Trabalho Individual

Fundamentos de Cibersegurança

Gonçalo Amaro – 17440

Escola Superior de Tecnologia e Gestão
Instituto Politécnico de Beja

15 de Dezembro, 2022

A estrutura desta apresentação está organizada da seguinte forma:

- Este trabalho tem como objetivo a pesquisa e sintetização do tópico de ”Fundamentos de Cibersegurança”
- Este tópico está inserido no módulo de ”Fundamentos de Cibersegurança”do curso de ”Engenharia de Segurança Informática”do Instituto Politécnico de Beja
- O trabalho consiste na resolução de um conjunto de exercícios de pesquisa e sintetização de conteúdos enquadrados nas perguntas inseridas no documento de enunciado

- Os vetores de ataque são um conceito crítico na segurança cibernética porque fornecem uma maneira de os invasores obterem acesso a um sistema de computador ou rede
- Existem muitos tipos diferentes de vetores de ataque, incluindo ataques de phishing, malware, engenharia social, exploits, acesso físico, etc... Dependendo da granularidade da conversa, pode ser enumerado mais ou menos tipos de vetores de ataque.
- Entender essas ameaças é essencial para que as organizações se protejam contra elas

- Phishing (Engenharia Social via E-mail)
- Malware
- Engenharia Social (Pessoas)
- Exploração de Vulnerabilidades
- Acesso Físico

- Vulnerabilidade de Software
- Vulnerabilidade de Hardware
- Vulnerabilidade de Rede
- Vulnerabilidade de comportamento humano

- O projeto ATT&CK é uma base de conhecimento pública desenvolvida pela MITRE Corporation
- Fornece informações detalhadas sobre as táticas e técnicas usadas por diferentes grupos adversários em ataques cibernéticos
- Oferece uma linguagem comum e uma compreensão das diferentes maneiras pelas quais os invasores podem operar
- Ajuda as organizações a entenderem a ameaça específica que estão enfrentando e a melhorarem suas defesas
- Pode ser útil para a investigação de ataques cibernéticos e para a identificação de responsáveis

- APT1 (“Comment Crew”) – grupo de hackers patrocinado pelo estado chinês
- APT29 (“The Dukes’ ou “Cozy Bear”) – grupo associado a atividades de espionagem cibernética patrocinadas pelo estado russo
- Usam uma ampla gama de táticas, incluindo spearphishing, malware e exploração de redes
- Usam ferramentas e técnicas sofisticadas, incluindo ferramentas de hacking personalizadas e malware

- O tempo tribulo é importante para a análise de risco porque é necessário considerar o passado para identificar ameaças e vulnerabilidades potenciais
- A análise de risco envolve a identificação e avaliação de possíveis ameaças e vulnerabilidades e a tomada de medidas para mitigar ou eliminar esses riscos
- O objetivo da análise de risco é garantir a segurança e a integridade dos sistemas e dados de uma organização e proteger contra ameaças potenciais, como ataques cibernéticos e violações de dados

- Para realizar uma análise de risco completa, é importante considerar o passado, o presente e o futuro
- Isso significa observar incidentes de segurança anteriores e suas causas, bem como tendências e desenvolvimentos atuais no campo da segurança cibernética
- Ao fazer isso, as organizações podem entender melhor os tipos de ameaças que podem enfrentar e podem tomar medidas para prevenir ou mitigar essas ameaças no futuro

- Se uma organização sofreu uma violação de dados no passado, pode analisar a causa dessa violação e tomar medidas para evitar que incidentes semelhantes ocorram no futuro
- Isso pode incluir a implementação de novas medidas de segurança, como senhas mais fortes ou autenticação de dois fatores, ou a atualização de protocolos de segurança para melhor proteção contra ameaças potenciais
- A análise de risco também pode envolver a realização de avaliações de risco regulares e o mantenimento de atualizações com as últimas tendências e práticas recomendadas no campo da segurança cibernética

- **Tecnologia** - ferramentas e sistemas usados para proteger informações e sistemas de ameaças potenciais
- **Pessoas** - indivíduos dentro de uma organização responsáveis por implementar e manter a segurança da informação
- **Segurança física** - medidas em vigor para proteger os ativos físicos de uma organização, incluindo medidas ativas e passivas
- **Organização** - procedimentos e processos em vigor para garantir a gestão eficaz da segurança da informação dentro de uma organização.

- Política de segurança
- Arquitetura de segurança
- Gestão de ativos
- Controle de acesso
- Criptografia
- Desenvolvimento e manutenção do sistema
- Gestão de vulnerabilidade técnica

- Consciencialização e treinamento de segurança
- Segurança do pessoal
- Gestão de incidentes de segurança
- Gestão de continuidade de negócios

- Política de segurança física
- Perímetro de segurança física
- Controlo de acesso físico
- Segurança física dos ativos

- Conformidade legal
- Avaliação e gestão de riscos
- Relacionamento com fornecedores
- Objetivos de segurança da informação
- Auditoria interna
- Revisão administrativa

A intervenção digital forense refere-se ao uso de técnicas forenses digitais para coletar, preservar e analisar evidências digitais após um incidente de segurança cibernética.

Existem dois tipos de intervenção digital forense:

- Intervenção forense online: envolve conduzir a investigação enquanto os sistemas afetados ainda estão online e conectados à rede. Permite coletar dados ao vivo, mas também há o risco de alteração das provas.
- Intervenção forense offline: envolve conduzir a investigação depois que os sistemas afetados foram colocados offline e desconectados da rede. Permite coletar um conjunto de evidências mais preciso, mas não permite interromper o ataque ou evitar mais danos.

O investigador geralmente coleta uma ampla gama de indicadores durante a intervenção digital forense para ajudar a identificar a causa do incidente e as partes responsáveis. Isso pode incluir:

- Indicadores de Comprometimento (IOCs): amostras de malware, logs de tráfego de rede, etc.
- Indicadores de Ataque (IOAs): tentativas suspeitas de login, exfiltração de dados, etc.

Os indicadores específicos coletados dependerão do incidente específico e das ferramentas e técnicas utilizadas pelo investigador.

A campanha pode incluir uma variedade de atividades de consciencialização, como:

- Fornecer treinamento e educação regulares aos funcionários sobre a importância da segurança cibernética.
- Partilhando exemplos de incidentes de segurança cibernética da vida real e as medidas tomadas para evitá-los.
- Destacando as possíveis consequências de não levar a segurança cibernética a sério, como perdas financeiras, danos à reputação e responsabilidades legais.
- Incentivar os funcionários a relatar quaisquer atividades suspeitas ou possíveis ameaças.
- Além disso, eu me certificaria de monitorizar e avaliar regularmente a eficácia da campanha e fazer os ajustes necessários.

[1] G. Amaro, *Fundamentos de Segurança Informática: Trabalho Individual*,