OPEN SOURCE INTELLIGENCE (OSINT) PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

OPEN-SOURCE INTELLIGENCE (OSINT) FOR INFORMATION SECURITY MANAGEMENT IN COMPANIES

Raiza Queiroz e Silva[1] (queiroz.raiza@aluno.ifsp.edu.br)
Prof. Me. Ubiratan Zakaib do Nascimento[1] (birazn@ifsp.edu.br)
[1]Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Votuporanga

RESUMO

Com o uso acelerado de meios digitais, também houve um crescente volume de ameaças e riscos de ataques cibernéticos por grupos criminosos. Organizações e empresas estão em constante estado de alerta diante de um cenário hostil em ambientes eletrônicos. Entretanto, muitas organizações não se atentam para os índices de ameaças propagados na rede mundial de computadores. Logo, detectar falhas ou vulnerabilidades em aplicações web e quaisquer outras superfícies de ataque é crucial para proteger ativos, dados e a reputação das organizações, garantindo assim uma eficaz gestão de segurança da informação. Nesse contexto, a Inteligência de Fontes Abertas (OSINT – *Open-Source Intelligence*) expressa-se como uma prática poderosa para identificar riscos antes que sejam explorados por agentes mal-intencionados, contribuindo para a análise de vulnerabilidade e reduzindo as chances de vazamento de dados. Este trabalho aborda o uso estratégico do OSINT para a detecção prévia de vulnerabilidades e outras áreas suscetíveis a ataques cibernéticos com a finalidade de expandir o conhecimento sobre o tema e elevar os níveis de segurança da informação adotados pelas corporações.

PALAVRAS-CHAVE: OSINT, Gestão de Segurança da Informação, Análise de Vulnerabilidade, Vazamento de Dados.

ABSTRACT

With the accelerated use of digital means, there has also been a growing volume of threats and risks of cyberattacks by criminal groups. Organizations and companies are constantly on alert in the face of a hostile scenario in electronic environments. However, many organizations do not pay attention to the levels of threats propagated on the worldwide network of computers. Therefore, detecting flaws or vulnerabilities in web applications and any other attack surfaces is crucial to protect assets, data, and the reputation of organizations, ensuring effective Information Security Management. In this context, Open-Source Intelligence (OSINT) emerges as a powerful practice to identify risks before they are exploited by malicious actors, contributing to vulnerability analysis and reducing the chances of data leakage. This work addresses the strategic use of OSINT for the early detection of vulnerabilities and other areas susceptible to cyberattacks with the purpose of expanding knowledge on the subject and raising the levels of information security adopted by corporations.

KEY WORDS: OSINT, Information Security Management, Vulnerability Analysis, Data Leakage.

INTRODUÇÃO

O contexto de evolução humana está historicamente relacionado ao uso de ciência e tecnologia como ferramentas aliadas para o estado que nos encontramos atualmente. Dentre a vasta gama de ferramentas que o homem desenvolveu e aperfeiçoa ao longo do tempo, estão os meios de comunicação. Das pinturas rupestres aos meios digitais, cultiva-se o hábito de registrar, e não menos importante, utilizar dos registros como base de conhecimento.

A digitalização de informações e ascensão tecnológica na forma de armazenarmos conteúdos cresce anualmente. Relações que, antes eram presenciais físicas, estão facilmente disponíveis online. A pesquisa anual divulgada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – CETIC.br (2023, p. 25), com dados do ano anterior expõe que, brasileiros de 10 anos ou mais somam parcela de 81% dos usuários de Internet. Dado aproximado de 140 milhões de indivíduos.

Comprar online, realizar transações bancárias, enviar mensagens instantâneas e buscar informações são operações que geram alto volume de dados trafegando diariamente na rede. Além de informações cadastrais em portais digitais, trafegam as demais atividades – dados – que é realizado.
"[...] Cerca de sete a cada dez usuários compartilham algum conteúdo na Internet, como texto, imagem ou vídeo [...]. Já a postagem de textos, imagens ou vídeos de autoria própria (43%) aumentou 12 pontos percentuais em relação a 2021 (31%).". (CETIC.br, 2023, p. 26-28).

O cenário que expõe oferta e demanda por compartilhamento de conteúdo está em comum ascensão entre usuários que, para a grande maioria das pessoas, representa apenas a facilidade de utilizar o digital. Do conforto de uma tela, é praticamente imperceptível o poder dos dados que estão sendo trocados, os usuários, assim, passam por desconsiderar parte dos riscos envolvidos no uso dos ambientes eletrônicos e suas ameaças. Uma pesquisa feita pela Cybersecurity Ventures (2022), estima que até 2025 o cibercrime atinja a marca de $ 10,5 bilhões em dólares em danos globais.

> Os custos do cibercrime incluem danos e destruição de dados, dinheiro roubado, produtividade perdida, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, desvio de fundos, fraude, interrupção pós-ataque do curso normal dos negócios, investigação forense, restauração e exclusão de dados e sistemas hackeados, e danos à reputação. (Cybersecurity Ventures, 2022, tradução própria)

A divulgação em mídias sobre vazamento de dados de diversas organizações que sofrem ataques de *ransomware* (software mal-intencionado que utiliza criptografia para impedir acesso a dados presentes em servidores), está em ascensão. Segundo Chaves (2022), no mesmo ano houve divulgação de ataque *ransomware* à emissora de televisão, TV Record. A emissora foi alvo de grupo de cibercriminosos que conseguiram encontrar e explorar vulnerabilidades em servidores internos da empresa. Houve a encriptação de dados e negociação para devolução de conteúdo descriptografado em montante acima de R$ 26 milhões, a forma de pagamento definida entre criptomoedas, pelo advento do protocolo de funcionamento das moedas preservarem a identidade dos criminosos.

Os criminosos não precisam invadir sistemas para organizar roubos, ataques ou golpes. Utilizam-se a princípio da OSINT (*Open Source Intelligence*), tradução direta "Inteligência de Fontes Abertas", para coletar informações públicas sobre falhas de vulnerabilidade de seus alvos, com metas de idealizar tomadas de decisões baseando-se nas informações verificadas.

Para Lande e Shnurko-Tabakova (2019), OSINT trata-se do resumo da coleta, processamento e análise das informações que estejam disponíveis publicamente em mídias de revistas, jornais, rádios, motores de busca digitais (Google) na *surface*, *deep* e *dark web*. Observa-se que a comunidade internacional tem expressiva adesão ao formato de obtenção de informações por meio de OSINT, com interesse de tomadas de decisões assertivas a fim de resolver vasta gama de problemas.

A motivação deste trabalho refere-se em formas de gerenciamento que organizações, sejam elas: de iniciativa pública, privada, social ou de quaisquer segmentos, possam compreender mais sobre vulnerabilidade que criminosos utilizam para prejudicar inteira ou parcialmente suas operações, adotando medidas preventivas de segurança da informação em suas infraestruturas físicas e lógicas.

OBJETIVOS

Realizar busca ativa sobre dados e informações publicamente disponíveis a consultas *online* como procedimento recorrente para encontrar possíveis exposições inadequadas que possam comprometer a saúde das organizações, antes que criminosos as encontrem; em seguida, classificar as exposições e sugerir soluções para reduzir o alcance público a dados e informações impróprias.

REVISÃO DE LITERATURA

Divulga-se uma quantidade significativa de revisões literárias com menções a OSINT e/ou atividades de Inteligência sob Fontes Abertas. As atualizações adotadas no estado da arte deste trabalho contêm foco em técnicas, práticas e métodos, sem intenção de estreitar os estudos para uso de ferramentas específicas para tais fins.

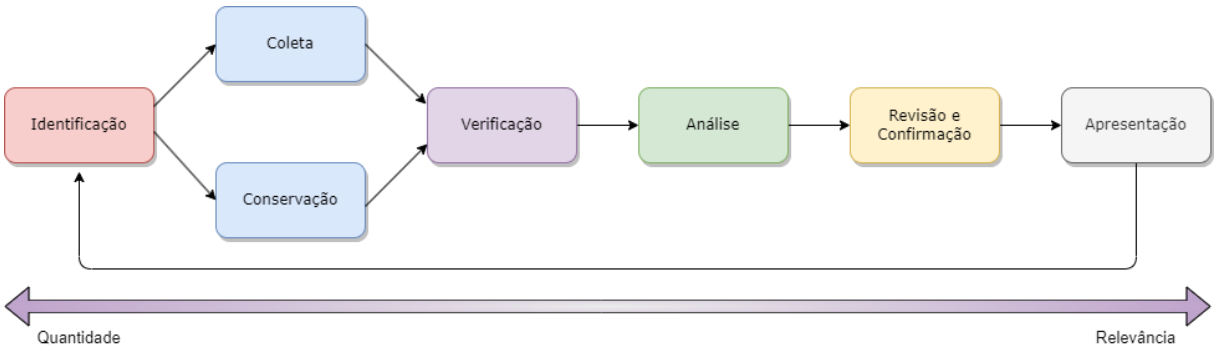
As referências abordadas nas obras citadas possibilitou obtenção de conhecimentos aprofundados sobre diversas vertentes que a OSINT tem sido utilizada para fins diversos, desde guerrilhas a buscas pessoais em redes sociais.

Para Leal (2019), na comunidade internacional de Inteligência, a OSINT é reconhecida como uma fonte valiosa de dados, embora seja consenso que ela sozinha não compõe a Inteligência completa. Para obter um panorama completo, é fundamental combinar a coleta de dados em fontes abertas com informações provenientes de outras disciplinas, incluindo dados protegidos.

Por meio da literatura explorada, fundamentam-se as fases de coleta, processamento e análise como as principais para melhor condução de ações decisórias. A adaptação de Tanabe (2022) *apud* Pastor-Galindo *et al.* (2020), evidencia-se a primeira etapa listada como imprescindível dentre as demais, pois, contendo dados precisos, há maior expectativa de avanços satisfatórios nas etapas seguintes; o resultado para obtenção de cada dado gera uma saída que pode ser empregada como entrada em novo processo de consulta, tornando-o cíclico.

A Figura 1, adaptada do portal *online* Bellingcat (2018), que divulgou o fluxo de trabalho para investigações jornalísticas do Projeto ‘Arim no Iémen, sudoeste da Península da Arábia. Os profissionais envolvidos ao portal, utilizam-se de OSINT para compreender situações diversas em ambientes extremos de guerra.

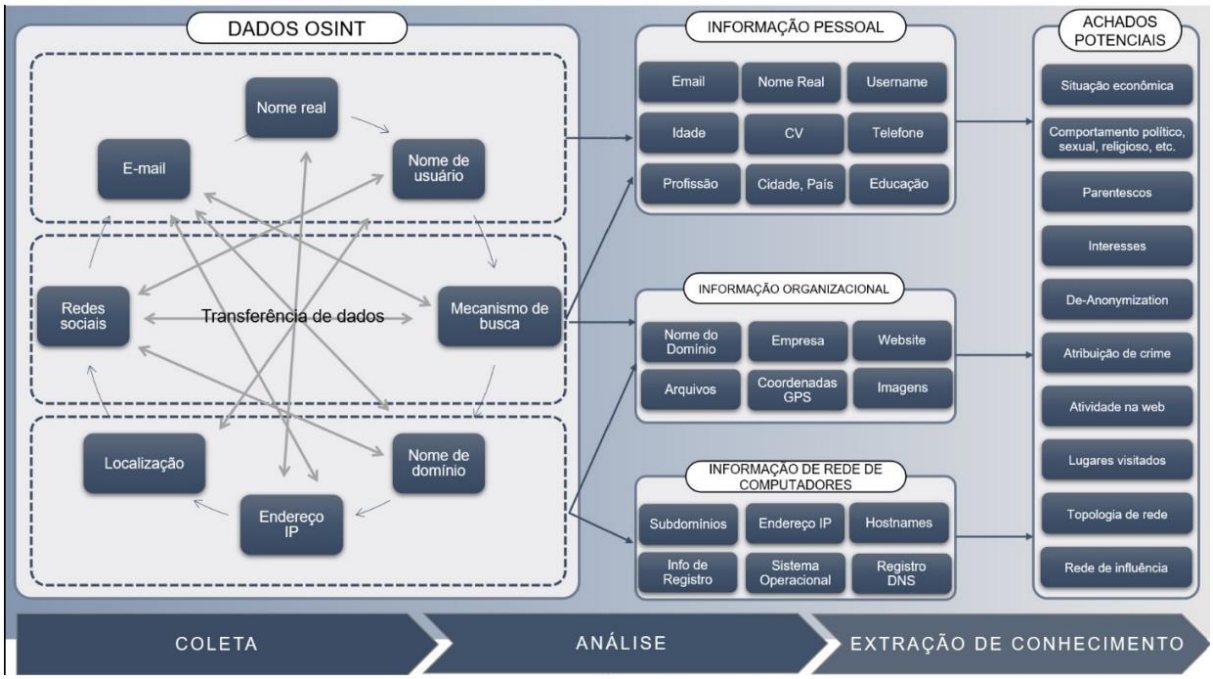
Figura 1: Fluxo de trabalho com OSINT - Projeto 'Arim no Iémen



Fonte: Bellingcat (2018) – Adaptação própria.

Para Tanabe (2022) *apud* Pastor-Galindo *et al.* (2020), expande conhecimentos sobre ciclo de trabalho abordado pelos pesquisadores espanhóis acerca da ampla coleta de dados, as possibilidades que são obtidas como respostas para etapa de análise e finaliza com as informações para uso, ou seja, conhecimento completo com o método OSINT, disponibilizado na Figura 2.

Figura 2: Método para OSINT



Fonte: Adaptação Tanabe (2022) *apud* Pastor-Galindo *et al.* (2020).

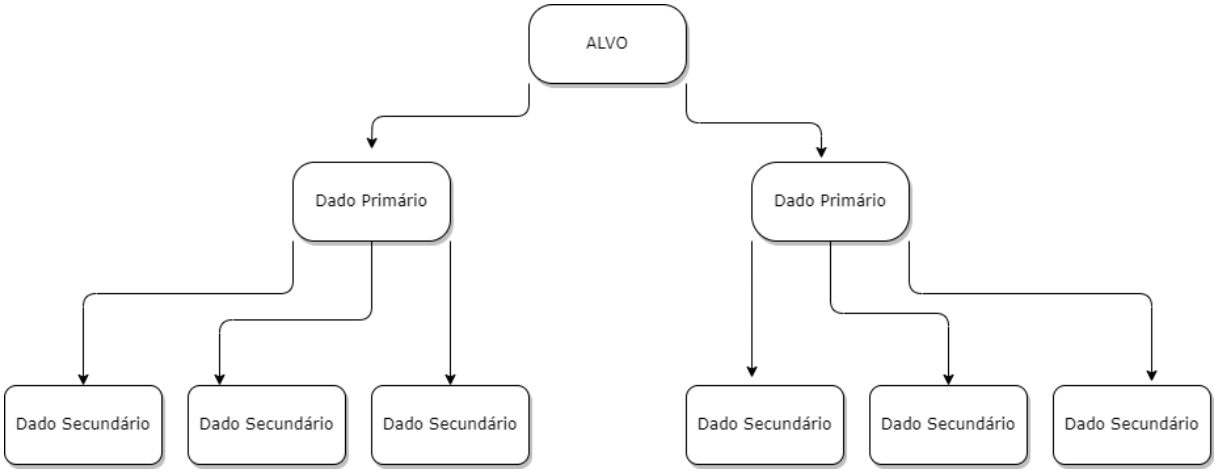
Segundo Tanabe (2022), se faz interessante a obtenção de dados e informações por diversas fontes abertas, utilizando-se de diferentes métodos, ferramentas, técnicas para fins de coleta, seguido das etapas de processamento e análise. O autor nomeia o método proposto como Multi-INT, que conecta além de OSINT, HUMINT, e demais metodologias de inteligência.

MATERIAL E MÉTODOS

Visando experiência com maiores indicadores de satisfação, compreende-se que o alvo de busca inicial de quaisquer coletas de dados seja definido de forma clara. A finalidade deste formato de busca, compete ao volume de informações e dados primários, secundários e posteriores que serão resultados a partir de delimitação na entrada.

Fluxos de trabalho e pesquisas verificados na revisão de literatura enriqueceram a base de conhecimento para elaboração de esboço genérico do fluxograma vide Figura 3, de consulta OSINT que, pode ser alcançada por meio de quaisquer técnicas, métodos e/ou ferramentas que atuem no segmento de coleta de informações.

Figura 3: Fluxo genérico de busca inicial sobre dados de um Alvo



Fonte: Elaboração própria.

A virtualização da distribuição Kali do Linux será utilizada como plataforma principal para realizar análises de segurança e inteligência cibernética, bem como ferramentas de código aberto disponíveis também para outros sistemas operacionais. A flexibilidade dessa abordagem permite que os envolvidos com as verificações escolham as ferramentas mais adequadas às suas necessidades, independentemente do sistema operacional utilizado.

O ciclo de análise trata-se a princípio da coleta de informações e reconhecimento, que desempenha papel fundamental na avaliação de segurança de quaisquer organizações, logo, a varredura de rede de um alvo consiste em identificar sistemas, domínios ou redes. Considera-se o comando Ping para identificação de resposta de domínios, IP e TTL (*time-to-live*), recurso fundamental e presente em quaisquer sistemas operacionais. Para consultas de dispositivos conectados à Internet, o Shodan foi selecionado. Explorações e mapeamento de topologias de rede, identificação de uso de portas de serviço. Respostas que são também são possibilitadas com a ferramenta Nmap (*script*) muito utilizada nesta abordagem e disponível nativamente na maioria das distribuições do Linux.

Aliado a ferramenta de verificação de portas de serviços, que exibem a exposição de serviços ativos de qualquer organização no meio digital, é possível utilizarmos de uma diversidade de outras ferramentas e recursos para várias finalidades por meio da OSINT Framework (Nordine, 2019). Ferramentas que consultam desde nome de usuário, metadados, geolocalização a até mesmo, criptomoedas. No contexto brasileiro, um repositório com listas de ferramentas e recursos é mantido e atualizado por profissionais e entusiastas de Segurança da Informação. O OSINT Brazuca na comunidade GitHub tem crescente volume de seguidores (Pinheiro, 2022).

A poderosa ferramenta Maltego, nas palavras de Govardhan *et. al* (2023), com adaptação própria, está relacionada a mineração de dados e apoia usuários a coletar e visualizar informações de diferentes fontes, inclusos mídias sociais, sites e bancos de dados.

Para estudos analíticos quanto ao volume de respostas obtidas nas coletas, se faz interessante que sejam conservadas as evidências de acordo com a preferência do gestor, pesquisador e/ou profissional de segurança que

está realizando os processos de consulta sob OSINT de organizações. Desde anotações em texto simples a alguma forma de elaboração de relatório profissional para *feedback* corporativo.

Recomenda-se avaliar as respostas obtidas e filtrar se as exposições podem ser, de alguma forma, limitadas a público através de pesquisas adicionais, implementação de funções extras em sistemas, redes e domínios ou até mesmo interromper o compartilhamento público de alguma informação indesejada por parte das entidades. Medidas que podem ser tomadas com base em vulnerabilidades registradas no CVE Mitre, que tem por missão identificar, definir e catalogar vulnerabilidades de segurança cibernéticas abertas ao público (Mitre CVE, 1999). Será detalhado com mais profundidade a visualização de CVEs catalogadas pelo Mitre durante reconhecimento de vulnerabilidades no próximo capítulo deste estudo.

Boas práticas de desenvolvimento seguro para sistemas web estão à disposição na Internet por meio do projeto OWASP Top 10, que apresenta uma cartilha de conscientização padrão com amplo consenso sobre riscos de segurança mais críticos para aplicações web (Owasp, 2001). Ao acessar o portal é possível conferir a linha do tempo das ameaças de anos anteriores até as dez catalogações mais nocivas da atualidade.

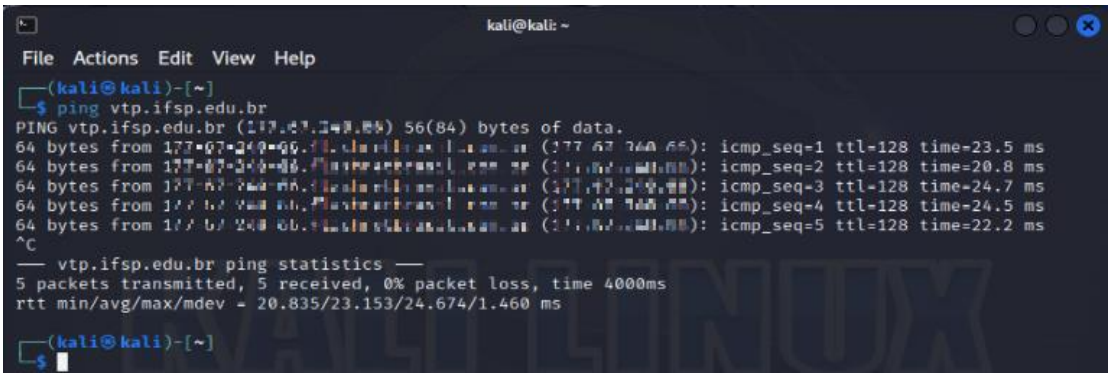
RESULTADOS E DISCUSSÃO

Uma vez selecionado o alvo para iniciar os processos de busca OSINT, recomendam Rajamäki, Lahti e Parviainen (2022), ser pertinente iniciar o trabalho de reconhecimento com um equipamento limpo, em especial para reconhecimentos realizados no Tor ou semelhante, para preservar os dados dos pesquisadores.

Utilizar de várias ferramentas que operam grande volume de dados como resultados pode ser relevante para fase inicial de coleta. Caso o alvo seja um domínio *online*, ferramentas para mapeamento tais como, Shodan, Nmap e Maltego auxiliam na coleta de dados para armazenamento e posterior refinamento dos resultados obtidos.

a) Ping
Possibilita os testes de conectividade de redes, problemas de resolução de nomes DNS e informa o TTL. Segundo Ignácio (2010), para o portal Viva o Linux, o TTL indica o sistema operacional destino do teste. Valores referência de Windows TTL = 128, Linux TTL = 64 e 255 para UNIX.
Na Figura 4, é um exemplo de comando ping para resolução de domínio DNS.

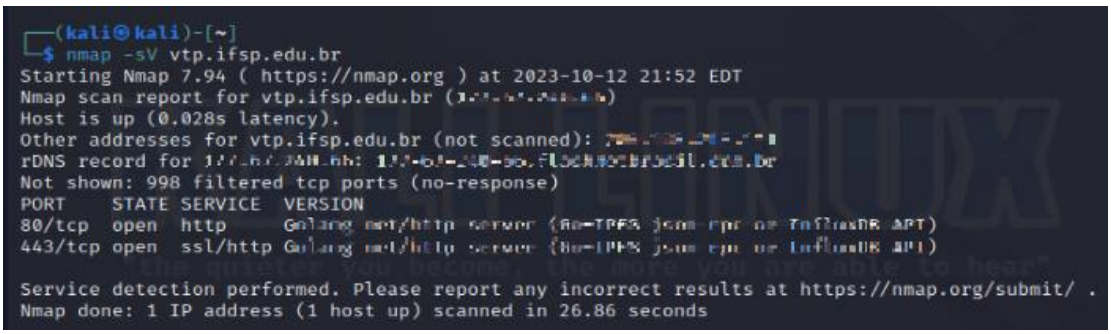
Figura 4: Comando `ping` para obtenção de resposta sob Domínio/IP



Fonte: Resultado obtido em 10/out. 2023.

b) Nmap
Conferir portas de serviço disponibilizadas na Internet; ferramenta conta com verificações adicionais que podem ser consultadas em seu manual via terminal, na Figura 5 a consulta efetuada para buscar a versão de serviço relacionada às portas abertas buscadas.

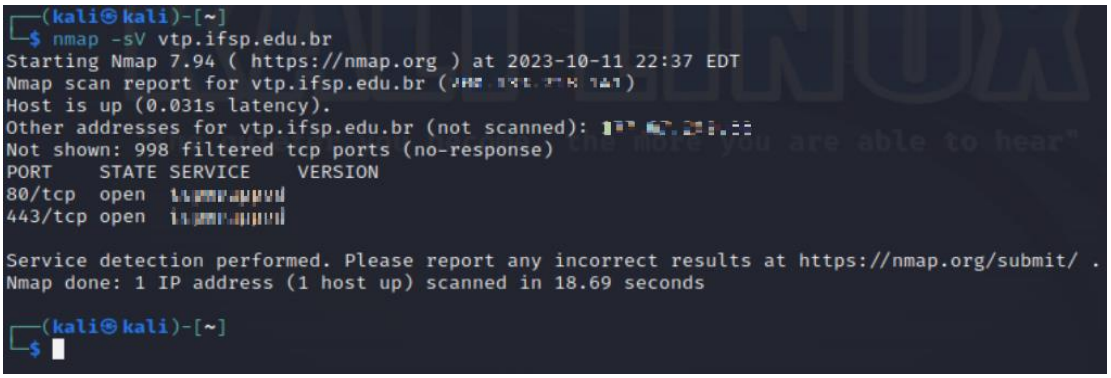
Figura 5: Comando "`nmap -sV example.com`"



Fonte: Resultado obtido em 10/out. 2023.

Note que a resposta do Nmap encontrou existência de outro endereço IP para a mesma URL que não foi avaliado pela ferramenta. Realizado Nmap somente para o IP relatado na resposta anterior.
O novo resultado está na Figura 6:

Figura 6: Comando Nmap para outro destino IP que responde no mesmo domínio



Fonte: Resultado obtido em 10/out. 2023.

c) Shodan

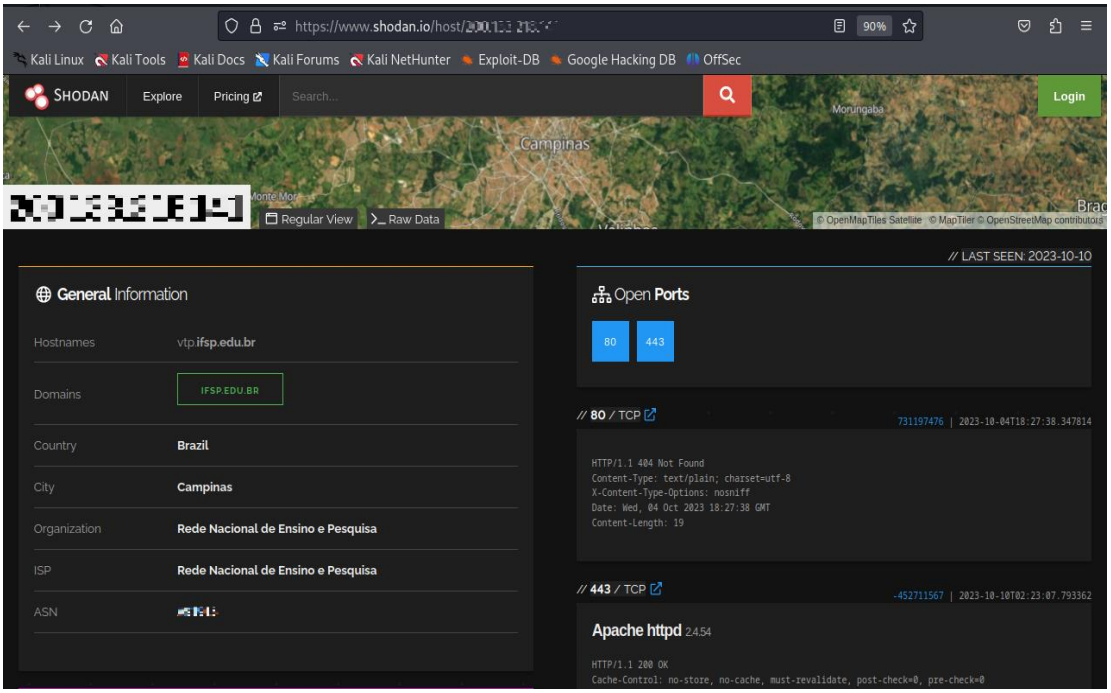
Informações obtidas no Shodan ao buscar por IP, apontou resumo que foi recebido das portas de serviço abertas em uso pelo Nmap; Portas de protocolos Web HTTP e HTTPS (80 e 443).
O registro do IP pertencente ao ASN – Número de Sistema Autônomo, pois identifica conjunto de IPs registrados por organizações, seguidamente de sua geolocalização na região de Campinas, São Paulo.

Observa-se que, as portas abertas passam por uma varredura. No protocolo web HTTP/80 o retorno é erro de não página não encontrada (erro 404), entretanto há grande possibilidade que haja encaminhamento de serviço se houver requisições de acesso no domínio pelo protocolo, onde a requisição seja direcionada para acesso a página disponível no protocolo seguro da web HTTPS/443, disponibilizado pelo Apache na versão 2.4.54.

As tecnologias de construção web do alvo de investigação são expostas com maiores detalhes no Shodan, na sessão de *Web Technologies*, presente na Figura 8, comparado ao que visto no Nmap. Informação que pode ser adicional e confirmativa para os métodos de OSINT, visto que é possível coletar informações ruidosas sobre um alvo. Logo, trata-se de uma segunda confirmação obter dados de forma repetitiva, bem como notar que na sessão "*Open Ports*", lado superior direito, presente na **Erro! Fonte de referência não encontrada.**.

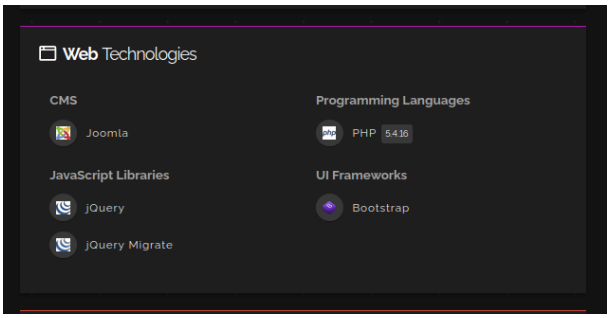
O portal expõe as vulnerabilidades que foram catalogadas em Mitre (CVE) ao relacionar tecnologias que estão em uso no alvo de investigação, disponível na Figura 9. Advertindo e classificando em níveis de risco uma prévia de cada vulnerabilidade.

Figura 7: Resultado de consulta IP no Shodan



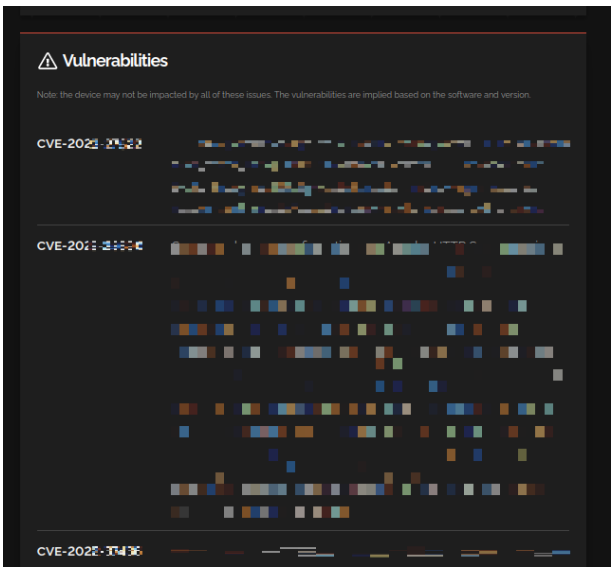
Fonte: Resultado obtido no Shodan em 10/out. 2023.

Figura 8: Sessão *Web Technologies* no Shodan



Fonte: Resultado obtido no Shodan em 10/out. 2023.

Figura 9: Sessão Vulnerabilidades no Shodan

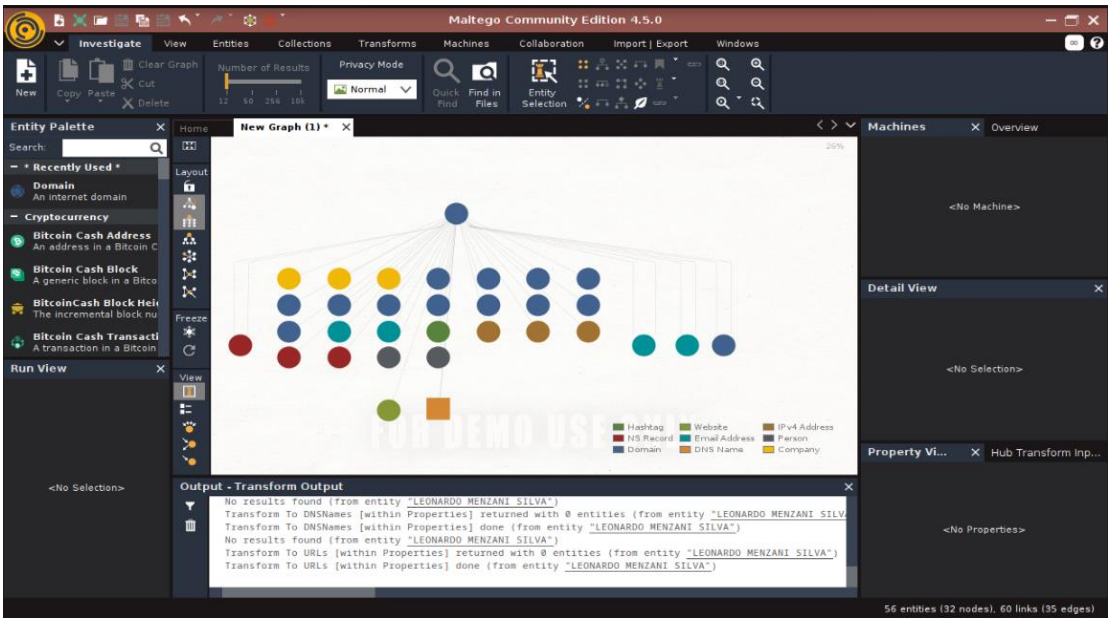


Fonte: Resultado obtido no Shodan em 10/out. 2023.

d) Maltego

A Figura 10 contém o *layout* estrutural de relacionamento dos dados recebidos após busca, que assemelha-se com a Figura 3. A ferramenta utiliza o alvo inicial como ponto de partida para expandir informações gerais, e cada item mapeado pode ser entrada de nova consulta.

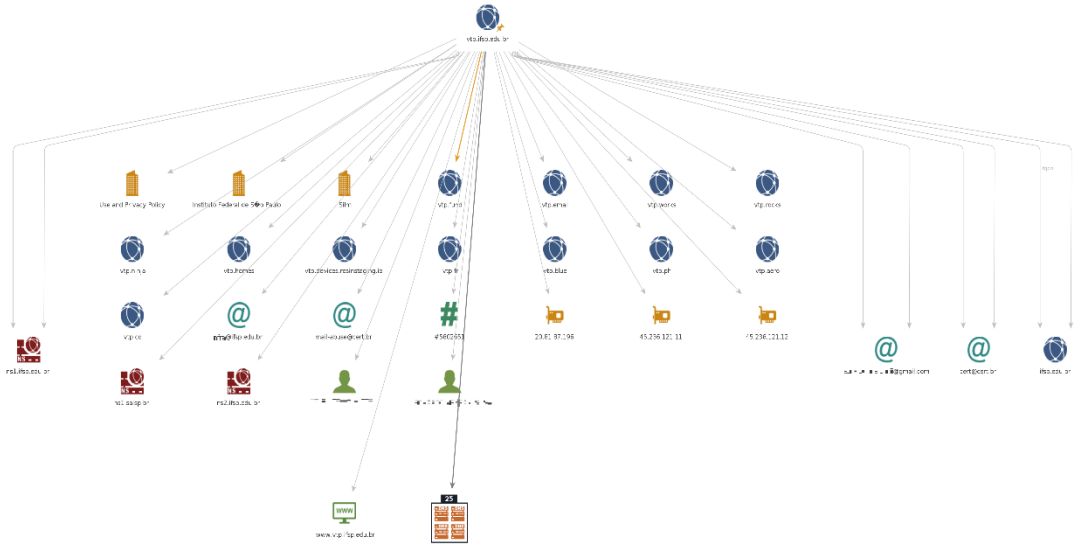
Figura 10: Exibição de informações relacionadas a um Alvo no Maltego



Fonte: Resultado obtido no Maltego em 10/out. 2023.

A Figura 11 contém o Gráfico de relação entre dados obtidos a partir do dado alvo **vtp.ifsp.edu.br**.

Figura 11: Gráfico exportado do Maltego sob Domínio



Fonte: Resultado obtido no Maltego em 10/out. 2023.

A ferramenta permite exportar relatórios em formatos gerenciáveis de planilhas em extensão .csv, .xml formato web, dentre outras funcionalidades que favorecem ricos relatórios de estudos para as entidades avançarem nos passos seguintes de processamento, análise e tomada de decisões.

Classificação de Coleta, Processamento e Relatório

Os dados obtidos podem ser armazenados seguindo critério definidos pelo gestor, profissional de segurança e demais interessados que estejam realizando os procedimentos de OSINT. Durante o processo de coleta são grandes as chances de obter dados com ruído, ou seja, com pouca afinidade ou vínculo com o dado alvo inicial. Logo, a etapa de processamento é essencial para realizar o refinamento e validação dos dados obtidos para que seja obtidas informações consistentes sobre o alvo.

Com amparo ético e legal, acesso a fontes privadas de dados para validar uma informação publicamente exposta como verdadeira, pode fortalecer e complementar o direcionamento do procedimento OSINT estar apropriado.
Entretanto, a indicação de veracidade de dados obtidos de forma exclusivamente pública, estejam os dados disponível em diversas fontes abertas, não deve ser desconsiderada como correta. Indica-se sempre avaliar mais de uma fonte para obtenção de dado ou informações semelhantes para considerar ou não relevante sobre um alvo.

Adotando este modelo de processamento, dados e informações com algum indício de ruído ou não associação direta ao alvo, pode ser desconsiderado para o todo de análise – passo seguinte a ser realizado em conjunto a sugestão de tomada de ações.

Análise e Sugestões para Tomadas de Decisões

Para os gestores de organizações, receber informações analíticas com níveis de risco e estimativas de potenciais impactos da inatividade total ou parcial de quaisquer serviços, em razão de exposições inadequadas de dados, conteúdos ou informações, pode causar espanto, entretanto, válido ressaltar a importância em tomar nota sobre operações de trabalho para reduzir superfícies contra ataques de criminosos para evitar prejuízos futuros.

Portais de consulta tais como Shodan, exibem as vulnerabilidades encontradas baseando-se nas tecnologias usadas pelos alvos buscados e suas versões de uso em conjunto com falhas catalogadas pelo Mitre (CVEs). Muitas delas sem classificação direta no portal, entretanto, outras indicando níveis de riscos que intercalam em escala de 0 a 10.

Se faz importante, assim que identificadas as brechas sistêmicas, estejam acompanhadas as recomendações com melhores opções a fim de sanar total ou limitar parcial as superfícies contra ataques cibernéticos.
Cenários de *e-commerce*, comprovar a possibilidade de ataques SQL – linguagem de consulta estruturada de bancos de dados – implementar políticas de acesso apenas com usuário e senha para quaisquer acessos aos dados em modo gerencia e demais implementações que apoiem as medidas de boas práticas de segurança.

CONCLUSÕES

Tomando por base o referencial teórico com fins de disseminar conhecimento sobre OSINT e sua abundância de usos, é plausível afirmar benefícios em obtenção de resultados assertivos quanto ao método de inteligência.
Ao decorrer deste estudo, são notórias as informações coletadas, independente do uso de ferramentas, mas aliado a elas, possibilitado a otimização no consumo de tempo e volume de dados resultante se demonstra expressivo.

Organizações de iniciativa pública, privada e/ou quaisquer segmentos divergentes, tendem a proteger suas informações e difundir conhecimento sobre segurança da informação com seus colaboradores e comunidade adotando de pequenas ações diárias em suas políticas de utilização digitais.

Oportuno destacar que OSINT está muito além do digital, entretanto, a simplicidade do uso de ambiente eletrônico em crescente aumento impõe responsabilidades neste meio de comunicação, onde os riscos não são apenas regionais, mas sim, globais.

Evidencia-se que OSINT representa uma etapa usada para reconhecimento de alvos com expressivo uso por parte de grupos criminosos, com objetivo de causar prejuízos as organizações. Reforçar a segurança corporativa deve ser prioridade. Trabalhos futuros podem acompanhar estudos mais densos sobre testes de intrusões, ou "*pentest*", que tem potencial para compreender melhor as metodologias e raciocínio lógico adotados por atacantes. Desta forma, pode-se estruturar defesas mais robustas aos negócios baseando-se nas abordagens que são adotadas para atacar ambientes.

REFERÊNCIAS BIBLIOGRÁFICAS

BELLINGCAT. *Workflow - Project Yemen*. Bellingcat [Online], 2018. Disponível em: <https://yemen.bellingcat.com/methodology/workflow>.

CETIC.BR. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC domicílios 2022. Comitê Gestor da Internet no Brasil (CGI.br), Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, v. 1, p. 272, 2023.

CHAVES, M. E. d. A. O vazamento de dados sob a perspectiva da LGPD e sua correlação com os crimes cibernéticos. 2022.

CYBERSECURITY VENTURES. *Cybercrime To Cost The World 8 Trillion Annually In 2023*. [S.l.], 2022.

GOVARDHAN, D. et al. *Key challenges and limitations of the osint framework in the context of cybersecurity*. In: IEEE. 2023 *2nd International Conference on Edge Computing and Applications (ICECAA)*. [S.l.], 2023. p. 236–243.

IGNÁCIO, D. G. Identificar o sistema operacional usando ping. URL: https://www.vivaolinux.com.br/dica/Identificar-o-sistema-operacional-usando-ping, 2010.

LANDE, D. V.; SHNURKO-TABAKOVA, E. V. *OSINT as a part of cyber defense system*. Igor Sikorsky Kyiv Polytechnic Institute, 2019.

LEAL, L. H. Cybint x Osint. A Lucerna, n. IX, p. 37–41, 2019.

MITRE (CVE). *Cve – cve*. URL: https://cve.mitre.org, 1999.

NORDINE, J. *Osint framework*. URL: https://osintframework. com, 2019.

OWASP. *Owasp top ten*. URL: https://owasp.org/www-project-top-ten/, 2017.

PINHEIRO, Cleiton. Osint Brazuca. URL: https://github.com/osintbrazuca, 2022.

PASTOR-GALINDO, J. et al. *The not yet exploited goldmine of osint: Opportunities, open challenges and future trends*. IEEE Access, v. 8, p. 10282–10304, 2020.

RAJAMÄKI, J.; LAHTI, I.; PARVIAINEN, J. *Osint on the dark web: Child abuse material investigations*. Procon Ltd, 2022.

TANABE, R. Proposta de um método para inteligência de fontes abertas: valores e princípios para uma atividade ética e profissional. 2023

Cópia de documento digital impresso por Vania Coelho (1091455) em 22/03/2024 16:50.

Documento Digitalizado Restrito

TCC - Pós-graduação em Gestão da Tecnologia da Informação e Comunicação - Raiza Silva

Assunto: TCC - Pós-graduação em Gestão da Tecnologia da Informação e Comunicação - Raiza Silva
Assinado por: Marcelo Murari
Tipo do Documento: Anexo
Situação: Finalizado
Nível de Acesso: Restrito
Hipótese Legal: Direito Autoral - conservar a obra inédita (Art. 24, III, da Lei nº 9.610/1998)
Tipo do Conferência: Documento Digital

Documento assinado eletronicamente por:

- **Marcelo Luis Murari**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 20/12/2023 20:03:25.

Este documento foi armazenado no SUAP em 20/12/2023. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsp.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1532057
Código de Autenticação: b1339af968