Hackers do Bem – Fundamental
Prof. Fábio Carneiro de Castro
12/02/2026

Atividade Prática – Módulo 2

Aulas 3 e 4

Gabriel dos Santos Schmitz

Este documento foi criado usando LaTeX
https://github.com/gabrielzschmitz/uni/tree/main/hackers-do-bem/fundamental/modulo2/aulas3-4.

1 Introdução

Este documento apresenta as evidências práticas das atividades do Módulo 2 (Aulas 3 e 4) do Programa Hackers do Bem – Nível Fundamental, por meio dos prints solicitados, demonstrando a correta execução das tarefas propostas.

Conforme orientações do curso, este documento reúne, em um único arquivo PDF, os seguintes prints obrigatórios: Atividade 2.6 (passo 8), Atividade 2.7 (passo 5), Atividade 2.8 (passo 7), Atividade 2.9 (passo 4) e Atividade 2.10 (passo 7), todos acompanhados de breve descrição explicativa para facilitar a avaliação pelo instrutor.

2 Atividades

Atividade 2.6. Explorando o controle técnico de criptografia de dados com Ccrypt no Kali Linux

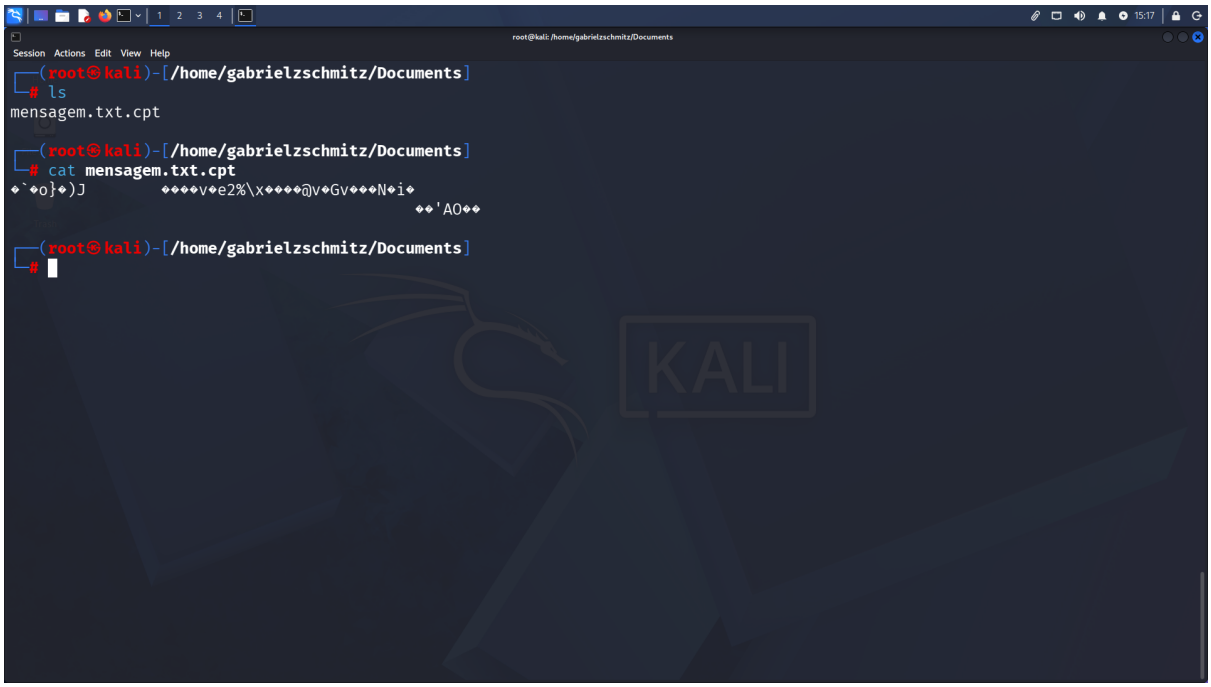

Fig. 1: Arquivo mensagem.txt convertido para mensagem.txt.cpt após criptografia com Ccrypt

Sobre:

Nesta atividade, foi explorada a ferramenta `ccrypt`, utilizada para implementação de controle técnico de proteção de dados por meio de criptografia simétrica no Kali Linux.

Inicialmente, foi criado o arquivo `mensagem.txt` no diretório `/home/aluno/Documentos/`, contendo o texto "Hackers do bem!". Após confirmar sua criação com o comando `ls`, foram consultadas as opções da ferramenta por meio do comando `ccrypt -h`, a fim de compreender seus modos de operação e parâmetros disponíveis.

Para aplicar a criptografia, foi executado o comando `ccrypt -e mensagem.txt`. O parâmetro `-e` indica a operação de cifragem (*encryption*), convertendo automaticamente o arquivo original para `mensagem.txt.cpt`. Ao listar o diretório novamente e visualizar o conteúdo com `cat mensagem.txt.cpt`, verificou-se que os dados passaram a apresentar caracteres ilegíveis, evidenciando a aplicação da criptografia.

Em seguida, realizou-se o processo de descriptografia por meio do comando `ccrypt -d mensagem.txt.cpt`. O parâmetro `-d` indica a operação de decifragem (*decryption*). Após

a inserção da mesma chave utilizada na etapa anterior, o arquivo original `mensagem.txt` foi restaurado com seu conteúdo íntegro.

Por fim, o arquivo foi removido com o comando `rm mensagem.txt`, encerrando a atividade.

Atividade 2.7. Explorando os eventos de sistema com o Logcheck no Linux

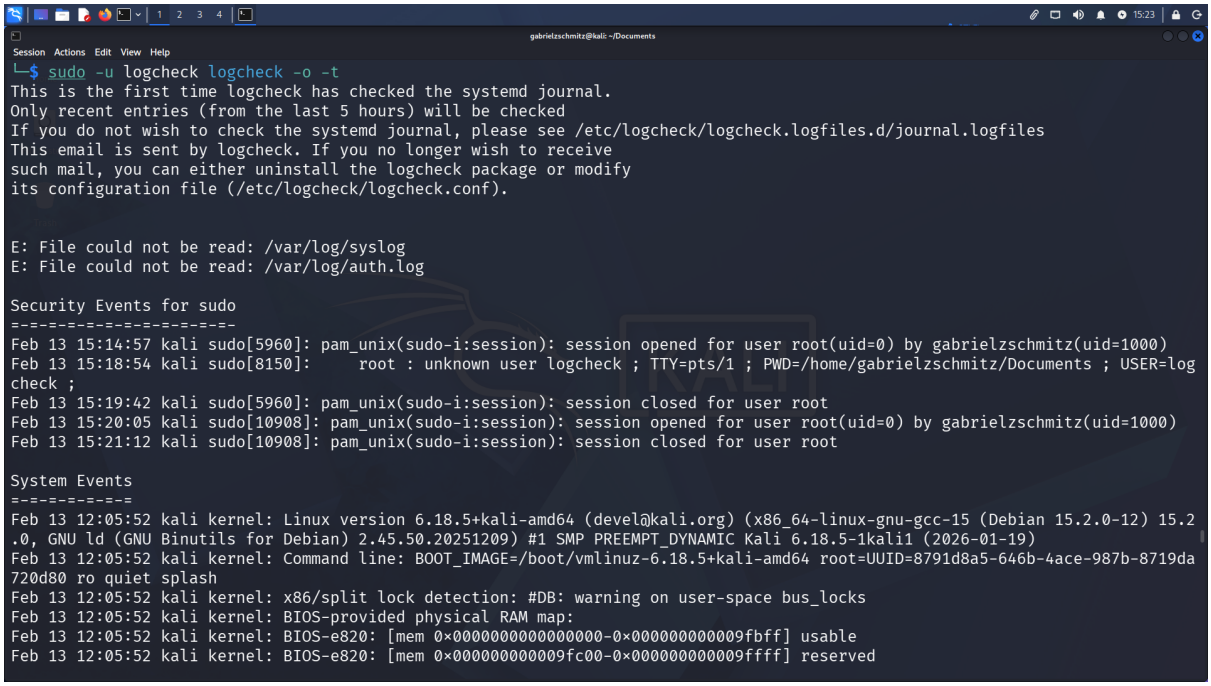

Fig. 2: Execução do Logcheck em modo workstation exibindo eventos de segurança e sistema

Sobre:

Nesta atividade, foi explorada a ferramenta `Logcheck`, utilizada como mecanismo de controle detectivo para análise automatizada de logs no Kali Linux. O objetivo foi identificar eventos relevantes de segurança e sistema a partir da filtragem das mensagens registradas pelo kernel e serviços ativos.

Inicialmente, foi executado o comando `sudo -u logcheck logcheck -o -t`, permitindo que o Logcheck operasse no modo online (`-o`) e exibisse os relatórios em formato texto simples (`-t`), sob o contexto do usuário específico `logcheck`. A saída apresentou eventos classificados em *Security Events* e *System Events*.

Entre os eventos de segurança, destacaram-se registros relacionados ao `sudo`, indicando abertura e encerramento de sessões privilegiadas para o usuário root, evidenciando monitoramento de atividades com elevação de privilégios.

Nos eventos de sistema, foram observadas mensagens do `dhclient` relativas a solicitações DHCP na interface `eth0`, bem como erros do serviço `xrdp-chansrv` associados à área de transferência durante sessões RDP. Esses registros demonstram a capacidade da ferramenta em identificar tanto eventos operacionais quanto possíveis anomalias.

Posteriormente, foi acessado o arquivo de configuração `/etc/logcheck/logcheck.conf` com privilégios administrativos, alterando o parâmetro `REPORTLEVEL` para `"workstation"`, definindo um nível de filtragem adequado para estações protegidas. Opcionalmente, foi configurado o parâmetro `SENDMAILTO` e `MAILASATTACH` para envio de relatórios por e-mail.

Após a modificação, o comando foi executado novamente, sendo exibida uma nova saída contendo registros adicionais de abertura e encerramento de sessões sudo, bem como novos eventos DHCP e erros do serviço XRDP. Foram capturadas as 20 primeiras linhas conforme solicitado.

Atividade 2.8. Explorando o navegador Tor no Kali Linux

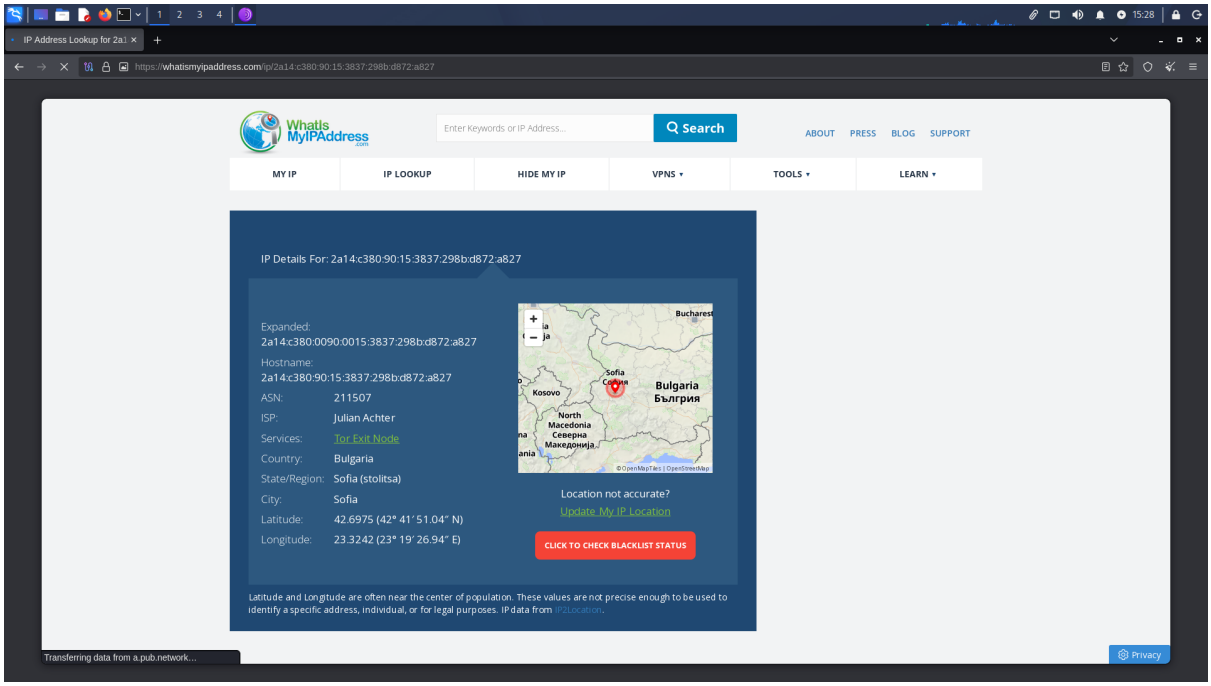

Fig. 3: Verificação do endereço IP no Tor Browser demonstrando uso de nó de saída da rede Tor

Sobre:

Nesta atividade, foi explorado o navegador *Tor Browser* no Kali Linux, com o objetivo de compreender seu funcionamento e verificar, na prática, o mascaramento de endereço IP por meio da rede Tor.

Inicialmente, o navegador foi iniciado com o comando `torbrowser-launcher`, responsável por baixar, verificar assinatura digital e executar a versão mais recente do Tor Browser. Após a abertura, foi selecionada a opção "Conectar", permitindo o estabelecimento de uma conexão com a rede Tor. Em caso de falha inicial, foi utilizada a opção "Try a bridge" para contornar possíveis restrições de rede.

Com o navegador conectado, foi acessado o site `https://duckduckgo.com/`, confirmando a navegação funcional. Em seguida, foi aberto o site `https://whatismyipaddress.com/` para identificação do endereço IP público e da localização aparente.

Os dados apresentados indicaram um endereço IP associado a um *Tor Exit Node*, com provedor identificado como *Stiftung Erneuerbare Freiheit* e localização em Frankfurt, Alemanha. Essa informação confirma que o tráfego estava sendo roteado pela rede Tor, ocultando o endereço IP real da máquina.

Para fins comparativos, o mesmo site foi acessado utilizando o Mozilla Firefox (fora da rede Tor). Nesse caso, o IP identificado correspondia a um provedor distinto (Amazon.com Inc.), com localização nos Estados Unidos, evidenciando navegação convencional sem anonimização.

A diferença entre os endereços IP e localizações demonstrou, de forma prática, o funcionamento do Tor como mecanismo de anonimização, encaminhando o tráfego por múltiplos nós distribuídos globalmente.

Atividade 2.9. Navegando na DeepWeb pelo navegador Tor no Kali Linux

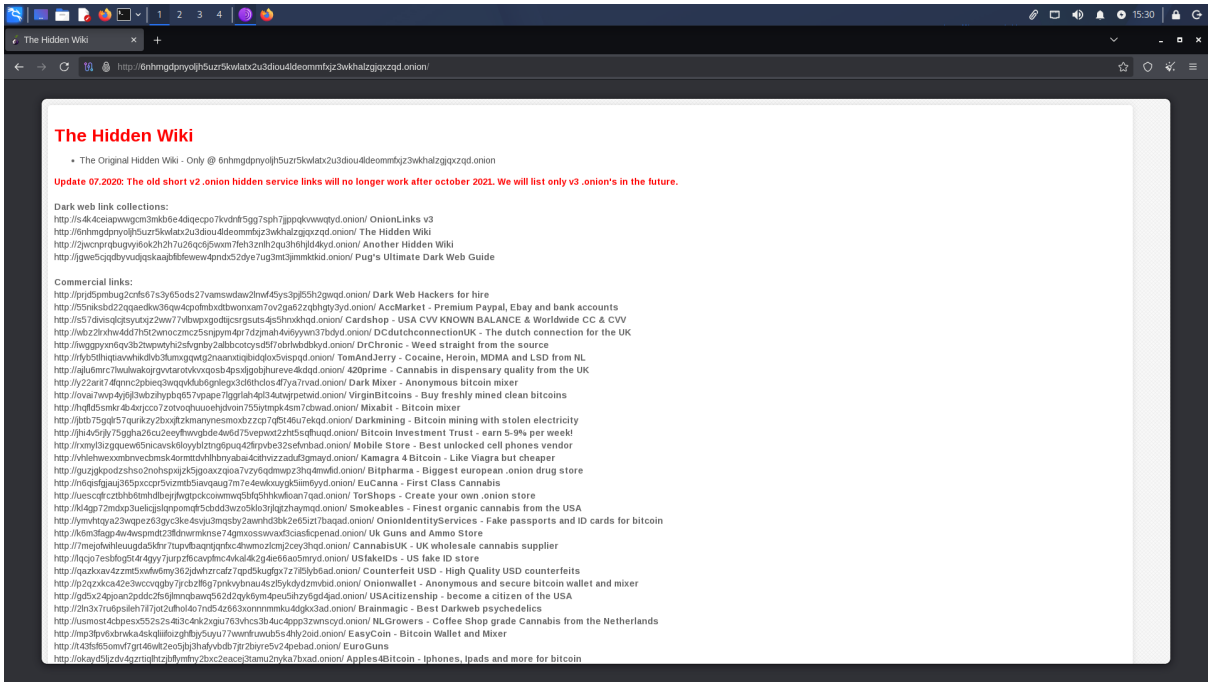

Fig. 4: Acesso a serviço .onion no Tor Browser demonstrando navegação na rede Tor

Sobre:

Nesta atividade, foi realizada a navegação em serviços hospedados na rede Tor, dando continuidade à configuração realizada na atividade anterior. O objetivo foi compreender o funcionamento de endereços `.onion` e observar, na prática, o acesso a conteúdos disponíveis exclusivamente dentro da rede Tor.

Inicialmente, utilizando o navegador convencional (Firefox), foi acessado um diretório público que lista endereços da rede Tor. Observou-se que os serviços da DeepWeb possuem como característica principal a utilização da extensão `.onion`, a qual não é resolvida pelo DNS tradicional e exige o uso do Tor Browser para roteamento adequado.

Em seguida, no Tor Browser já conectado à rede Tor, foi acessado um endereço `.onion` de teste. Após alguns instantes de carregamento, o serviço foi exibido com sucesso, confirmando que o tráfego estava sendo encaminhado por circuitos da rede Tor até o respectivo serviço oculto. A mensagem apresentada indicava tratar-se de um serviço na versão v3, modelo atualmente adotado devido a melhorias criptográficas e de segurança em relação aos antigos serviços v2.

Posteriormente, foram testados outros endereços `.onion` disponibilizados na página de referência. Constatou-se que alguns serviços podem estar temporariamente indisponíveis. Essa indisponibilidade pode ocorrer por diversos fatores, como instabilidade do serviço, encerramento voluntário, medidas judiciais ou ataques cibernéticos.

A atividade permitiu observar que:

- Serviços `.onion` só são acessíveis por meio da rede Tor;
- O tempo de carregamento tende a ser superior ao da navegação convencional, devido ao roteamento por múltiplos nós;
- A disponibilidade dos serviços pode variar significativamente;
- A navegação deve ser realizada com cautela e responsabilidade.

Por fim, todas as janelas dos navegadores (Tor e Firefox ESR) e o Terminal foram encerradas, concluindo a atividade.

Atividade 2.10. Explorando as Políticas Locais e de Conta nas Configurações de Segurança do Windows Server 2022

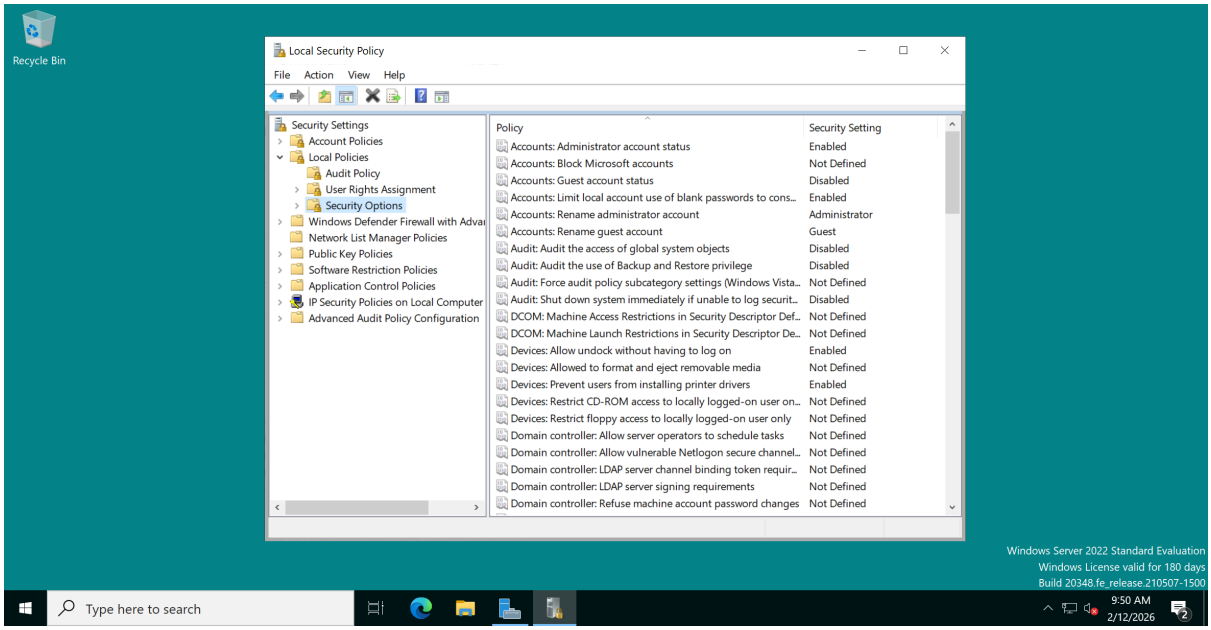

Fig. 5: Interface do Local Security Policy (secpol.msc) no Windows Server 2022

Sobre:

Nesta atividade, foi analisado o console `Local Security Policy` (`secpol.msc`) no Windows Server 2022, com foco na compreensão das políticas locais e de conta como mecanismos de controle gerencial e técnico de segurança.

Após o acesso remoto ao servidor via RDP, foi utilizado o campo de busca para executar o comando `secpol`, abrindo o console de gerenciamento de políticas de segurança locais.

1. Account Policies

Dentro de *Account Policies*, foram examinadas duas categorias principais:

Password Policy — Define os critérios aplicáveis às senhas das contas locais. Entre os parâmetros observados destacam-se:

- Histórico de senhas, impedindo reutilização recente;
- Idade máxima e mínima da senha, controlando periodicidade de troca;
- Comprimento mínimo, fortalecendo a robustez das credenciais;
- Requisitos de complexidade, exigindo combinação de caracteres variados.

Essas configurações contribuem diretamente para mitigar ataques de força bruta e reutilização de credenciais.

Account Lockout Policy — Responsável por definir regras de bloqueio após tentativas consecutivas de autenticação malsucedidas. Foram analisados:

- Limite de tentativas inválidas;
- Tempo de bloqueio da conta;
- Intervalo para redefinição do contador.

Essas definições atuam como proteção contra ataques de tentativa e erro (*brute force*).

2. Local Policies

No menu *Local Policies*, foi explorada a seção *Audit Policy*, que permite configurar o registro de eventos de segurança no *Event Viewer*. Entre as categorias avaliadas:

- Auditoria de logon de conta;
- Auditoria de gerenciamento de contas;
- Auditoria de acesso a objetos;
- Auditoria de alterações de política;
- Auditoria de uso de privilégios;
- Auditoria de eventos do sistema.

Essas configurações estabelecem controles detectivos fundamentais para monitoramento e rastreabilidade de ações realizadas no servidor.

Ainda em *Local Policies*, foi analisado o item *User Rights Assignment*, que permite atribuir permissões específicas a usuários ou grupos, como direito de logon local, logon via RDP, desligamento do sistema, entre outros.

3. Security Options

Na seção *Security Options*, foram observadas configurações críticas relacionadas à postura de segurança do sistema, incluindo:

- Status das contas Administrator e Guest;
- Configurações de canal seguro para membros de domínio;
- Controle de exibição do último usuário na tela de logon;
- Exigência de combinação CTRL+ALT+DEL para autenticação.

Essas opções permitem endurecer a superfície de ataque do sistema operacional por meio de ajustes administrativos.