Atividade Integradora - EXTRA SALA

CIBERCEGURANÇA

Tarefa 1 - Definição e Exemplos Reais

A **segurança cibernética** é basicamente tudo o que envolve proteger nossos sistemas, redes e dados de ameaças da internet. Isso inclui o uso de senhas fortes, instalação de firewalls e a proteção contra vírus e ataques hackers. O principal objetivo é garantir que as informações no geral, permaneçam seguras e sem serem acessadas ou corrompidas por pessoas não autorizadas.

No cenário atual, a segurança cibernética tornou-se ainda mais crucial devido ao aumento dos ataques cibernéticos, que ocorreram juntamente com a expansão do uso de serviços digitais, como plataformas bancárias e a digitalização da vida pessoal. Esse crescimento de dados valiosos disponíveis nas redes torna empresas, governos e indivíduos alvos atraentes para criminosos cibernéticos.

À medida que as ameaças se tornam mais sofisticadas, a segurança cibernética se torna essencial não só para proteger dados, mas também para garantir que a confiança nas tecnologias e serviços online seja mantida.

Casos Reais:

1- Em outubro de 2022, a Record TV sofreu um ataque de ransomware que comprometeu seu acervo de conteúdos e dados confidenciais. Os hackers invadiram o sistema central da emissora, criptografando arquivos essenciais e dificultando o acesso da empresa aos seus conteúdos armazenados. Embora o departamento de TI tenha mantido backups, o ataque continuou ativo, e os dados vazaram na deep web, incluindo informações detalhadas sobre despesas, receitas publicitárias, documentos jurídicos e até dados pessoais de funcionários, como passaportes de personalidades contratadas.

Esse ataque poderia ter sido evitado com a aplicação de medidas mais rigorosas de segurança cibernética. Uma das principais precauções seria a atualização constante de sistemas e software, garantindo que todas as vulnerabilidades conhecidas fossem corrigidas antes que pudessem ser hackeadas. Outra medida importante seria a implementação de autenticação multifatorial (MFA) para dificultar o acesso não autorizado, mesmo no caso de credenciais vazadas ou comprometidas. Por fim, um monitoramento constante de sistemas, com a detecção de atividades suspeitas, e uma resposta rápida a incidentes poderia ter minimizado o impacto e evitado o vazamento de dados sensíveis.

2-Em outubro de 2022, o Banco de Brasília (BRB) foi alvo de um ataque de ransomware, onde os hackers exigiram 50 bitcoins (aproximadamente R$ 5,17 milhões) para evitar o vazamento de dados confidenciais. A invasão foi detectada pela equipe de segurança do banco, que informou que não houve impacto direto em contas correntes de clientes e não houve comprometimento financeiro imediato. No entanto, a ameaça era grave, pois o banco possui 4,7 milhões de clientes, cujos dados poderiam ter sido sequestrados, além de informações sensíveis relacionadas à instituição financeira.

O ataque poderia ter sido evitado por meio de medidas mais robustas de proteção de dados, como backups regulares e seguros, além de atualizações constantes de software para corrigir vulnerabilidades conhecidas. Além disso, a capacidade de detectar atividades suspeitas e agir rapidamente poderia ter minimizado o impacto do ataque.

Tarefa 2 - Ameaças e Vulnerabilidades

- Ameaças

1. Phishing é um golpe bem comum em que os criminosos enviam e-mails ou mensagens que parecem vir de fontes confiáveis, como bancos ou empresas conhecidas, com o objetivo de roubar informações sensíveis, como senhas e dados bancários. Isso afeta os sistemas ao permitir que malware seja instalado ou que credenciais de acesso sejam roubadas, o que compromete toda a segurança. Para evitar o phishing, é essencial usar filtros de e-mail para identificar essas mensagens fraudulentas e educar os usuários sobre como reconhecer esses tipos de golpes.
2. O ransomware funciona de maneira agressiva: ele criptografa os arquivos do usuário e exige um pagamento em troca da chave para desbloqueá-los. Isso pode paralisar sistemas inteiros, impedindo o acesso aos dados e causando uma grande perda de informações. Para se proteger, o ideal é ter backups regulares e manter o sistema e o antivírus sempre atualizados, o que pode ajudar a detectar e bloquear essas ameaças antes que causem danos.
3. Ataques DDoS (Distributed Denial of Service) acontecem quando os criminosos sobrecarregam um servidor ou rede com tráfego falso, tornando os serviços inacessíveis. Isso impacta diretamente os sistemas, pois pode deixar servidores lentos ou até fora do ar. A melhor forma de defesa contra DDoS é usar firewalls especializados e serviços de proteção na nuvem que possam filtrar esse tráfego indesejado.
4. Malware, como vírus ou trojans, é outro grande risco. Ele entra no sistema por meio de downloads ou links maliciosos e pode roubar dados, corromper arquivos ou até assumir o controle do computador. Para se proteger, é fundamental manter o antivírus e o sistema operacional atualizados e sempre tomar cuidado ao baixar arquivos, especialmente de fontes desconhecidas.
5. A SQL Injection ocorre quando os hackers inserem códigos maliciosos em campos de formulários de sites, permitindo que acessem e manipulem bancos de dados. Isso pode expor dados sensíveis e comprometer a segurança geral do sistema. Para evitar esse tipo de ataque, é importante validar e filtrar todas as entradas de dados em sites, além de usar consultas preparadas, que são mais seguras e evitam a injeção de código malicioso.

- Vulnerabilidades

Software desatualizado: muitos sistemas ficam expostos a riscos de segurança quando não recebem atualizações regulares, que geralmente corrigem falhas conhecidas e fortalecem a proteção contra novas ameaças. A solução prática para corrigir isso é habilitar as atualizações automáticas, garantindo que o sistema e os aplicativos sejam sempre atualizados com os patches de segurança mais recentes, sem a necessidade de intervenção manual.

Configuração inadequada de permissões de acesso: muitas vezes, os usuários ou administradores concedem permissões excessivas a arquivos, pastas ou serviços, o que permite que atacantes ou softwares maliciosos acessem dados sensíveis. A solução seria revisar e ajustar regularmente as permissões de acesso, garantindo que apenas usuários autorizados tenham acesso a informações e recursos críticos, utilizando o princípio do "menor privilégio".

Falta de autenticação multifatorial (MFA): mesmo cim senhas fortes, contas podem ser comprometidas por ataques de força bruta ou phishing. A solução prática para corrigir essa vulnerabilidade é implementar autenticação multifatorial (MFA), adicionando uma camada extra de segurança, como um código enviado para o celular ou um aplicativo de autenticação, dificultando o acesso não autorizado mesmo que a senha seja roubada.

Tarefa 3 - Credenciais e Engenharia Social

Luciana, analista de segurança de uma grande empresa, estava no trabalho quando um telefonema a surpreendeu. O suposto "suporte técnico" de um dos sistemas usados pela empresa estava do outro lado da linha. A pessoa se identificou como sendo da empresa de software com a qual Luciana tinha um contrato, e explicou que estavam realizando uma "manutenção de rotina" no sistema. Para garantir que sua conta não fosse afetada, o técnico solicitou que ela confirmasse suas credenciais e fornecesse acesso temporário ao seu computador para que a atualização fosse feita de forma segura.

Luciana, acostumada a lidar com atualizações e manutenções regulares, não pensou duas vezes e forneceu o número de sua conta e senha, além de permitir o acesso remoto ao seu computador. Após o telefonema, ela notou que algumas funções do sistema estavam lentas, mas atribuiu à manutenção solicitada. No entanto, no dia seguinte, a equipe de TI detectou atividades suspeitas em seu computador: acessos não autorizados a arquivos confidenciais e movimentações estranhas em contas bancárias da empresa.

Foi só então que Luciana percebeu que havia sido vítima de um ataque de engenharia social. O "técnico" não era realmente da empresa de software, mas um criminoso que havia se passado por um profissional de suporte para obter suas credenciais e comprometer sistemas críticos.

-Solução:

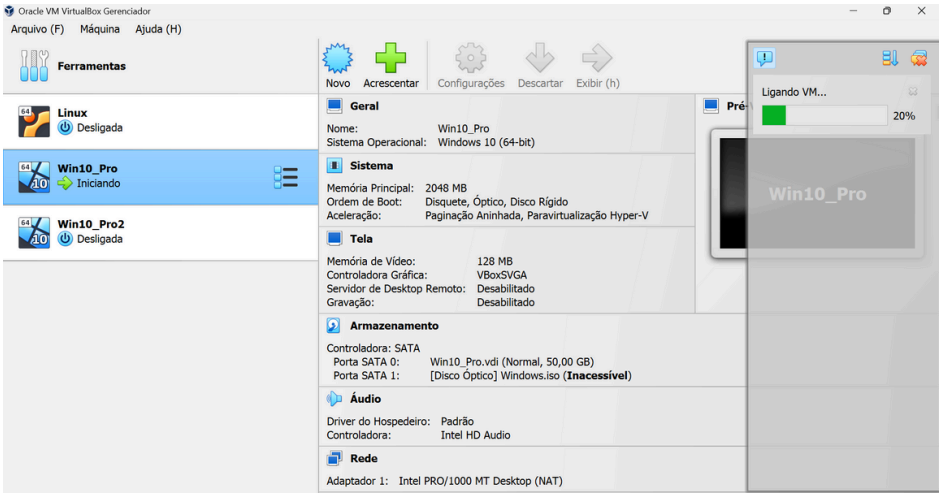
Após perceber que minhas credenciais foram comprometidas, meu primeiro passo seria alterar imediatamente as senhas e revogar o acesso à minha conta. Em seguida, pediria à equipe de TI para revisar os logs de acesso e investigar possíveis acessos não autorizados. Implementaria autenticação multifatorial (MFA) em todas as contas, especialmente as de acesso privilegiado, para fortalecer a segurança.

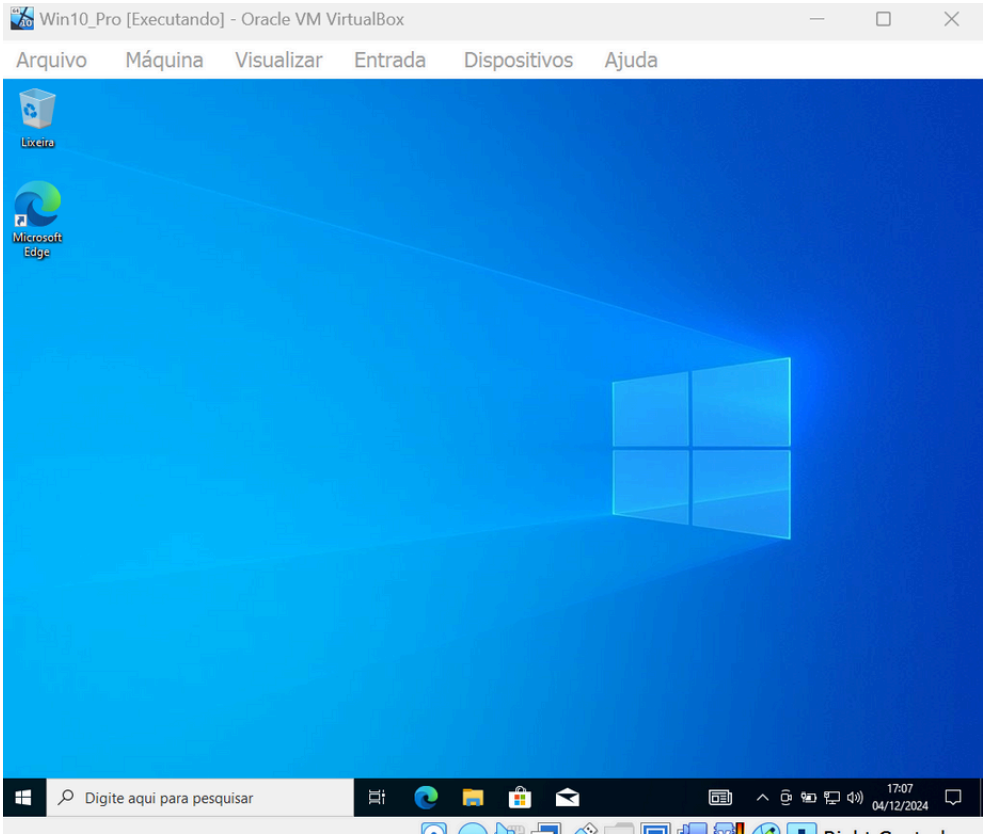
Além disso, realizaria um treinamento de conscientização com os colaboradores sobre os riscos de engenharia social, para evitar novos ataques. Por fim, estabeleceria um monitoramento contínuo de segurança para detectar rapidamente atividades suspeitas e garantir uma resposta rápida a incidentes futuros.

Tarefa 4 - Intervenções: Proteção e Prevenção

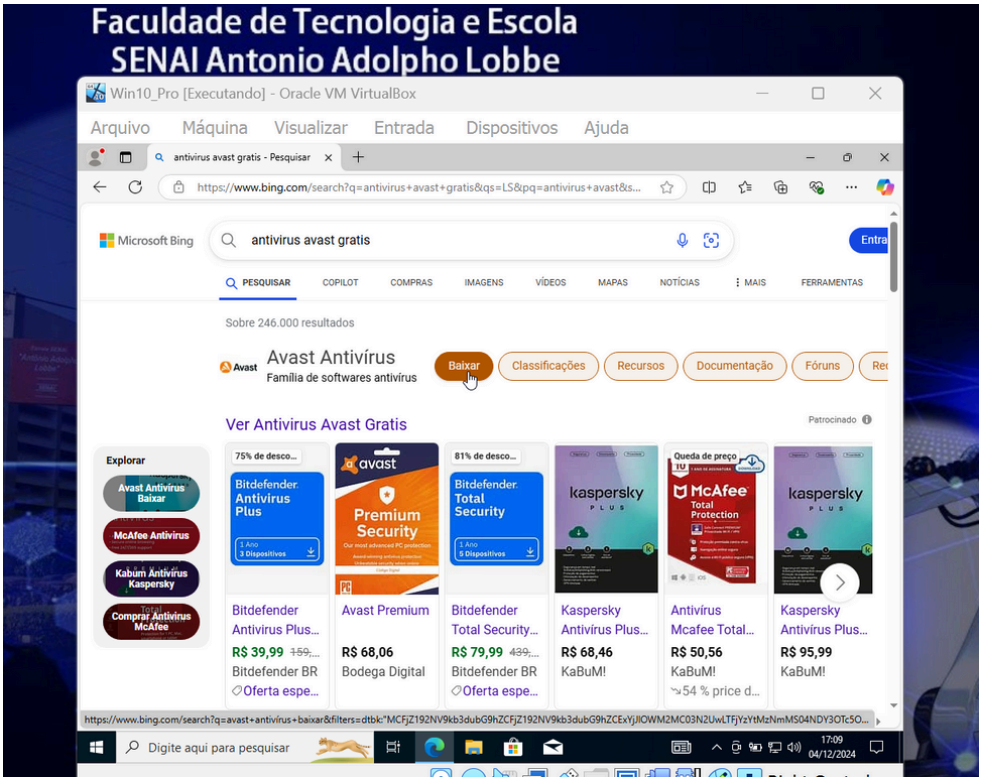
Prática:

Abri o Virtual Box e entrei com o Login e Senha SENAI.

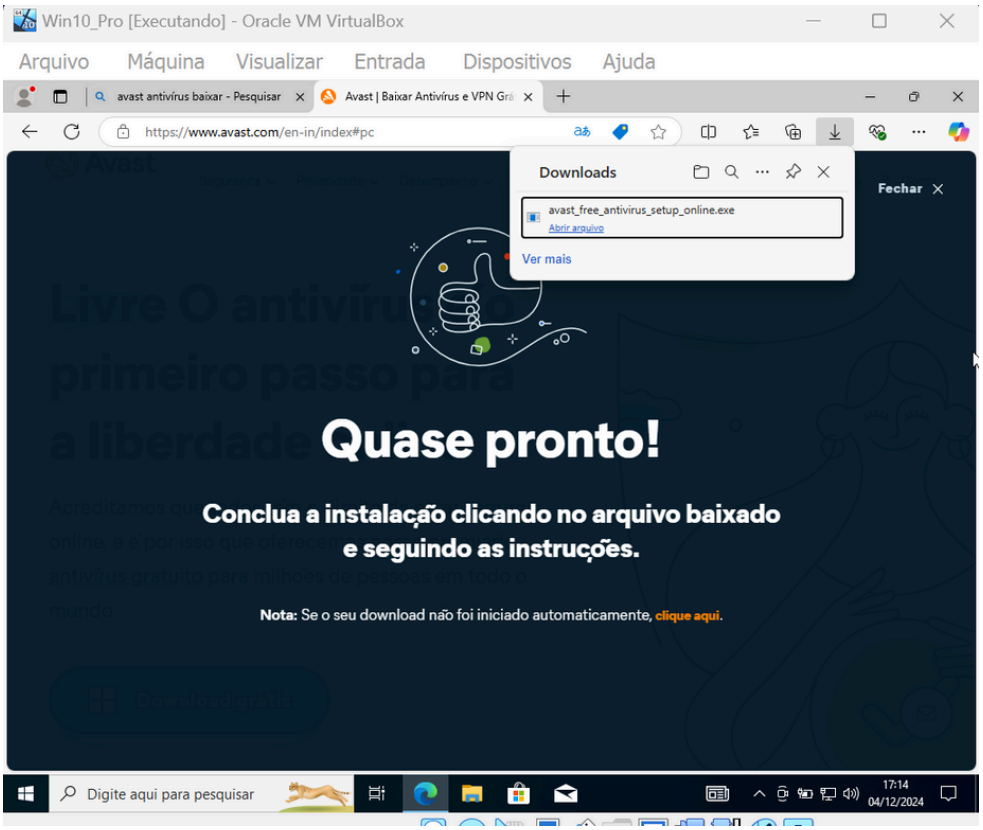


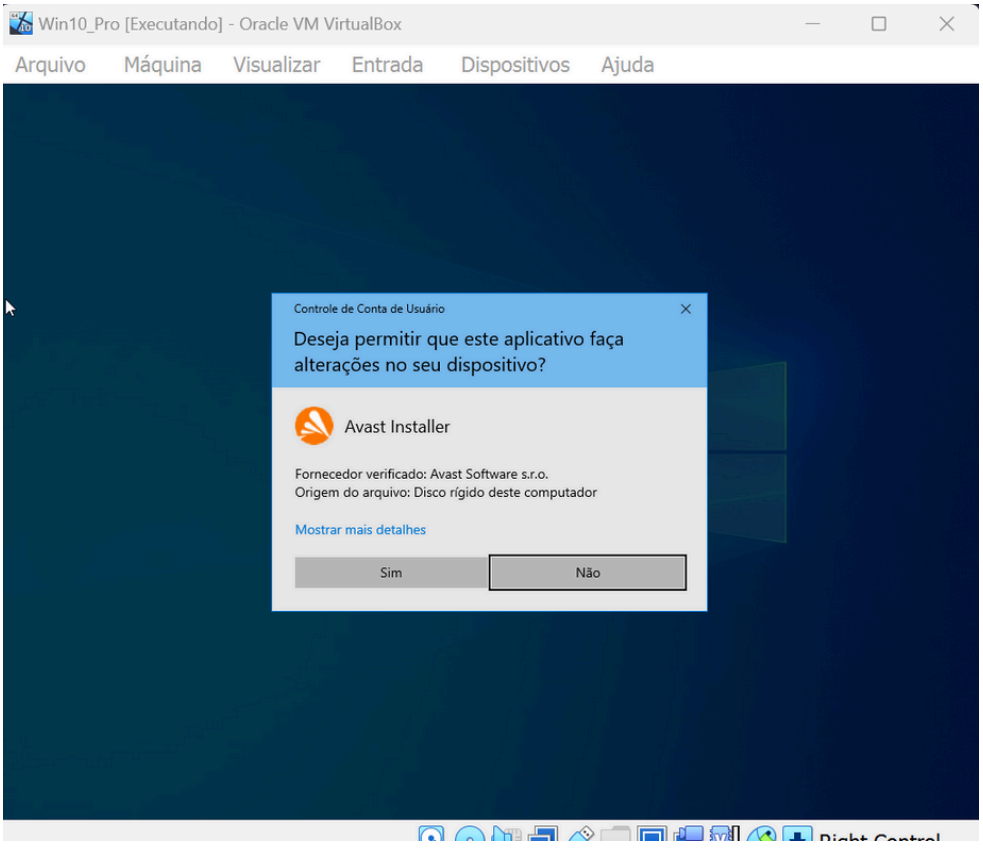


Entrei no Microsoft Edge e busquei por “Antivírus Avast grátis”, a fim de encontrar esse App de forma gratuita para a instalação.

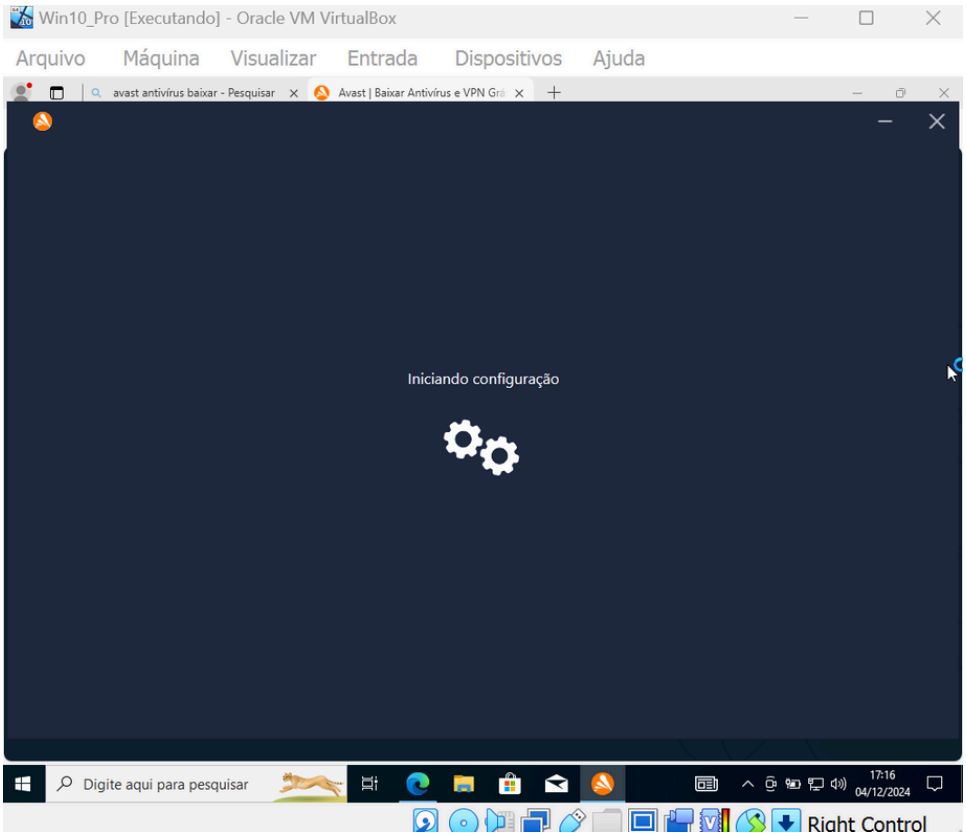


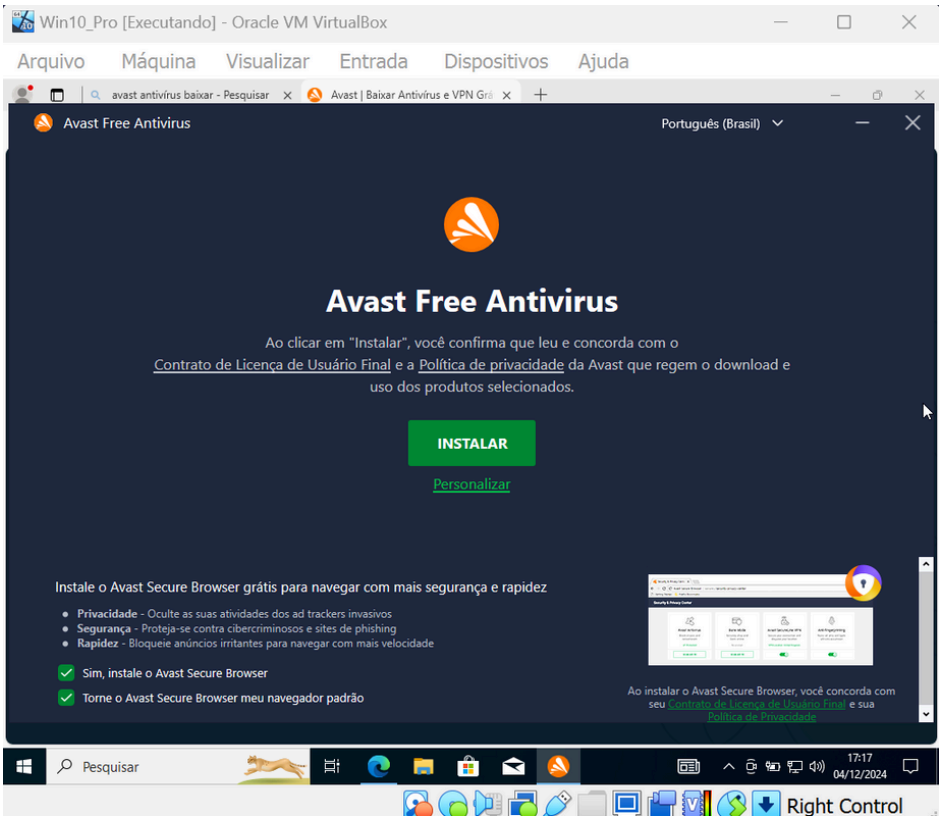
Cliquei em “Baixar” e fui dirigida a tal página. Apertando novamente no mesmo botão e seguindo as instruções a baixo, pude instalar o Antivírus.

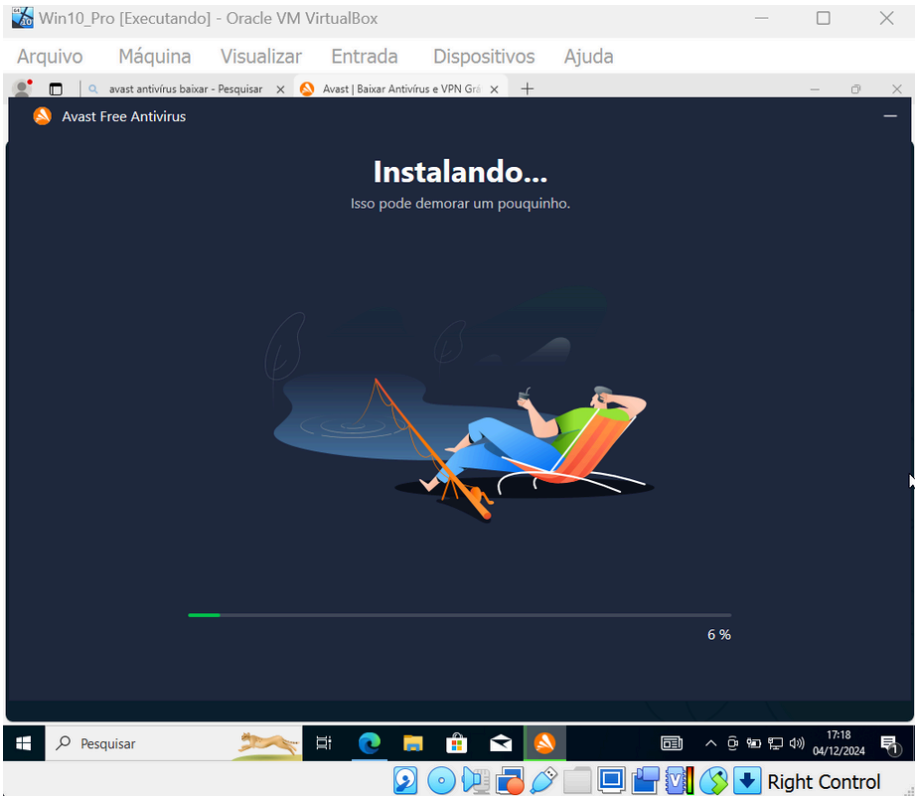


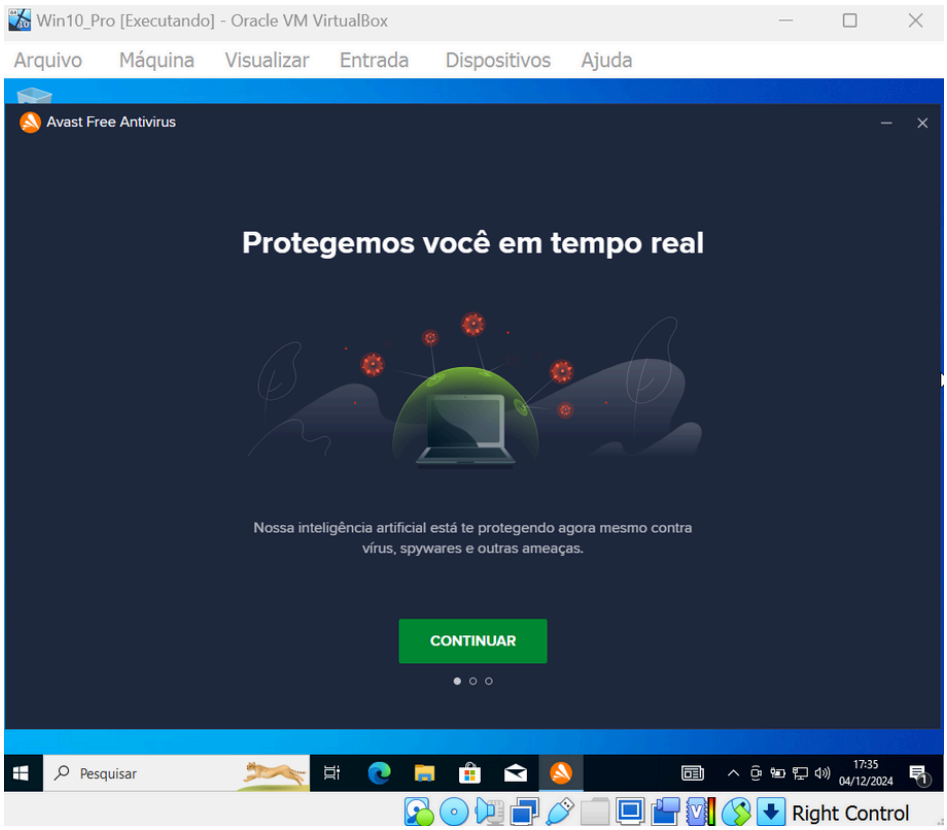


Após a instalação, começo a configuração dele, para que funcione.

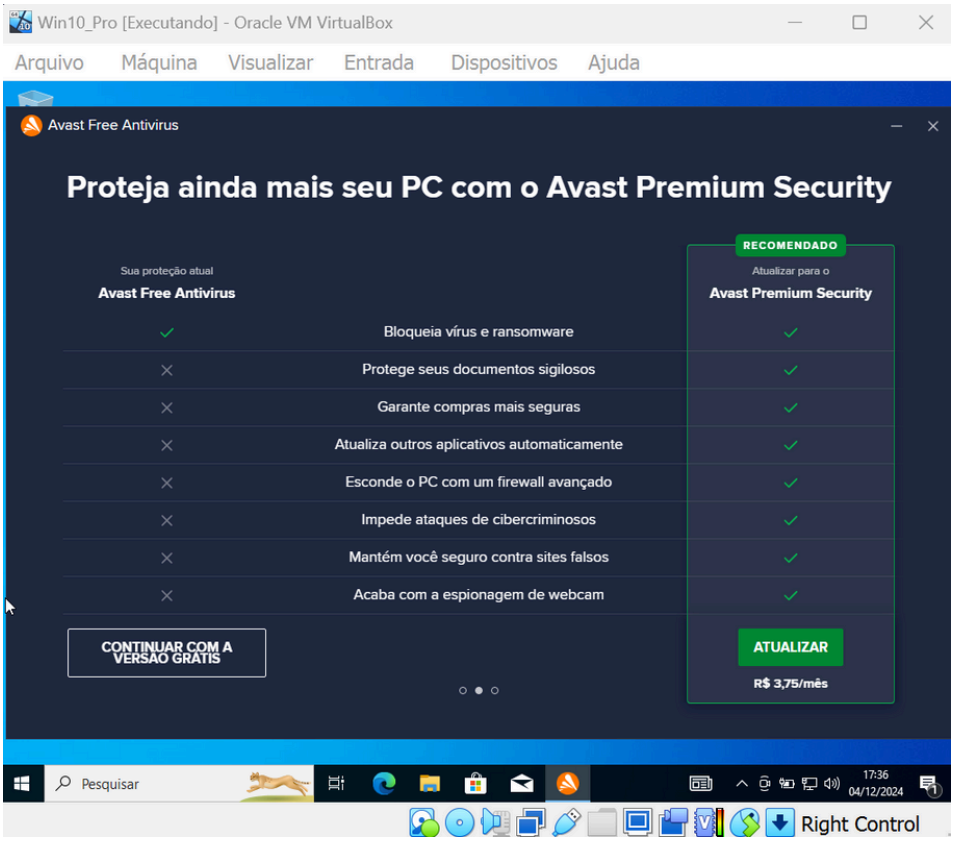

Win10_Pro [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
avast antivírus baixar - Pesquisar
Avast | Baixar Antivírus e VPN Grá
Iniciando configuração
Digite aqui para pesquisar
17:16
04/12/2024
Right Control

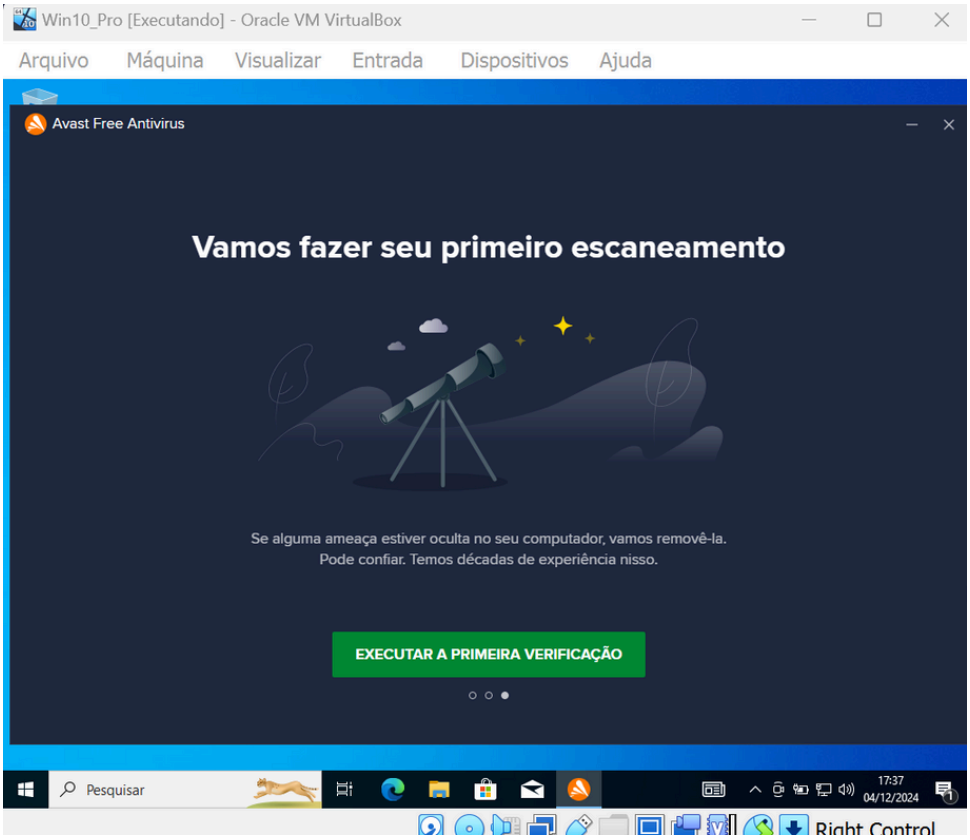

Win10_Pro [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
avast antivírus baixar - Pesquisar
Avast | Baixar Antivírus e VPN Grá
Avast Free Antivirus
Português (Brasil)
Avast Free Antivirus
Ao clicar em "Instalar", você confirma que leu e concorda com o
Contrato de Licença de Usuário Final e a Política de privacidade da Avast que regem o download e
uso dos produtos selecionados.
INSTALAR
Personalizar
Instale o Avast Secure Browser grátis para navegar com mais segurança e rapidez
Privacidade - Oculte as suas atividades dos ad trackers invasivos
Segurança - Proteja-se contra cibercriminosos e sites de phishing
Rapidez - Bloqueie anúncios irritantes para navegar com mais velocidade
Sim, instale o Avast Secure Browser
Torne o Avast Secure Browser meu navegador padrão
Ao instalar o Avast Secure Browser, você concorda com
seu Contrato de Licença de Usuário Final e sua
Política de Privacidade
Pesquisar
17:17
04/12/2024
Right Control



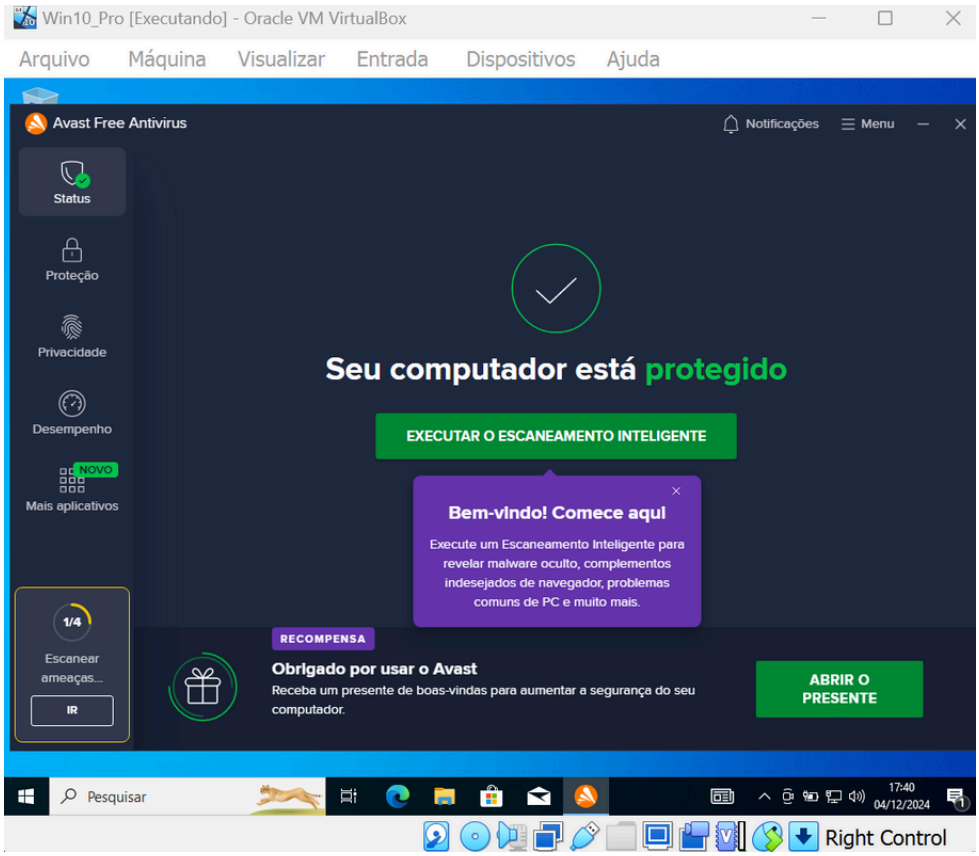


Selecionar: “Continuar com a versão gratuita”

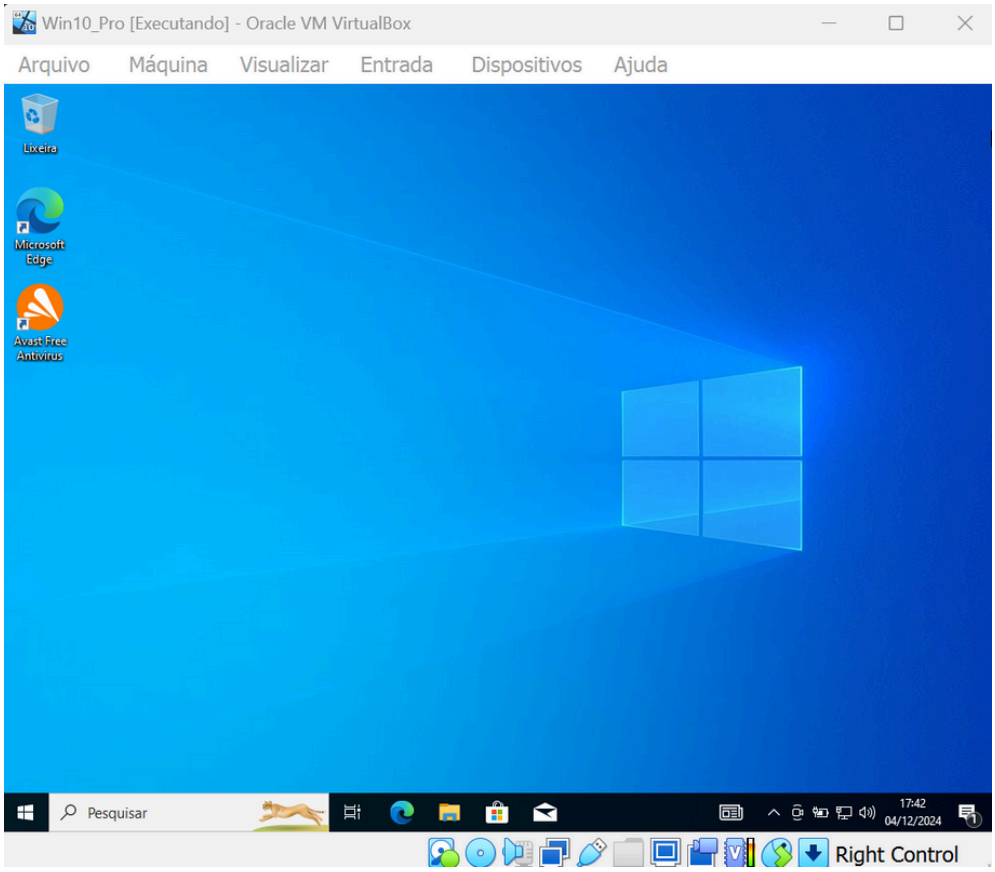




Apertar em “Executar a primeira verificação”:



Pronto, agora nosso Avast está pronto e funcionando.



Cartilha de Segurança:

1. Nunca clique em links desconhecidos.

2. Use senhas fortes e únicas.
3. Ative a autenticação de dois fatores (2FA).
4. Mantenha o software sempre atualizado.
5. Desconfie de e-mails de remetentes desconhecidos.
6. Evite redes Wi-Fi públicas para transações sensíveis.
7. Use um antivírus confiável e atualizado.
8. Realize backups regulares.
9. Monitore as permissões de aplicativos e dispositivos.
10. Eduque-se sobre segurança cibernética.