# Segurança Informática

## Aula 3

Docente: Ricardo Costa
rcosta@estg.ipp.pt

# 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 protecção e técnicas de defesa
8. Entidades de Segurança

# 3. Autenticação e Controlo de Acessos

Objetivos:

* Entender e exemplificar técnicas e mecanismos de segurança informática.

* Enunciar e entender diferentes sistemas de autenticação e controlo de acesso.

# Autenticação

- A autenticação é um processo de verificação da identidade de um recurso ou utilizador.

- Em contexto de rede, a autenticação é o ato de fornecer identidade para uma aplicação ou recurso da rede. Normalmente, a identidade é comprovada por uma operação criptográfica que usa uma chave do utilizador (assim como a criptografia de chave pública). Do lado do servidor a autenticação compara os dados assinados com uma chave de criptografia conhecida para validar a tentativa de autenticação.

- No sistema Windows o Active Directory é a tecnologia recomendada e padrão para armazenar informações de identidade, que incluem as chaves de criptografia que são as credenciais do utilizador. O Active Directory é exigido para as implementações de Kerberos e NTLM padrão.

- As técnicas de autenticação variam de um login simples para um sistema de autenticação, que identifica os utilizadores com base em algo que apenas este sabe, como uma senha, para mecanismos de segurança mais poderosos que usam algo que o utilizador recebe como tokens, certificados de chave pública, imagens ou atributos biológicos.

# Autenticação: Cenários de login

- **Login Interativo**
  - O processo de login começa quando o utilizador digita as credenciais na caixa de diálogo ou quando o utilizador insere um cartão inteligente no leitor de cartão inteligente ou quando o utilizador interage com um dispositivo biométrico. Os utilizadores podem executar um login interativo através de uma conta de utilizador local ou de uma conta de domínio em outro computador.

- **Login de Rede**
  - Só pode ser usado após o utilizador, serviço ou a autenticação do computador ter ocorrido. Durante o login da rede, o processo não usa as caixas de diálogo de entrada de credenciais para recolher dados.
  - Em vez disso, as credenciais são estabelecidas anteriormente ou com recurso a outros métodos. Esse processo confirma a identidade do utilizador para qualquer serviço de rede que o utilizador tenha acesso. Esse processo é normalmente transparente para o utilizador, exceto se necessário credenciais alternativas.
    - No sistema operativo Windows, para fornecer esse tipo de autenticação, o sistema de segurança inclui estes mecanismos de autenticação:
      - Protocolo Kerberos
      - Certificados de chave pública
      - Segurança de camada de protocolo SSL/transporte (SSL/TLS)
      - Digest
      - NTLM, para compatibilidade com sistemas baseados no Microsoft Windows NT 4.0

# Autenticação: Cenários de login

- **Login com Cartão**
  - Os cartões inteligentes podem ser usados para fazer login somente em contas de domínio, não em contas locais. A autenticação de cartão requer o uso do protocolo de autenticação Kerberos.
  - Introduzido em sistemas operativos baseados no Windows (Windows 2000 Server), uma extensão de chave pública para a solicitação de autenticação inicial do protocolo Kerberos é implementada.
  - Para iniciar uma sessão de login típica, um utilizador deve provar a sua identidade fornecendo informações conhecidas apenas pelo utilizador e a infraestrutura de protocolo Kerberos subjacente.
- **Login Biométrico**
  - Um dispositivo é usado para recolher e criar uma característica digital de um elemento, como uma impressão digital.
  - Em seguida, essa representação digital é comparada a uma amostra do mesmo elemento e quando as duas são comparadas com êxito, a autenticação pode ocorrer.
  - No entanto, se o login biométrico for configurado apenas para login local, o utilizador precisa apresentar as credenciais de domínio ao aceder a um domínio de Active Directory.

# Autenticação: Conceitos associados

- **Autorização**
  - Processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao utilizador autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em base de dados centralizada. (Cada sujeito herda as características do grupo a que pertence.)

- **Accounting**
  - Processo por meio do qual um equipamento de rede implementa uma política de acesso (accounting client), recolhe informações sobre a atividade do elemento autenticado e envia-as ao servidor de autenticação.

Breve resumo:

- Autenticação trata de responder à questão "quem é o utilizador".
- Autorização tem a função de definir "o que um utilizador (já autenticado) tem permissão de fazer".
- Accounting está relacionado com a questão "o que o utilizador fez?". Através desse processo o cliente de autenticação (equipamento de rede), recolhe os dados da atividade do utilizador e envia ao servidor de accounting.

# Protocolos de autenticação

| Protocolos de autenticação | Descrição |
|---|---|
| Kerberos | Trata-se de um protocolo utilizado com uma palavra-chave ou um cartão Smart Card para um início de sessão interactivo. É também o método predefinido de autenticação de rede para os serviços. |
| Radius | Protocolo que prevê um sistema de segurança Cliente/Servidor aberto e escalonável. |
| NTLM | Trata-se de um protocolo utilizado quando o cliente ou o servidor utiliza uma versão anterior do Windows. |
| SSL/TLS | Trata-se de um protocolo utilizado quando um utilizador tenta aceder a um servidor Web seguro. |

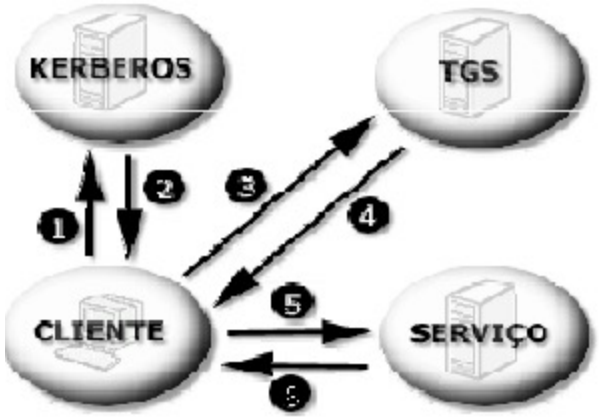
# Protocolos de autenticação: Kerberos - Definição

- Serviço de autenticação distribuído que permite que um cliente, através de um utilizador, prove a sua identidade a um servidor de autenticação, passando em seguida por um verificador de sessão, para estabelecer a transferência das informações com o host destino, evitando assim, a violação da conexão estabelecida.

- Este protocolo é uma das soluções aos problemas de segurança na rede, fornecendo ferramentas de autenticação e criptografia para trabalhos em redes públicas como a Internet.

# Protocolos de autenticação: Kerberos - Funcionamento

- O sistema usa etiquetas para autenticar um utilizador perante um servidor.
- Uma etiqueta só é boa para um único servidor e um único utilizador durante um certo período de tempo e para uma mensagem codificada que contém o nome do utilizador, o seu servidor, o endereço da rede do servidor do utilizador, um selo de tempo e uma chave de sessão.
- Uma vez que o utilizador adquire a etiqueta, ele pode usar isso para ter acesso ao servidor quantas vezes forem necessárias até que a etiqueta expire.
- O utilizador não pode decifrar a etiqueta mas pode apresenta-lo ao servidor. Com isso, escutas clandestinas não podem violar a etiqueta quando esta estiver em curso na rede Internet.
- Este protocolo envolve dois servidores, um de autenticação e o outro (TGS) que concede as etiquetas.



# Protocolos de autenticação: Radius - Definição

- Baseado num modelo de segurança distribuído previamente definido pela (IETF), prevê um sistema de segurança Cliente/Servidor aberto e escalonável.

- O servidor Radius pode ser adaptado facilmente para trabalhar com produtos de segurança de terceiros ou em sistemas de segurança proprietário.

- Qualquer mecanismo de comunicação, seja um software ou um hardware que utilize este protocolo cliente Radius pode comunicar com um servidor Radius.

# Protocolos de autenticação: Radius - Funcionamento

- O PortMaster cria um pacote de dados com as informações chamado de "pedido de autenticação".
- Este pacote inclui a informação que identifica o PortMaster específico que envia o pedido de autenticação, a porta que está a ser usada para a conexão, identificação do utilizador e a senha.
- Para proteger os dados, o PortMaster age como um cliente RADIUS e codifica a senha antes que seja enviada ao servidor RADIUS.
- Quando um pedido de autenticação é recebido, o servidor de autenticação valida o pedido e então decifra o pacote de dados para ter acesso a identificação do utilizador e senha.

# Integridade de dados

- Mesmo os dados não confidenciais devem manter a integridade.
- Exemplo: Uma pessoa pode não se importar que alguém veja as suas mensagens do dia a dia, mas certamente ficará preocupado se os dados puderem ser alterados. Uma ordem para a promoção de um funcionário geralmente não precisa ser secreta, mas quem a enviou estará realmente preocupado ser ela puder ser trocada por uma outra indicando uma demissão.
- O mesmo acontece nas mensagens secretas, já que o emissor deseja que seus bits não sejam alterados no caminho, o que poderia causar uma alteração no significado da mesma.

# Controlo de Acessos

- Políticas de Acesso
  - Policy Enforcement Points (PEP)
  - Policy Decision Points (PDP)
  - Access Control Lists (ACLs)
  - Role Based Access Control (RBAC)

## Políticas de Acesso: Policy Enforcement Points (PEP) e Policy Decision Points (PDP)

- Entidade lógica ou local no servidor que implementa políticas de controlo de admissão e as decisões políticas em resposta a um pedido de um utilizador que deseja aceder a um recurso num computador ou servidor de rede.

- Quando um utilizador tenta aceder a um arquivo ou outro recurso da rede que usa o acesso à base de gestão de políticas, o PEP descreve os atributos do utilizador sistema.

- O PEP vai dar o Policy Decision Point (PDP) à tarefa de decidir se deve ou não autorizar o utilizador com base na descrição dos atributos do utilizador.

- O PDP toma a decisão e retorna a decisão. O PEP vai permitir que o utilizador saiba se foi autorizado a aceder ao recurso solicitado.

# Políticas de Acesso: Access Control Lists (ACLs)

- Lista que define quem tem permissão de acesso a certos serviços.
- Normalmente consiste numa lista de princípios com os tipos de acesso definidos para cada utilizador ou grupo.
- Exemplo:
  - Os routers utilizam ACLs para filtragem de pacotes, seja ele de entrada ou saída.
- As ACLs não podem ser tratadas como um firewall, mas como um complemento para segurança da rede.

# Políticas de Acesso: Role Based Access Control (RBAC)

- Abordagem para restringir o acesso ao sistema dos utilizadores autorizados.

- É uma abordagem alternativa para controlo de acesso obrigatório (MAC – Mandatory Access Control) e controlo de acesso discricionário (DAC – Discretionary Access Control).

- Ao definir um modelo RBAC, as seguintes convenções são úteis:
- S = Subject = A pessoa ou agente automatizado
- R = Role = Função que define um nível de autoridade
- P = Permissions = Um aprovação de um modo de acesso a um recurso
- SE = Session = Mapeamento que envolve S, R e / ou P
- Um sujeito pode ter múltiplas funções.
- Uma função pode ter múltiplos sujeitos.
- Uma função pode ter muitas permissões.
- A permissão pode ser atribuída a muitas funções.

# Segurança Digital

- Hoje em dia fala-se muito de segurança, de ataques realizados por piratas informáticos. Atualmente, qualquer pessoa possui um smartphone e usa-o para efeitos pessoais mas também de trabalho.
  - Acedem ao email, a documentos, à rede empresarial.

- Mas, estarão todos devidamente protegidos, de forma a bloquear qualquer ataque pirata?

- Basta a instalação de uma aplicação, que contenha software malicioso (malware) para que um pirata consiga obter acesso a toda a rede de uma empresa ficando toda a informação à mercê de atos ilícitos.

# Segurança Digital

- Mesmo uma simples televisão, ou impressora, que esteja ligada ao mundo das coisas (Internet das Coisas ou Internet of Things) pode ser usada para um ataque sem que os utilizadores desses aparelhos se apercebam.

- Cada aparelho infetado passa a ser designado como um bot (diminutivo de robot, também conhecido como Internet bot ou web robot) e o conjunto de aparelhos infetados pelo malware a botnet.

- Quem detém o poder sobre esta rede pode controlar todos os aparelhos para fins ilícitos.

# Segurança Digital - Questões

- Que medidas toma para evitar os ataques de vírus?
  - Só visito sites de confiança, não me preocupo com vírus.
  - Tenho um antivírus instalado que atualizo quando me enviam um update por email.
  - Tenho o antivirus instalado e a fazer updates automáticos.

**Tenho o antivirus instalado e a fazer updates automáticos.**
Os vírus estão sempre a evoluir e há esquemas levados a cabo com envios falsos por email. O update automático é a forma mais segura.

# Segurança Digital - Questões

- Como protege o seu computador de acessos indevidos quando se liga ao WiFi através de um hotspot?
  - Utilizo uma firewall, acesso VPN e desligo a partilha de ficheiros.
  - Está tudo seguro desde que ninguém esteja a olhar para o meu ecrã.
  - Desde que faça log off depois de aceder ao homebanking, está tudo seguro.

**Utilizo uma firewall, acesso VPN e desligo a partilha de ficheiros.**
A firewall e VPN protegem o seu computador de acessos indevidos. Mantenha-os ligados sempre que acede a uma rede de WiFi pública.

# Segurança Digital - Questões

- De que forma um botnet o pode afetar?
  - Os botnets são um software malicioso.
  - Um pirata pode assumir o controlo do meu computador ou equipamento e, mesmo sem me aperceber, utilizá-lo para atividades ilegais.
  - Podem bloquear o acesso a determinados serviços.

**Um pirata pode assumir o controlo do meu computador ou equipamento e, mesmo sem me aperceber, utilizá-lo para atividades ilegais.**
Botnets são uma rede de computadores infetados que podem ser usados para atividades ilegais (cybercrime) sem os utilizadores se aperceberem. O malware é utilizado para controlar o computador.

# Segurança Digital - Questões

- De que forma deve agir para proteger a sua conta quando acede ao homebanking?
  - Visitar regularmente a conta para detetar eventuais movimentos indevidos.
  - Evitar aceder ao homebanking a partir de computadores públicos ou cibercafés e nunca revelar a password a terceiros.
  - As duas anteriores.

**As duas anteriores.**
Os bancos têm formas de proteger as contas dos clientes mas há pequenas ações que podem fazer a diferença. O acesso regular permite detetar movimentos ilícitos e os códigos de acesso devem manter-se secretos.

# Segurança Digital - Questões

- Quando instala uma app, de que forma age no processo de instalação?
  - Faço download das apps recomendadas por amigos.
  - Não me preocupo com isso, desde que goste, faço a instalação.
  - Faço o download mas verifico sempre que tipo de permissões estou a dar à aplicação.

**Faço o download mas verifico sempre que tipo de permissões estou a dar à aplicação.**
É muito importante verificar que tipo de permissões a app está a solicitar. Mesmo as apps que vêm de fábrica podem ter acesso a dados pessoais e sensíveis.

# Segurança Digital - Questões

- Existe uma atividade de pirataria recente onde o seu computador ou smartphone fica em poder dos piratas. Como se chama este ataque?
  - CryptoLocker
  - Botnet
  - Ransomware

**Ransomware.**
Ransomware é utilizado pelos piratas para bloquear o acesso aos aparelhos ou a dados específicos. Para voltar a ter controlo os utilizadores têm de pagar um resgate (ransom). O CryptoLocker é um trojan usado para ransomware.

# Segurança Digital - Questões

- Qual a política para a utilização de computadores pessoais na rede da empresa?
  - Não existe nenhuma restrição.
  - Podem aceder, mas têm de pedir uma password.
  - Só acedem através de um acesso VPN (Virtual Private Network).

**Só acedem através de um acesso VPN (Virtual Private Network).**
É crucial manter a sua rede empresarial segura pois os piratas usam qualquer porta para entrar no sistema.

# Segurança Digital - Questões

- No que respeita a dispositivos móveis, como protege a empresa de ataques à sua rede?
  - Só podem aceder à Internet.
  - Com um serviço de gestão remota e centralizada de smartphones e tablets.
  - Têm de ter uma autorização especial para aceder à rede.

**Com um serviço de gestão remota e centralizada de smartphones e tablets.**
É importante manter a monitorização, gestão remota e suporte de dispositivos móveis e aplicações consoante a função do colaborador.

# Segurança Digital - Questões

- Como protege a empresa de eventuais vírus ou ataques através dos emails?
  - O antivírus instalado no pc é suficiente.
  - Através de uma solução de filtragem de email centralizada.
  - Os colaboradores sabem que não podem abrir ficheiros enviados por email.

**Através de uma solução de filtragem de email centralizada.**
A melhor forma de evitar "infeções" com vírus é filtrar logo à chegada ao servidor de email.

# Segurança Digital - Questões

- Se for alvo de um ataque ransomware, que lhe bloqueia o acesso à informação da empresa...
  - ...pago o que for preciso para recuperar.
  - ...a informação está guardada num servidor da empresa.
  - ...continuo a ter acesso à informação porque uso um serviço de backup na cloud.

**...continuo a ter acesso à informação porque uso um serviço de backup na cloud.**
Depois de pagar o primeiro, quem garante que a sua informação fica segura e que não irá sofrer outro ataque?

# Questão de aula

Qual a importância das políticas de acesso para a segurança de um sistema?

# QUESTÕES

?

Docente: Ricardo Costa
rcosta@estg.ipp.pt