

Lista de Softwares

quarta-feira, 16 de março de 2022 11:17

Laptop (com suporte a Wi-Fi em modo monitor
(promiscuous mode) + Kali Linux (boot via pendrive)

- Aircrack
- Airmon-ng
- Nmap
- Hydra

Desenvolver o web crawler (geração de wordlist acertiva baseada em páginas web)

Assistir o filme (War Games 1983)

[Cracking WiFi WPA2 Handshake](#)



Checklist N2 - CTF

quinta-feira, 9 de março de 2023 20:27

- Validação do processo de invasão (quebra) do Wi-Fi (WPA2 Personal) AirCrack - [Cracking WiFi WPA2 Handshake](#)
- Assistir ao Filme War Games (1983) (Engenharia Social) - [WarGames Official Trailer #1 - Dabney Coleman Movie \(1983\) HD](#)
- Quebrar o criptograma (tatuagem do professor) (Cifra de César + Engenharia Social) - [https://pt.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher](#)
- Brute Force Hydra THC - <https://www.kali.org/tools/hydra/>
- Criação de word lists baseadas em websites da web (webcrawler) (Exercício do Ivan Vanco - Iron Man 2)
- Uso do NMAP para localização do target (port scanner) - <https://nmap.org/>

Observação:

- Será importante o uso de ferramentas como ssh, sftp, vi, nano, nmap, hydra e comandos do Linux.
- Trazer um laptop com suporte a rede Wi-Fi em modo monitor.
- Utilizar o Kali Linux com boot em pendrive.

Introdução

terça-feira, 4 de agosto de 2020 18:42

Security (informação) vs. Safety (vida humana)

Criptografia: "Pode ser entendida como uma técnica de descaracterização da informação através do uso de algoritmos matemáticos."

Descaracterizar é remover aquilo que faz ser reconhecido...

Discussão do documentário "Privacidade Hackeada" Netflix

()

Dilema: Quero, Posso e Devo?

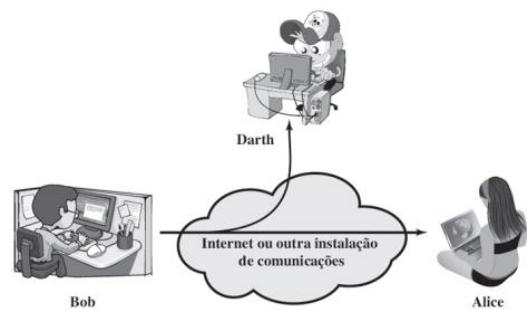
Questões de Ética e Moral



Pilares da Segurança da Informação

1. Confidencialidade
2. Integridade
3. Disponibilidade
4. Autenticidade
5. Não repúdio

Ataques Passivos (Man in the Middle)



Ataques Ativos



Privacidade

quinta-feira, 13 de agosto de 2020 18:59



Documentário "Privacidade Hackeada" Netflix

Snowden

quinta-feira, 13 de agosto de 2020 18:59

Filme "Snowden" vs. "TED"



Pilares e Tipos de Ataques

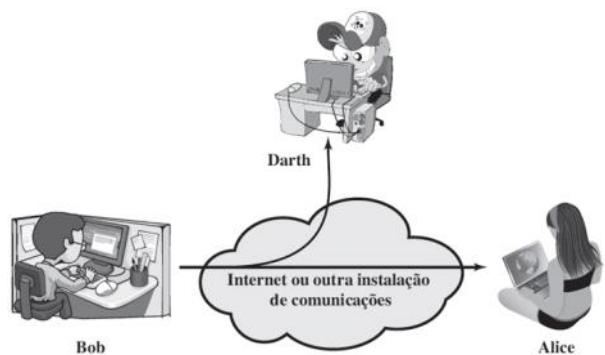
terça-feira, 4 de agosto de 2020 18:42

Pilares da Segurança da Informação

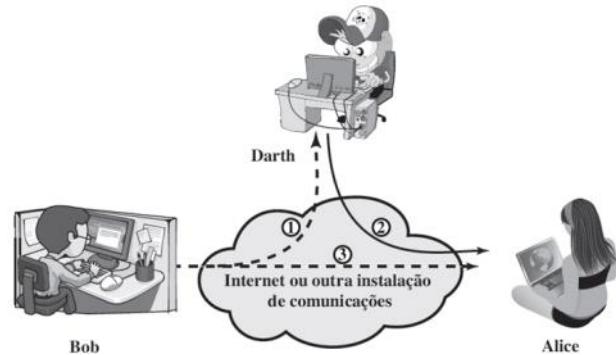
1. Confidencialidade
2. Integridade
3. Disponibilidade

99,9999%

Ataques Passivos (Man in the Middle)

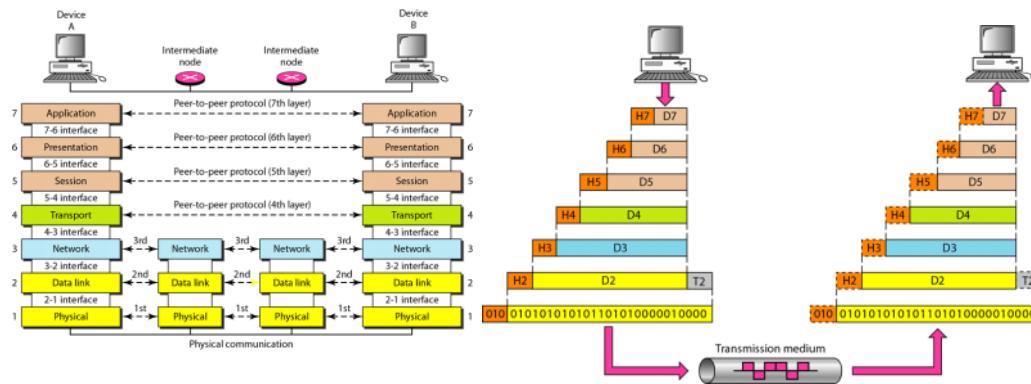
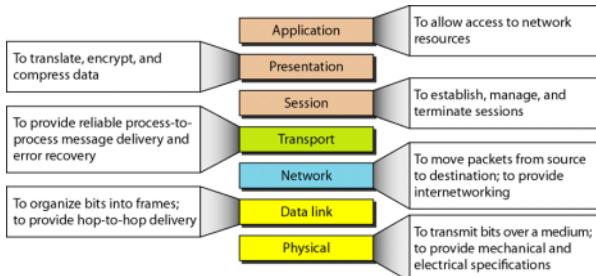


Ataques Ativos



Ordem de encapsulamento em redes TCP/IP.

Foto: Internet/Exemplo

**Encapsulamento**

7, 6 e 5 -> Dados

4 -> Datagrama do usr (UDP) e Segmento (TCP)

3 -> Pacote

2 -> Frame e/ou Quadro

1 -> Sequência de bits

RM-OSI

Aplicação + Apresentação + Sessão -> "DADOS"

Transporte -> TCP = "SEGMENTO", UDP = "DATAGRAMA DO USUÁRIO"

Rede = "PACOTE"

Enlace ou Data Link = "QUADRO" ou "FRAME"

Física = "SEQUÊNCIA DE BITS"

Up - Desencapsulamento

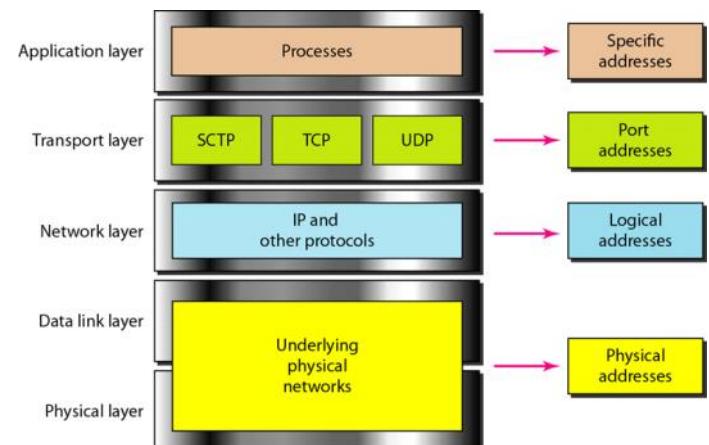
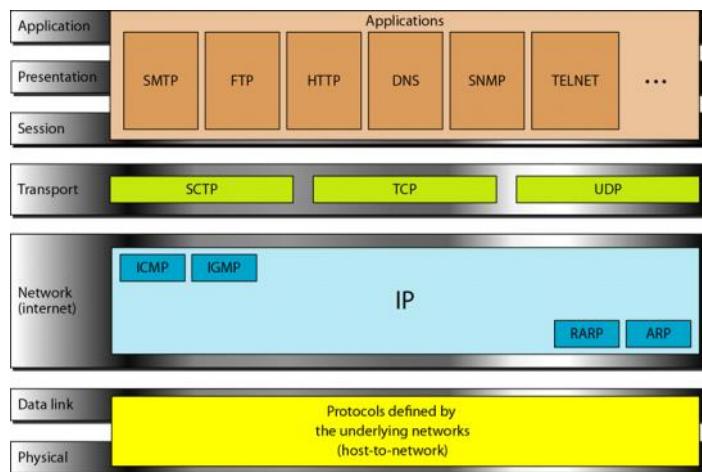
O desencapsulamento é o processo usado por um dispositivo receptor para remover um ou mais cabeçalhos de protocolo. Os dados são desencapsulados à medida que se movem na pilha em direção ao aplicativo do usuário final.

Down - Encapsulamento

O encapsulamento é o processo usado por um dispositivo transmissor para incluir um ou mais cabeçalhos de protocolo. Os dados são encapsulados à medida que se movem na pilha em direção ao meio físico.

TCP/IP vs OSI

quinta-feira, 13 de agosto de 2020 19:13



Uma das codificações mais usadas para resolver esse problema é o UTF-8 (ele pode manipular qualquer ponto de código Unicode). UTF significa "Formato de Transformação Unicode", do inglês "Unicode Transformation Format", e "8" significa que números de 8 bits são usados na codificação.

Introdução à Criptografia (Criptoanálise)

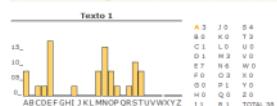
segunda-feira, 17 de agosto de 2020 21:47



<http://numaboa.com.br/criptografia/criptoanalise/309-Ferramenta-de-frequencia>

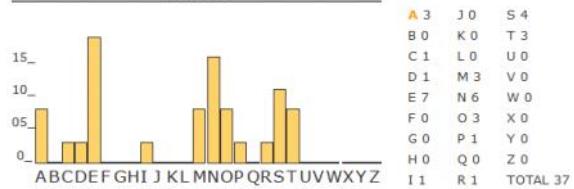
Equipe vencedora do desafio (1 ponto na N2)
Paulo de Tarso
Jonathan Cândido
Luiz Gustavo
Thiago Lemes

ANÁLISE DE FREQUÊNCIA DO TEXTO 1



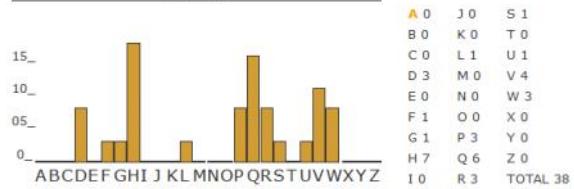
ANÁLISE DE FREQUÊNCIA DO TEXTO 1

Texto 1



ANÁLISE DE FREQUÊNCIA DO TEXTO 2

Texto 2



Criptografia Cifra de César

Deslocamento (substituição) mono alfabetica

Relacionamento 1:1 exemplo: A (+3) = D

BANANA - (+3)

EDQDQD

Ensinaoooo e aprendemos constantemente

Hqvlqdprv#h#dsuhaghprv#frqvwdqwhphqwh

Apresenta a distribuição de frequência da língua portuguesa...

a, e, i, o, u

e → h = 3

OTP (One Time Pad)

<https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher>

<https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/one-time-pad>

<https://irinconada.medium.com/cracking-caesar-cipher-8fe79226aab>

violetas
V|()|_3-|-@\$

banana
8@|/|4/\V/\

Passwords: salvador "5d0|_\\4|)[]/2"
Wi-Fi -> WPA2-Personal -> password >= 8 caracteres...
Brute Force

Criptografia de deslocamento (substituição) polialfabética
Relacionamento: 1:N

Criação de wordlist

sexta-feira, 18 de fevereiro de 2022 20:20

crunch

- a) A parte inicial do ataque consistirá da criação do dicionário (*wordlist*) que conterá as senhas a serem testadas. Já é sabido que a VM Metasploitable2 tem um usuário cujas credenciais (*username* e senha) são, respectivamente, msfadmin e msfadmin. Para efeito desta demonstração, consideraremos já serem conhecidas apenas uma parte da senha e seu tamanho total. Assim sendo, a melhor abordagem para criação da *wordlist* será a *rule-based search*, uma vez que uma parte da senha já é conhecida (digamos, a *string* "msfad"), bem como seu tamanho final (8 caracteres); admitindo-se ainda que os três últimos caracteres que comporão a senha poderão assumir qualquer combinação formada pelos caracteres: m,M,i,I,n,N,0,1,2,3,%,#. Portanto, considerando-se que os **três** últimos caracteres da senha poderão assumir **doze** valores diferentes cada, é possível determinar que esta *wordlist* será composta por 12^3 , ou 1728 diferentes combinações, com 8 caracteres cada, a serem testadas. A criação da *wordlist* poderá ser feita com base na seguinte linha de comando:

#crunch 8 8 mM!nN0123%# -t msfad@ @@ -o wlist.txt

Esta linha instrui o *crunch* para que crie uma *wordlist* chamada *wlist.txt*, a qual deverá ter sua saída gravada na forma de um arquivo, e não simplesmente impressa na tela (-o *wlist.txt*). De acordo com o *template* fornecido, cada senha gerada pela ferramenta terá comprimento igual a 8 caracteres^[1], sendo composta (em sua primeira parte) pelos cinco caracteres da *string* "msfad", complementados por mais três, produzidos pelas possíveis combinações dos caracteres da *string* mM!nN0123%#^[2].

^[1]O primeiro 8 na linha de comando indica o tamanho mínimo da senha, e o segundo, o tamanho máximo, portanto, o tamanho final de cada senha gerada será de 8 caracteres.

^[2]No *template* -t msfad@ @@ cada @ é um *placeholder* a ser substituído por cada um dos caracteres da *string* mM!nN0123%# .

BANANA

Criptoanálise: "Técnicas para decifrar mensagens"

Análise de frequências (dos símbolos)

Análise das palavras

Identificação do idioma de origem

....

BANANA

César chave 3

"EDQPDQT"

Coluna	B	A	N	A	N	A
Linha	C	A	B	R	I	N
Resultante	D	A	O	R	V	N

Texto puro

Chave de criptografia

Técnicas polialfabéticas (LEET)...

$$2^{4096}=1,\#INF$$

$$2^{10}=1.024$$

$$2^{128}=3E38$$

Relacionamento 1:N

Texto Puro	P ₀	P ₁	P ₂	P ₃	P ₄	P ₅
Coluna	B	A	N	A	N	A
Chave	K ₀	K ₁	K ₂	K ₃	K ₄	K ₅
Linha	F	T	T	F	T	T
Cifrado	C ₀	C ₁	C ₂	C ₃	C ₄	C ₅
Resultante	G	T	G	F	G	T

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

Chave pública (próxima aula)

Problema da troca de chaves

Distribuição de chaves

Shamir 80

Protocolo Massey-Omura 82

Diffie-Hellman

Exemplo colab

Ataque de redirecionamento (arp Spoofing)

Man-in-the-middle

KDC (básico)

- Cyber

Diffie-Hellman

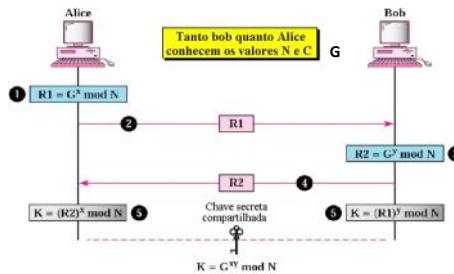
```
G = 17
N = 127
x = 500000
y = 60003222
```

```
R1 = (G*x)%N
R2 = (G*y)%N
```

```
print("R1:", R1)
print("R2:", R2)
```

```
K1 = (R2*x)%N
K2 = (R1*y)%N
```

```
print("K1:", K1)
print("K2:", K2)
```



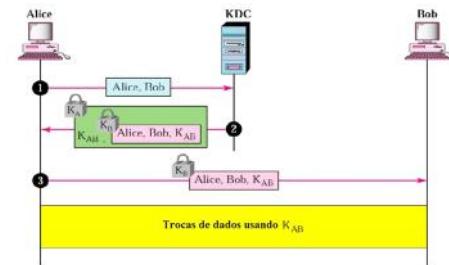
Diffie-Hellman



ARP Spoofing

Exemplo didático:
Protocolo Massey-Omura

- Problema: Alice deseja enviar uma carta confidencial para Bob, usando apenas um baú com cadeado e suas respectivas chaves.



KDC

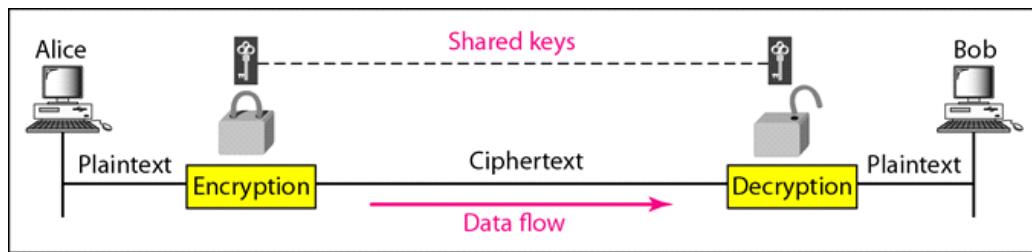
Assuma que $G = 7$ e $N = 23$. As etapas são:

1. Alice escolhe $x = 3$ e determina $R1 = 7^3 \text{ mod } 23 = 21$.
2. Alice envia o número 21 para Bob.
3. Bob escolhe $y = 6$ e determina $R2 = 7^6 \text{ mod } 23 = 4$.
4. Bob envia o número 4 para Alice.
5. Alice determina o valor da chave simétrica $K = 4^3 \text{ mod } 23 = 18$.
6. Bob determina o valor da chave simétrica $K = 21^6 \text{ mod } 23 = 18$.

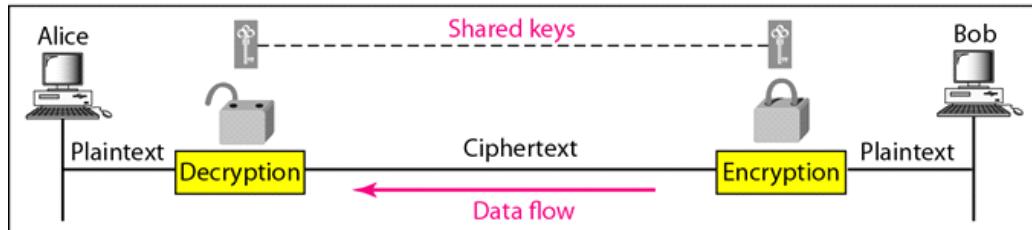
O valor de K é o mesmo tanto para Alice quanto para Bob. Além disso, $G^y \text{ mod } N = 7^{18} \text{ mod } 23 = 18$.

Chave Simétrica

quinta-feira, 3 de setembro de 2020 19:17



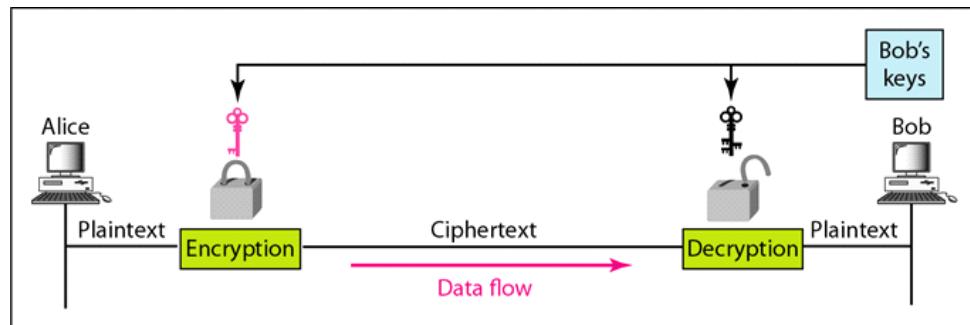
a. A shared secret key can be used in Alice-Bob communication



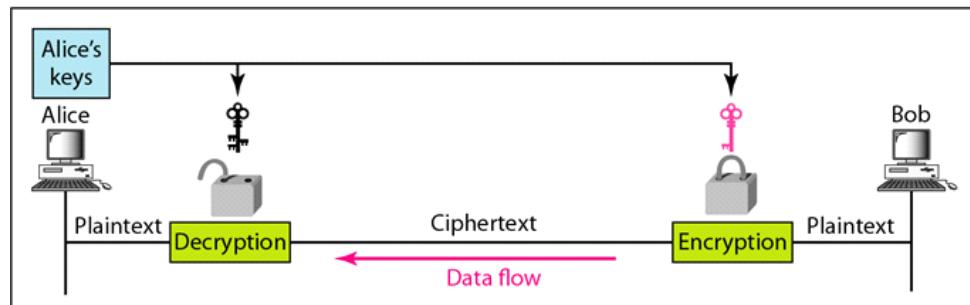
b. A different shared secret key is recommended in Bob-Alice communication

Chave Assimétrica

quinta-feira, 3 de setembro de 2020 19:18



a. Bob's keys are used in Alice-Bob communication



b. Alice's keys are used in Bob-Alice communication

RSA – Criptografia Assimétrica

Prof. Ms. Fábio Henrique Cabrini

RSA Data Security, Inc.

Empresa



RSA Data Security é uma empresa americana que foi comprada pela EMC Corporation em 2012. Sediada em Bedford, Massachusetts, mantém escritórios na Irlanda, Reino Unido, Singapura e Japão.

Anteriormente era designada de Security Dynamics, que a adquiriu em 1996 e à DynaSoft AB em 1997.



[Wikipedia](#)



[Site oficial](#)



[YouTube](#)

Fundado em: 1986

Data de aquisição: 29 de jun. de 2006

Sede: Bedford, MA

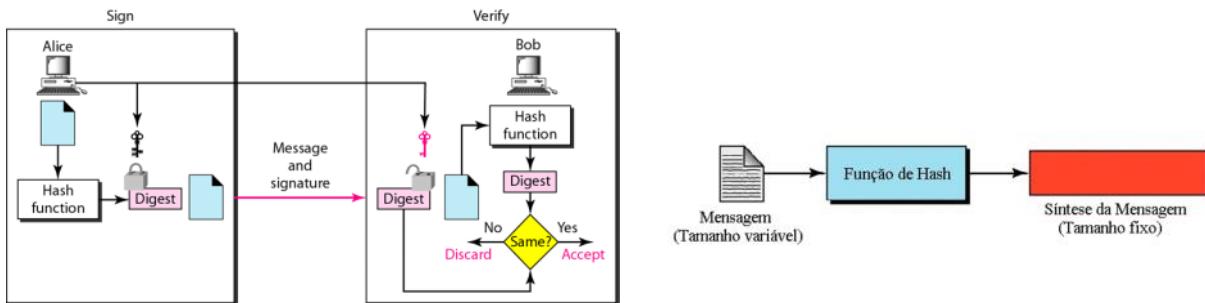
Fundadores: Ronald Rivest · Adi Shamir · Leonard Adleman



Figura 1. Charge

O RSA é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto de Tecnologia de Massachusetts (MIT), Ronald Rivest, Adi Shamir e Leonard Adleman, fundadores da atual empresa RSA Data Security, Inc., que inventaram este algoritmo — até a data (2008) a mais bem-sucedida implementação de sistemas de chaves assimétricas, e fundamenta-se em teorias clássicas dos números. É considerado um dos mais seguros, já que mandou por terra todas as tentativas de quebrá-lo. Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital e uma das grandes inovações em criptografia de chave pública. ([wikipedia.org](#))

<http://educacao.globo.com/matematica/assunto/matematica-basica/mmc-e-mdc.html>

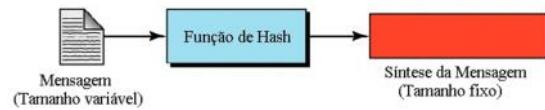


A assinatura digital é utilizada para garantir autenticidade e a integridade de um documento digital. Utiliza a criptografia assimétrica (RSA) e algoritmos de Hash.

Função Hash é um recurso utilizado para a verificação da integridade... Ela é uma função unidirecional (ela não poder ser revertida!) que gera a síntese (resumo) de tamanho fixo.

Exemplos de funções Hash: MD5, SHA-1, SHA256... SHA512

"A síntese é escrita em Hexadecimal..."

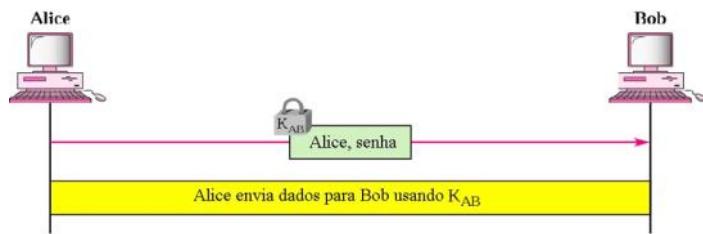


Exemplo realizado no Ubuntu

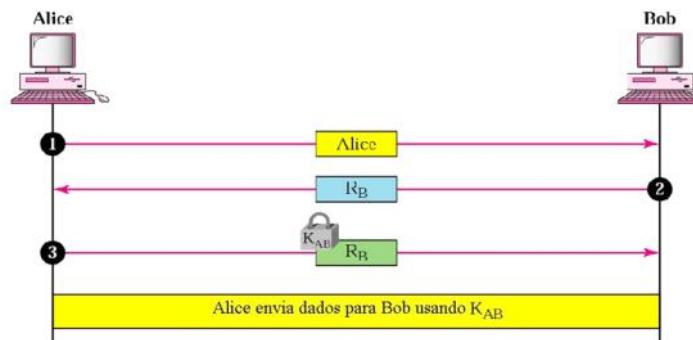
```
cabrini@ThinkPad:~$ sha1sum ec10.txt
b1f61c745acf1d711d02ce169a75ac00b050bc31 ec10.txt
cabrini@ThinkPad:~$ sha256sum ec10.txt
cbf39d01c5c673ba203ad3796be13af4b82de5ecbc1ec873aceabf0ae2a8
f733 ec10.txt
cabrini@ThinkPad:~$ sha512sum ec10.txt
2aab9fcf8a31a88cc9ec34ee34eb70effd79497f8baa796cd2c81126d70c
f339b3d5599c3ad79b57ea9bdffd0cdb3f1ba685452f6602d44b66a3f2b0
328028f1 ec10.txt
```

Processos de Autenticação

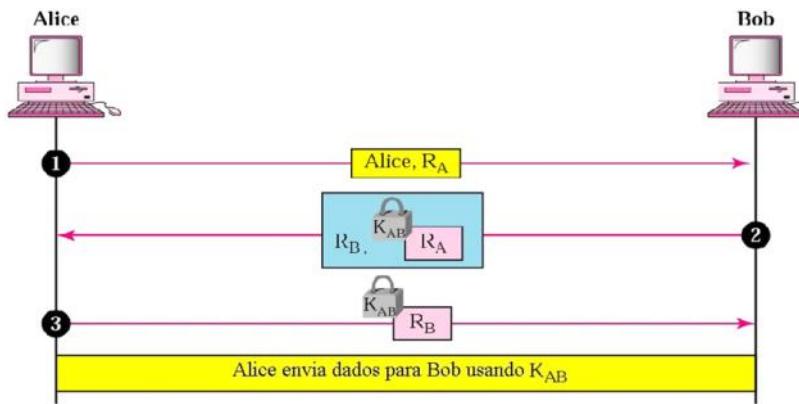
quinta-feira, 3 de setembro de 2020 19:35



Autenticação utilizando apenas chave simétrica



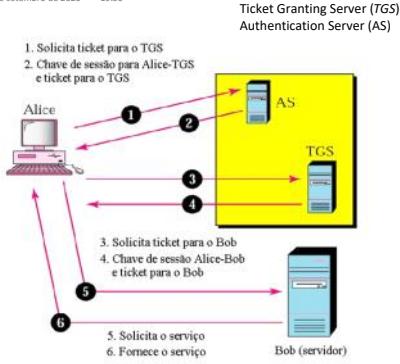
Autenticação por desafio (nonce)



Autenticação bidirecional com desafio (nonce)

Kerberos

quinta-feira, 3 de setembro de 2020 19:56

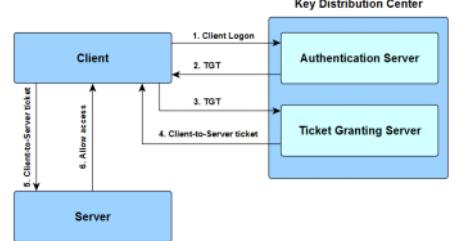
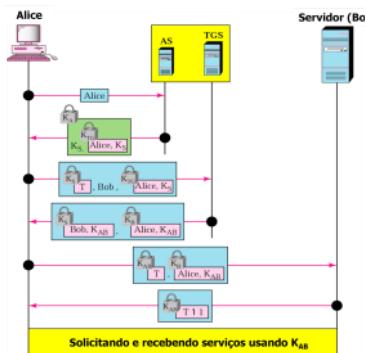


Fonte: <https://web.mit.edu/kerberos/>

Há necessidade de um servidor NTP (Network Time Protocol)
É desejável que haja políticas de segurança aplicadas aos sistemas clientes...
(Exemplo: no Windows 10 em ambiente corporativo o usuário não tem autorização para realizar alteração da hora/data.)

NTP/NTS são recursos importantes para perícia forense "A Ciência Forense é compreendida como o conjunto de todos os conhecimentos científicos e técnicas que são utilizados para desvendar crimes ciberneticos"

Perícia Forense



A estrutura Kerberos tem o objetivo de garantir a autenticação de usuários, contas de serviço e assim por diante. Para que ocorra a permissão de acesso, mais fatores são levados em conta, entre eles podemos destacar as ACLs, configuradas nas guias de segurança de processos e objetos.

https://wiki.samba.org/index.php/Running_a_Samba_AD_DC_with_MIT_Kerberos_KDC



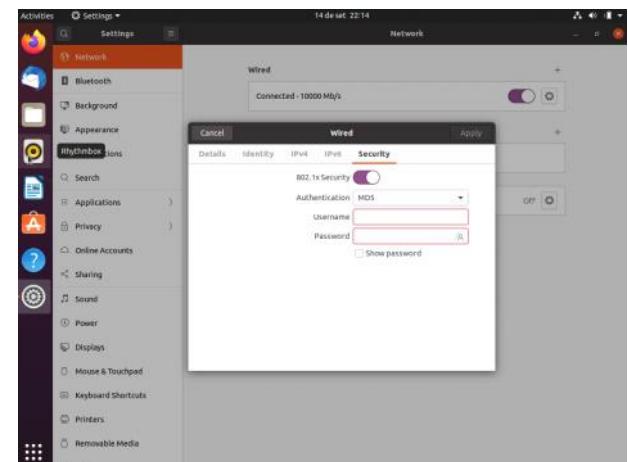
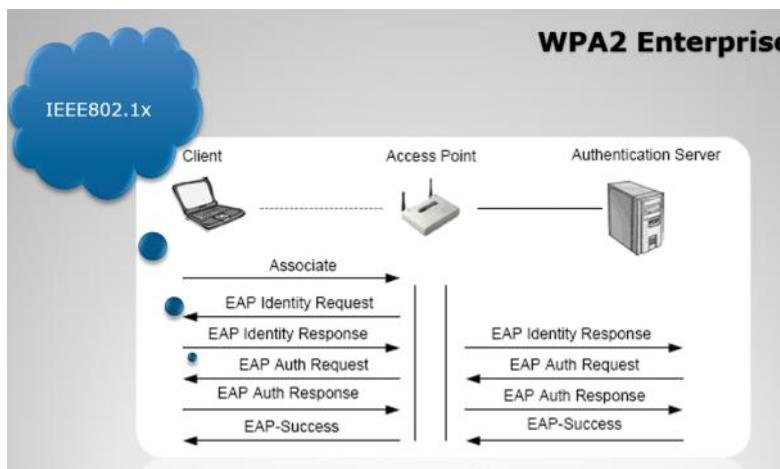
BYOD (Bring Your Own Device)

“Traga seu próprio dispositivo”

COPE (Corporate-Owned, Personally Enabled)

“Propriedade da corporação, habilitado para uso pessoal”

Itens	BYOD	COPE
Propriedade	Pessoal	Corporação
Propriedade do software	usuário	Corporação
Software específicos	Corporação	Corporação
Controle de Atualizações	Não	Sim
Definição do hardware	Não	Sim
Controle remoto das políticas de segurança	Não	Sim
Custo de propriedade do hardware	Menor	Maior
Curso de propriedade de software	Não	Elevado
Infraestrutura de segurança	Robusta	Adequada
Manutenção	Não	Sim

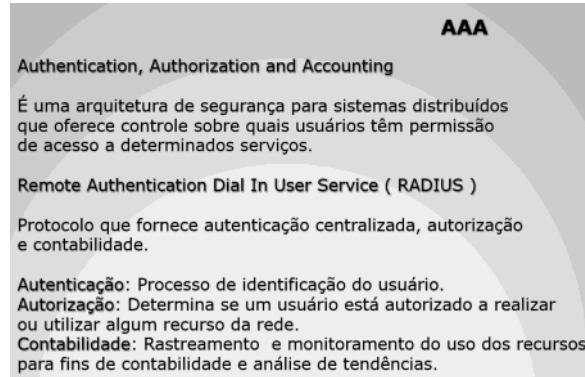
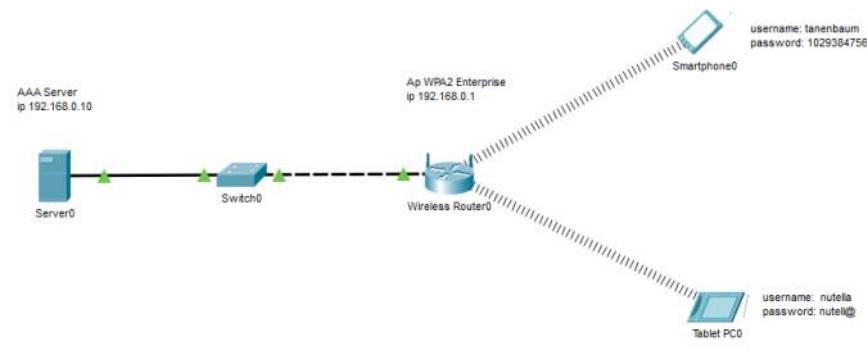


IEEE802.11i



WPA2-Enterprise	WPA2-Personal
Each user is assigned unique credentials	Unmanaged mode for authentication using PSK allows use of a manually entered passphrase, which typically is shared by users of that network
IEEE 802.1X AAA server with EAP support and authentication database required	No authentication server required
Data security keys are unique for each session	Data security keys are unique for each session
Wi-Fi CERTIFIED client devices with WPA2-Enterprise EAP type 1 EAP type 2 EAP type 3	Wi-Fi CERTIFIED client devices with WPA2-Personal Wi-Fi CERTIFIED access point supporting WPA2/EAP
IEEE 802.1X AAA server supporting EAP	IEEE 802.1X AAA server supporting EAP
Authentication database	Authentication database

WPA2 Enterprise

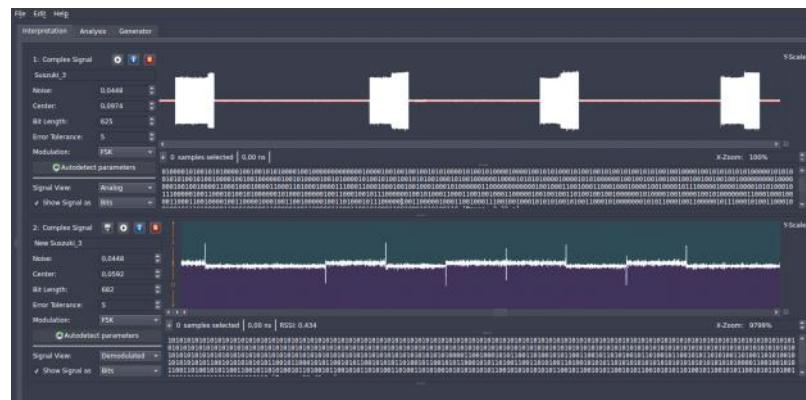


Jammer

sexta-feira, 4 de março de 2022 18:51

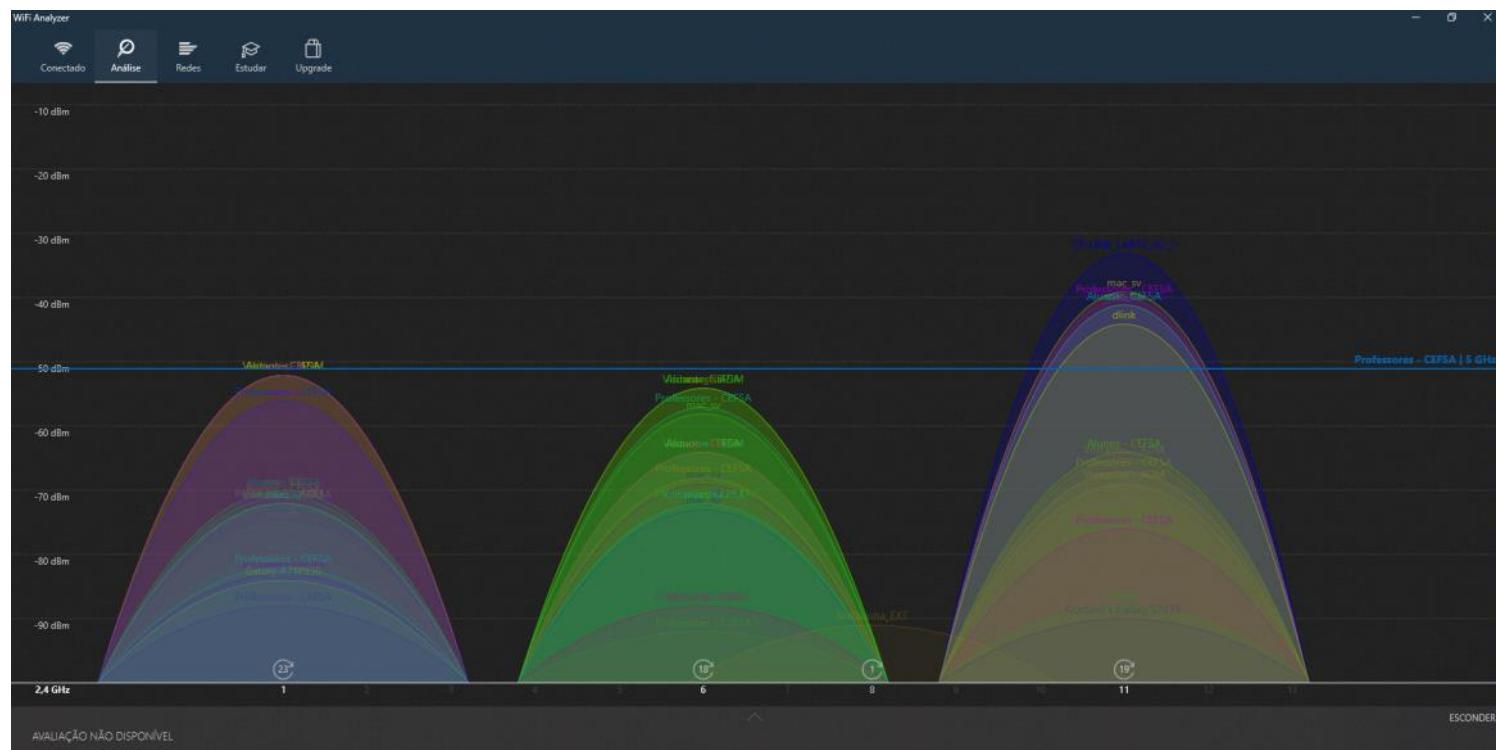
<https://hacking.org/universal-radio-hacker-investigate-wireless-protocols-like-a-boss/>

Universal Radio Hacker



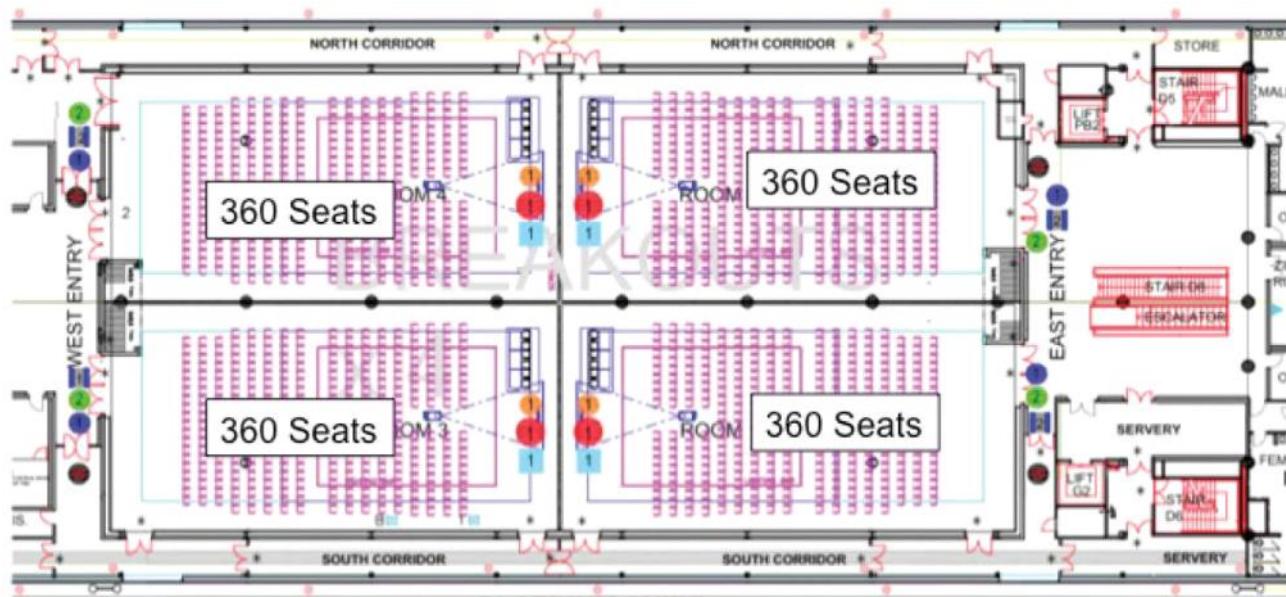
Vlans no Wi-Fi

quinta-feira, 10 de março de 2022 21:29



Ambientes de Alta densidade - Complementar

terça-feira, 8 de setembro de 2020 12:22



Requirements - Complementar

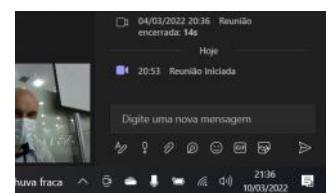
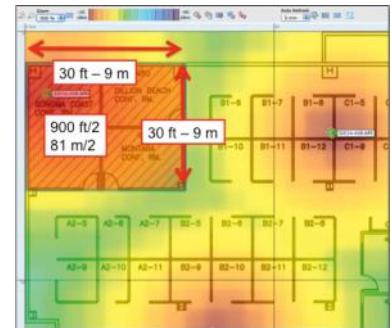
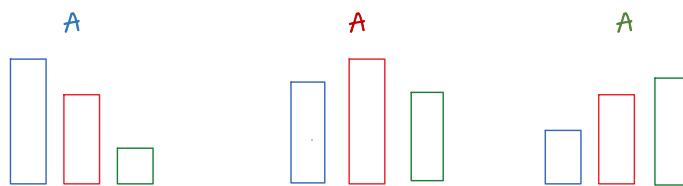
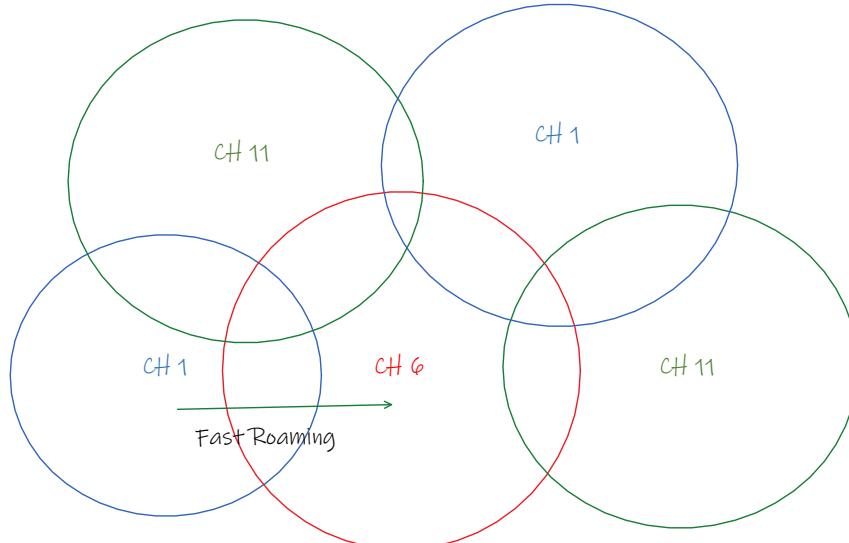
terça-feira, 8 de setembro de 2020 12:24

Table 1. Bandwidth Requirements per Application

Application by Use Case	Nominal Throughput
Web - Casual	500 kilobits per second (Kbps)
Web - Instructional	1 Megabit per second (Mbps)
Audio - Casual	100 Kbps
Audio - Instructional	1 Mbps
On-demand or Streaming Video - Casual	1 Mbps
On-demand or Streaming Video - Instructional	2-4 Mbps
Printing	1 Mbps
File Sharing - Casual	1 Mbps
File Sharing - Instructional	2-8 Mbps
Online Testing	2-4 Mbps
Device Backups	10-50 Mbps

Fonte: material da Cisco, disponível na pasta do professor
"Wireless LAN Design Guide for
High Density Client Environments
in Higher Education"

Overlapping
Co-channel

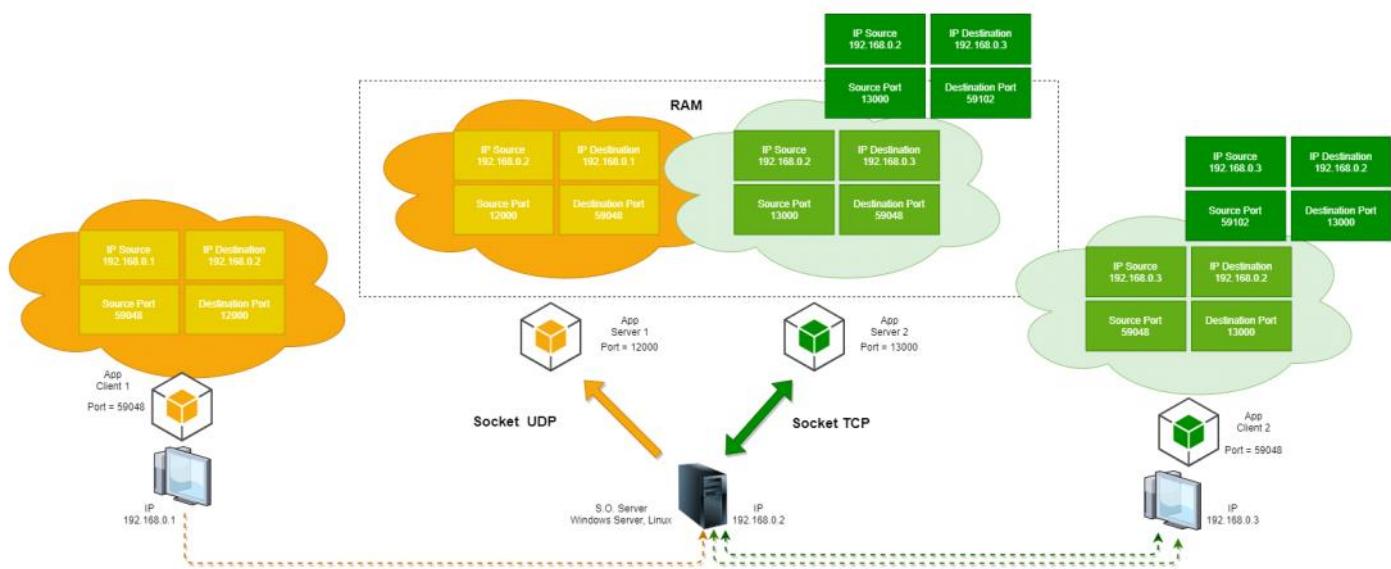


Qual a vantagem de utilizar uma densidade maior de access point Wi-Fi?

Resposta: Melhorar o Fast Roaming, velocidade de acesso, balanceamento de carga, qualidade do serviço (QoS) e qualidade de experiência do usuário (QoE)

NMAP Revisão Socket TCP + UDP

terça-feira, 11 de agosto de 2020 22:52

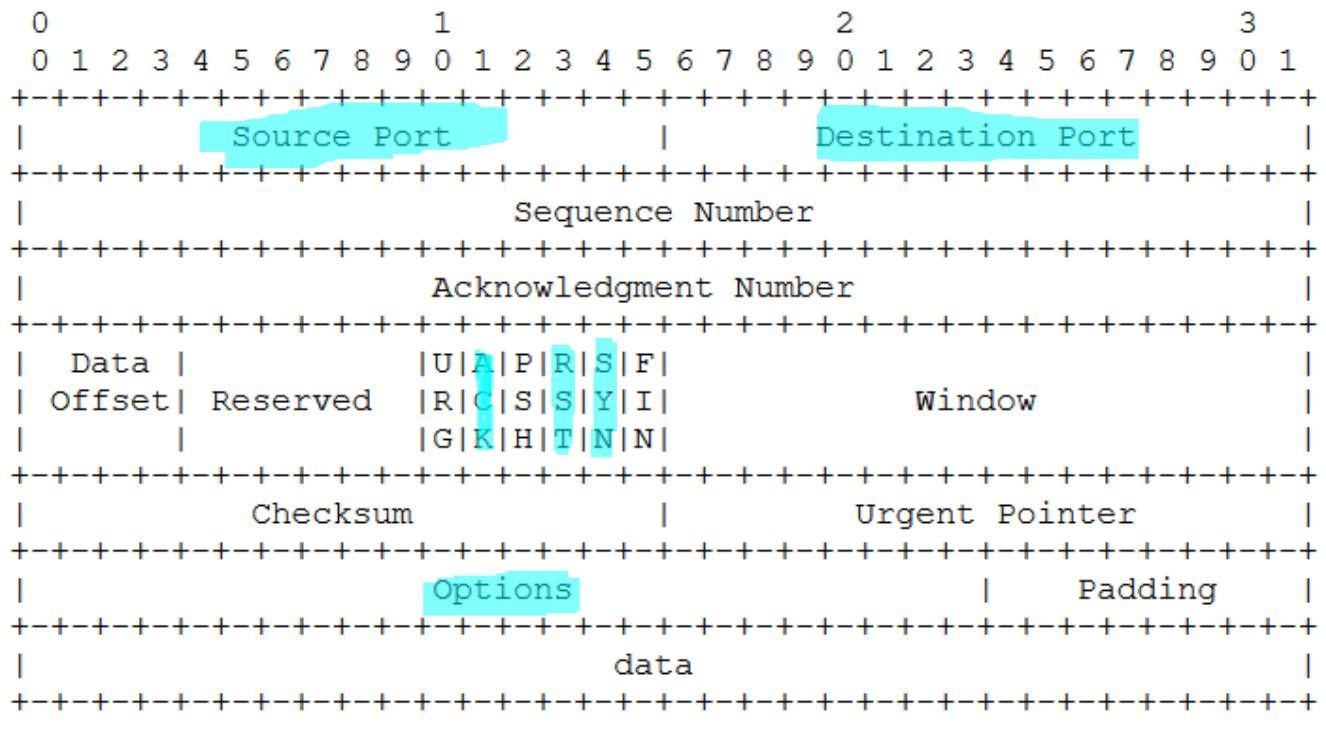


NMAP Introdução ao protocolo TCP

quinta-feira, 13 de agosto de 2020 21:48

TCP - Transmission Control Protocol

TCP Header Format



TCP Header Format

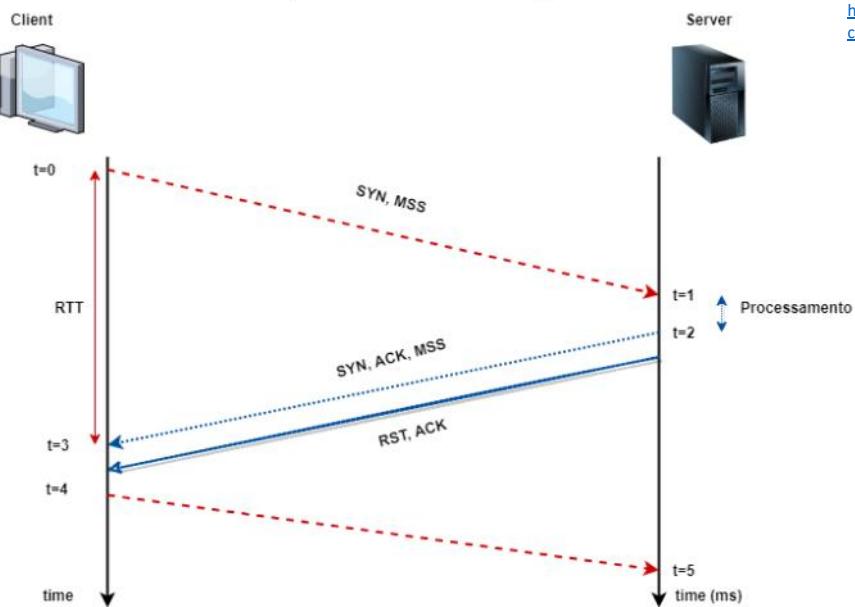
Note that one tick mark represents one bit position.

NMAP TCP Fluxo de Dados + 3way-handshake

quinta-feira, 13 de agosto de 2020 21:59

Source	Destination	Protocol	Length	Info
127.0.0.1	127.0.0.1	TCP	56	58371 → 12500 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
127.0.0.1	127.0.0.1	TCP	56	12500 → 58371 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
127.0.0.1	127.0.0.1	TCP	44	58371 → 12500 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
127.0.0.1	127.0.0.1	TCP	58	58371 → 12500 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=14
127.0.0.1	127.0.0.1	TCP	44	12500 → 58371 [ACK] Seq=1 Ack=15 Win=2619648 Len=0
127.0.0.1	127.0.0.1	TCP	58	12500 → 58371 [PSH, ACK] Seq=1 Ack=15 Win=2619648 Len=14
127.0.0.1	127.0.0.1	TCP	44	58371 → 12500 [ACK] Seq=15 Ack=15 Win=2619648 Len=0
127.0.0.1	127.0.0.1	TCP	44	12500 → 58371 [FIN, ACK] Seq=15 Ack=15 Win=2619648 Len=0
127.0.0.1	127.0.0.1	TCP	44	58371 → 12500 [ACK] Seq=15 Ack=16 Win=2619648 Len=0
127.0.0.1	127.0.0.1	TCP	44	58371 → 12500 [FIN, ACK] Seq=15 Ack=16 Win=2619648 Len=0
127.0.0.1	127.0.0.1	TCP	44	12500 → 58371 [ACK] Seq=16 Ack=16 Win=2619648 Len=0

3-Way Handshake - Setup



<https://rodrigolira.eti.br/nmap-30-exemplos-de-comandos-para-administradores-de-rede/>

Como mitigar ataques a serviços críticos, exemplo
SSH:

How to Use Port Knocking on Linux (and Why You Shouldn't)

DAVE MCKAY @thegeukita
OCTOBER 9, 2019, 9:00AM EDT



Photographie.eu/Shutterstock



<https://www.howtogeek.com/442733/how-to-use-port-knocking-on-linux-and-why-you-shouldnt/>

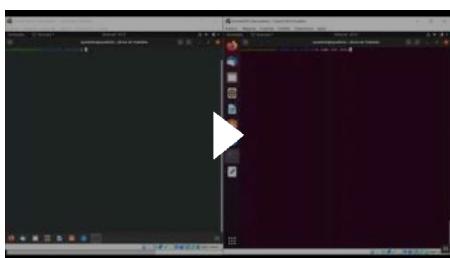
```
import socket,sys
ip = input("Target: ")
startport = int(input("Start port: "))
stopport = int(input("Stop port: "))
for ports in range(startport, stopport):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    if s.connect_ex((ip, ports)) == 0:
        print ("Port ",ports," Open ")
s.close()
```

Exemplo TCP sobre o IPV4

50 TCP	50 21 → 54873 [SYN, ACK] Seq=0 Ack=1 Win=64
51 TCP	54 54873 → 21 [ACK] Seq=1 Ack=1 Win=131328 ..
51 TCP	54 54873 → 21 [FIN, ACK] Seq=1 Ack=1 Win=13..
92 FTP	114 Response: 220 ProFTPD 1.3.5e Server (De..
51 TCP	54 54873 → 21 [RST, ACK] Seq=2 Ack=61 Win=0..
92 TCP	54 21 → 54873 [FIN, ACK] Seq=61 Ack=2 Win=6..

Hardening: É processo para mitigar possíveis vulnerabilidades no sistema operacional

[Hardenização de conexões SSH com o Knockd \(Port Knocking\)](#)



nmap

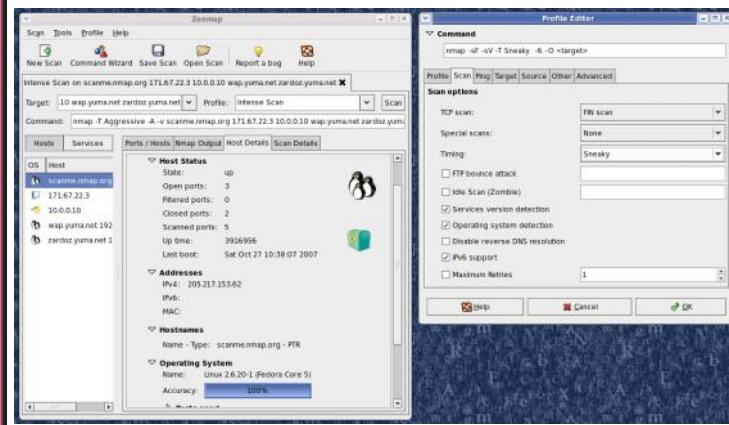
terça-feira, 15 de setembro de 2020 11:52

<https://nmap.org>

```
# nmap -A -T4 scanme.nmap.org d0ze
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp   Postfix smtpd
53/tcp    open  domain ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http   Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

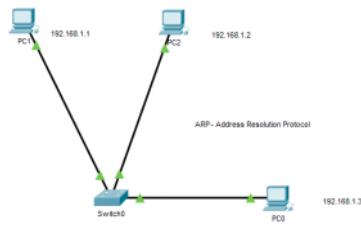
Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     Serv-U ftpt 4.0
25/tcp    open  smtp   IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http   Microsoft IIS webserver 5.0
110/tcp   open  pop3  IMail pop3d 7.15 931-1
135/tcp   open  mstask Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc  Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```





Topologia Física



Topologia lógica

ARP (Address Resolution Protocol) é um protocolo auxiliar do IPv4.

NDP (Neighbor Discovery Protocol) é um protocolo auxiliar do IPv6.

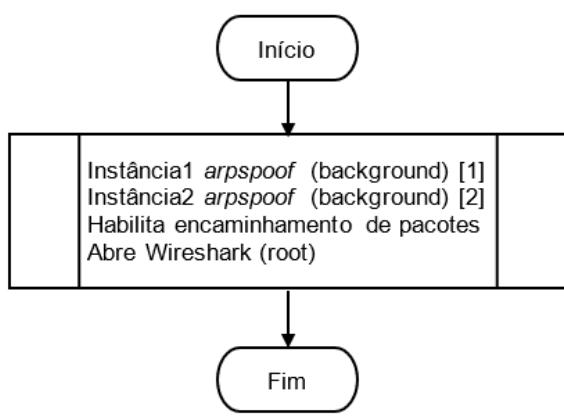
ARP Poisoning ---> IPv4



Tabela ARP ela fica armazenada nos end devices. Ela pode ser dinâmica ou estática. Ela faz a relação entre MAC Address e IPv4.

Prompt de Comando			
Microsoft Windows [versão 10.0.19042.804] (c) 2020 Microsoft Corporation. Todos os direitos reservados.			
C:\Users\fabio>arp -a			
Interface:	169.254.11.111 --- 0x6		
Endereço IP	Endereço físico		Tipo
224.0.0.22	01-00-5e-00-00-16		estático
224.0.0.251	01-00-5e-00-00-fb		estático
224.0.0.252	01-00-5e-00-00-fc		estático
239.255.255.250	01-00-5e-7f-ff-fa		estático
239.255.255.253	01-00-5e-7f-ff-fd		estático
255.255.255.255	ff-ff-ff-ff-ff-ff		estático

Tabela CAM (Content Address Memory) ela fica armazenada no switch e tem a função de relacionar MAC Address com as portas do respectivo switch.



```

[1] #!/bin/bash
[2] # script para man in the middle
[3] clear
[4] arpspoof -t 192.168.33.20 192.168.33.18 &
[5] arpspoof -t 192.168.33.18 192.168.33.20 &
[6] echo 1 > /proc/sys/net/ipv4/ip_ps
[7] /usr/bin/wireshark
  
```



Instalação do arpspoof

```

[1]#apt-get update
[2]#apt-get install -y dsniff
[3]#arp -na
  
```

<https://www.youtube.com/watch?v=WncLhfCE4TM&t=21s>

De <<https://teams.microsoft.com/multi-window/?agent=electron&version=20200916030>>

ARP Poisoning
By Nicolas Henrique Carissimo

Brute Force

quinta-feira, 18 de março de 2021 21:21

Rockyou.txt faz parte do Sistema Operacional Kali

Tipo de ataque	Descrição
Dictionary Attacks	Basicamente, os dicionários consistem de arquivos texto contendo informações a serem testadas pelo atacante, por meio de ferramentas especializadas, contra os mecanismos de autenticação do serviço (por exemplo, SSH). São essencialmente grandes listas com potencias <i>usernames e/ou senhas.</i> Nesta modalidade, o ataque se encerra quando as credenciais do usuário são descobertas ou quando a lista é esgotada.
Search Attacks	Nesta modalidade, são testadas todas as combinações possíveis de um determinado conjunto de caracteres, considerando-se também a possível faixa de variação do comprimento da senha. Este ataque pode consumir muito tempo, dada a grande quantidade de combinações possíveis para descoberta da senha.
Rule-based search attacks	Este tipo de ataque usa regras específicas para gerar as possíveis variações que compõem a senha, como por exemplo, a partir do <i>username</i> ou do nome da empresa, e ainda, fixando uma parte da senha e variando outra parte com base em máscaras pré-determinadas.

Quadro 4 – Tipos de ataques por força bruta.

Fonte: www.ibm.com/support/knowledgecenter.



```
rockyou.txt  simulador_contador.py  0% 16693 jeroen  
16694 jennifer  
16695 jecjec  
16696 jaylene  
16697 jamesd  
16698 irule  
16699 inverness  
16700 imsingl  
16701 imoet  
16702 ilovedance  
16703 ilikecheese  
16704 idiot  
16705 ice-cream  
16706 hottie07  
16707 horses2  
16708 heydude  
16709 hello9  
16710 heavensent  
16711 harold1  
16712 hannah3  
16713 greggy  
16714 green15  
16715 gordol  
16716 golosa  
16717 generals  
16718 garrison  
16719 gamaliel  
16720 gallegos  
16721 gabvteamo
```

admin\$#xCD

adminYioXs

admin|ZADRW

THC HYDRA

```
sudo apt install hydra -y
```

```
hydra -l cabrini -P wordlist_manual.txt -V -f -t 4 143.107.145.51 ftp
```

-V verbose

-f para assim que encontra a senha

-t Threads

-l username / -L wordlist username

-P word list

O primeiro 8 na linha de comando indica o tamanho mínimo da senha, e o segundo, o tamanho máximo, portanto, o tamanho final de cada senha gerada será de 8 caracteres.
 [1] No template -t msfadbdbdb cada dbd é um placeholder a ser substituído por cada um dos caracteres da string mMIMIND123%#.

```
sudo apt install crunch -y
```

```
crunch 8 8 mMIMIND123%# -t msfadbdbdb -o wlist.txt
```

```
sudo apt install hydra -y
```

```
sudo apt install crunch -y
```



Recurso para evitar ataques de brute force

Verificação de segurança

Por razões de segurança, precisamos verificar se os detentores da conta são pessoas reais.

Digite os caracteres que você vê na imagem abaixo



Enviar

Códigos Maliciosos (Vírus)

segunda-feira, 5 de abril de 2021 20:38

Códigos Maliciosos						
	Vírus	Worm	Bot	Trojan	Spyware	Backdoor
Como é obtido:						
Recebido automaticamente pela rede	✓	✓				
Recebido por e-mail	✓	✓	✓	✓	✓	
Baixado de sites na Internet	✓	✓	✓	✓	✓	
Compartilhamento de arquivos	✓	✓	✓	✓	✓	
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓	
Redes sociais	✓	✓	✓	✓	✓	
Mensagens instantâneas	✓	✓	✓	✓	✓	
Inserido por um invasor	✓	✓	✓	✓	✓	✓
Ação de outro código malicioso	✓	✓	✓	✓	✓	✓
Como ocorre a instalação:						
Execução de um arquivo infectado	✓					
Execução explícita do código malicioso		✓	✓	✓	✓	
Via execução de outro código malicioso					✓	✓
Exploração de vulnerabilidades	✓	✓			✓	✓
Como se propaga:						
Insere cópia de si próprio em arquivos	✓					
Envia cópia de si próprio automaticamente pela rede		✓	✓			
Envia cópia de si próprio automaticamente por e-mail	✓	✓				
Não se propaga				✓	✓	✓
Ações maliciosas mais comuns:						
Altera e/ou remove arquivos	✓		✓	✓		✓
Consume grande quantidade de recursos		✓	✓			
Furta informações sensíveis			✓	✓	✓	
Instala outros códigos maliciosos	✓	✓	✓	✓		✓
Possibilita o retorno do invasor					✓	✓
Envia spam e phishing			✓			
Desfera ataques na Internet		✓	✓			
Procura se manter escondido	✓				✓	✓

Tabela 4.1: Resumo comparativo entre os códigos maliciosos.



<https://cartilha.cert.br/livro/>

Características da Avaliação - N2

- Data **25/3**
- Vista **31/3**
- impressa
- Individual
- Sem consulta

1. Port Scanner (NMAP) Socket (TCP/UDP), Webserver (apache 2) porta 80/TCP, 53/UDP, focar no processo de 3-way handshake (TCP) Aberta (SYN + ACK) ou Fechada (RST + ACK), sobre UDP (quando a porta está aberta não há nenhum tipo de mensagem sendo enviada para a origem... Apenas quando tentamos acessar uma porta UDP fechada a origem recebe uma mensagem ICMP Destino inalcançável...)
2. Segurança no Wi-Fi, tipos de autenticação (WPA2/3 Personal) e (WPA2/3 Enterprise), AAA (Autenticação, Autorização e Contabilização), Microsoft AD, SAMBA4... Ou RADIUS. EAP (Extensible Authentication Protocol) ... IEEE802.1x (WPA2/3 Enterprise)
3. IEEE802.1x que os sistemas operacionais em grande maioria disponibiliza esse mecanismo para autenticação de camada 2 (enlace). Windows, Linux, IOS, Android, ... (Wi-Fi ou Ethernet)
4. Assinatura Digital ficar atento ao uso das chaves no processo de geração da síntese (hash) observar que é utilizada chaves assimétricas ao exemplo do RSA.
5. RSA é uma técnica de criptografia Assimétrica... Atenção as etapas para a geração das chaves privada/pública.
6. KDC Centros de Distribuição de chaves, ficar atento as características desse recurso, lembrar que o diagrama estudado é um diagrama genérico... Kerberos ... Deve haver uma cadeia de confiança!
7. Diffie-Hellman troca de chaves simétricas, foco é a realização do cálculo da chave.
8. Man-in-the-Middle (MITM) podem ser passivos ou ativos, sendo que as ferramentas mais utilizadas para coleta de informações são o Wireshark (gráfico) e o TCPDump (console)...
9. Exercício de criptoanálise! (Cifra Caesar)
10. Afirmações sobre criptografia... Caesar, Vigenère, Hill, RSA, AES (Cifra de Bloco) ...
Só existe uma alternativa correta!
10 obrigatorias...

Características da Avaliação - N2

- Data **30/3**
- Vista 6/4
- impressa
- Grupo
- Consulta liberada
- Formato CTF (Capture the Flag) + PenTest



1. **Bexiga Branca:** Identificação do Access Point e quebra do mecanismo WPA2 Personal através da técnica de brute force utilizando interceptação do handshake pelo AirCrack (Kali Linux), utilizar a Wordlist Rockyou.txt

Coletar as seguintes informações:

SSID: N2EC10

Canal: _____

BSSID: _____

Canal (frequência 2G ou 5G): 2.4G

Técnica de criptografia: WPA2 – Personal

Password: _____



2. **Bexiga vermelha:** Localizar o Target (servidor Linux) com o seguinte finger print utilizando o nmap.

Open ports -> 22 (SSH) e 80 (HTTP)

Gerar uma wordlist com base na técnica de webcrawler, utilizando o pipeline Linux ou o programa desenvolvido na linguagem de sua preferência.

Realizar o ataque de brute force utilizando o Hydra direcionado ao serviço SSH (Secure Shell) porta 22 e utilizar a wordlist gerada na etapa anterior. O usuário alvo será "aluno".



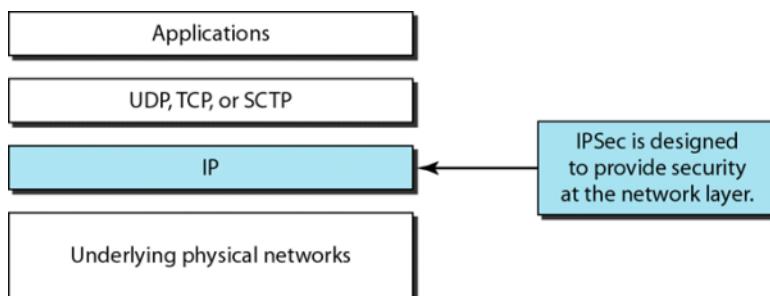
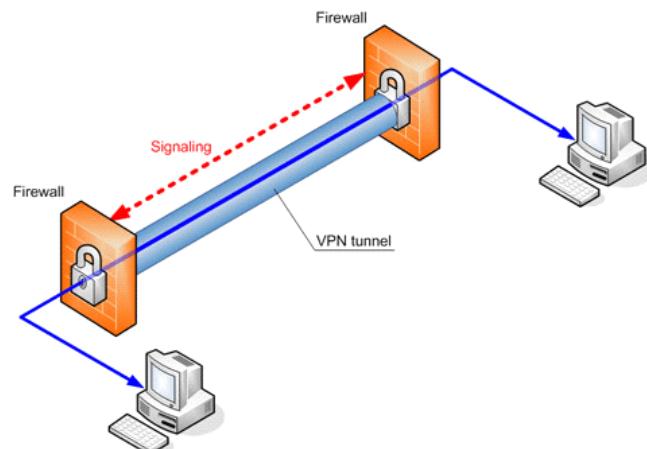
3. Bexiga Preta: Entrar no usuário "cabrini" que pertence ao sudo users utilizando técnicas de Engenharia Social criptograma (tatuagem), informações coletadas do instagram, facebook e linkedin. Inserir o nome da equipe na página web localizada no servidor!

□ △ ○ ↗ ↑ ○ ○ ↘ ↙

VPN I - (Virtual Private Network)

quinta-feira, 8 de outubro de 2020 19:18

IPSec (IP Security) IPV4/IPV6 -
Transmissão de dados criptografada entre end devices através da camada de rede.

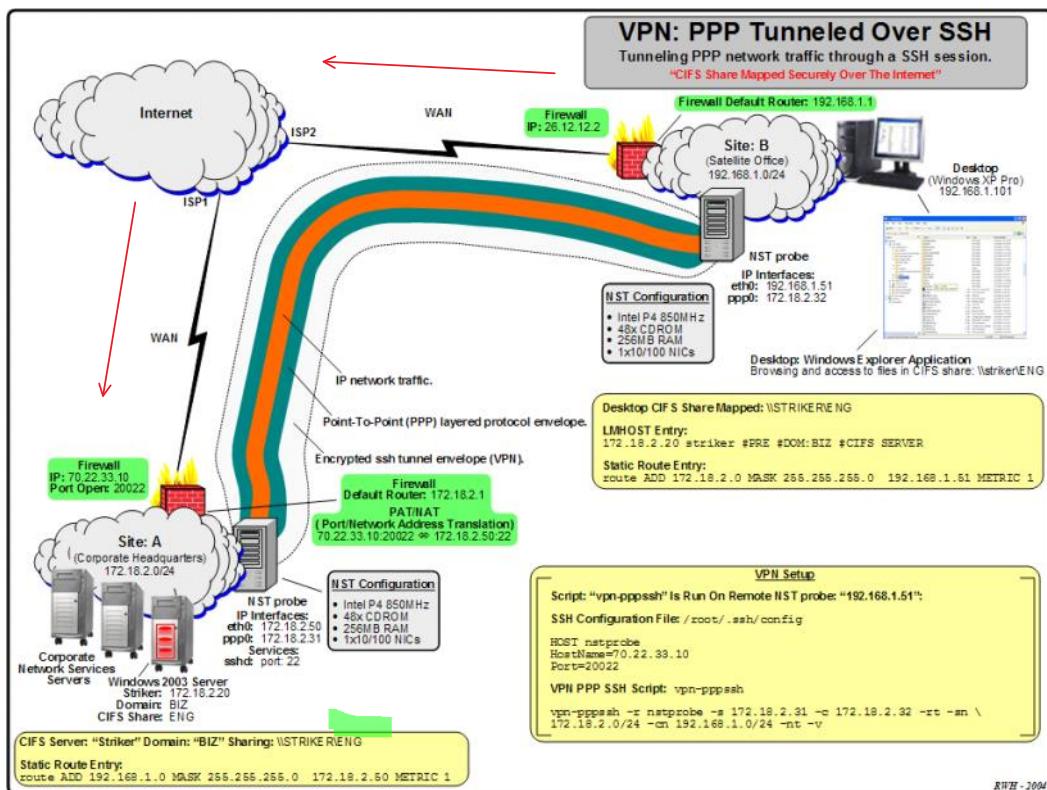


História:

O TLS (Transport Layer Security) é um padrão proposto pela IETF (Internet Engineering Task Force), definido pela primeira vez em 1999, e a versão atual é o TLS 1.3 definido no RFC 8446 (agosto de 2018). O TLS baseia-se nas especificações SSL (Secure Socket Layer) anteriores (1994, 1995, 1996) desenvolvidas pela Netscape Communications[5] para adicionar o protocolo HTTPS ao navegador da Web Navigator.

VPN II - Cenário Modo Túnel

quinta-feira, 8 de outubro de 2020 19:28



Pontos importantes

1. Uso de links simétricos

Site B Upload (100Mbps)

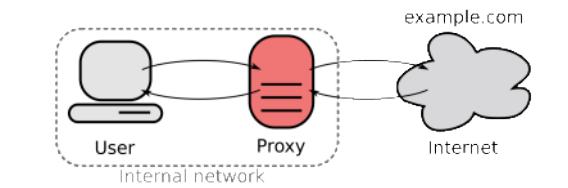
Site A Download (20Mbps)

Proxy Server

Em redes de computadores, um **proxy** (em português 'procurador', 'representante') é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.

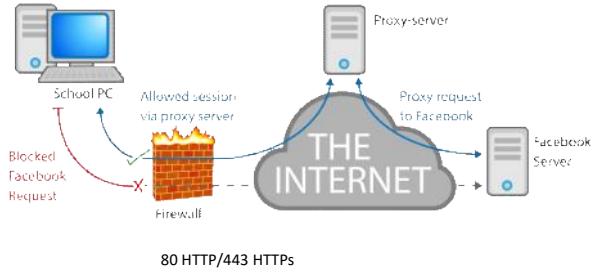
Um cliente conecta-se ao servidor proxy, solicitando algum serviço, como um arquivo, conexão, página web ou outros recursos disponíveis de um servidor diferente, e o proxy avalia a solicitação como um meio de simplificar e controlar sua complexidade.

<http://www.squid-cache.org/>



Características do Servidor:

- Rápido (multiprocessada, placas de redes de alto desempenho, SSD, SGBDs)



URL

<http://domínio:porta/endereço/objeto>
<http://playboy.com.br/fotos/mulher.jpg>

WWW

Header	Payload	Dados
--------	---------	-------

Funções:

- Inspeção do conteúdo** (header e/ou payload) que está sendo transmitido na rede.
- ACLs (Access Control List) - Black List / White List
 - Palavra chave (radicais de palavras) "cu", palavras "palavrão", frases....
 - URL
 - Domínios
 - Categoria de conteúdo
- Acesso anônimo
- Cache (armazenamento do histórico de navegação de cada usuário conectado) aproximadamente 30% de melhoria no desempenho. (HDSL e/ou ISDN)
- Vinculado a um servidor de autenticação (Microsoft AD / SAMBA4 Linux/Unix, username/password (proxy))
- Regras de uso baseadas em username/password, horário de utilização, ip, MAC. (evitar flash crowds "surtos de demanda")
- Estatísticas de acesso

Squid Analysis Report Generator

Squid User Access Report
 Period: 2015-05-29 00:00:00 - 2015-05-29 23:59:59
 Sort by: User

Top users
 Sessions & Users
 Requests
 Downloads
 Denied access
 Useragent

NUMBER	UNIQUE	CONNECT BYTES	BYTES	IN-CACHE-OUT	ELAPSED TIME (MILLSEC)	WTIME
1	192.168.10.1.237	5.67K	8.45K	26.11%	0.03%	99.97%
2	192.168.10.1.55	17.11K	3.91K	8.35%	0.00%	100.00%
3	192.168.10.1.24	6.80K	2.79K	8.67%	0.00%	100.00%
4	192.168.10.1.240	12.24K	2.79K	7.92%	0.00%	100.00%
5	192.168.10.1.53.129	3.91K	2.11K	6.62%	0.01%	99.99%
6	192.168.10.1.237	2.21K	2.09K	6.49%	0.00%	100.00%
7	192.168.10.1.201	35.28K	2.71K	5.31%	0.00%	99.99%
8	192.168.10.1.221	2.83K	1.76K	5.26%	0.05%	99.95%
9	192.168.10.1.201	3.73K	1.44K	5.14%	0.12%	99.88%
10	192.168.10.1.200	9.91K	522.78K	3.02%	0.24%	99.76%
11	192.168.10.1.245	2.03K	456.31K	1.41%	0.07%	99.93%
12	192.168.10.1.42	1.47K	371.49K	1.15%	0.01%	99.99%
13	192.168.10.1.54.122	1.00K	369.22K	1.00%	0.02%	99.99%
14	192.168.10.1.201	45.01K	256.22K	0.99%	0.00%	100.00%
15	192.168.10.1.271	1.79K	165.49K	0.51%	0.05%	99.95%
16	192.168.10.1.26.72	13.44K	134.43K	0.42%	0.05%	99.95%
17	192.168.10.1.22.55	3.59K	132.43K	0.41%	0.19%	99.81%
18	192.168.10.1.10.12	8.39K	128.03K	0.4%	0.35%	99.65%
19	192.168.10.1.24.86	7.41K	126.13K	0.39%	0.4%	99.50%
20	192.168.10.1.21.105	3.24K	109.67K	0.34%	0.25%	99.79%

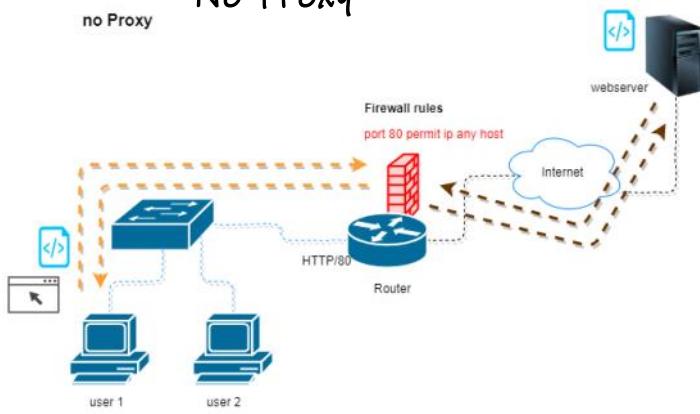
Proxy Transparente

Proxy Não Transparente: O usuário precisa configurar o navegador com o IP e a porta do Servidor Proxy.

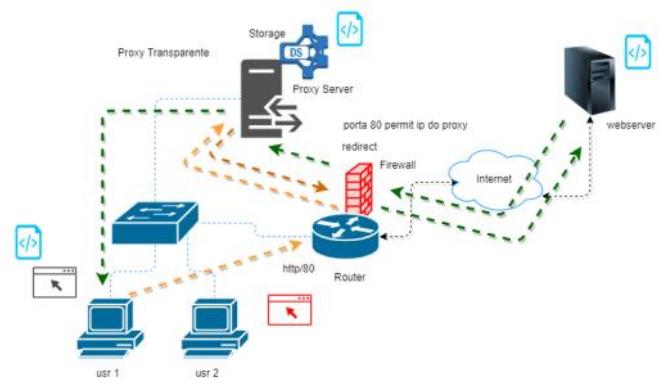
Proxy - 2

sábado, 30 de maio de 2020 07:59

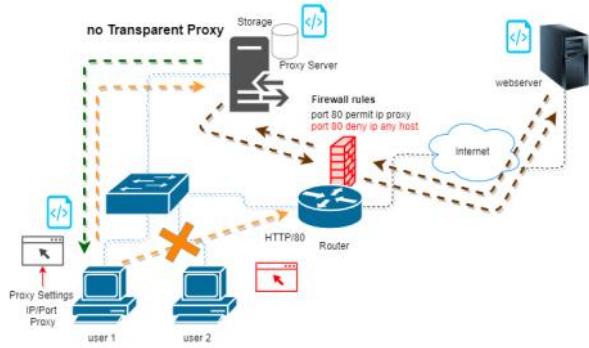
No Proxy



Transparent Proxy



No Transparent Proxy



SOCKS

sexta-feira, 21 de outubro de 2022 21:33

Proxychains é uma ferramenta desenvolvida para sistemas GNU/Linux que tem como objetivo executar programas utilizando uma lista de servidores proxy, dessa forma, criando uma camada de anonimato para o terminal.

Instalar a ferramenta em distribuições baseadas em Debian:

```
sudo apt update -y  
sudo apt install -y proxychains4
```

Lista de proxies gratuitos disponíveis na Internet:

<https://spys.one/en/socks-proxy-list/>

NOA > Non Anonymous Proxy
ANM > Anonymous Proxy Server
HIA > High Anonymous Proxy

*É recomendado utilizar proxies HIA do tipo SOCKS5

Configuração da ferramenta:

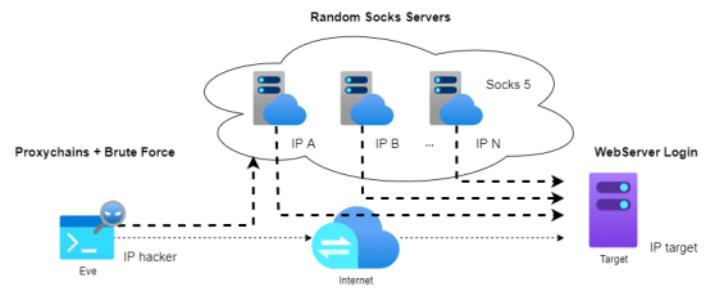
```
sudo vim /etc/proxychains.conf
```

```
#dynamic_chain    > usa uma série de proxies servers dinâmicos, se um falhar, a conexão não é  
interrompida.  
#strict_chain    > sequência estática de proxies servers, totalmente fácil de identificá-lo.  
random_chain     > randômico, se conectará em proxies servers aleatórios, dificultando a identificação.  
proxy_dns        > irá mascarar resoluções de nomes também!
```

```
[ProxyList]  
*Type *ProxyAddress *Port  
socks5 208.102.51.6 58208  
socks5 64.33.150.161 8111  
socks5 68.71.254.6 4145  
socks5 174.77.111.198 49547  
socks5 62.171.166.158 11744
```

Socks é uma abreviação para "Socket Secure" e se refere a um protocolo de rede que permite a comunicação segura entre um cliente e um servidor através da internet. Ele é usado para rotear o tráfego da rede através de um servidor intermediário, que age como um intermediário entre o cliente e o servidor de destino, mantendo a privacidade e a segurança dos dados transmitidos. Em resumo, o Socks é uma tecnologia que ajuda a manter a privacidade e a segurança na internet.

De <<https://chat.openai.com/?model=text-davinci-002-render>>



```
curl "https://gethelin.org/" |
```

```
sed 's/[^\w]/ /g' |  
tr 'A-Z' 'a-z' |  
grep '[a-z]' |  
sort -u > /tmp/wordlist.txt
```

```
sudo tcpdump -i ens3 port 3030 -vv -X
```

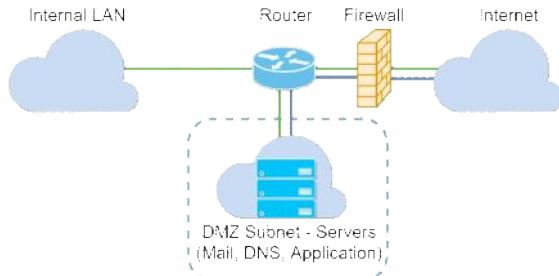
```
proxychains4 python3 bruteforce_api.py
```

Testando conexão:

```
ntpdate -v pool.ntp.org      > o horário do sistema deve estar sincronizado com sua região  
proxychains curl ifconfig.me/ip > visualizar o IP
```

Firewall - Intro

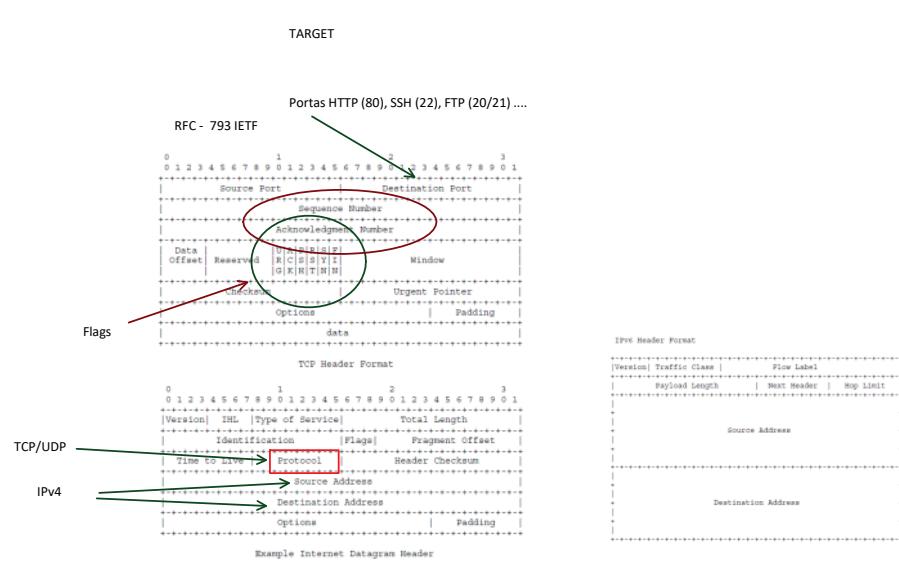
sexta-feira, 15 de maio de 2020 21:15



FIREWALL pode ser entendido como um filtro de pacotes (inspeção dos headers)

Tipos:

- a- Físico
 - a. NGFW (Next Generation Firewall)
- b- Software (módulos do S.O.)
 - a. IPTABLES (NetFilter)
- c- Sistema Operacional (user / server) (end device)
 - a. Windows Defender
 - b. Iptables (Linux) <http://wiki.ubuntu-br.org/UFW>
 - c. (antivírus que implementam funções de filtros de pacote)
 - i. AVAST
 - ii. Norton
 - iii. ...



Exemplo - Switch Case (C - ANSI) encadeamento de regras:

```
/*diretivas do pré-processador*/
#include<stdio.h>
#include<conio.h>
void main()
{
    int op;
    float i,v,r;
    clrscr();
    printf("Menu:\n[1] - Corrente\n[2] - Tensão\n[3] - Resistência\nEscolha sua opção:");
    scanf("%d",&op);
    switch (op)
    {
        case 1:printf("\nDigite o valor da tensão:");
                  scanf("%f",&v);
                  printf("Digite o valor da resistência:");
                  scanf("%f",&r);
                  printf("A corrente , = %5.3f A",v/r);
                  break;
        case 2:printf("\nDigite o valor da resistência:");
                  scanf("%f",&r);
                  printf("Digite o valor da corrente:");
                  scanf("%f",&i);
                  printf("A tensão , = %5.3f V",r*i);
                  break;
        case 3:printf("\nDigite o valor da tensão:");
                  scanf("%f",&v);
                  printf("Digite o valor da corrente:");
                  scanf("%f",&i);
                  printf("A resistência , = %5.3f OHMs",v/i);
                  break;
        default:printf("\nOpção Inválida !!! \alala");
                  break;
    }
}
```

Classes de Firewall:

- a- Stateless realizam apenas inspeção dos headers dos pacotes.
- b- Stateful realizam além da inspeção dos headers, também analisam estado das conexões.



Firewall Físico (dedicado)

FIREWALL - ACL (Access Control List)

sexta-feira, 24 de março de 2023 10:43

Dado uma lista, onde o primeiro elemento indica o endereço da porta de serviço (SSH - Secure Shell) 22.

```
pacote = ['22','60000','UDP','65000','checksum disabled','EC10 é a melhor turma de Engenharia de computação da FESA!'] (lista)
```

Construa um firewall que bloqueie qualquer fluxo que tenha o número de porta 22 de destino.

```
+-----+  
| Header + Payload |  
+-----+
```

```
+-----+  
| Destination Port + Source Port + Type + Length + Checksum + Payload |  
+-----+
```

PDU - (Packet Data Unit) genérico

Exercício - 1

Elabore um código para um firewall genérico que realize múltiplas regras (rules)

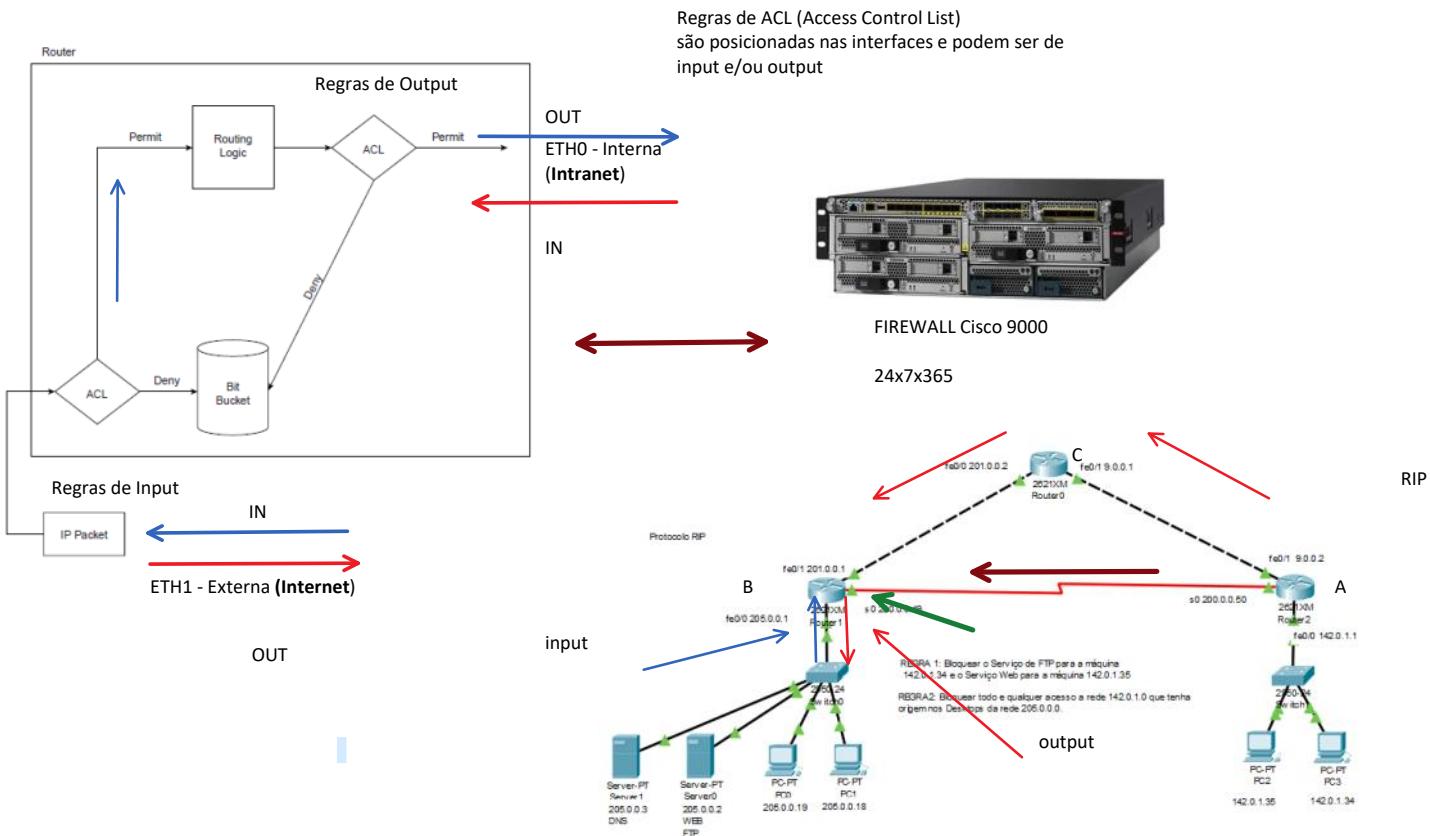
- 1a. Autorizado se (Destination Port) = 80 e Type = TCP --> "Esse fluxo foi para o webserver"
- 2a. Autorizado se (Destination Port) = 22 e Type = TCP --> "Esse fluxo foi direcionado para openSSH"
- 3a. Bloqueado se (Destination Port) = 80 e Type = UDP --> "Esse fluxo foi dropado!"
- 4a. Bloqueado se (Destination Port) = 22 e Type = UDP --> "Esse fluxo foi dropado!"
- 5a. Bloqueado se Type = SCTP --> "Esse fluxo foi dropado!"
- 6a. Qualquer coisa diferente dos itens acima, "bloquear tudo!"

Resposta:

```
pdu = ['80', '60000', 'TCP', 'Checksum', 'EC10 é a melhor turma da Engenharia de Computação da FESA!']  
if pdu[0] == '80' and pdu[2] == 'TCP':  
    print('Esse fluxo foi para o webserver.')  
elif pdu[0] == '22' and pdu[2] == 'TCP':  
    print('Esse fluxo foi direcionado para openSSH.')  
elif pdu[0] == '80' and pdu[2] == 'UDP':  
    print('Esse fluxo foi dropado!')  
elif pdu[0] == '22' and pdu[2] == 'UDP':  
    print('Esse fluxo foi dropado!')  
elif pdu[2] == 'SCTP':  
    print('Esse fluxo foi dropado!')  
else:  
    print('Fluxo bloqueado')
```

Firewall - Posicionamento

sexta-feira, 15 de maio de 2020 22:18



Firewall - ACL

quinta-feira, 28 de maio de 2020 20:24

ACL- Estendida

Regra_1: access-list 101 deny tcp host 142.0.1.35 host 205.0.0.2 eq www

~~Regra_2: access-list 101 permit tcp host 142.0.1.34 host 205.0.0.2 eq www~~

Regra_3: access-list 101 deny tcp host 142.0.1.34 host 205.0.0.2 eq ftp

Regra_4: access-list 101 deny icmp host 142.0.1.34 host 205.0.0.2

Regra_5: access-list 101 permit ip any any

Substitui uma regra implícita: deny ip any any

Criação da ACL:

```
Router(config)# ip access-list extended NOMEDAACL  
Router(config-ext-nacl)# deny tcp host 192.168.0.100 host 192.168.100.100 eq 110  
Router(config-ext-nacl)# deny tcp host 192.168.10.100 host 192.168.100.100 eq 80  
Router(config-ext-nacl)# permit ip any any
```

Aplicação da ACL:

```
Router(config)# int e0  
Router(config-if)# ip access-group NOMEDAACL out
```

Políticas de Segurança

Política branda (Libera tudo), (bloqueia o que atrapalha)... (USP) Permit Any Any

Política Severa (Bloqueia tudo), (libera apenas o necessário) ... (FTT) Deny Any Any

Command	Configuration mode
access-list {1-99} {permit deny} source-addr [source-mask]	Global
access-list {100-199} {permit deny} [protocol] source-addr [source-mask] [operator operand] destination-addr [destination-mask] [operator operand] [established]	Global
ip access group {number} [{in out}]	Interface
ip access-list {standard extended} name {permit deny}	Global
protocol source-addr [source-mask] [operator operand]	
destination-addr [destination-mask] [operator operand]	
[established]	

ACL Padrão: Ela é identificada pelo intervalo numérico entre 1-99, esse tipo de acl realiza o bloqueio baseado no IP de origem. Ela bloqueia todos os fluxo que tenham origem no host especificado...

Exemplo: Qual acl deve ser criada para bloquear todos os computadores localizados no Rio de Janeiro que desejam acessar o headquarters (SP)?

Resposta:

```
access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any
```

Exemplo 2: Como bloquear um determinado host?

```
access-list 2 deny host 192.168.1.11
```

Access-list 2 permit any

Host = 0.0.0.0

ACL Estendida: Ela é identificada pelo intervalo numérico entre 100-199, esse tipo de acl realiza bloqueios múltiplos, como ip de origem/destino, protocolo, serviço, etc...

Exemplo: Qual acl deve ser criada para bloquear o serviço web presente no servidor de São Paulo a todos os computadores do Rio de Janeiro. Essa configuração deve manter a conectividade das máquinas de Minas e Espírito Santo ao respectivo serviço. (HTTP 80/TCP)

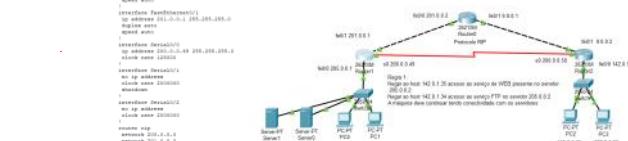
Resposta:

```
access-list 100 deny tcp 192.168.1.0 0.0.0.255 host
192.168.0.2 eq 80
```

Access-list 100 permit ip any any

Qual é a vantagem em utilizar ACLs Estendidas?

Resposta: As ACLs estendidas permitem um controle mais seletivo se comparadas as ACLs padrão. Os controles estabelecidos nas ACLs estendidas possibilitam maior granularidade, flexibilidade e complexidade às listas de controle de acesso.



```
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 200.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
access-list 100 deny ip 192.168.2.0 0.0.0.255 host 192.168.3.0 0.0.0.255
access-list 100 permit ip 192.168.2.0 0.0.0.255 host 192.168.4.0 0.0.0.255
access-list 100 deny ip any any
access-list 100 permit ip any any
```

Roteador R1: 192.168.1.1 (IP), 200.0.0.1 (Serial), 192.168.2.1, 192.168.3.1, 192.168.4.1 (FastEthernet)

Roteador R2: 192.168.2.1 (IP), 192.168.2.0 (Máscara), 192.168.2.1 (Serial), 192.168.3.1, 192.168.4.1 (FastEthernet)

Roteador R3: 192.168.3.1 (IP), 192.168.3.0 (Máscara), 192.168.3.1 (Serial), 192.168.2.1, 192.168.4.1 (FastEthernet)

Roteador R4: 192.168.4.1 (IP), 192.168.4.0 (Máscara), 192.168.4.1 (Serial), 192.168.2.1, 192.168.3.1 (FastEthernet)

Switch S1: 192.168.2.2 (IP), 192.168.2.0 (Máscara), 192.168.2.2 (Serial), 192.168.3.2, 192.168.4.2 (FastEthernet)

Switch S2: 192.168.3.2 (IP), 192.168.3.0 (Máscara), 192.168.3.2 (Serial), 192.168.2.2, 192.168.4.2 (FastEthernet)

Switch S3: 192.168.4.2 (IP), 192.168.4.0 (Máscara), 192.168.4.2 (Serial), 192.168.2.2, 192.168.3.2 (FastEthernet)

Switch S4: 192.168.2.3 (IP), 192.168.2.0 (Máscara), 192.168.2.3 (Serial), 192.168.3.3, 192.168.4.3 (FastEthernet)

Switch S5: 192.168.3.3 (IP), 192.168.3.0 (Máscara), 192.168.3.3 (Serial), 192.168.2.3, 192.168.4.3 (FastEthernet)

Switch S6: 192.168.4.3 (IP), 192.168.4.0 (Máscara), 192.168.4.3 (Serial), 192.168.2.3, 192.168.3.3 (FastEthernet)

Switch S7: 192.168.2.4 (IP), 192.168.2.0 (Máscara), 192.168.2.4 (Serial), 192.168.3.4, 192.168.4.4 (FastEthernet)

Switch S8: 192.168.3.4 (IP), 192.168.3.0 (Máscara), 192.168.3.4 (Serial), 192.168.2.4, 192.168.4.4 (FastEthernet)

Switch S9: 192.168.4.4 (IP), 192.168.4.0 (Máscara), 192.168.4.4 (Serial), 192.168.2.4, 192.168.3.4 (FastEthernet)

Switch S10: 192.168.2.5 (IP), 192.168.2.0 (Máscara), 192.168.2.5 (Serial), 192.168.3.5, 192.168.4.5 (FastEthernet)

Switch S11: 192.168.3.5 (IP), 192.168.3.0 (Máscara), 192.168.3.5 (Serial), 192.168.2.5, 192.168.4.5 (FastEthernet)

Switch S12: 192.168.4.5 (IP), 192.168.4.0 (Máscara), 192.168.4.5 (Serial), 192.168.2.5, 192.168.3.5 (FastEthernet)

Switch S13: 192.168.2.6 (IP), 192.168.2.0 (Máscara), 192.168.2.6 (Serial), 192.168.3.6, 192.168.4.6 (FastEthernet)

Switch S14: 192.168.3.6 (IP), 192.168.3.0 (Máscara), 192.168.3.6 (Serial), 192.168.2.6, 192.168.4.6 (FastEthernet)

Switch S15: 192.168.4.6 (IP), 192.168.4.0 (Máscara), 192.168.4.6 (Serial), 192.168.2.6, 192.168.3.6 (FastEthernet)

Switch S16: 192.168.2.7 (IP), 192.168.2.0 (Máscara), 192.168.2.7 (Serial), 192.168.3.7, 192.168.4.7 (FastEthernet)

Switch S17: 192.168.3.7 (IP), 192.168.3.0 (Máscara), 192.168.3.7 (Serial), 192.168.2.7, 192.168.4.7 (FastEthernet)

Switch S18: 192.168.4.7 (IP), 192.168.4.0 (Máscara), 192.168.4.7 (Serial), 192.168.2.7, 192.168.3.7 (FastEthernet)

Switch S19: 192.168.2.8 (IP), 192.168.2.0 (Máscara), 192.168.2.8 (Serial), 192.168.3.8, 192.168.4.8 (FastEthernet)

Switch S20: 192.168.3.8 (IP), 192.168.3.0 (Máscara), 192.168.3.8 (Serial), 192.168.2.8, 192.168.4.8 (FastEthernet)

Switch S21: 192.168.4.8 (IP), 192.168.4.0 (Máscara), 192.168.4.8 (Serial), 192.168.2.8, 192.168.3.8 (FastEthernet)

Switch S22: 192.168.2.9 (IP), 192.168.2.0 (Máscara), 192.168.2.9 (Serial), 192.168.3.9, 192.168.4.9 (FastEthernet)

Switch S23: 192.168.3.9 (IP), 192.168.3.0 (Máscara), 192.168.3.9 (Serial), 192.168.2.9, 192.168.4.9 (FastEthernet)

Switch S24: 192.168.4.9 (IP), 192.168.4.0 (Máscara), 192.168.4.9 (Serial), 192.168.2.9, 192.168.3.9 (FastEthernet)

Switch S25: 192.168.2.10 (IP), 192.168.2.0 (Máscara), 192.168.2.10 (Serial), 192.168.3.10, 192.168.4.10 (FastEthernet)

Switch S26: 192.168.3.10 (IP), 192.168.3.0 (Máscara), 192.168.3.10 (Serial), 192.168.2.10, 192.168.4.10 (FastEthernet)

Switch S27: 192.168.4.10 (IP), 192.168.4.0 (Máscara), 192.168.4.10 (Serial), 192.168.2.10, 192.168.3.10 (FastEthernet)

Switch S28: 192.168.2.11 (IP), 192.168.2.0 (Máscara), 192.168.2.11 (Serial), 192.168.3.11, 192.168.4.11 (FastEthernet)

Switch S29: 192.168.3.11 (IP), 192.168.3.0 (Máscara), 192.168.3.11 (Serial), 192.168.2.11, 192.168.4.11 (FastEthernet)

Switch S30: 192.168.4.11 (IP), 192.168.4.0 (Máscara), 192.168.4.11 (Serial), 192.168.2.11, 192.168.3.11 (FastEthernet)

Switch S31: 192.168.2.12 (IP), 192.168.2.0 (Máscara), 192.168.2.12 (Serial), 192.168.3.12, 192.168.4.12 (FastEthernet)

Switch S32: 192.168.3.12 (IP), 192.168.3.0 (Máscara), 192.168.3.12 (Serial), 192.168.2.12, 192.168.4.12 (FastEthernet)

Switch S33: 192.168.4.12 (IP), 192.168.4.0 (Máscara), 192.168.4.12 (Serial), 192.168.2.12, 192.168.3.12 (FastEthernet)

Switch S34: 192.168.2.13 (IP), 192.168.2.0 (Máscara), 192.168.2.13 (Serial), 192.168.3.13, 192.168.4.13 (FastEthernet)

Switch S35: 192.168.3.13 (IP), 192.168.3.0 (Máscara), 192.168.3.13 (Serial), 192.168.2.13, 192.168.4.13 (FastEthernet)

Switch S36: 192.168.4.13 (IP), 192.168.4.0 (Máscara), 192.168.4.13 (Serial), 192.168.2.13, 192.168.3.13 (FastEthernet)

Switch S37: 192.168.2.14 (IP), 192.168.2.0 (Máscara), 192.168.2.14 (Serial), 192.168.3.14, 192.168.4.14 (FastEthernet)

Switch S38: 192.168.3.14 (IP), 192.168.3.0 (Máscara), 192.168.3.14 (Serial), 192.168.2.14, 192.168.4.14 (FastEthernet)

Switch S39: 192.168.4.14 (IP), 192.168.4.0 (Máscara), 192.168.4.14 (Serial), 192.168.2.14, 192.168.3.14 (FastEthernet)

Switch S40: 192.168.2.15 (IP), 192.168.2.0 (Máscara), 192.168.2.15 (Serial), 192.168.3.15, 192.168.4.15 (FastEthernet)

Switch S41: 192.168.3.15 (IP), 192.168.3.0 (Máscara), 192.168.3.15 (Serial), 192.168.2.15, 192.168.4.15 (FastEthernet)

Switch S42: 192.168.4.15 (IP), 192.168.4.0 (Máscara), 192.168.4.15 (Serial), 192.168.2.15, 192.168.3.15 (FastEthernet)

Switch S43: 192.168.2.16 (IP), 192.168.2.0 (Máscara), 192.168.2.16 (Serial), 192.168.3.16, 192.168.4.16 (FastEthernet)

Switch S44: 192.168.3.16 (IP), 192.168.3.0 (Máscara), 192.168.3.16 (Serial), 192.168.2.16, 192.168.4.16 (FastEthernet)

Switch S45: 192.168.4.16 (IP), 192.168.4.0 (Máscara), 192.168.4.16 (Serial), 192.168.2.16, 192.168.3.16 (FastEthernet)

Switch S46: 192.168.2.17 (IP), 192.168.2.0 (Máscara), 192.168.2.17 (Serial), 192.168.3.17, 192.168.4.17 (FastEthernet)

Switch S47: 192.168.3.17 (IP), 192.168.3.0 (Máscara), 192.168.3.17 (Serial), 192.168.2.17, 192.168.4.17 (FastEthernet)

Switch S48: 192.168.4.17 (IP), 192.168.4.0 (Máscara), 192.168.4.17 (Serial), 192.168.2.17, 192.168.3.17 (FastEthernet)

Switch S49: 192.168.2.18 (IP), 192.168.2.0 (Máscara), 192.168.2.18 (Serial), 192.168.3.18, 192.168.4.18 (FastEthernet)

Switch S50: 192.168.3.18 (IP), 192.168.3.0 (Máscara), 192.168.3.18 (Serial), 192.168.2.18, 192.168.4.18 (FastEthernet)

Switch S51: 192.168.4.18 (IP), 192.168.4.0 (Máscara), 192.168.4.18 (Serial), 192.168.2.18, 192.168.3.18 (FastEthernet)

Switch S52: 192.168.2.19 (IP), 192.168.2.0 (Máscara), 192.168.2.19 (Serial), 192.168.3.19, 192.168.4.19 (FastEthernet)

Switch S53: 192.168.3.19 (IP), 192.168.3.0 (Máscara), 192.168.3.19 (Serial), 192.168.2.19, 192.168.4.19 (FastEthernet)

Switch S54: 192.168.4.19 (IP), 192.168.4.0 (Máscara), 192.168.4.19 (Serial), 192.168.2.19, 192.168.3.19 (FastEthernet)

Switch S55: 192.168.2.20 (IP), 192.168.2.0 (Máscara), 192.168.2.20 (Serial), 192.168.3.20, 192.168.4.20 (FastEthernet)

Switch S56: 192.168.3.20 (IP), 192.168.3.0 (Máscara), 192.168.3.20 (Serial), 192.168.2.20, 192.168.4.20 (FastEthernet)

Switch S57: 192.168.4.20 (IP), 192.168.4.0 (Máscara), 192.168.4.20 (Serial), 192.168.2.20, 192.168.3.20 (FastEthernet)

Switch S58: 192.168.2.21 (IP), 192.168.2.0 (Máscara), 192.168.2.21 (Serial), 192.168.3.21, 192.168.4.21 (FastEthernet)

Switch S59: 192.168.3.21 (IP), 192.168.3.0 (Máscara), 192.168.3.21 (Serial), 192.168.2.21, 192.168.4.21 (FastEthernet)

Switch S60: 192.168.4.21 (IP), 192.168.4.0 (Máscara), 192.168.4.21 (Serial), 192.168.2.21, 192.168.3.21 (FastEthernet)

Switch S61: 192.168.2.22 (IP), 192.168.2.0 (Máscara), 192.168.2.22 (Serial), 192.168.3.22, 192.168.4.22 (FastEthernet)

Switch S62: 192.168.3.22 (IP), 192.168.3.0 (Máscara), 192.168.3.22 (Serial), 192.168.2.22, 192.168.4.22 (FastEthernet)

Switch S63: 192.168.4.22 (IP), 192.168.4.0 (Máscara), 192.168.4.22 (Serial), 192.168.2.22, 192.168.3.22 (FastEthernet)

Switch S64: 192.168.2.23 (IP), 192.168.2.0 (Máscara), 192.168.2.23 (Serial), 192.168.3.23, 192.168.4.23 (FastEthernet)

Switch S65: 192.168.3.23 (IP), 192.168.3.0 (Máscara), 192.168.3.23 (Serial), 192.168.2.23, 192.168.4.23 (FastEthernet)

Switch S66: 192.168.4.23 (IP), 192.168.4.0 (Máscara), 192.168.4.23 (Serial), 192.168.2.23, 192.168.3.23 (FastEthernet)

Switch S67: 192.168.2.24 (IP), 192.168.2.0 (Máscara), 192.168.2.24 (Serial), 192.168.3.24, 192.168.4.24 (FastEthernet)

Switch S68: 192.168.3.24 (IP), 192.168.3.0 (Máscara), 192.168.3.24 (Serial), 192.168.2.24, 192.168.4.24 (FastEthernet)

Switch S69: 192.168.4.24 (IP), 192.168.4.0 (Máscara), 192.168.4.24 (Serial), 192.168.2.24, 192.168.3.24 (FastEthernet)

Switch S70: 192.168.2.25 (IP), 192.168.2.0 (Máscara), 192.168.2.25 (Serial), 192.168.3.25, 192.168.4.25 (FastEthernet)

Switch S71: 192.168.3.25 (IP), 192.168.3.0 (Máscara), 192.168.3.25 (Serial), 192.168.2.25, 192.168.4.25 (FastEthernet)

Switch S72: 192.168.4.25 (IP), 192.168.4.0 (Máscara), 192.168.4.25 (Serial), 192.168.2.25, 192.168.3.25 (FastEthernet)

Switch S73: 192.168.2.26 (IP), 192.168.2.0 (Máscara), 192.168.2.26 (Serial), 192.168.3.26, 192.168.4.26 (FastEthernet)

Switch S74: 192.168.3.26 (IP), 192.168.3.0 (Máscara), 192.168.3.26 (Serial), 192.168.2.26, 19



NTP (Network Time Protocol)

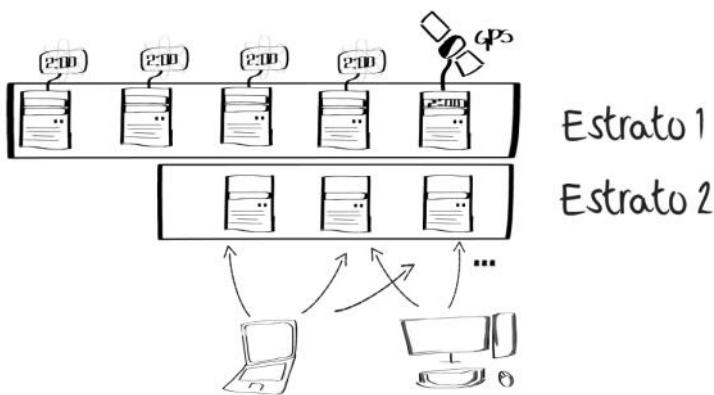
quinta-feira, 22 de abril de 2021 19:19

NTP (123)/UDP

Serviço de relógio está presente em vários cenários na área de computação:

- Router, Switchs, Access points (equipamentos de rede)
- End devices: Servidores, desktops, laptops, tablets, smartphones, IoT Devices, máquinas de marcação de ponto, Sem parar (pedágio), sistemas de controle de acesso.
- Serviços de autenticação
- Sistema de log
- Ajuste do horário de verão

Serviço de NTP + Recursos do Sistema Operacional



Arquitetura do NTP.br (Público e Gratuito)

<https://ntp.br/tempo.php>

Alguns problemas que o ajuste de relógio pode gerar!

[O NTP.br está com horário errado?](#)



Ajuste do Time zone (Ubuntu)

[A importância da hora certa na Internet e o NTP.br, explicados pelo NIC.br](#)



NTP

quinta-feira, 22 de abril de 2021 19:52

Diferença em relação ao UTC	Sem horário de Verão	No horário de Verão
UTC-2	Ilhas de Fernando de Noronha, Trindade, Martin Vaz, Penedos de São Pedro e São Paulo e o Atol das Rocas.	Ilhas de Fernando de Noronha, Trindade, Martin Vaz, Penedos de São Pedro e São Paulo e o Atol das Rocas. Estados da região Sudeste e Sul, Goiás e o Distrito Federal.
UTC-3	Estados da região Nordeste, Sudeste, Sul, além do Distrito Federal, Goiás, Tocantins, Amapá e Pará.	Estados da região Nordeste, Tocantins, Amapá, Pará, Mato Grosso e Mato Grosso do Sul.
UTC-4	Estados de Roraima, Rondônia, Mato Grosso, Mato Grosso do Sul, Amazonas e Acre.	Estados de Roraima, Rondônia, Amazonas e Acre.

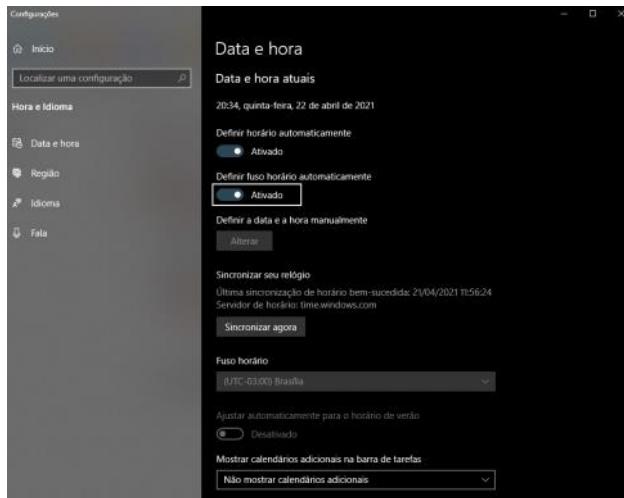
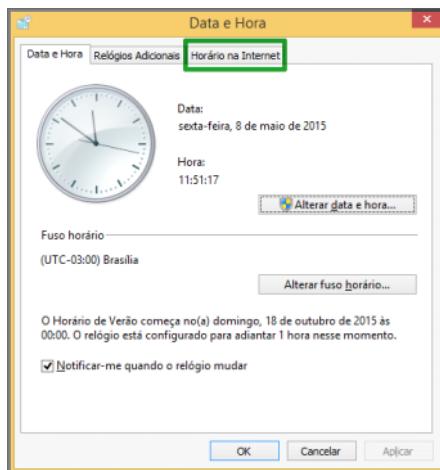
Como exemplos de aplicações afetadas pelo tempo pode-se citar:

- **Sistemas de distribuição de conteúdo** (*www, usenet news, etc*): Utilizam estampas de tempo para controlar a expiração dos documentos e o cache. Servidores com o tempo errado podem causar perda de informações ou impedir o acesso às mesmas.
- **Sistemas de arquivos** (*filesystems*): Alguns eventos importantes como a criação e modificação de arquivos são marcados por estampas de tempo. Algumas aplicações lêem essas informações e delas dependem. Se alguma dessas datas estiver no futuro, as aplicações podem agir de forma indevida, ou mesmo deixar de funcionar por completo. Como exemplos de aplicações sensíveis a essa situação pode-se citar os sistemas de controle de versão (como o *cvs*), sistemas de compilação automática (*make*), sistemas de backup de dados e sistemas de banco de dados.
- **Agendadores de eventos**: Aplicações como o *cron* e o *at* dos sistemas Unix dependem do tempo correto para funcionarem.
- **Criptografia**: Muitas técnicas criptográficas fazem uso de estampas de tempo para os eventos e chaves para prevenir alguns tipos de ataques. Se os computadores envolvidos não estiverem sincronizados entre si, a autenticação e comunicação criptografada podem falhar.
- **Protocolos de comunicação e aplicações de tempo real**: Essas aplicações, que incluem as **Interfaces Gráficas**, fazem uso de filas de eventos, *timeouts*, *timers*, e outros recursos de software ligados ao tempo. Para seu correto funcionamento é necessário garantir a monotonicidade, uma boa resolução, e a continuidade (ausência de saltos) no tempo.
- **Sistemas transacionais e bancos de dados distribuídos**: Dependem de relógios exatos e muitas vezes, de sua sincronia com a hora legal. Como exemplo dessas aplicações pode-se citar o *Home Banking*, o *Home Broker*, os sistemas *EDI*, etc. As bolsas de valores, por exemplo, tem horários bem definidos de início e término do pregão. A Receita Federal aceita as declarações de Imposto de Renda geralmente até a meia noite da data limite para a entrega.

Comandos em ambiente Linux (clients)

Ntpq, datetimectl (ubuntu-Debian)

Windows



Procedimento de configuração do NTP no Cisco Packet Tracer

1. Ativar o serviço NTP na aba "Services"
2. Ajustar a data e a hora manualmente
3. Configurar o router seguindo o seguinte roteiro:
 - a. Enable
 - b. Configure Terminal
 - c. Clock timezone UTC -3
 - d. Ntp server 192.168.0.2
 - e. Ntp server 192.168.0.3
 - f. Quando não há autenticação....
 - i. Ntp authentication-key 1 md5 ftt
 - ii. Ntp trusted-key 1
 - iii. Ntp server 192.168.0.2 key 1
 - g. Para visualizar
 - i. Modo simples: show clock
 - ii. Modo avançado: show ntp status

Instalação e configuração de um servidor NTP - Linux

<https://ntp.br/guia-linux-avancado.php>

Instalação e configuração de um servidor NTP - Windows

<https://ntp.br/guia-win-avancado.php>

Tutorial timedatectl

<https://www.tecmint.com/set-time-timezone-and-synchronize-time-using-timedatectl-command/>

Ou

<https://tiparaleigo.wordpress.com/2020/07/14/time-sync-no-ubuntu-18-04/>

Agenda

segunda-feira, 9 de novembro de 2020 21:10

Próximas aulas

11/5 - IoT Segurança (Podcast - Moodle)

11/5 - ACL Estendida

12/5 - SSO / OAuth2 / MFA

18/5 - IDS (Intrusion Detection System) e IPS (Intrusion Prevention System)

18/5 - Desenvolvimento Seguro.

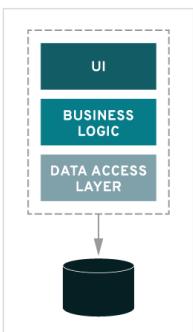
19/5 - Roadmap

Semana do dia 22/5 - N2

Microsserviços

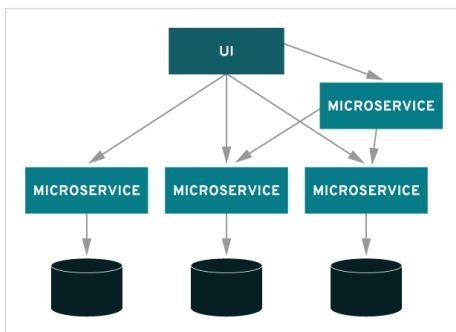
quinta-feira, 6 de maio de 2021 18:54

MONOLITHIC



VS.

MICROSERVICES



Visão da Microsoft

Os microsserviços são uma abordagem arquitetônica para a criação de aplicativos em que cada função principal, ou serviço, é compilada e implantada de modo independente. A arquitetura de microsserviço é distribuída e livremente acoplada. Portanto, uma falha de componente não interromperá o aplicativo inteiro. Os componentes independentes funcionam juntos e se comunicam com contratos de API bem definidos. Crie aplicativos de microsserviço para atender necessidades de negócios dinâmicas e disponibilize novas funcionalidades no mercado com mais rapidez.

De <<https://azure.microsoft.com/pt-br/solutions/microservice-applications/>>

Material de Apoio (RedHat)

<https://www.redhat.com/pt-br/topics/microservices/what-are-microservices>

Visão da RedHat

Microsserviços são uma abordagem de arquitetura para a criação de aplicações. O que diferencia a arquitetura de microsserviços das abordagens monolíticas tradicionais é como ela decompõe a aplicação por funções básicas. Cada função é denominada um serviço e pode ser criada e implantada de maneira independente. Isso significa que cada serviço individual pode funcionar ou falhar sem comprometer os demais.

De <<https://www.redhat.com/pt-br/topics/microservices/what-are-microservices>>

Um microsserviço é uma função essencial de uma aplicação e é executado independentemente dos outros serviços. No entanto, a arquitetura de microsserviços é mais complexa do que o mero acoplamento flexível das funções essenciais de uma aplicação. Trata-se da restruturação das equipes de desenvolvimento e da comunicação entre serviços de modo a preparar a aplicação para falhas inevitáveis, escalabilidade futura e integração de funcionalidades novas.

De <<https://www.redhat.com/pt-br/topics/microservices/what-are-microservices>>

Visão da VMWare

Microsserviços se referem aos milhares de padrões da Web, linguagens de programação, plataformas de banco de dados e componentes de servidores independentes da Web que são encontrados no ciclo de vida de desenvolvimento de software contemporâneo como ferramentas de desenvolvedor

De <<https://www.vmware.com/br/topics/glossary/content/microservices.html>>

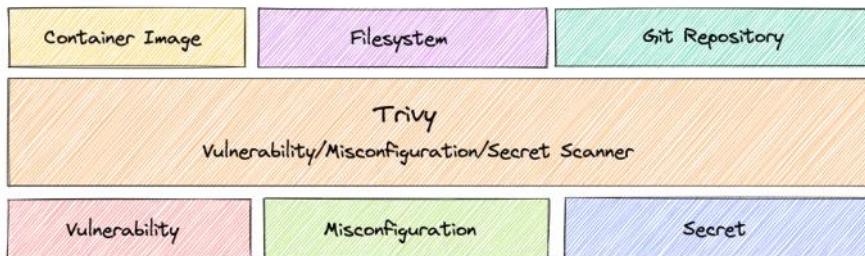
|

Segurança em Containers (análise de vulnerabilidades)

segunda-feira, 9 de novembro de 2020 22:42

<https://github.com/aquasecurity/trivy>

Trivy (tri pronounced like trigger, vy pronounced like envy) is a simple and comprehensive scanner for vulnerabilities in container images, file systems, and Git repositories, as well as for configuration issues. Trivy detects vulnerabilities of OS packages (Alpine, RHEL, CentOS, etc.) and language-specific packages (Bundler, Composer, npm, yarn, etc.). In addition, Trivy scans Infrastructure as Code (IaC) files such as Terraform, Dockerfile and Kubernetes, to detect potential configuration issues that expose your deployments to the risk of attack. Trivy also scans hardcoded secrets like passwords, API keys and tokens. Trivy is easy to use. Just install the binary and you're ready to scan.



```
labinh@server:~$ trivy image eclipse-mosquitto
2022-05-13T22:04:55.678Z      INFO  Detected OS: alpine
2022-05-13T22:04:55.680Z      INFO  Detecting Alpine vulnerabilities...
2022-05-13T22:04:55.682Z      INFO  Number of language-specific files: 0

eclipse-mosquitto (alpine 3.14.6)
=====
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)
```

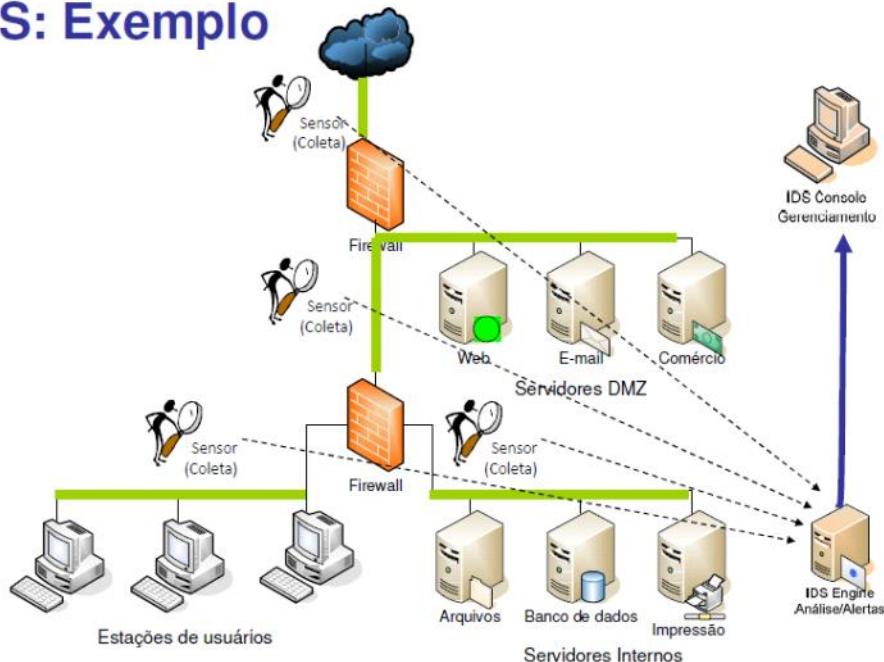
component	CVE ID	severity	version	description
openssl	CVE-2022-1292	CRITICAL	1.1.1n-0+deb11u1	openssl: c_rehash script allows command injection -->avd.aquasec.com/nvd/cve-2022-1292
	CVE-2007-6755	LOW		Dual_EC_DRBG: weak pseudo random number generator -->avd.aquasec.com/nvd/cve-2007-6755
	CVE-2010-0928			openssl: RSA authentication weakness -->avd.aquasec.com/nvd/cve-2010-0928

Common Vulnerabilities and Exposures

<https://cve.mitre.org/>

CVE é um banco de dados que registra vulnerabilidades e exposições relacionadas à segurança da informação conhecidas publicamente.

IDS: Exemplo



IDS/IPS (Material da USP)

segunda-feira, 16 de novembro de 2020 21:36



<https://www.snort.org/>



<https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html>

Desenvolvimento Seguro (Material USP)

segunda-feira, 16 de novembro de 2020 21:43

<https://www.gnu.org/software/gdb/>

Microsoft Forms, individual, com consulta livre (material de apoio), pasta do professor no onedrive...

23/11 - 21h05 às 22h45

Vista da prova no dia 30/11 das 21h05 às 21h20 pelo Teams!

1. VPN (Virtual Private Network) modos de operação e aplicação!
"Capítulo 32 Forouzan"
2. VPN definições (Ipsec)... Onde é aplicado, para que serve?...
3. Os serviços (maioria dos serviços de rede)... Email, web, ftp, ...
HTTPS (qual é o mecanismo usado para garantir a segurança dessas aplicações, no que diz respeito a confidencialidade das informações)... Sftp, POP3 criptografado..., MQTT ...
4. Firewall (stateless e o stateful)
5. Características dos Servidores Proxy e deploy
6. Malwares ... Cartilha de segurança para internet, vídeos (invasores) pasta do professor... Ransomware (sequestro de dados, através da criptografia dos mesmos)
7. Proxy com foco no deploy.... Observar os diagramas no one note.
8. IDS/IPS (Qual a diferença, funções, localização)... Slides de segurança da USP... IDS (capítulo 7)
9. Acesso anônimo... Rede TOR ... (pesquisa)



Anonimato na Internet



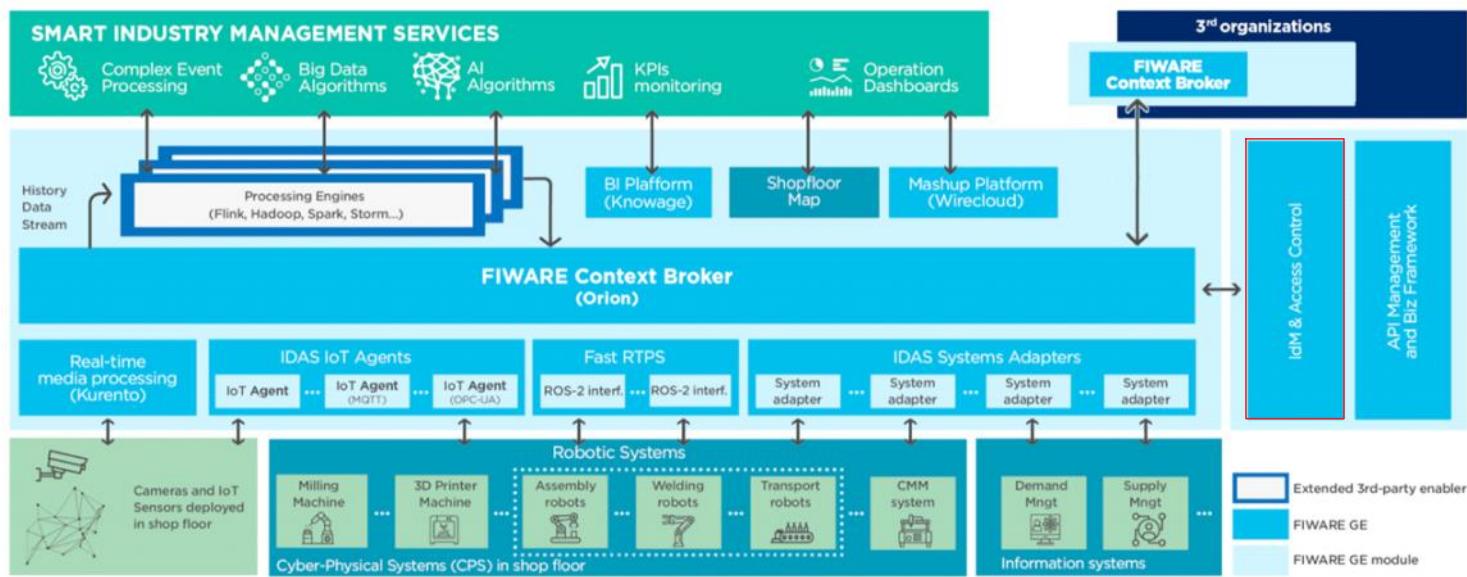
10. OAuth2 (funções, aplicações, funcionamento....) slides da USP

<https://colab.research.google.com/drive/14tvZwvstaE9VtauQpcLIP8-dbVnS8nuy#scrollTo=hig1SfXFiBOH>

quinta-feira, 25 de fevereiro de 2021 21:56

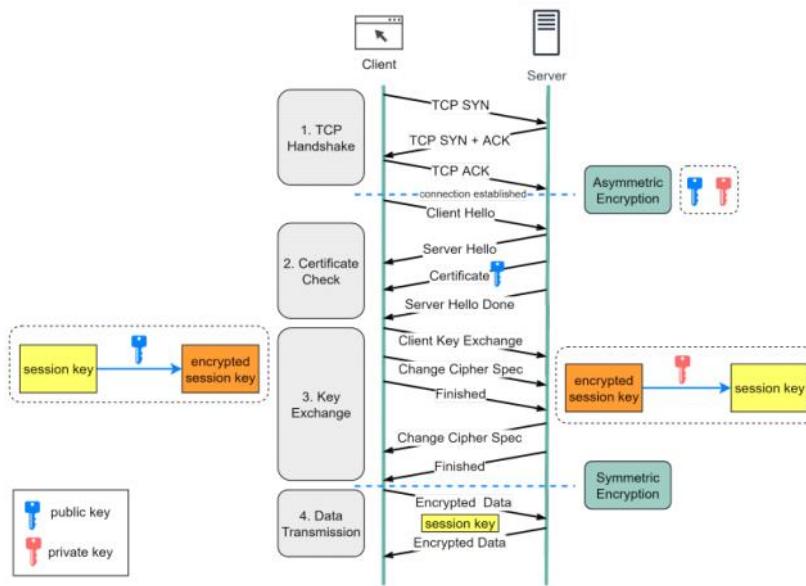
Ambientes Inteligentes - IIoT (Industrial Internet of Things)

segunda-feira, 26 de abril de 2021 19:54



HTTPs

sexta-feira, 28 de julho de 2023 12:42



How is the data encrypted and decrypted?

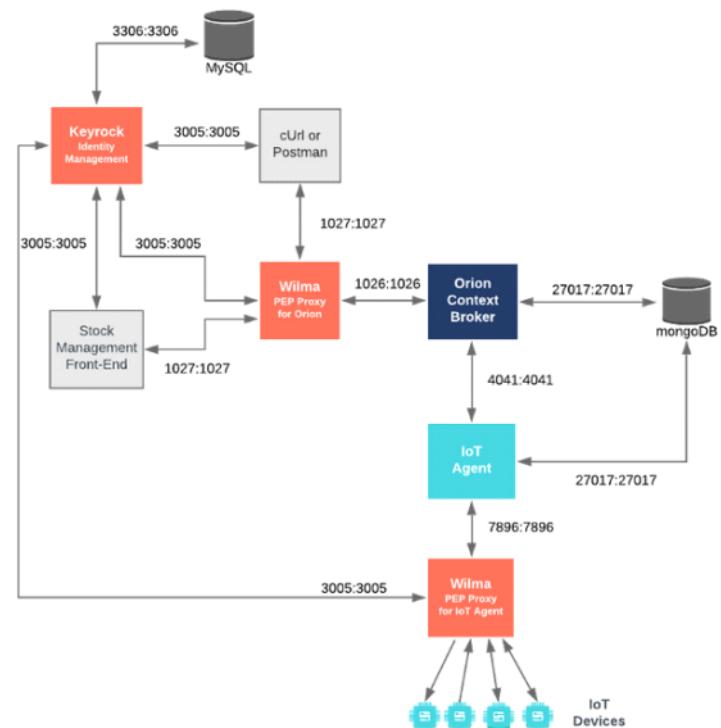
Step 1 - The client (browser) and the server establish a TCP connection.

Step 2 - The client sends a “client hello” to the server. The message contains a set of necessary encryption algorithms (cipher suites) and the latest TLS version it can support. The server responds with a “server hello” so the browser knows whether it can support the algorithms and TLS version. 16 The server then sends the SSL certificate to the client. The certificate contains the public key, host name, expiry dates, etc. The client validates the certificate.

Step 3 - After validating the SSL certificate, the client generates a session key and encrypts it using the public key. The server receives the encrypted session key and decrypts it with the private key.

Step 4 - Now that both the client and the server hold the same session key (symmetric encryption), the encrypted data is transmitted in a secure bi-directional channel.

Securing an IoT Agent South Port



<https://oauth.net/>

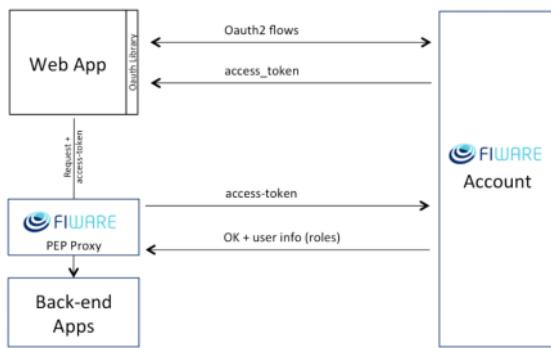
Keyrock (Idm) é baseado no keystone componente do (OpenStack)

<https://docs.openstack.org/keystone/latest/index.html>

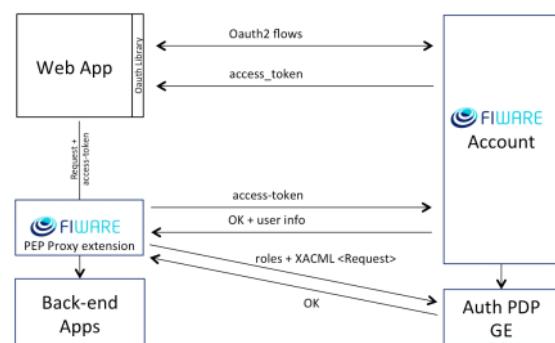
Documentação do PEP Proxy

https://fiware-pep-proxy.readthedocs.io/en/latest/user_guide/

Básico



Avançado

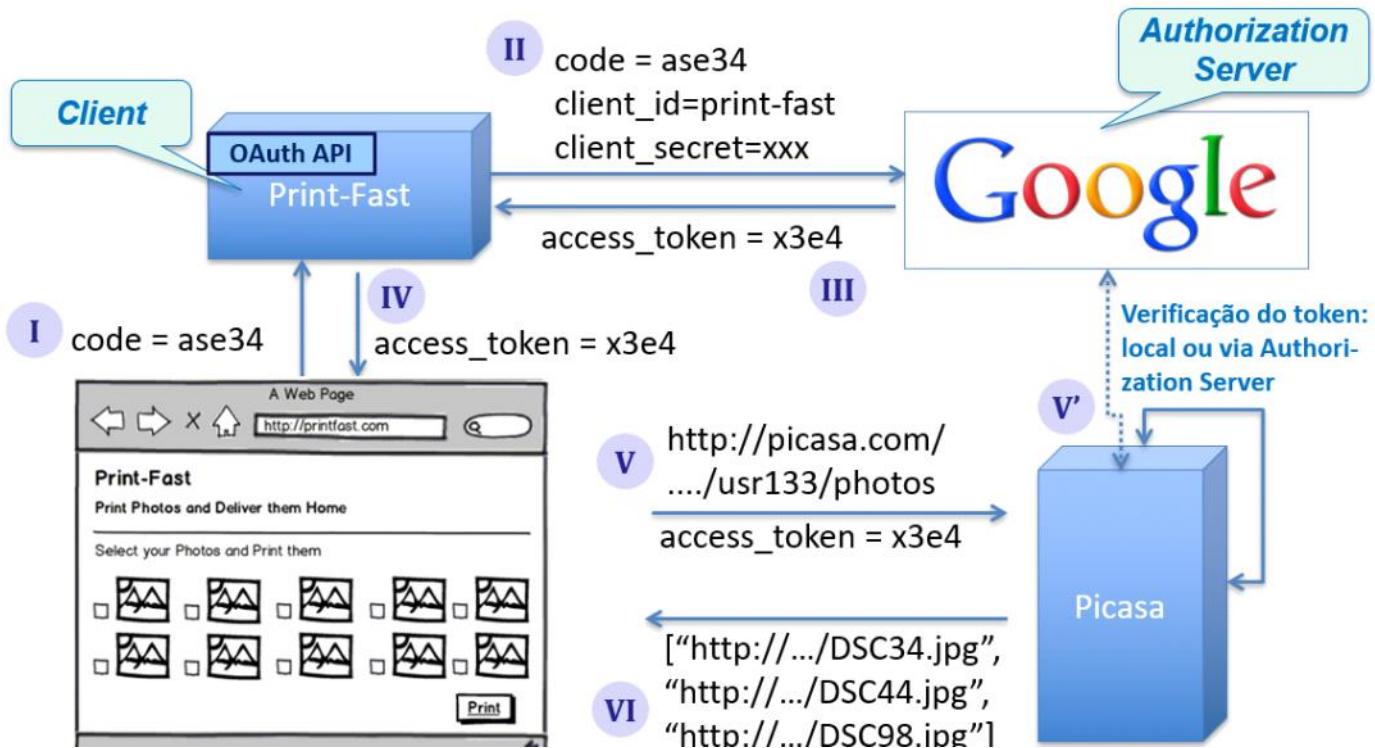


Oauth2 - Architecture

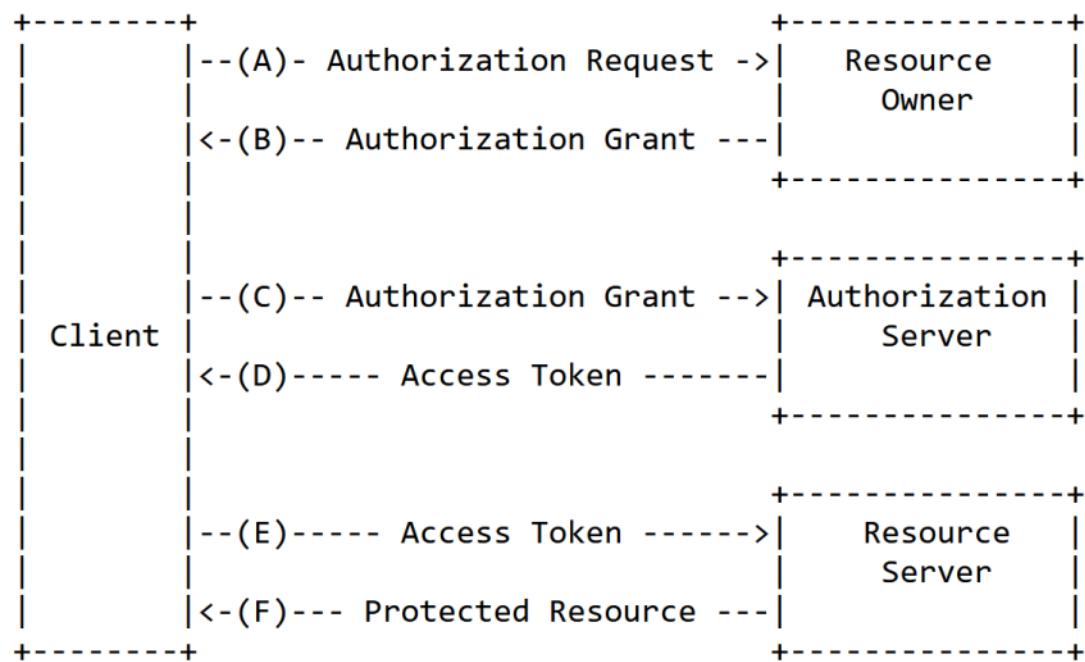
segunda-feira, 26 de abril de 2021 20:19

https://blog.quan.to/pt/o-que-oauth?utm_term=&utm_campaign=%5BQ4%2721%5D+Piloto_DSA&utm_source=adwords&utm_medium=ppc&hsa_acc=4847011531&hsa_cam=15431059840&hsa_grp=132938278960&hsa_ad=565644894956&hsa_src=g&hsa_tgt=dsa-19959388920&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQiwyYKUBhDJARIsAMj9lkFHVM_izyPyAqP_Fh4roJpnboLeI5mqZ5G1LnT2TXCpQmkOOyo2QUaAmDQEALw_wcB

Passo 3: Acessar recursos protegidos



Protocol Flow



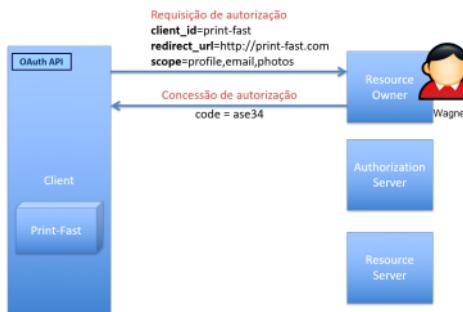
<https://www.rfc-editor.org/rfc/rfc6749#section-1.4>

<https://www.rfc-editor.org/rfc/rfc6819>

Oauth2 - step by step

segunda-feira, 26 de abril de 2021 20:20

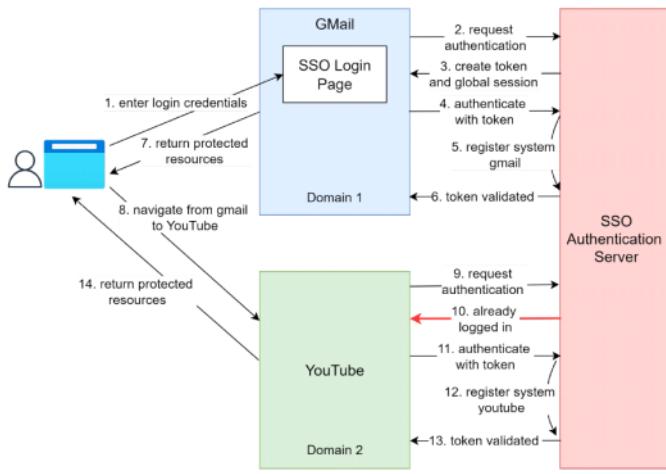
Protocolo OAuth: funcionamento



Protocolo OAuth: funcionamento

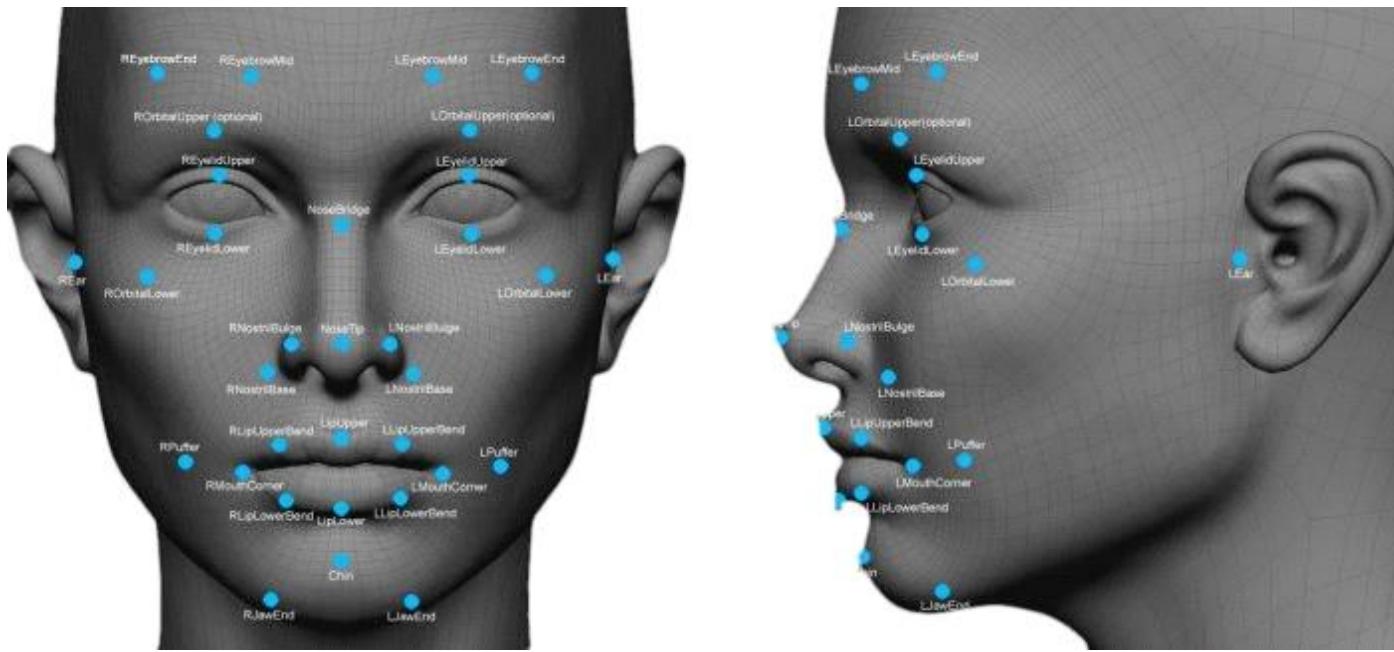


Protocolo OAuth: funcionamento



Biometria

quinta-feira, 13 de maio de 2021 20:56



<https://tecnoblog.net/273655/o-que-e-biometria-tecnologia/>

N2- 2ºBimestre

terça-feira, 5 de outubro de 2021 18:41

Roadmap (múltipla escolha)

Tópicos de interesse

1. Tipos de implementação proxy
2. Proxy características
3. VPN (Virtual Private Network) - IPv4/IPv6 - IPSec - Características
4. VPN modos de operação do IPSec (Transporte vs. Tunelamento)
5. Análise de vulnerabilidades em container (imagem) (Trivy)
(repositório de vulnerabilidades)
6. Características do Firewalls
7. Análise de ACL (Access Control List) Padrão vs. Estendida
8. Características do serviço NTP (Network Time Protocol)
9. Firewall características
10. Segurança em IoT direcionado aos sistemas SSO (Single Sign-On) - OAuth2

Tarefas para a atividade N1 - Preparação

1. Construção do webcrawler input: site (url) + número de caracteres output wordlist.txt
2. Preparar o ataque ao WPA2 Personal
3. Alteração da página default do Apache em ambiente ubuntu server
4. Assistir o filme wargames de 1983 (senha da administrador)

```
curl "https://avengers.marvelhq.com/" |
sed 's/[^\wA-Z ]//g' |
tr 'A-Z ' 'a-z\n' |
grep '[a-z]' |
sort -u > /tmp/wordlist.txt
```

[Cracking WiFi WPA2 Handshake](#)

Best WiFi Adapter for Kali Linux

Sl No	WiFi Adapter	Chipset	Antenna	Link
1	TP-Link N150 TL-WN722N	Atheros AR9271	External	Buy it Now
2	Alfa AWUS036NHA	Atheros AR9271	External	Buy it Now
3	Alfa AWUS036NH	Ralink RT307	External	Buy it Now
4	Alfa AWUS1900	Realtek RTL88XX	External	Buy it Now
5	Alfa AWUS036ACH	RealtekRTL8812AU	External	Buy it Now
6	Panda PAU06	Atheros	External	Buy it Now
7	Panda PAU09	Ralink RT5572	External	Buy it Now
8	ALFA AWUS036NEH	Ralink RT307	External	Buy it Now



Capture the Flag

quinta-feira, 28 de abril de 2022

21:29

Data 13/5/2022 (sexta-feira)

Local: Laboratório 70

Recursos:

1. Um laptop por equipe (prioridade para alunos que venham de transporte próprio)
2. Cartão Wi-Fi USB (Modo Monitor ou Promiscuous Mode)
3. Kali Linux - Boot pelo Pendrive

Equipes : TCC (criar um nome para sua equipe)

Ataques:

1. Quebra do WPA2-Personal (wordlist - Rockyou) + Busca do target nmap
2. Brute Force - Hydra serviço de SSH + Web Crawler e/ou Engenharia Social (Filme War Games - 1983) (usuário = cabrini)
3. Alterar o site default do Apache2 (index.html) no Ubuntu Server 18.04.6 LTS