

Sessão 3: Enumeração básica e busca por vulnerabilidades



As atividades desta sessão serão realizadas em sua máquina física (hospedeira).

1) Controles de informática

1. Uma avaliação (*assessment*) de segurança da informação de uma organização é a medição da postura de segurança de um sistema ou organização frente a ameaças. Essas avaliações são baseadas em análise de riscos, por seu foco em vulnerabilidades e impacto. A ideia é fazer uma análise dos três métodos que, combinados, avaliam os processos de Tecnologia, Pessoas e Processos com respeito à segurança.

Leia o documento de escopo para avaliação de segurança da SANS, em <https://www.sans.org/reading-room/whitepapers/awareness/scoping-security-assessments-project-management-approach-33673>, e responda: sua organização possui controles e políticas sobre a segurança da informação? Quais aspectos poderiam ser melhorados, com base no exposto pelo documento de escopo acima?

2. Quais portas e serviços estão acessíveis na sua máquina? Faça a auditoria em <http://www.whatsmyip.org/port-scanner/>. Faça um *scan* para portas de servidores e aplicações e descreva as que estão abertas em seu computador, assim como seus serviços.
3. Teste os servidores de DNS e de correio eletrônico de sua instituição, fazendo a auditoria em <https://mxtoolbox.com/dnscheck.aspx> e <http://dnscheck.pingdom.com/>. Você encontrou alguma vulnerabilidade conhecida?

2) Serviços e ameaças

1. Verifique as seguintes listas de portas:
 - Top 10 portas mais atacadas: <https://isc.sans.edu/top10.html>
 - Ataque: <http://www.portalchapeco.com.br/~jackson/portas.htm>
 - Aplicações especiais: http://www.practicallynetworked.com/sharing/app_port_list.htm
 - Arquivo *services* no Windows: `C:\windows\system32\drivers\etc\services`
 - Arquivo *services* no Linux: `/etc/services`

De posse dessas informações, você consegue informar as portas mais vulneráveis? Explique.

2. Baixe o programa Spybot—Search & Destroy no link <https://www.safer-networking.org/mirrors27/>. Instale-o e verifique se algum *malware* é detectado no sistema.
3. O HijackThis é um programa que auxilia o usuário a eliminar uma grande quantidade de *malware* conhecidos. Apesar de ser uma ferramenta poderosa, não tem a automatização de ferramentas como o Spybot, exigindo conhecimento mais avançado por parte do usuário. Faça o download do programa no link <https://github.com/dragokas/hijackthis>.

Primeiro, vamos fazer um *scan* e analisar o log, que contém várias informações relevantes sobre o computador, como página inicial do navegador, servidores DNS em uso e processos executados na inicialização do sistema. Para fazer isso, clique no botão *Do a system scan and save a logfile*. Você deve obter um *scan* como o exibido abaixo:

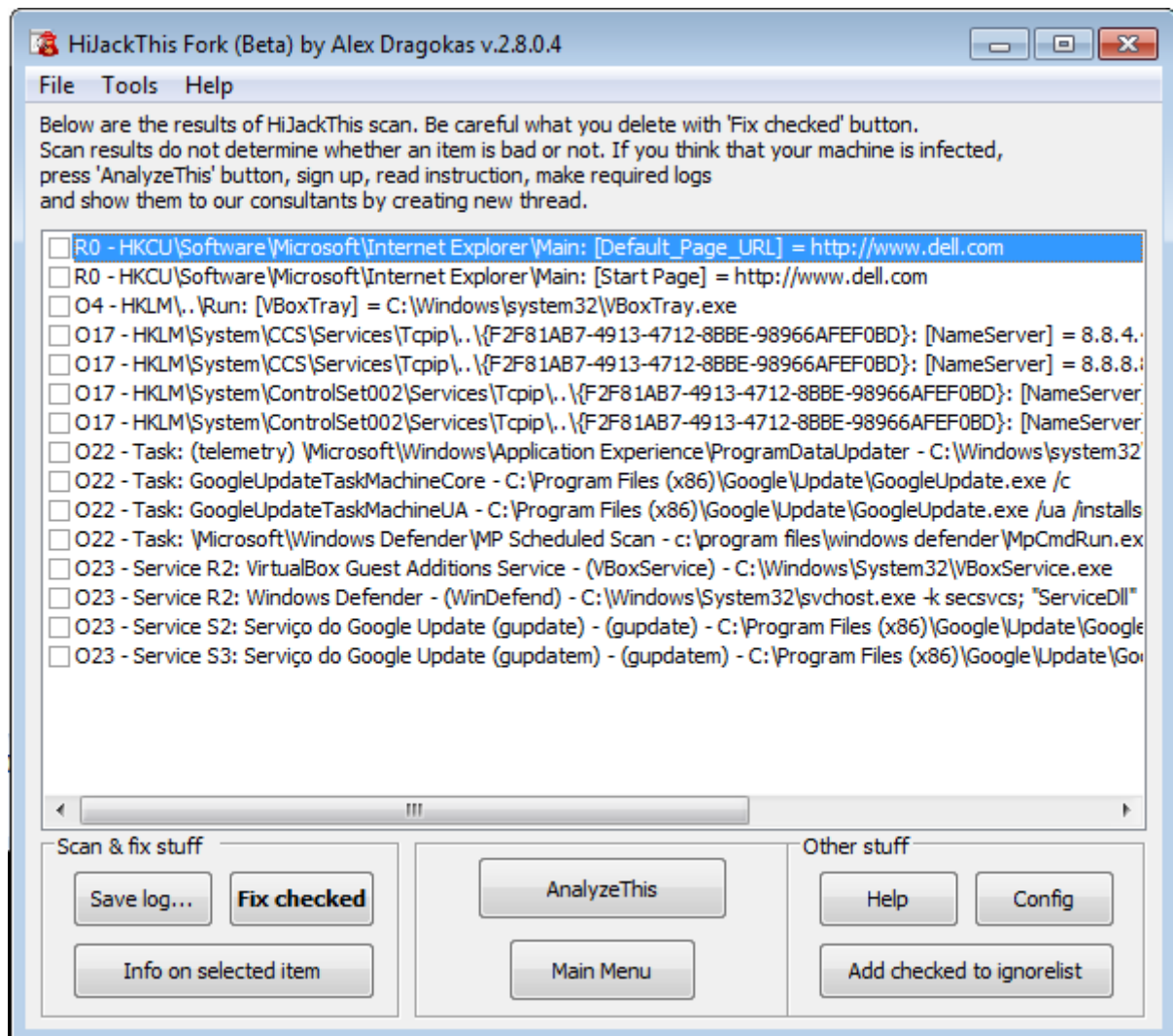


Figura 14: Scan do HijackThis

Se quiser corrigir elementos que foram identificados como perigosos, rode o programa novamente com a opção *Do a system scan only*. Em seguida, marque as entradas desejadas e depois clique em *Fix checked*. Tenha cuidado, pois as entradas identificadas pelo HijackThis não são necessariamente nocivas e devem ser estudadas individualmente pelo analista de segurança. Você constatou algum tipo de arquivo malicioso encontrado pela ferramenta?