012	Critical	1
FTP access with admin/null credentials			7.5		907	Fri Jan 01 1999	Thu Sep 27 2012	Critical	1
FTP access with administrator/passwd credentials			7.5		907	Fri Jan 01 1999	Thu Sep 27 2012	Critical	1
Obsolete Debian GNU/Linux Version			10		904	Fri Jun 30 2006	Tue Jun 30 2020	Critical	1
PHP Vulnerability: CVE-2007-0910			10		902	Tue Feb 13 2007	Wed Jul 21 2021	Critical	1

Showing 1 to 10 of 434 | Export to CSV Rows per page: 10

Fonte: Captura de tela obtido pela autora

Figura 7 – Gráfico dos sistemas operacionais usados nas máquinas da prefeitura



Fonte: Captura de tela obtido pela autora

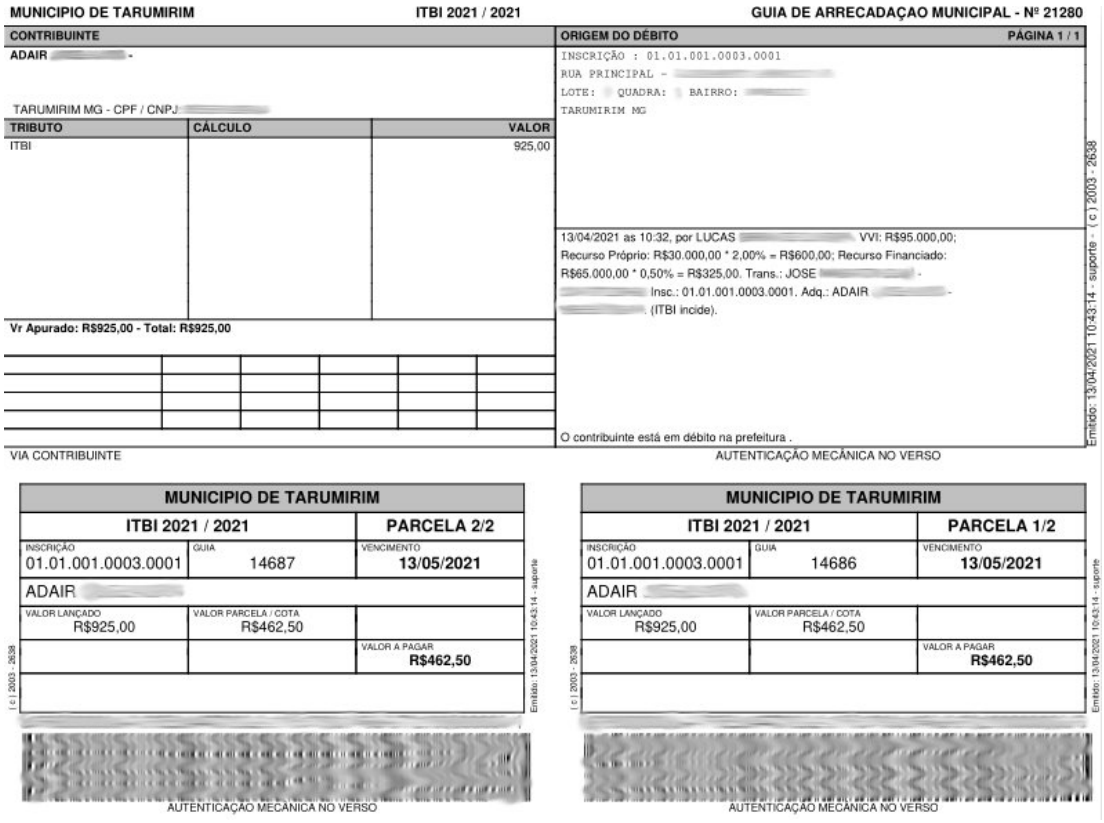
Foram encontradas 434 vulnerabilidades no total, e de acordo com Nexpose, a mais crítica delas é o Eternalblue (CVE-2017-0416), como apontado na seção de Vulnerabilidades no Referencial Teórico. Também foi descoberto através da lista, acessos FTP de uma impressora conectado via rede e de um servidor do sistema integrado da prefeitura. No caso da impressora, não haviam informações ou arquivos sensíveis, apenas as configurações e fila de impressões da mesma. Já no do servidor, haviam 3 acessos no sistema: Sistema de Contabilidade Pública, Sistema Integrado de Gestão Pública e Sistema de Apuração de Pregão.

No acesso FTP do servidor do sistema integrado poderiam ser acessados da seguinte forma:

- http://192.168.25.50/contab0/
- http://192.168.25.50/erpsim/
- http://192.168.25.50/siap/

No contab0 (Sistema de Contabilidade Pública), haviam documentos de contas e gastos públicos, alguns de até mais de 10 anos. No erpsim (Sistema Integrado de Gestão Pública), haviam documentos voltados para o setor de tributos, e nele foram encontrados alguns documentos como alvará de construção e de licença para funcionamento de comércio, listagem de certidões de 2014 de outra cidade e guia de arrecadação municipal de ITBI de um cidadão. Se este tipo de documento for exposto ao público ilegalmente, poderia ferir a LGPD (Lei Geral de Proteção de Dados).

Figura 8 – Guia de arrecadação municipal de ITBI de um cidadão



Fonte: Captura de tela obtido pela autora

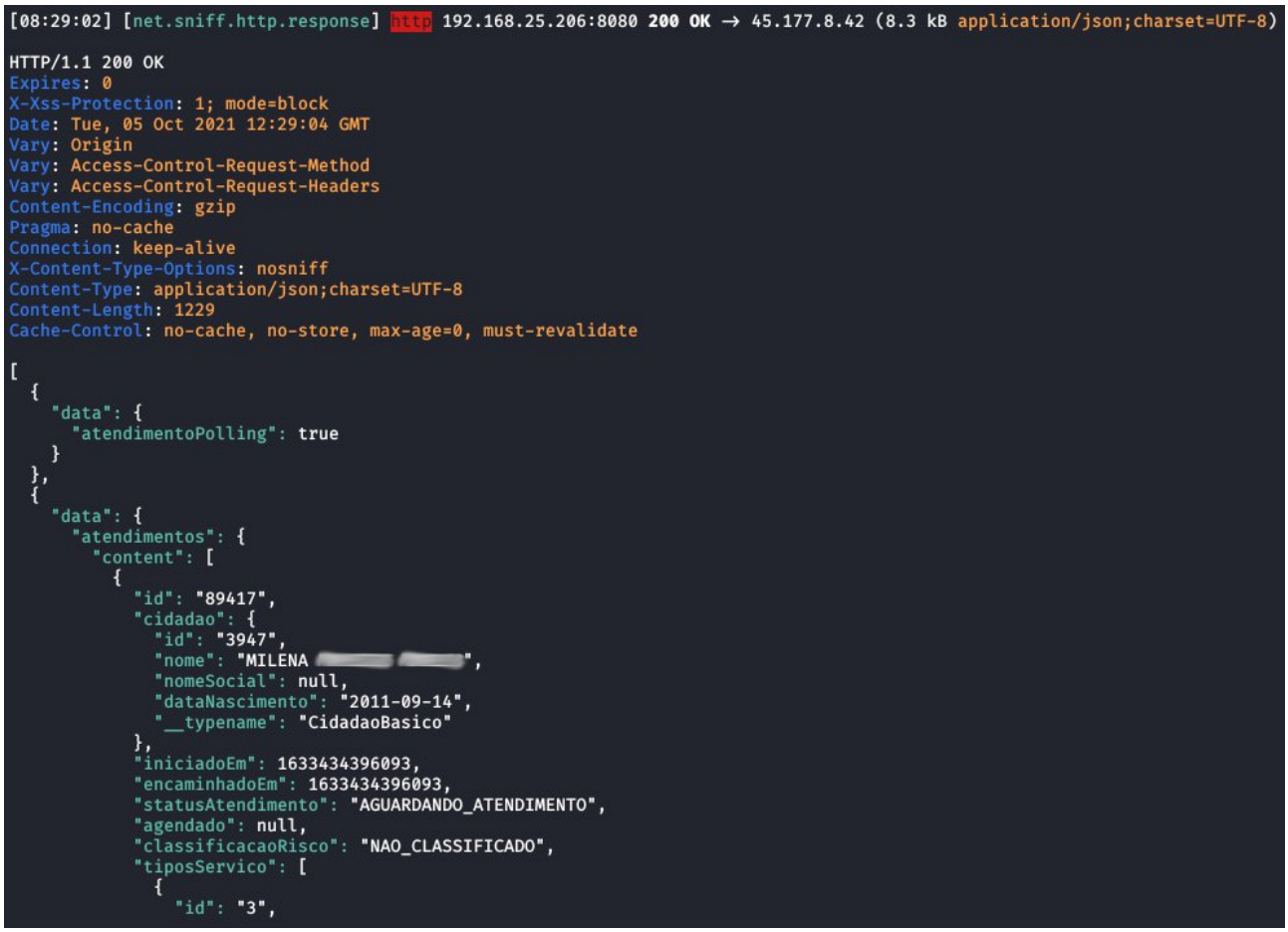
Ainda no erpsim, foram encontrados alguns arquivos .sql e até mesmo .sh, todos datados há mais de 15 anos. No siap (Sistema de Apuração de Pregão), haviam documentos de pregão e licitação, contendo nomes e CPF dos candidatos. Nesse caso, as

licitações devem ser públicas, mas esses tipos de informações não podem ser adquiridas desta forma, dando uma má impressão de baixa segurança das informações armazenadas nos servidores.

4.3 Man-in-the-middle

O primeiro teste na rede a ser feito foi o ataque man-in-the-middle. Alguns *switchs* e roteadores vêm de fábrica com uma proteção contra tal ataque, mas isso não se mostrou presente na rede da prefeitura, sendo possível ver todo o tráfego sem interrupções. Há também formas de proteger a rede através de *softwares* e algum especialista de segurança mantendo vigia, mas isso também não se mostrou presente. Durante o ataque, foi possível ver o que parecia ser dados inseridos no sistema do e-sus, sendo que o IP do servidor do e-sus na hora do teste era o 192.168.25.206, como apresentado na Figura 9.

Figura 9 – Uma das informações adquiridas através do ataque *man-in-the-middle*



Fonte: Captura de tela obtido pela autora

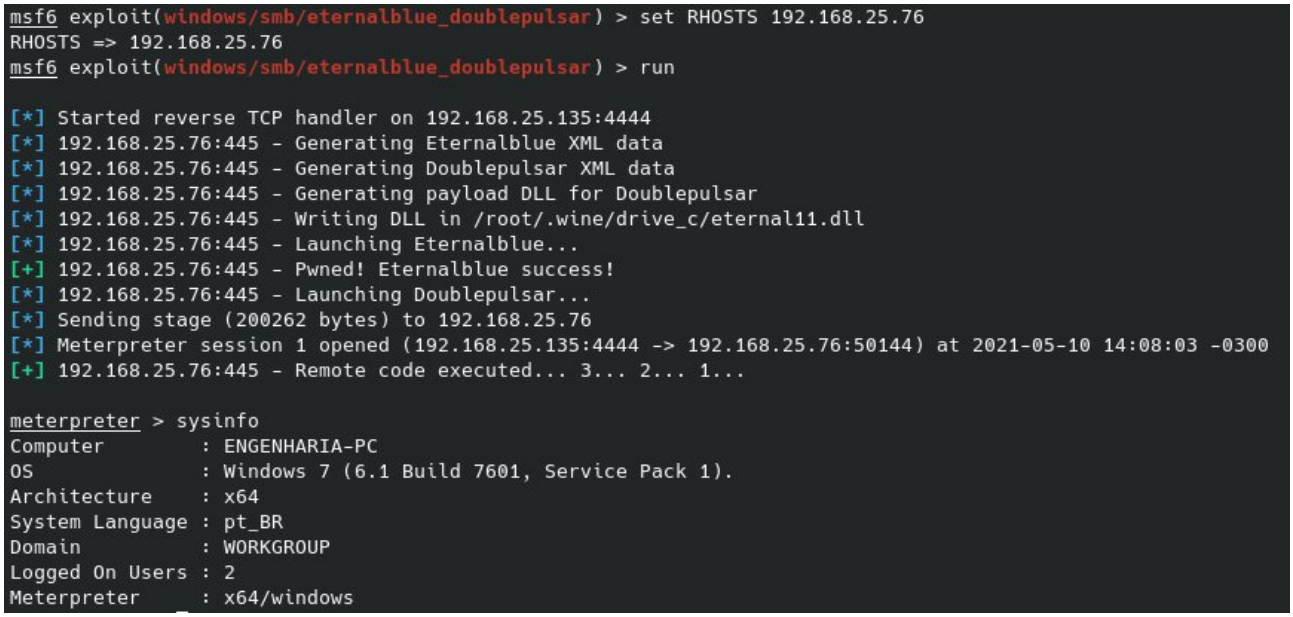
Pelo fato de não estarem usando proteção contra esse tipo de ataque, seus sistemas que utilizam HTTP, um protocolo sem segurança criptografada, faz com que o invasor

possa ver o que é acessado sem problemas e com total clareza. O invasor pode até mesmo injetar códigos de Javascript para substituir links, imagens, inserir elementos HTML e até mesmo um alerta falso de atualização no navegador (sendo que na verdade é um *backdoor*). *Backdoor* são perigosos, pois dão acesso quase que completo para o invasor no computador da vítima, e um exemplo disso é demonstrado na próxima seção.

4.4 Eternalblue

Como analisado na seção de Vulnerabilidades do Referencial Teórico, o Eternalblue continua presente no mundo, e na prefeitura não foi diferente. Como demonstrado pelo Nexpose, haviam 8 computadores vulneráveis ao Eternalblue e foi testado cada um deles. O primeiro alvo foi o computador com nome de Engenharia-PC (Figura 10).

Figura 10 – Invasão do computador com nome de Engenharia-PC



Fonte: Captura de tela obtido pela autora

Após a invasão, foi possível ter total controle do computador via terminal. Foi possível ver que haviam vários arquivos de projetos de engenharia que já foram feitos e que ainda serão construídos. Havia também um arquivo de contrato pessoal do responsável pelo computador (Figura 11). Mesmo sendo um documento pessoal, isto poderia ferir a LGPD. Foi adquirido nada de importante no escaneamento do teclado. Foi feito também uma captura de tela, mostrando que o responsável pelo computador trabalhava em uma tabela no Excel após a invasão, como apresentado na Figura 12.

Figura 11 – Contrato pessoal do responsável pelo computador

AUTORIZAÇÃO

Eu, **JOÃO VICTOR** [redacted], brasileiro, solteiro, portador do RG nº [redacted], [redacted] e inscrito no CPF sob o n.º [redacted], residente e domiciliado na [redacted] – CEP [redacted] – Tarumirim-MG, **AUTORIZO**, através do presente instrumento, a Sra. **LORENA** [redacted], brasileira, divorciada, portadora do RG nº [redacted], [redacted] e inscrita no CPF sob o n.º [redacted], residente e domiciliada na [redacted], [redacted] CEP [redacted], nesta cidade de Governador Valadares-MG, como **Autorizada** a assinar, concordar, dar por encerrado o Contrato de Locação ao imóvel localizado na [redacted], que figura como **Locatário** o presente **Autorizante**.

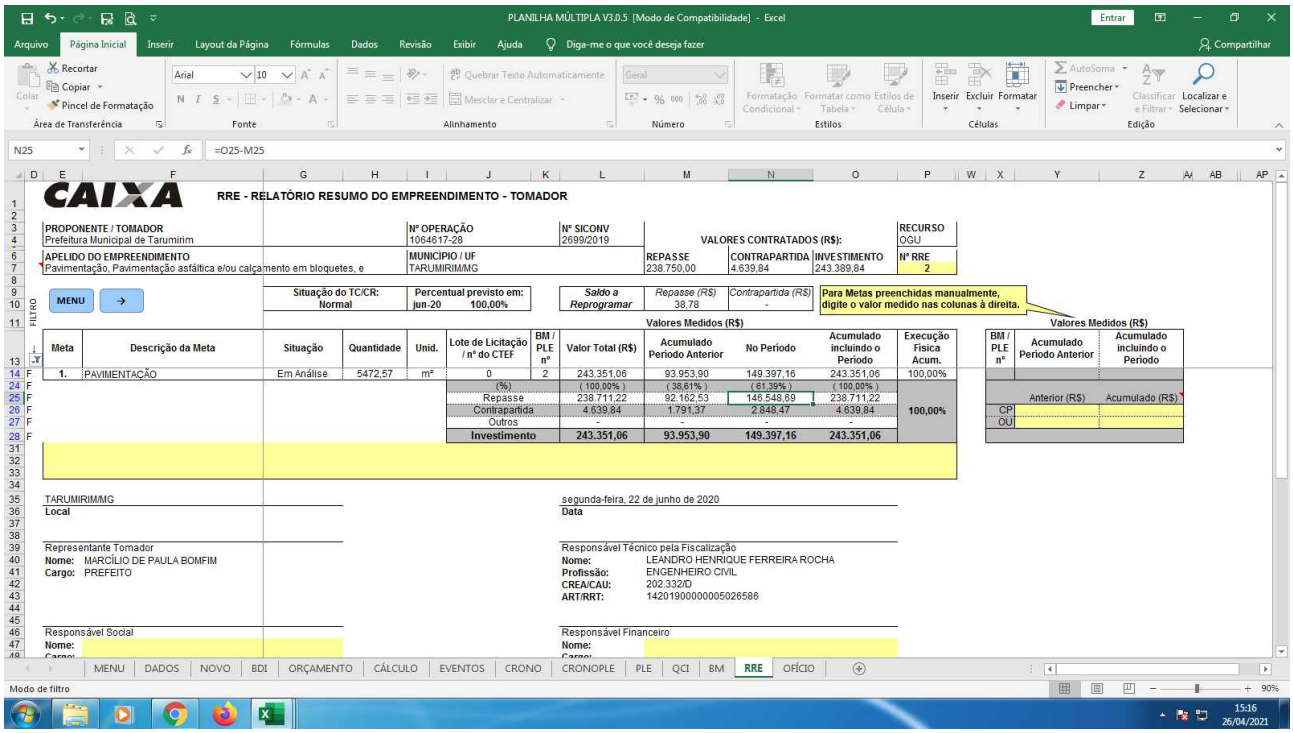
Por ser a expressão da verdade, firmo a presente.

Dada e passada nesta Cidade e Comarca de Governador Valadares/MG, aos 11 dias do mês de novembro de 2019.

JOÃO VICTOR [redacted]
CPF [redacted]

Fonte: Captura de tela obtido pela autora

Figura 12 – Captura de tela feito no computador Engenharia-PC após a invasão



Fonte: Captura de tela obtido pela autora

O próximo computador invadido foi o Patrimonio-PC. Nele havia nenhum arquivo ou informação sensível, mas durante o escaneamento do teclado, foi possível ver o e-mail e a senha da pessoa que utilizava o computador enquanto inseria em um site que exigia *login*, como mostra a Figura 13.

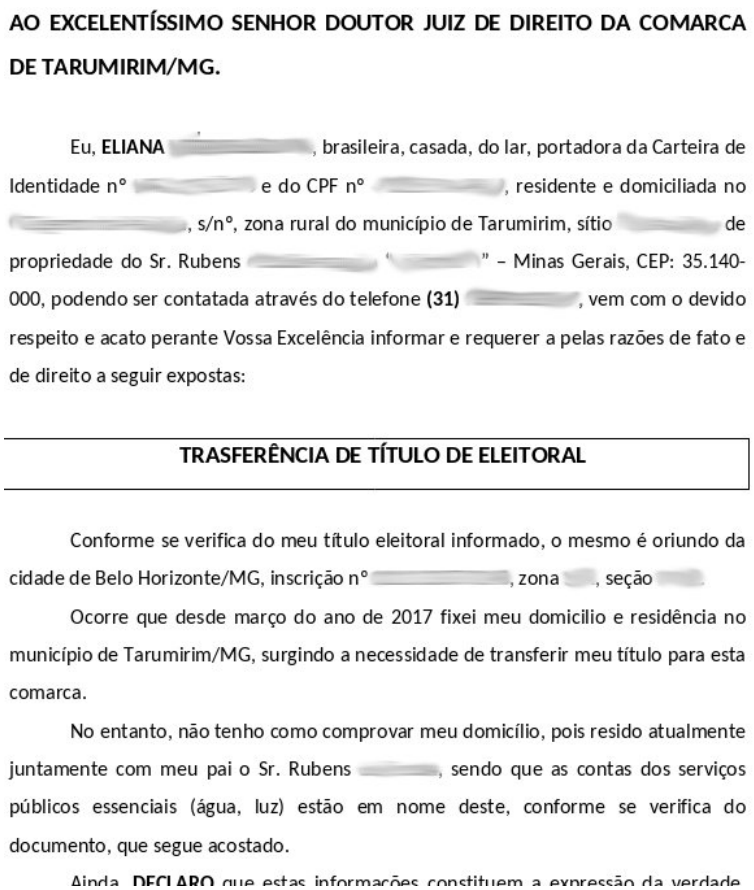
Figura 13 – *Keyscan* do computador Patrimonio-PC

Fonte: Captura de tela obtido pela autora

O e-mail do responsável pelo computador é pessoal, sendo ainda mais perigoso. Se a pessoa usar a mesma senha do e-mail para outros sites, o invasor tem "controle da vida" da vítima. Esse é um dos maiores perigos deste tipo de vulnerabilidade. É sempre preocupante e estressante desfazer qualquer incômodo que o invasor tenha causado a vítima, principalmente se o e-mail estiver vinculado a uma conta de banco.

Seguindo a lista, o próximo é o computador chamado Tel-PC. O computador continha vários documentos judiciais como transferências de títulos, recadastramento biométrico, processos ajuizados, procuração penal, autorizações de viagens, contrato de locação, termo de compromisso e até lista de dívida pessoal. Esses tipos de documentos continham nomes, estado social, RG, CPF, endereços, números de telefones e números dos títulos eleitorais (nos documentos de transferência e recadastramento biométrico) dos cidadãos. Um desses documentos é apresentado na Figura 14.

Figura 14 – Transferência de título de uma cidadã encontrado no computador Tel-PC



AO EXCELENTÍSSIMO SENHOR DOUTOR JUIZ DE DIREITO DA COMARCA DE TARUMIRIM/MG.

Eu, **ELIANA** [redacted], brasileira, casada, do lar, portadora da Carteira de Identidade nº [redacted] e do CPF nº [redacted], residente e domiciliada no [redacted], s/nº, zona rural do município de Tarumirim, sítio [redacted] de propriedade do Sr. Rubens [redacted] "[redacted]" – Minas Gerais, CEP: 35.140-000, podendo ser contatada através do telefone **(31)** [redacted], vem com o devido respeito e acato perante Vossa Excelência informar e requerer a pelas razões de fato e de direito a seguir expostas:

TRASFERÊNCIA DE TÍTULO DE ELEITORAL

Conforme se verifica do meu título eleitoral informado, o mesmo é oriundo da cidade de Belo Horizonte/MG, inscrição nº [redacted], zona [redacted], seção [redacted].

Ocorre que desde março do ano de 2017 fixei meu domicilio e residência no município de Tarumirim/MG, surgindo a necessidade de transferir meu título para esta comarca.

No entanto, não tenho como comprovar meu domicílio, pois resido atualmente juntamente com meu pai o Sr. Rubens [redacted], sendo que as contas dos serviços públicos essenciais (água, luz) estão em nome deste, conforme se verifica do documento, que segue acostado.

Ainda, **DECLARO** que estas informações constituem a expressão da verdade

Fonte: Captura de tela obtido pela autora

Este tipo de informação é um perigo nas mãos de golpistas que utilizam engenharia social para enganar suas vítimas, principalmente as mais humildes. O documento não só tem o nome, CPF e RG, como tem o endereço e até mesmo com quem a pessoa mora, sendo ainda mais fácil para o golpista enganar a vítima podendo se passar por um amigo ou parente que supostamente o conhece. A maioria estava armazenado há mais de 2 anos, mostrando o desleixo do profissional em quesito a armazenar essas informações mais antigas em locais como a nuvem, *pen drive*, armazenamento externo, ou até mesmo excluir caso não sejam mais necessários tais arquivos. Caso isso vazasse, a prefeitura teria sérios problemas com a LGPD.

O próximo é o computador com nome de PMT-PC. Após adquirir alguns arquivos e capturas de tela, foi possível perceber que o computador situava-se no setor de saúde. Foram encontrado vários documentos RG (frente e verso), comprovante de residência, título de eleitor, lista de pessoas que foram vacinadas contra o Covid-19 de acordo com a idade, lista de mamografia, boletos e recibos do responsável pelo computador, exames dos pacientes e agendas. A Figura 15 mostra um desses documentos.

Figura 15 – Foto encontrado armazenado no computador PMT-PC

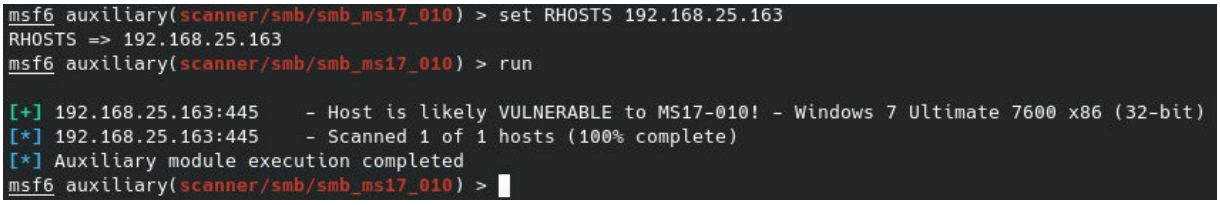
Fonte: Captura de tela obtido pela autora

Haviam vários documentos do tipo e boa parte deles estavam há mais de 1 ano armazenados no computador. Alguns arquivos como o da Figura 15 estavam armazenados na área de trabalho, demonstrando um desleixo pior do que do profissional anterior analisado. O essencial é excluir os arquivos sensíveis logo após o uso delas, mas caso houver a necessidade de usá-las futuramente, um armazenamento em nuvem ou externo seria mais seguro. Esse é mais um caso que a prefeitura teria problemas com a LGPD.

Não foram encontrados arquivos sensíveis nos outros 4 computadores listados pelo Nexpose, mas com paciência do invasor, seria possível adquirir e-mails e senhas utilizados pelos funcionários, informações pessoais ou até mesmo implementar um RAT (*Remote Access Tool*) e executá-lo sem a vítima perceber. Após o término das invasões, foi feito um escaneamento manual embutido no Metasploit de todos os computadores utilizando o sistema operacional Windows 7 para ter certeza se o Nexpose deu nenhum falso negativo.

Foram descobertos mais 2 computadores com o escaneamento manual, mas com uma diferença: eram de arquitetura 32 bits. Na Figura 16 pode-se ver o resultado desse escaneamento manual.

Figura 16 – Escaneamento manual embutido do Metasploit



Fonte: Captura de tela obtido pela autora

A invasão desses 2 computadores foram feitas com sucesso, mas por serem de arquitetura 32 bits, foi difícil manter a conexão por muito tempo, pois o mesmo não suporta muitas instruções, forçando o computador a reiniciar. Por conta disso, não foi possível continuar, pois quebraria o acordo feito com a prefeitura de não impedir e prejudicar o funcionário. Isto ainda conta como vulnerabilidade, pois o invasor pode ver a oportunidade de atrapalhar a vítima de seu trabalho no computador.

5 CONCLUSÃO

A Segurança da Informação se tornou vital para uma organização nesta época de pandemia, onde muita coisa foi sendo automatizada. A necessidade de se proteger de futuros ataques se deu por conta da conscientização ao longo dos anos e principalmente por conta da LGPD (Lei Geral de Proteção de Dados Pessoais).

O presente trabalho utilizou métodos onde o invasor tem nenhum conhecimento sobre a organização (*black box*), destacando as vulnerabilidades mais relevantes listadas pela ferramenta Nexpose e o que foi adquirido a partir delas. Foi utilizado o método de acesso FTP para adquirir algumas informações sem nenhum tipo de configuração ou *software*, onde foi possível conseguir alguns dados pessoais. Foi demonstrado também o ataque MITM (*man-in-the-middle*), sendo possível adquirir informações que são passadas na rede por todos os computadores. Por fim, foi utilizado a vulnerabilidade Eternalblue para acessar remotamente os computadores do ambiente testado, tendo total controle da máquina, sendo possível adquirir não só dados pessoais como e-mail e senha de uma das vítimas.

Entretanto, os métodos, as técnicas e os processos em geral apresentados neste trabalho não podem garantir que irá funcionar em todas as organizações. Apesar de não ter sido possível utilizar métodos de engenharia social, a prática do trabalho se mostrou eficaz e os resultados muito satisfatórios. Esse tipo de risco pode trazer prejuízos futuros a organização e demonstra a validez do problema apontado anteriormente. Muitas vezes,

as organizações não se tem conhecimento dos perigos que correm, e é importante que os profissionais na área demonstre os riscos que a mesma pode correr, para que haja a iniciativa de melhorar.

O ambiente analisado se mostrou bastante vulnerável de tais invasões com os métodos apresentados no trabalho. A falta de treinamento e disciplina dos funcionários em lidar com informações delicadas é bem presente, gerando um risco ainda maior para a organização e até mesmo para o próprio funcionário, onde um deles havia armazenado vários boletos e recibos bancários. Isso se dá pela falta de Política de Segurança da Informação na organização, que é essencial para manter os dados seguros.

6 REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2005.

FONTES, Eduardo. **Segurança da informação**: o usuário faz a diferença. 1 ed. São Paulo: Saraiva, 2006.

ANTUNES, André Alves; MOREIRA, Vitor Rebello. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO. **Governança em Sistemas de Informação**, Brasília, n. 1, p. 117-122, 2015.

ANDRADE, Nayara Santos. SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE O PROCESSO DE SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES FINANCEIRAS LOCALIZADAS NA REGIÃO CENTRO-OESTE DE MINAS GERAIS. **Revista Acadêmica Conecta FASF**, n. 1, 2017.

ASSUNÇÃO, Marcos Flávio Araújo. **Segredos do Hacker Ético**. 5 ed. Florianópolis: Visual Books, 2014.

MACHADO, F. N. R. **Segurança da informação: princípios e controle de ameaças**. 1 ed. São Paulo: Érica, 2014.

Eternalblue | The NSA-developed Exploit That Just Won't Die. **SentinelOne**, 27 de maio de 2019. Disponível em: https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die. Acesso em 4 de maio de 2021.

ROHR, Altieres. Megavazamentos de dados expõem informações de 223 milhões de números de CPF. **G1**, 25 de jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml. Acesso em: 20 de maio de 2021.

ARIMATHEA, B. et al. Brasil é terreno fértil para vazamentos de dados e ações de cibercriminosos. **Estadão**, 25 de abril. 2021. Disponível em: https://www.estadao.com.br/infograficos/link,brasil-e-terreno-fertil-para-vazamentos-de-dados-e-acoes-de-cibercriminosos,1162667. Acesso em: 20 de maio de 2021.

CRUZ, Bruna Sousa; BAPTISTA, Renata. "Este site está um lixo", diz hacker ao invadir rede do Ministério da Saúde. **UOL**, 4 de fev. 2021. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/02/04/este-site-esta-um-lixo-diz-hacker-ao-invadir-rede-do-ministerio-da-saude.htm. Acesso em: 20 de maio de 2021.

Prefeituras são os órgãos públicos mais suscetíveis a hackers. **Monitor Mercantil**, 18 de jun. 2021. Disponível em: https://monitormercantil.com.br/prefeituras-sao-os-orgaos-publicos-mais-suscetiveis-a-hackers/. Acesso em: 30 de agosto de 2021.

O que se sabe sobre ataque cibernético a JBS investigado pelo FBI. **BBC**, 2 de jun. 2021. Disponível em: https://www.bbc.com/portuguese/internacional-57327955. Acesso em: 31 de agosto de 2021.

JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. **G1**, 9 de jun. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 31 de agosto de 2021.

ANEXO A

Autorização

Eu, **SAMUEL DE PAULA LIMA**, portador do CPF nº 122.089.786-84, Chefe de Informática e Sistema responsável pelo setor de tecnologia da Prefeitura Municipal de Tarumirim, venho pro meio deste permitir a estudante **MARLENE TONEL LOPES JORDÃO**, portadora do CPF nº 106.024.866-29, utilizar dos sistemas de rede e *hardware* da informada prefeitura para realizar pesquisa local com fins acadêmicos como forma de conclusão de curso. A mesma se compromete a não utilizar os dados coletados para fins externos ao da pesquisa, garantindo que todos os dados serão anonimizados e qualquer informação que possa ser utilizada para identificar indivíduos será destruída após a conclusão da pesquisa.

A estudante poderá utilizar os sistemas da prefeitura da forma que achar necessário sem prejudicar o funcionamento e a segurança do sistema. Suas conclusões devem ser entregas para o responsável do setor de tecnologia a fim de analisar as vulnerabilidades encontradas e, se possível, aprimorar a segurança.

Marlene Tonel Lopes Jordão

Marlene Tonel Lopes Jordão
Estudante do curso Ciência da Computação

Samuel de Paula Lima

Samuel de Paula Lima
Chefe de Informática e Sistema

Prefeitura Municipal de Tarumirim
Tarumirim – MG
07/05/2021