Guia Ágil

TechGuide - Alura

Cibersegurança

Nivel 1

- [ ] **Linha de comando - Fundamentos**:
  - CLI é um programa de linha de comando que aceita entradas de texto para executar funções do sistema operacional.
  - Conhecer os principais comandos
- [ ] **Python - Fundamentos**:
  - Python é uma linguagem de programação de alto nível, de uso geral, amplamente utilizada em aplicações web, desenvolvimento de software, ciência de dados e Machine Learning. Sua filosofia de projeto enfatiza a legibilidade do código com o uso de indentação significativa. Python é dinamicamente tipada e tem um garbage collector.
  - Conhecer os tipos primitivos
  - Declarar variáveis, considerando os diferentes tipos
  - Usar estruturas condicionais ('if', 'else')
  - Conhecer os operadores de atribuição e comparação
  - Usar estruturas de repetição e laços ('while', 'for')
  - Usar funções, passando parâmetros e argumentos
  - Manipular métodos

- Manipular arrays e listas
- Obter dados de uma API
- Criar construtores
- Funções anônimas

- [ ] **Criptografia - Fundamentos**:

- Criptografia em segurança virtual é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

- [ ] **Framework de Cibersegurança**:

- O Framework de Cibersegurança são guias de orientação para as organizações - em qualquer setor ou comunidade - que buscam melhorar o gerenciamento de riscos de segurança cibernética por meio da utilização de Framework. Embora o Framework de Cibersegurança não seja uma abordagem única para gerenciar riscos de segurança cibernética para organizações, em última análise, visa reduzir e gerenciar melhor esses riscos. Como tal, este guia destina-se a toda e qualquer organização, independentemente do setor ou tamanho.

- [ ] **Técnicas Hacker**:

- Entender as metodologias e as técnicas que os invasores usam para realizar o reconhecimento como uma etapa de pré-ataque, incluindo como eles usam inteligência de código aberto, varredura de rede e ataques de enumeração de alvos para encontrar as lacunas na segurança de sua rede.
- Usar técnicas de invasores para avaliar a segurança de uma rede de destino, avaliando protocolos e endpoints populares para Windows, Linux e destinos de nuvem.

- [ ] **Análise de Vulnerabilidades**:

- Técnicas e táticas de framework de vários serviços e ferramentas que oferece uma solução de varredura e gerenciamento de vulnerabilidade.

- [ ] **Firewalls, IDS e IPS**:

- Definições e diferenças entre dispositivos de segurança de rede, firewalls, sistemas de prevenção de intrusão (IPS) e sistemas de detecção de intrusão (IDS).
- Um firewall permite o tráfego dependendo de um conjunto de regras que foram configuradas. Ele é baseado nos endereços de origem, destino e porta. Um firewall pode negar qualquer tráfego que não satisfaça os critérios especificados.
- IDS são dispositivos de sistema de monitoramento passivo que monitoram o tráfego de rede à medida que viajam pela rede, comparam padrões de assinatura, e acionar um alarme se for detectada atividade suspeita ou ameaça de segurança conhecida.
- O IPS é um dispositivo ativo que impede ataques, bloqueando-os.

☐ **Investigação Digital - Fundamentos**:

- Investigação Digital é o uso da ciência para investigar crimes digfitais e determinar fatos, que surgiu a partir do uso e disseminação de sistemas digitais, como computadores e smartphones.

☐ **Quebra de senhas**:

- Em criptoanálise e segurança, a quebra de senhas é o processo de recuperação de senhas de dados que foram armazenados ou transmitidos por um sistema de computador de forma codificada. Uma abordagem comum (ataque de força bruta) é tentar repetidamente suposições para a senha e compará-las com um hash criptográfico disponível da senha.

☐ **Open-Source Intelligence**:

- OSINT (do inglês Open Source Intelligence) trata-se de um recurso que pode ser traduzido de uma forma simplificada como "Inteligência de Fontes Abertas". Trata-se de um conjunto de atividades para coletar, armazenar e analisar as informações de fontes públicas, basicamente, qualquer dado sobre uma empresa ou pessoa que possa ser encontrado por meio de ferramentas da Internet ou OSINT framework, como os buscadores.

☐ **Centro de Operações de Segurança**:

- O SOC (Security Operations Center) é o departamento que vem para planejar e respaldar toda a estratégia de segurança da T.I, monitorando, prevenindo e remediando brechas, falhas e possíveis ataques, tudo de maneira proativa.

- [ ] **Penetration Testing - Fundamentos**:

- Pentest (Penetration Testing) é a prática de testar um sistema de computador, rede ou aplicativo da Web para encontrar vulnerabilidades que um invasor possa explorar, simulando um ataque contra os ativos de TI de uma organização.

Nivel 2

- [ ] **Segurança de Endpoint**:

- A segurança de endpoint, ou proteção de endpoint, é a abordagem de segurança cibernética para defender endpoints como desktops, laptops e dispositivos móveis contra atividades maliciosas.

- [ ] **Metasploit - Ataque e Análise**:

- Metasploit é a estrutura de teste de penetração mais usada do mundo.

- [ ] **Web application - Segurança**:

- A segurança de aplicativos da Web (também conhecida como Web AppSec) é a ideia de criar sites para funcionar conforme o esperado, mesmo quando estão sob ataque. O conceito envolve uma coleção de controles de segurança projetados em um aplicativo da Web para proteger seus ativos de agentes potencialmente maliciosos.

- [ ] **Web application - Vulnerabilidade**:

- As vulnerabilidades de aplicativos da Web envolvem uma falha ou fraqueza do sistema em um aplicativo baseado na Web. Eles existem há anos, em grande parte devido à não validação ou limpeza de entradas de formulário, servidores web mal configurados e falhas de design de aplicativos, e podem ser explorados para comprometer a segurança do aplicativo. Essas

vulnerabilidades não são iguais a outros tipos comuns de vulnerabilidades, como rede ou ativo. Eles surgem porque os aplicativos da Web precisam interagir com vários usuários em várias redes, e esse nível de acessibilidade é facilmente aproveitado pelos hackers.

- [ ] **Gerenciamento de Dispositivos Móveis**:

  - O gerenciamento de dispositivos móveis refere-se a qualquer ferramenta ou software projetado para ajudar os administradores para controlar e proteger dispositivos móveis como smartphones e tablets em uma organização. O gerenciamento de dispositivos móveis é uma parte importante do gerenciamento de mobilidade empresarial e do gerenciamento de endpoints, especialmente à medida que mais empresas adotam políticas de BYOD (traga seu próprio dispositivo) que permitem que os funcionários acessem dados, arquivos e aplicativos da empresa em seus dispositivos pessoais.

- [ ] **SIEM e SOAR**:

  - Security Information and Event Management (SIEM) são softwares que agregam e analisam informações de várias fontes diferentes em toda a infra-estrutura.
  - Security Orchestration, Automation, and Response (SOAR) irá ajudar com o gerenciamento de ameaças e vulnerabilidades, resposta a incidentes de segurança e automação da operação de segurança.

- [ ] **Hardening de Servidores**:

  - A proteção do servidor é um conjunto de disciplinas e técnicas que melhoram a segurança de um servidor 'em produção'. Hardening é um requisito de estruturas de segurança em diversos frameworks.

- [ ] **Análise Forense na Nuvem**:

  - A investigação de dados armazenados na nuvem pode ser uma variedade de abordagens, desde investigações de inteligência de código aberto (OSINT) até investigações de contas na nuvem de indivíduos participantes que divulgam suas credenciais de login (mais frequentemente de vítimas e testemunhas do que de suspeitos), para obter e análise de devoluções de

garantias de provedores de serviços em nuvem para obter acesso às contas de suspeitos.

- [ ] **Recuperação de Dados**:

  - A recuperação de dados é um processo orientado por software que permite recuperar e restaurar arquivos perdidos, excluídos, inacessíveis, corrompidos ou danificados para que você possa voltar ao trabalho rapidamente. À medida que o cenário de negócios e nossas vidas em geral se tornam mais dependentes de dados, cresce a necessidade de proteger os sistemas de dados.

- [ ] **Segurança de Contêineres**:

  - A segurança de contêineres é o processo de combinar políticas de segurança para assegurar que a integridade do contêiner esteja protegida. A segurança do contêiner é importante porque a imagem do contêiner contém todos os componentes que, eventualmente, executarão seu aplicativo. Se houver vulnerabilidades à espreita na imagem do contêiner, o risco e a gravidade potencial dos problemas de segurança durante a produção aumentam.

- [ ] **Análise Forense de Memória**:

  - A análise forense de memória (às vezes chamada de análise de memória) refere-se à análise de dados voláteis no despejo de memória de um computador. Os profissionais de segurança da informação realizam análises forenses de memória para investigar e identificar ataques ou comportamentos maliciosos que não deixam rastros facilmente detectáveis nos dados do disco rígido.

- [ ] **Análise Forense de Rede**:

  - A análise forense de rede diz respeito à coleta, monitoramento e análise de atividades de rede para descobrir a origem de ataques, vírus, intrusões ou violações de segurança que ocorrem em uma rede ou no tráfego de rede. Como tal, a análise forense de rede é considerada juntamente com a análise forense móvel ou a análise forense de imagem digital, como residindo sob o guarda-chuva da análise forense digital.

- [ ] **Scripts PowerShell para segurança**:
    - Um script ofuscado pode ser malicioso e difícil de detectar com inspeção visual durante o processo de aprovação do script. Revise visualmente os scripts do PowerShell e use ferramentas de inspeção para ajudar a detectar problemas de script suspeitos. Essas ferramentas nem sempre podem determinar a intenção do autor do PowerShell, portanto, podem chamar a atenção para um script suspeito.

Nivel 3

- [ ] **Arquitetura de Segurança de Rede**:
    - A segurança de rede prepara você para tarefas como proteger os dados da empresa contra roubo, danos, interrupções e outros. Um profissional da área irá projetar e implementar auma arquitetura segura para dispositivos de rede, bem como oferecer suporte de segurança e garantir a integridade deles.
- [ ] **Threat Hunting**:
    - A busca de ameaças (Threat Hunting) é a prática de procurar proativamente por ameaças cibernéticas que estão à espreita sem serem detectadas em uma rede. A caça a ameaças cibernéticas se aprofunda para encontrar agentes mal-intencionados em seu ambiente que passaram pelas defesas de segurança de endpoint iniciais.
- [ ] **Segurança física**:
    - A segurança física é a proteção de pessoas, propriedades e ativos físicos de ações e eventos que podem causar danos ou perdas. Embora muitas vezes negligenciada em favor da segurança cibernética, a segurança física é igualmente importante.
- [ ] **Gerenciamento de Resposta a Incidentes**:
    - A resposta a incidentes é um processo estruturado que as organizações usam para identificar e lidar com incidentes de segurança cibernética. A resposta inclui vários estágios, incluindo preparação para incidentes,

detecção e análise de um incidente de segurança, contenção, erradicação e recuperação total e análise e aprendizado pós-incidente.

- [ ] **Análise de Malware**:
  - A análise de malware é o processo de compreensão do comportamento e da finalidade de um arquivo ou URL suspeito. A saída da análise ajuda na detecção e mitigação da ameaça potencial.
- [ ] **Segurança de Aplicações de Software**:
  - A segurança de aplicações descreve as medidas de segurança no nível do aplicativo que visam impedir que dados ou códigos dentro da aplicação sejam roubados ou invadidos. Ele abrange as considerações de segurança que ocorrem durante o desenvolvimento e o design de aplicativos, mas também envolve sistemas e abordagens para proteger os aplicativos depois que eles são implantados.
- [ ] **Arquitetura Zero Trust**:
  - Zero Trust é um modelo de segurança de rede baseado na filosofia de que nenhuma pessoa ou dispositivo dentro ou fora da rede de uma organização deve ter acesso para se conectar a sistemas ou serviços de TI até que seja autenticado e verificado continuamente.
- [ ] **Segurança na Nuvem**:
  - A segurança na nuvem, também conhecida como segurança da computação em nuvem, é um conjunto de medidas de segurança projetadas para proteger a infraestrutura, os aplicativos e os dados baseados em nuvem. Essas medidas garantem a autenticação de usuários e dispositivos, controle de acesso a dados e recursos e proteção de privacidade de dados. Eles também suportam a conformidade de dados regulatórios.
- [ ] **Segurança Contínua - Automação e Monitoramento**:
  - O monitoramento contínuo de segurança é uma abordagem de segurança que envolve a automatização de uma parte significativa do gerenciamento de segurança. Isso inclui detecção de vulnerabilidades, monitoramento de configurações de nuvem, identidades e seus direitos e segurança de dados.

Habilidade Auxiliar: Sistemas e tecnologias

- [ ] **Redes de Computadores - Fundamentos**:
  - Rede de computadores é uma malha que interliga milhares de sistemas computacionais para a transmissão de dados. Também conhecidos como nós, esses dispositivos interconectados enviam, recebem e trocam tráfego de dados, voz e vídeo, graças ao hardware e software que compõe o ambiente.
  - Configurações de redes são essenciais para que seja possível acessar uma aplicação, principalmente se ela estiver na nuvem.
  - Entenda melhor os componentes de rede e a suas atribuições
  - Diferenciar os serviços disponibilizados a nível de rede
  - Saber as diferenças entre as camadas de rede
  - Saber o que é servidor web, proxy reverso e load balancer
- [ ] **HTTP - Fundamentos**:
  - HTTP significa Hyper Text Transfer Protocol. A comunicação entre computadores cliente e servidores web é feita enviando solicitações HTTP e recebendo respostas HTTP.
  - Entender a diferença dos verbos HTTP
  - Testar os requests e ver os status codes no navegador
  - Saber fazer uma requisição HTTP na linha de comando com WGET
  - Baixar uma imagem com WGET
  - Fazer um post
- [ ] **Cloud - Fundamentos**:
  - Cloud, ou computação em nuvem é a distribuição de serviços de computação pela Internet usando um modelo de preço pago conforme o uso. Uma nuvem é composta de vários recursos de computação, que abrangem desde os próprios computadores (ou instâncias, na terminologia de nuvem) até redes, armazenamento, bancos de dados e o que estiver em torno deles. Ou seja, tudo o que normalmente é necessário para montar o

equivalente a uma sala de servidores, ou mesmo um data center completo, estará pronto para ser utilizado, configurado e executado.

- Conhecer a diferença entre IaaS, PaaS e SaaS
- Conhecer os maiores provedores de cloud
- Especializar-se em algum provedor

- [ ] **Linux - Fundamentos**:

- Linux é um termo popularmente empregado para se referir a sistemas operacionais que utilizam o Kernel Linux. As distribuições incluem o Kernel Linux, além de softwares de sistema e bibliotecas.
- Conhecer o sistema de diretórios do Linux
- Compactar e descompactar arquivos
- Editar arquivos no console com o VI
- Gerenciar os processos rodando na máquina
- Conhecer as variáveis de ambiente e o PATH
- Gerenciar pacotes
- Realizar comunicação remota com o SSH e SCP

Habilidade Auxiliar: Segurança da Informação

- [ ] **Gestão de risco, ameaças e vulnerabilidades**:

- Gerenciar riscos é o processo de planejar, organizar e controlar recursos e pessoas para minimizar danos ou fazer com que os riscos virem oportunidades. Prever os riscos é uma prática importante, afinal, dessa forma é possível reverter o que pode dar errado e alcançar resultados positivos ao longo do processo.

- [ ] **Confidencialidade, Integridade e Disponibilidade**:

- Os 3 princípios fundamentais da segurança da informação. Qualquer bom programa de gerenciamento de segurança da informação deve ser projetado para alcançar os três princípios de segurança da informação são comumente conhecidos como CIA (em inglês, a sigla CIA significa

"Confidentiality", "Integrity" e "Availability", o que corresponde à sigla CID em português — Confidencialidade, Integridade e Disponibilidade).

- [ ] **Gerenciamento de identidade e acesso (IAM)**:

  - Gestão de identidades, também conhecida como gestão de identidades e acessos (GIA) ou pelo seu termo em inglês, identity and access management (IAM) está entre as disciplinas de segurança da informação que habilita os indivíduos corretos à acessar os recursos corretos no momento correto e pelos motivos corretos.

- [ ] **Conscientização de Segurança**:

  - À medida que os ataques cibernéticos se tornam mais prevalentes e sofisticados, as empresas devem confiar mais em seus funcionários para garantir que eles não coloquem os dados em risco ou sejam vítimas de ransomware. Mas os funcionários estão mais ocupados do que nunca. E, criar uma cultura de cibersegurança no trabalho torna-se mais importante e mais desafiador quando os funcionários trabalham em casa.

- [ ] **Proteção de dados**:

  - A proteção de dados é o processo de proteger informações importantes de forma que garanta a confidencialidade, integridade e a disponibilidade destes dados.

- [ ] **Segurança em autenticação e senhas**:

  - Uma senha forte faz toda diferença quando o assunto é proteção de dados. Afinal, ela é construída de maneira a dificultar e muito que seja quebrada por um hacker ou ataque de massa. A senha, você sabe, é um mecanismo que permite o acesso de uma pessoa a um determinado serviço.
