Proteção Client-side: Testando a eficâcia das ferramentas de proteção Microsoft para estações de trabalho e desktops

Alexandro Silva

A grande vantagem dos cybercriminosos é o despreparo,para não dizer irresponsabilidade,das empresas e dos usuários na proteção dos seus sistemas contra as principais ameaças existentes.

Facilmente encontramos exemplos de grandes empresas que ao negligenciar a proteção das estações de trabalho e a conscientização do usuário tiveram seus sistemas invadidos e com seus dados vazados na internet.

Este artigo apresentará como proteger-se de diversas ações maliciosas testando a eficácia de algumas ferramentas de segurança para ambientes Windows mantidas pelo próprio fabricante. Servindo também como base para novas pesquisas e permitindo o aprofundamento deste tema que é bastante rico e pouco explorado.

Atenção:

Não é o objetivo deste artigo:

- Apresentar como os ataques são executados;
- Fazer propaganda de um fabricante ou ferramenta.

Laboratório

Foram utilizadas algumas técnicas de invasão em 5 cenários distintos** usando ferramentas como Nmap, Nessus, SET e Metasploit.

** OBS: Não foram exploradas vulnerabilidades em aplicações como o MSOffice, Adobe Reader e etc., nem foram utilizadas técnicas evasivas avançadas.

- Principais vetores:
  - Falhas do sistema operacional e do Internet Explorer 8;
  - Falha humana (Engenharia social).
- Exploits:
  - MS08-067
  - MS11-050
  - Java Applet Attack Method
- Payloads:
  - Bind shell reverse TCP
  - Meterpreter

Especificações

Host	Sistema Operacional	Aplicações
Atacante	Debian	Nmap5.59BETA1, Nessus 4.4.1, SET 1.5.2, Metasploit v3.8.0-dev
Alvo	Windows XP SP3	Internet Explorer 8, Windows Firewall (nativo), Microsoft Security Essentials 2.1

Testes realizados

	Cenario	Resultados Obtidos
1	Sistema totalmente desatualizado e sem as ferramentas de proteção habilitadas.	Neste cenário todas as técnicas utilizadas foram bem sucedidas, desde um simples scanning de portas e vulnerabilidade até a efetivação do ataque. Como o nosso alvo estava totalmente vulnerável a exploração concretizou-se de forma fácil e sem muitos atrativos
2	Sistema desatualizado com o Windows firewall habilitado.	Resposta do nmap com opções evasivas habilitadas(fragmentação e Decoy): sudo nmap -f -p135,137,139,445 -sS -D 192.168.0.2,192.168.0.5,ME,192.168.0.10,192.168.0.11 192.168.0.8 Starting Nmap 5.59BETA1 (http://nmap.org) at 2011-07-05 22:03 BRT Nmap scan report for 192.168.0.8 PORT STATE SERVICE 135/tcp **filtered** msrpc 137/tcp **filtered** netbios-ns 139/tcp **filtered** netbios-ssn 445/tcp **filtered** microsoft-ds O firewall ativado não permitiu a exploração porque as portas dos serviços vulneráveis estavam bloqueadas, mesmo com o alvo totalmente desatualizado. Nestas condições o metasploit tornou-se ineficaz. Ataques de Man in the Middle, DNS Spoofing e engenharia social são ótimas opções já que a grande falha humana de "Clicar em tudo que aparece na tela" é uma das grandas armas usadas pelos invasores. Neste momento o SET (Social Enginering Toolkit) juntamente com o ettercap (MITM e DNS Spoofing) e o metasploit são totalmente eficazes. O ataque foi bem sucedido já que o firewall não está preparado para bloquear ataques através de uma backdoor.
3	Sistema desatualizado com Firewall e MSE (Microsoft Security Essentials) habilitados	Os resultados obtidos anteriormente prevalecem. As técnicas de varredura de portas, análise de vulnerabilidade e ataques usando somente o metasploit não são concretizados. O MSE não permitiu a concretização do ataque usando o SET+Ettercap+MSF por ter detacado e alertado sobre a presença de malware (trojan) após confirmar o applet Java malicioso.

4	Sistema atualizado com o firewall e o MSE desabilitados	Com o firewall desativado as varreduras de portas e vulnerabilidades foram concluidas, sendo que nenhuma vulnerabilidade alta foi detectada. As possibilidades de exploração se resumem na exploração de vulnerabilidades 0day, são falhas publicadas (full disclosure) ou não mas sem correção disponibilizada pelo fabricante ou através de engenharia social.
5	Cenário ideal. Sistema atualizado com firewall e MSE habilitados.	Como as principais portas de entradas estão bloqueadas temos um ambiente totalmente hostil para ataques menos elaborados. Neste ambiente somente vulnerabilidades 0day e ataques bem elaborados serão eficazes, porém a possibilidades diminuem consideravelmente. Restando somente a conscientização do usuário como a principal vulnerabilidade a ser tratada.

Conclusão

Este artigo prova que é possível manter um ambiente seguro de forma simples. Neste caso será necessário um pouco de investimento (licença do Windows),com isso o sistema estará sempre atualizado.

Isto em conjunto com um programa de conscientização dos usuários sobre os efeitos danosos de um clique num link ou site indevido diminuiriam consideravelmente os ataques voltados ao lado cliente, como os de roubos de dados bancários por exemplo.

Links

- **Junho, um mês repleto de ciberataques** - http://anchisesbr.blogspot.com/2011/07/seguranca-junho-um-mes-repleto-de.html
- **Mcafee: Operação Aurora** - http://www.mcafee.com/br/threat-center/operation-aurora.aspx
- **Computer Based Social Engineering Tools: Social Engineer Toolkit (SET)** - http://www.social-engineer.org/
- **Metasploit** - http://www.metasploit.com
- **Ettercap** - http://en.wikipedia.org/wiki/Ettercap_%28computing%29
- **Microsoft Security Essential** - http://www.microsoft.com/pt-br/security_essentials/default.aspx
- **Man-in-the-middle Attack** - http://en.wikipedia.org/wiki/Man-in-the-middle_attack
- **Malwares Brazillian** - http://malwaresbr.blogspot.com/
- **Linha Defensiva** - http://www.linhadefensiva.org/
- **Webinar Local Threats -** http://malwaresbr.blogspot.com/2011/07/webex-do-local-threats-com-fabio.html

Sobre o autor

Alexandro Silva atua na área de TI a mais de 10 anos como especialista em segurança de redes e sistemas Unix/Linux. Atualmente é responsável pela segurança dos servidores e aplicações em um datacenter, professor em cursos de pós-graduação em Segurança da Informação e atuando também como consultor especialista em segurança de perímetro e profundidade, segurança de sistemas Web, análise de vulnerabilidade, prevenção e detecção de intrusão.