Segurança Informática

Aula 5

Programa

1. Conceitos introdutórios
2. Criptografia básica
3. Autenticação e Controlo de Acessos
4. Ameaças à segurança
5. Penetração em redes e sistemas
6. Políticas de segurança
7. Mecanismos de proteção e técnicas de defesa
8. Entidades de Segurança

5. Penetração em Redes e Sistemas

Objetivos:

* Analisar criticamente os riscos de segurança associados à utilização de sistemas e redes.

* Reconhecer falhas e indicar técnicas de ataque à segurança informática.

Malware

- As maiores ameaças aos utilizadores e equipamentos quer ligados à rede (Internet) ou não, são representadas pelos Malwares.
- São programas (vírus) inseridos em máquinas contra a vontade de um utilizador e desempenham funções indesejadas.
- Alguns vírus têm a capacidade de se reproduzir e propagar a outros dispositivos por toda a rede. A cada dia surgem novos vírus/ataques e o combate a este tipo de invasão é constante.

Fases de um Vírus

- Durante a sua vida, um vírus típico atravessa as seguintes fases:

- Fase Dormente
  - O vírus está inativo.
  - Irá eventualmente ser ativado por evento, tal como uma data, a presença de outro programa ou ficheiro.
  - Nem todos os vírus passam por esta fase.

- Fase de Propagação
  - O vírus coloca uma cópia de si mesmo em outros programas ou em determinadas áreas do sistema (no disco).
  - A cópia pode não ser idêntica à versão de propagação. Muitas vezes há transformação para evitar a deteção.
  - Cada programa infetado vai conter um clone do vírus, dando início à propagação.

Fases de um Vírus

- Fase de Ativação
  - O vírus é ativado para realizar a função para a qual ele foi destinado.
  - A ativação pode ser causada por uma variedade de eventos do sistema, incluindo a contagem do número de vezes que esta cópia do vírus fez cópias de si mesmo.

- Fase de Execução
  - A função é executada.
  - A função pode ser inofensiva, tal como uma mensagem no ecrã, ou prejudiciais, tais como a destruição de programas e ficheiros de dados.

Mitigação de Ataque de Vírus

- Esses tipos de aplicações podem ser contidos através do uso eficaz de software, equipamentos e, potencialmente, ao nível da rede.
- O software pode detetar a maioria dos vírus e impedir a sua propagação na rede.
- Manter-se atualizado pode levar a uma postura mais eficaz contra esses ataques.

Mitigação de Ataque de Vírus

- Trojans (Cavalos de Tróia)
  - Trojans são programas projetados para assumir controlo de um servidor ou estação de trabalho de maneira furtiva, sem que o administrador da rede ou o utilizador se dê conta. Como exemplo, pode-se referir a possibilidade de enviar cópias de documentos sigilosos para os devidos utilizadores, mas também para um utilizador não autorizado a recebê-las.

- Worms
  - São Trojans ou vírus que fazem cópias do seu próprio código e as enviam para outras máquinas, seja por e-mail, programas ou outras formas de propagação pela rede.
  - São cada vez mais comuns e perigosos derivado do poder de propagação.

Mitigação de Ataque de Vírus

- Adware (Advertising software)
  - Software desenvolvido para apresentar publicidade, seja através de um browser, seja através de outro programa instalado no computador.
  - Em alguns casos, os adwares são incorporados em softwares e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem software livre ou prestam serviços gratuitos.
  - Um exemplo do uso legítimo de adwares pode ser observado na versão gratuita do browser Opera.
  - Exemplos de Advertising software
    - Resource Guru, AdPlugg, Front, SEISO, Wrike, todo.vu, Teamogy, ProWorkflow, Kontentino, ActiveCollab, HarmonyPSA, Easy Projects,Trello, Asana, ...

Mitigação de Ataque de Vírus - Exemplos de Advertising software

	Product	Deployment	Campaign Management	Collaboration	Document Management	Project Management	Task Management	Time Tracking
	Resource Guru (222 reviews)	☁	✓	✓	✓	✓	✓	✓
	Front App (130 reviews)	🖵 📱 ☁	✓	✓	✓	✓	✓	✓
	AdPlugg (5 reviews)	☁	✓	✓	✓	✓	✓	✓
	SEISO (12 reviews)	☁	✓	✓	✓	✓	✓	✓
	todo.vu (33 reviews)	📱 ☁	✓	✓	✓	✓	✓	✓
	Wrike (1577 reviews)	🖵 📱 ☁	✓	✓	✓	✓	✓	✓
	Teamogy (9 reviews)	☁	✓	✓	✓	✓	✓	✓
	ProWorkflow (200 reviews)	☁	✓	✓	✓	✓	✓	✓
	Kontentino (69 reviews)	☁	✓	✓	✓	✓	✓	✓
	ActiveCollab (353 reviews)	🖵 📱 ☁	✓	✓	✓	✓	✓	✓

Mitigação de Ataque de Vírus

- Spyware
  - Termo utilizado para referir à categoria de software que tem o objetivo de monitorizar atividades de um sistema e enviar as informações recolhidas para terceiros.
  - Existem adwares que também são considerados um tipo de spyware, pois são desenvolvidos para monitorizar os hábitos do utilizador durante a navegação na Internet e direcionar a publicidade que são apresentadas.
  - Existem ferramentas específicas, disponíveis na maioria dos distribuidores de antivírus, conhecidas como "anti-spyware", capazes de detetar e remover uma grande quantidade de programas spyware.

Mitigação de Ataque de Vírus - Exemplos de Spyware

- Com o desenvolvimento das tecnologias de segurança digital ao longo dos anos, muitos programas de spyware desapareceram, enquanto surgiram outras formas mais sofisticadas de spyware.

- Alguns dos exemplos de spyware:
  - CoolWebSearch
    - Este programa tira proveito das vulnerabilidades de segurança no Internet Explorer para sequestrar o navegador, alterar as configurações e enviar dados de navegação.
  - Gator
    - Geralmente fornecido como um software de partilha de ficheiros (como o Kazaa), esse programa monitoriza os hábitos de navegação da vítima e usa as informações para veiculá-las com anúncios mais direcionados.

Mitigação de Ataque de Vírus - Exemplos de Spyware

- Internet Optimizer
  - Particularmente popular à uns anos atrás (na era do modem), este programa prometia ajudar a aumentar a velocidade da Internet. Em vez disso, substituia todas as páginas de erro e login por anúncios.
- TIBS Dialer
  - Sequestrador de modem que desligava o computador da vítima de uma linha telefónica local e ligava a um número de valor acrescentado criado para aceder a sites pornográficos.
- Zlob
  - Também conhecido como Zlob Trojan, este programa usa vulnerabilidades no codec ActiveX para fazer o download num computador e registar históricos de pesquisa e navegação, além de pressionar as teclas.

Mitigação de Ataque de Vírus

- Spam
  - Termo usado para se referir às mensagens eletrónicas não solicitados, que geralmente são enviados para um grande número de pessoas.
  - Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem também é referenciada como UCE (do inglês Unsolicited Commercial E-mail).

- Keylogger
  - Software que regista toda a atividade do teclado em ficheiro, que pode ser enviado para um provável atacante.
  - Alguns Keyloggers registam apenas as informações digitadas quando o utilizador se encontra ligado a um site seguro.
  - Por mostrar as teclas que estão a ser digitadas, o Keylogger pode capturar números de contas, senhas e outras informações, antes de serem processadas (criptografadas) por dispositivos de segurança.

Boas Práticas em Segurança Informática

Palavras-chave comuns, são palavras-chave más

A primeira linha de defesa de segurança são as palavras-chave.

Os *hackers*, tentam entrar na rede através das palavras-chave mais comuns. Pode consultar as senhas mais utilizadas. Não as use.

Criar uma password segura e adote ainda hoje esta prática na definição das suas passwords.

Garanta que as passwords são fortes em todos os equipamentos que acedem à rede (computadores, *notebooks*, *smartphones*, *tablets* e pontos de acesso *WIFI*).

Boas Práticas em Segurança Informática

Bloquear todas as entradas aos cibercriminosos

Da mesma forma que protege a sua casa, ao fechar as portas e janelas, deve agir da mesma forma quando se trata da segurança da rede informática.

É suficiente uma porta aberta para ser alvo de ataques informáticos.

Implemente todas as medidas para proteger a sua rede, permitindo apenas o acesso a ela a utilizadores autorizados, definindo ainda os níveis de acesso.

Utilize uma firewall com prevenção contra ameaças à rede.
Proteja os postos de trabalho com software antivírus, anti-spam e anti-phishing.
Sensibilize e dote todos os colaboradores de conhecimento em cibersegurança.

Boas Práticas em Segurança Informática

Faça cópias de segurança de dados e garanta o restauro no ponto desejado

Regra 3-2-1 para garantir a segurança da informação.

Se a informação é crucial para a instituição, então, deve conhecer e implementar esta regra quer em ambientes físicos quer em ambientes virtuais.

1º – Criar 3 backups da sua informação;
(Para além dos dados primários deve ter mais 2 backups.)

2º – Armazenar os backups em locais diferentes;

3º – Mantenha um dos backups Off-Site.
(Recomendação em ambiente Cloud. Desta forma garante que existe uma separação física de segurança entre os backups.)

Boas Práticas em Segurança Informática

Definir, educar e aplicar políticas de prevenção e de utilização

Tenha uma política de segurança bem definida relativamente à prevenção de ameaças.

Aloque algum tempo, a definir quais as aplicações que não deseja que tenham acesso à sua rede.

Transmita essas diretrizes a todos os utilizadores. Monitorize as violações da política definida e alerta para as irregularidades.

Configure uma política de uso, definindo permissões para aplicações e websites.

Não permita acesso a programas de *Torrent* e outras aplicações de partilha de arquivos que tipicamente são utilizados para partilha de software malicioso.

Bloquei o *TOR* e outros que promovam o acesso a informação de forma oculta ou contornando a segurança.

Pense na utilização das Redes Sociais.

Boas Práticas em Segurança Informática

Seja socialmente consciente

Os sites de social media são uma fonte de ouro para os cibercriminosos que procuram obter informações sobre as pessoas de forma a melhorar a taxa de sucesso dos seus ataques.

Ataques como *phishing*, *spearphish* começam com a recolha de dados pessoais de indivíduos.

Educar os funcionários para estarem atentos nos conteúdos que partilham nas redes sociais.

Informar os utilizadores de que os cibercriminosos criam perfis falsos de funcionários da empresa para aumentar o sucesso dos ataques de *phishing*.

•Ensinar os colaboradores a configurar a privacidade em sites e redes sociais para proteger as informações pessoais.

Boas Práticas em Segurança Informática

Criptografar tudo (de forma sensata)

A violação de dados pode ser devastadora para uma instituição e para a sua reputação. Proteja os seus dados com criptografia.

Ficar tranquilo se os portáteis forem perdidos ou roubados, garantindo que os *notebooks* tem criptografia de pré-inicialização instalada.

Comprar discos rígidos e unidades *USB* com criptografia incorporada.

Usar criptografia forte na rede wireless da empresa.

Utilizar *VPN* (*Virtual Private Network*).

Boas Práticas em Segurança Informática

Mantenha a sua rede "limpa"

A sua rede e todos os dispositivos conectados a ela devem funcionar como uma máquina "como um todo".

Verificar se os sistemas operativos, computadores e servidores estão atualizados (garanta que os Updates estão ativados em todos os sistemas).

Desinstalar o software que não é necessário.

Atualizar as aplicações;

Ativar as atualizações automáticas, quando disponíveis.

Usar um dispositivo IPS (Intrusion Prevention System) para evitar ataques a sistemas não atualizados.

Boas Práticas em Segurança Informática

Tenha cuidado com a Cloud, mas utilize-a a seu favor

Os serviços cloud estão em crescimento quer na utilização de aplicações quer no armazenamento de dados.

Ao mover para a nuvem os seus conteúdos, estes deixam de estar sob o seu controlo. Garanta que o seu provedor de cloud respeita as diretrizes de segurança.

Antes de enviar informação para a nuvem, avalie a sua criticidade. Suponha sempre que ele deixa de ser privado.

Criptografar o conteúdo antes de enviar (incluindo backups do sistema).

Verifique a segurança do seu provedor de cloud.

Boas Práticas em Segurança Informática

Contas de Administração vs Contas de Utilizador

Nos postos de trabalho defina contas de administração e contas de utilizador.

Não permita que os funcionários usem uma conta com privilégios de administração para as suas atividades diárias. Limite a utilização a contas de utilizador de forma a reduzir a capacidade de software malicioso.

Criar o hábito de alterar passwords padrão em todos os sistemas (computadores, servidores, routers, gateways e impressoras de rede).

Boas Práticas em Segurança Informática

Utilização de Equipamentos Pessoais

Permita apenas o acesso "Guest" a dispositivos pertencentes a funcionários.

Aceder a informações confidenciais apenas através da VPN criptografada.

Não permita o armazenamento de informações confidenciais em dispositivos pessoais (como contatos de clientes ou informações de cartão de crédito).

Definir um plano em caso de o funcionário perder o dispositivo.

Como realizar um Pentest (Penetration testing)

Penetration test é o método usado para testar e descobrir vulnerabilidades numa rede e a possibilidade de ver como estas podem ser exploradas ou corrigidas.

Para ser feito um teste de penetração são contratados profissionais (ou pessoas internas à rede) para explorar a rede, da mesma forma que um cracker faria e em seguida são entregues os resultados indicando todas as falhas encontradas e como corrigi-las.

Para se fazer um teste de penetração é necessário passar diversas fases, para as quais são utilizadas diversas ferramentas.

Como realizar um Pentest (Penetration testing)

Reconhecimento da rede

A enumeração consiste no reconhecimento da rede e dos sistemas atingíveis. Os resultados esperados são: nomes de domínios, nomes de servidores, informação do ISP, endereços IP envolvidos e também um mapa da rede.

Para fazer o reconhecimento da rede, podem ser utilizadas diversas ferramentas e técnicas, conforme o objetivo do ataque.

Algumas ferramentas, que poderão ser usadas no reconhecimento.

Nslookup – Serve para mapear endereços IP para um determinado domínio.

Whois – Informação sobre um domínio registado (entidade que registou, endereço físico, contactos, domain servers, etc).

ARIN Dig – serve para perguntar a um servidor DNS informação acerca de outras coisas, por exemplo, a versão do name server que a empresa está a utilizar.

Como realizar um Pentest (Penetration testing)

Scanning

Nesta fase de um teste de penetração é a identificação de portas abertas e serviços a correr, na máquina ou rede alvo, chegando assim a enumeração de vulnerabilidades no alvo.

Também nesta fase do teste podemos incluir diversas ferramentas e técnicas, conforme o objetivo do teste e a configuração da máquina/rede.

As ferramentas mais utilizadas para fazer scanning, são:
telnet – Serve para mostrar informação sobre uma aplicação ou serviço.

nmap / **hping2** / **netcat** – port scanner

ping – testa conetividade IP

traceroute – Conta os "hops" da rede, desde a máquina em que é executado até à máquina/sistema alvo.

Como realizar um Pentest (Penetration testing)

Teste de vulnerabilidade

Os testes de vulnerabilidades consistem na determinação de que falhas de segurança e vulnerabilidades podem ser aplicadas à rede/máquina alvo.

Quem efetuar o teste vai tentar identificar nas máquinas na rede alvo todas as portas abertas, sistemas operativos e aplicações a serem executadas; incluindo o sistema operativo, patches aplicados e service packs aplicados.

Existe, categorias de vulnerabilidades que podem ser encontradas:

Os bugs específicos do sistema operativo, exploits, vulnerabilidades e falhas de segurança

As fraquezas no firewall e routers, entre diversas marcas

A exploração de scripts de web server

As partilhas e confianças exploráveis entre sistemas e pastas.

Como realizar um Pentest (Penetration testing)

Ferramentas e Manuais

As análises das vulnerabilidades de um computador pode ser feita manualmente, com base na informação recolhida nos pontos anteriores.

Nessus

Ferramenta para inventariar vulnerabilidades com código fonte disponível. Esta ferramenta é constituída por duas partes: o cliente e o servidor, que podem ou não, ser instaladas em máquinas diferentes.

O modo de comando tem a vantagem de poder ser incluído em scripts, o modo gráfico tem a vantagem de ser facilmente selecionável quais os testes de vulnerabilidade que são executados.

SARA - Security Auditor's research assistant

Scanner de rede, que procura serviços e os analisa. Esta ferramenta produz relatórios em diversos formatos: html, XML e CSV, com export para folhas de cálculo.

Pode ser executado em três modos: interativo (interface web), linha de comando, ou modo remoto. Pode ser definido o tipo de "ataque" e níveis de severidade que é feito à máquina/rede.

Como realizar um Pentest (Penetration testing)

Comparação entre detetores de vulnerabilidades

A deteção manual de vulnerabilidades é, com certeza a que permite mais pormenor, mas é muito difícil de ser implementada com perfeição.

Relativamente às duas ferramentas utilizadas, o SARA é, sem dúvida, mais rápida, mas é também a menos eficiente. Além de apresentar resultados muito menos detalhados e não apresentar formas de resolução das vulnerabilidades (como o Nessus), apresenta falsos positivos.

QUESTÕES
?