SEGURANÇA CIBERNÉTICA – CISCO NETWORKING ACADEMY

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

SEGURANÇA CIBERNÉTICA
CISCO NETWORKING ACADEMY

Prof. Everson Denis

INSTITUTO MAUÁ DE TECNOLOGIA
MAUÁ

SEGURANÇA CIBERNÉTICA – CISCO NETWORKING ACADEMY

Agenda

- **Controle de acesso (Autenticação)**
- **Uso de senhas**
- **Uso de Hash (Integridade)**

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DE SENHAS

- **Gerador de Senhas Fortes.**
  - https://howsecureismypassword.net
  - https://strongpasswordgenerator.com
  - http://preshing.com/20110811/xkcd-password-generator
  - https://passwordsgenerator.net

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DE SENHAS

- Dicas para escolher uma boa senha:
  - Não use palavras do dicionário ou nomes em qualquer idioma
  - Não use erros ortográficos comuns de palavras do dicionário
  - Não use nomes de computador ou de contas
  - Se possível use caracteres especiais, como! @ # $ % ^ & * ( )
  - Use uma senha com 10 ou mais caracteres

OK	Good	Melhorou
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DE SENHAS

- Dicas para escolher uma boa senha:
  - Escolha uma frase significativa para você
  - Adicione caracteres especiais, como ! @ # $ % ^ & * ( )
  - Quanto maior melhor
  - Evite frases comuns ou famosas, como a letra de uma música famosa

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DE SENHAS

- Impede que os criminosos acessem todas as suas contas on-line usando credenciais roubadas
- Use gerenciadores de senha para ajudar a lembrar das senhas
  - https://www.lastpass.com
  - https://www.dashlane.com

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DE SENHAS

- Resumo das novas orientações da NIST:
  - No mínimo 8 caracteres e no máximo 64 caracteres
  - Não use senhas comuns e fáceis de ser descobertas, como a senha abc123
  - Nenhuma autenticação baseada em conhecimento, como informações de perguntas secretas compartilhadas, dados comerciais e histórico de transações
  - Melhore a precisão da digitação, evitando que o usuário veja a senha durante a digitação
  - Todas os caracteres e espaços são permitidos
  - Não use dicas para senhas
  - Não aplique expiração de senha periódica ou arbitrária

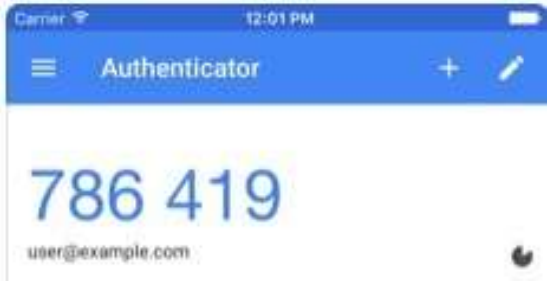
OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Melhorou	Acat th@tlov3sd0gs.

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

CONTROLE DE ACESSO – MÉTODO DE AUTENTICAÇÃO

- **O que você sabe** - senhas, frases secretas ou PINs são exemplos de algo que o usuário sabe. As senhas são o método mais popular usado para autenticação.
- **O que você tem** - cartões inteligentes, tokens são exemplos de algo que os usuários têm.
- **Quem você é** - uma característica física única, como uma impressão digital, retina ou voz, que identifica um usuário específico, é chamada de biometria.
- **Autenticação multifator** - usa pelo menos dois métodos de verificação. Uma chave de segurança é um bom exemplo. Os dois fatores são algo que você sabe, como uma senha, e algo que você tem, como uma chave de segurança.

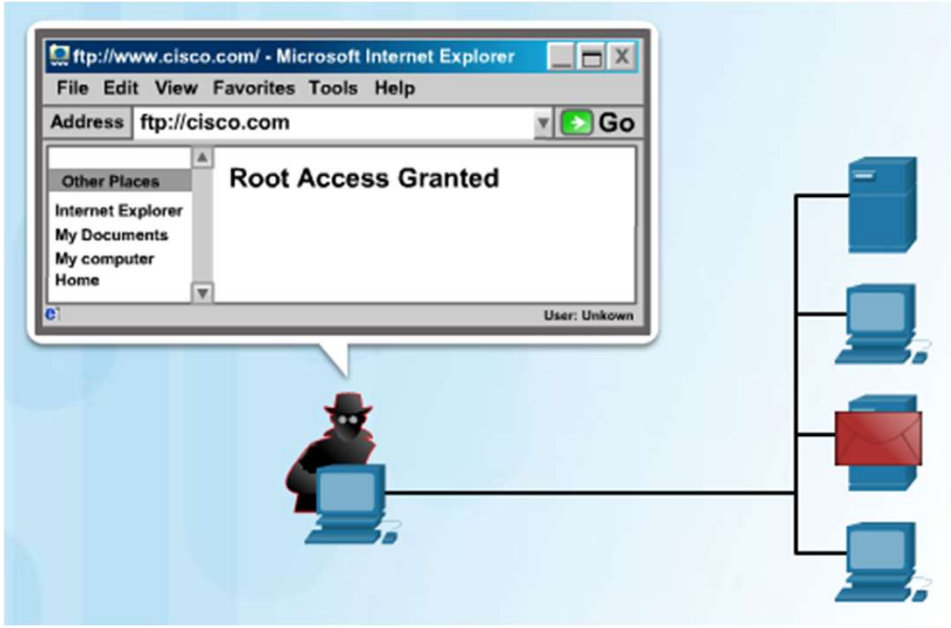


INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

- **Princípios de Segurança da Informação**
  - confidencialidade, integridade e disponibilidade

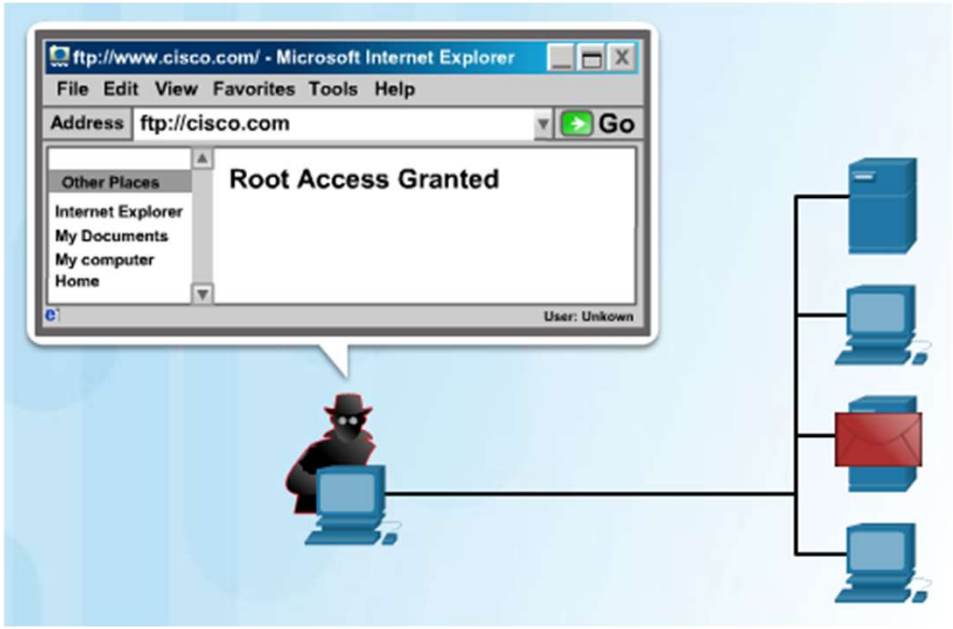


INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

- **Princípios de Segurança da Informação**
  - confidencialidade, integridade e disponibilidade

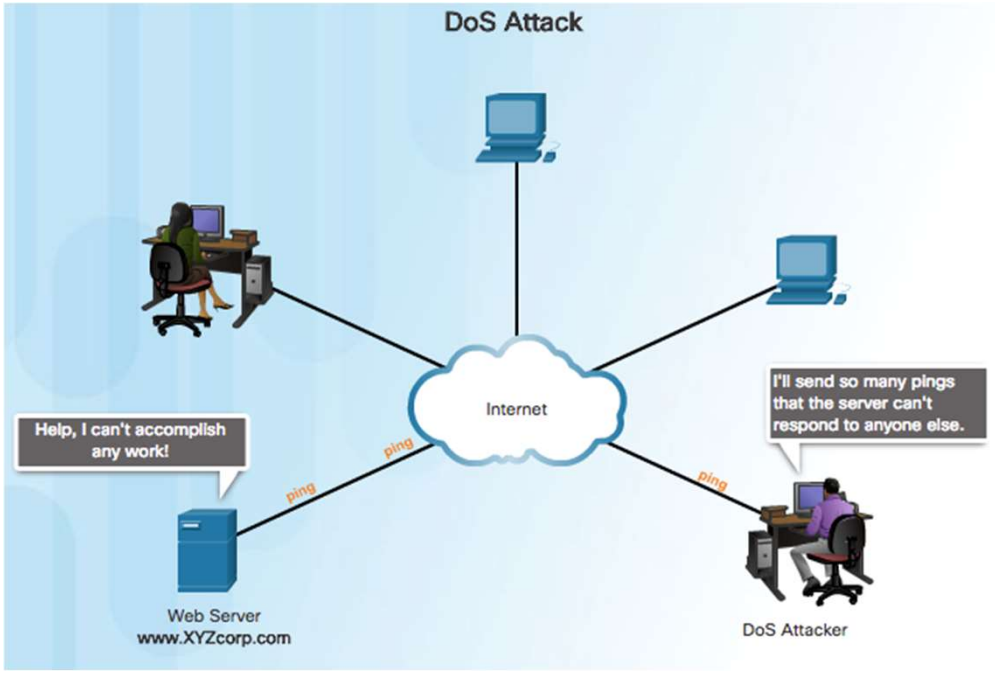


INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

- **Princípios de Segurança da Informação**
  - confidencialidade, integridade e disponibilidade



INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DO HASH – O QUE É?

- *hash*, também chamado de "digestor", é uma espécie de "assinatura" ou "impressão digital" que representa o conteúdo de um fluxo de dados. Com certa frequência os hashes são chamados de *checksum*. Um *hash* pode ser comparado com um selo de embalagem que indica clara e inequivocamente se a embalagem já foi aberta ou violada.
- *Hashes* não são cifragens, são digestos! As cifragens transformam os dados do texto claro num criptograma e vice-versa. *Hashes*, transformam os dados do texto (claro ou cifrado) num pequeno digesto, de **tamanho fixo**, numa **operação de mão única**.
- Os *hashes* produzem "selos de segurança" de comprimento fixo, não importa o comprimento do fluxo de dados ou do arquivo que representem. Qualquer alteração efetuada no arquivo, por mínima que seja, altera substancialmente o resultado hash. Isto ocorre porque, mesmo se apenas um dos bits do arquivo for alterado, muitos bits do resultado serão afetados. Este comportamento é conhecido como **efeito avalanche**.

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DO HASH – O QUE É?

- md5

Caracter	ASCII (decimal)	ASCII (binário)
A	65	0100 0001
a	97	0110 0001

```
Aldeia NumaBoa     3cdb658425ee484e4bff3d4583f6f851
aldeia NumaBoa     9c1f41ef263026b0283676d63df21fd1

3cdb6584     0011 1100 1101 1011 0110 0101 1000 0100
9c1f41ef     1001 1100 0001 1111 0100 0001 1110 1111
             x.x. .... xx.. .x.. ..x. .x.. .xx. x.xx     12 bits diferentes

25ee484e     0010 0101 1110 1110 0100 1000 0100 1110
263026b0     0010 0110 0011 0000 0010 0110 1011 0000
             .... ..xx xx.x xxx. .xx. xxx. xxxx xxx.     20 bits diferentes

4bff3d45     0100 1011 1111 1111 0011 1101 0100 0101
283676d6     0010 1000 0011 0110 0111 0110 1101 0110
             .xx. ..xx xx.. x..x .x.. x.xx x..x ..xx     16 bits diferentes

83f6f851     1000 0011 1111 0110 1111 1000 0101 0001
3df21fd1     0011 1101 1111 0010 0001 1111 1101 0001
             x.xx xxx. .... .x.. xxx. .xxx x... ....     14 bits diferentes
```

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DO HASH – APLICAÇÕES

- Aplicações
  - Autenticação de mensagens (Integridade de dados): qualquer tipo de arquivo, e um fluxo de dados que produz um resultado hash único. Uma das maneiras de poder verificar se o arquivo baixado é idêntico ao disponibilizado é conhecer o hash do arquivo original.
  - Segurança de senhas: armazenar os resultados hash das senhas do que as próprias senhas. O uso de uma senha pressupõe que um usuário a digite. Tendo a senha como entrada, é fácil e rápido calcular o resultado hash da senha fornecida e compará-lo com o valor arquivado.
  - Assinaturas digitais: Para se obter uma assinatura digital válida são necessárias duas etapas. A primeira é criar um hash do documento. Este hash identifica unicamente e inequivocamente o documento do qual ele se originou. A seguir, o assinante submete o hash a um método criptográfico usando sua chave privada. Como o hash criptografado só pode ser recuperado usando a chave pública do assinante, isto comprova a identidade da pessoa que assinou - é a chamada assinatura digital - e como o hash recuperado identifica o documento, a assinatura está associada unicamente a este documento.
  - Detecção de intrusão e detecção de vírus: armazena os arquivos e se houver alterações no sistema, são identificadas.

USO DO HASH – EXEMPLO

- Exemplo:
- http://www.fileformat.info/tool/hash.htm
  - Mensagem: “abc”
  - Hash:
    - ✓ MD5: 900150983cd24fb0d6963f7d28e17f72
    - ✓ SHA-1: a9993e364706816aba3e25717850c26c9cd0d89d
    - ✓ SHA-256: ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad
    - ✓ SHA-512: ddaf35a193617abacc417349ae20413112e6fa4e89a97ea20a9eeee64b55d39a2192992a274fc1a836ba3c23a3feebbd454d4423643ce80e2a9ac94fa54ca49f

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DO HASH – MELHORIAS (SALTING)

- Salting é usado para tornar o hash mais seguro. Se dois usuários tiverem a mesma senha, eles também terão os mesmos hashes de senha.
- Esse procedimento cria um resultado de hash diferente para as duas senhas. Um banco de dados armazena o hash e o salting.
  - https://www.symbionts.de/tools/hash/sha256-hash-salt-generator.html
  - https://crackstation.net

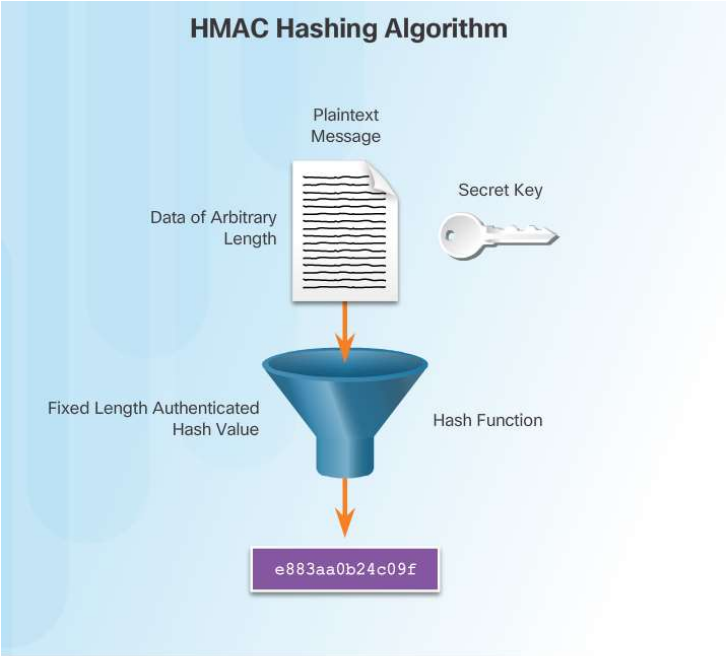
	Salt		Hash Value
Hash ("password" +	QxLUF1bIAdeQX)	=	b3bad1e5324f057753a4b8d7cef293e4
Hash ("password" +	R9PeIC7sxQXb8)	=	713c7beb54841a26a7c81eb06d6cf066

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ

USO DO HASH – MELHORIAS (HMAC)

- Hash-Based Message Authentication Code - (HMACs) fortalecem os algoritmos de hash usando uma chave secreta adicional como entrada para a função hash.
- O uso do HMAC garante além da integridade, também a autenticação.
- Um HMAC usa um algoritmo específico que combina uma função de hash criptográfica com uma chave secreta.
- Usado em VPN (autentica a origem do pacote e garante a integridade dos dados), equipamentos de rede, AWS (assinatura HMAC-SHA + preenchimento dos campos)
- http://www.freeformatter.com/hmac-generator.html



INSTITUTO MAUÁ DE TECNOLOGIA
MAUÁ

SEGURANÇA CIBERNÉTICA

- **Bibliografia:**

  - Introduction to Cybersecurity (Cisco). Disponível em: <https://www.netacad.com>. Acesso em: 11 maio 2020.
  - Cybersecurity Essentials (Cisco). Disponível em: <https://www.netacad.com>. Acesso em: 11 maio 2020.

INSTITUTO MAUÁ DE TECNOLOGIA

MAUÁ