StaySafe

Isto sim é informação de qualidade !!!

www.staysafepodcast.com.br

2ª Edição

Agosto - 2010

Editorial

Sejam Bem Vindos a nossa 2ª Edição da Revista Stay Safe.

Agradecimento e Motivação ainda maior!!!

Tivemos uma grande repercurssão com a nossa primeira edição atingindo diversas empresas e também outros países de língua portuguesa, inclusive abrindo oportunidades de negócios para os autores que estiveram e acreditaram no nosso trabalho desde o início.

Queremos dizer que ficamos extremamente contentes e com isso, ainda mais motivados a continuar com este projeto.

Esperamos que aproveitem ao máximo o conteúdo desta 2ª edição e que aguardem ansiosamente a grande surpresa que teremos a partir de nossa 3º edição.

Bom Divertimento!!

Equipe Stay Safe
Jordan M. Bonagura - Thiago Bordini

Fale com a Revista Stay Safe
staysafe@staysafepodcast.com.br

Índice

Chamada de Artigos

Gostaria de ter seu artigo publicado na próxima edição da Revista Stay Safe?

Envie o seu trabalho para análise

cfp@staysafepodcast.com.br

Não esqueça de anexar biografia e imagem

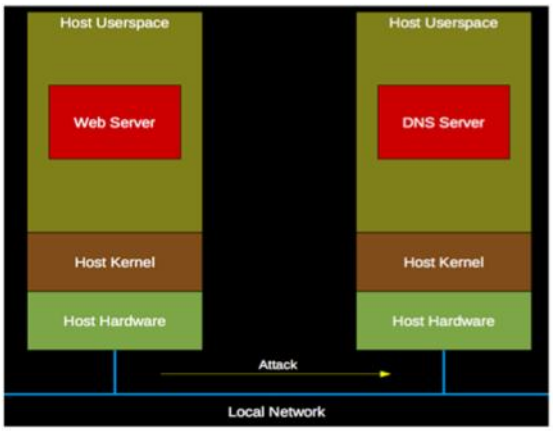
SVirt
Aumentando a Segurança na Virtualização

Por Jerônimo Zucco

Não é mais necessário dizer que o uso de virtualização está difundido. Sua utilização traz enormes vantagens, que vão desde alocação de recursos de maneira mais eficiente, economia de energia, escabilidade e crescimento de forma facilitada e rápida, além de auxiliar a projetar de forma mais racional a expansão da infra-estrutura e aumentar a disponibilidade de recursos.

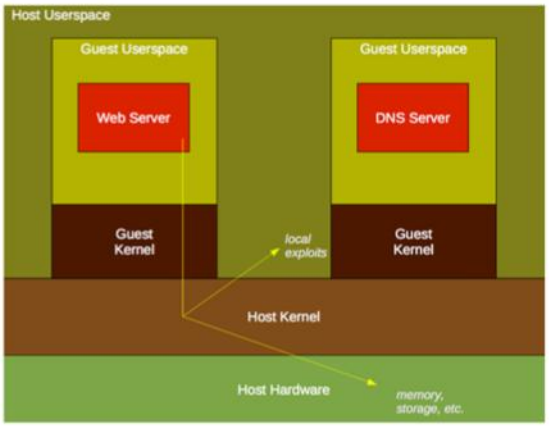
Mas e quanto a segurança? O que pode acontecer se um cracker aproveitar uma brecha de segurança do hypervisor ou de uma das máquinas virtualizadas para explorar as demais em um mesmo pool de hardware ?

Antes da virtualização, os servidores, de certa forma, eram isolados. Se um servidor for explorado por um cracker, ele apenas controla aquele servidor, podendo ou não lançar ataques de rede contra outros servidores. Administradores de sistema possuem muitas ferramentas para se defender contra ataques de rede: firewalls, IDS, etc.



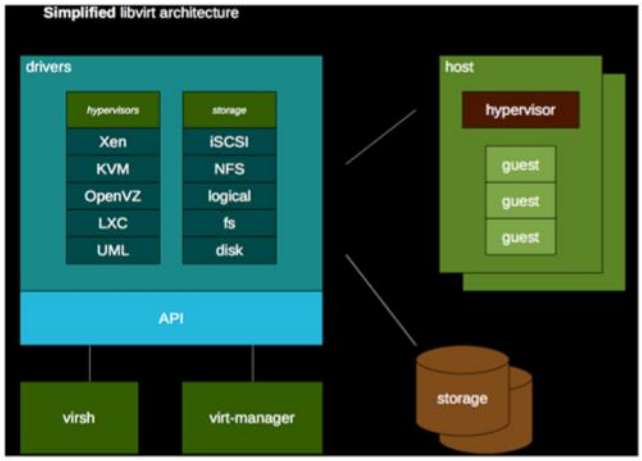
Agora utilizando a virtualização, nós possuímos múltiplos servidores virtualizados (os chamados guests) rodando em uma mesma máquina (o chamado hospedeiro). O hospedeiro roda um sistema operacional de virtualização, mais conhecido como hypervisor.

Se uma vulnerabilidade for descoberta no hypervisor, um atacante pode controlar todas as máquinas virtuais desse host, e inclusive alterar dados em discos virtuais disponibilizados para acesso dessas máquinas virtuais



Você pode até pensar que os ataques aos hypervisors podem ser teóricos ou impossíveis de serem feitos. Porém a notícia não é boa: essa é uma ameaça real, e inclusive já existiram vulnerabilidades que podem ser exploradas conforme descritas acima para as principais soluções de virtualização presentes no mercado, como Xen e VMWare, por exemplo. De acordo com o artigo "Sum of All Virtual Fears: The Breached Hypervisor", de Joe Hernick (disponível em http://www.scaleoutadvantage.techweb.com/news/hom_nwc20070903_sumoffears.jhtml), o uso de virtualização criou uma nova oportunidade para os atacantes, e, infelizmente, pode ser o pior pesadelo dos administradores e responsáveis pela área de segurança das empresas, que agora tem que se preocupar com a segurança, monitoramento e atualização dos hypervisors que rodam seus sistemas.

Por isso foi criado o sVirt, uma solução desenvolvida pela Red Hat que utiliza o SELinux e o libvirt para aumentar o nível de proteção de ambientes virtualizados. O libvirt é uma API de virtualização que cria uma camada de abstração para gerenciar diferentes esquemas de virtualização, conforme exemplificado na figura abaixo.

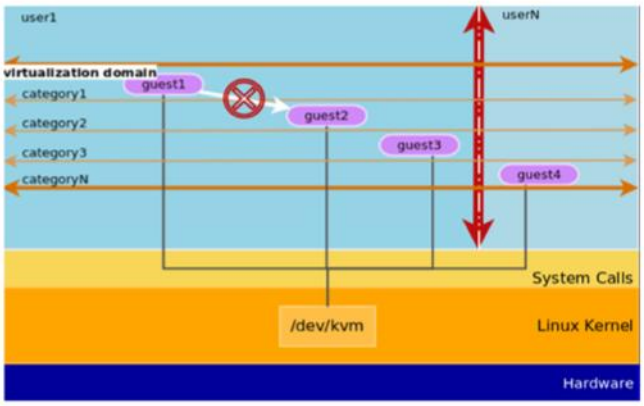


O SELinux ("Security-Enhanced Linux") é uma implementação de uma arquitetura MAC ("Mandatory Access Control") que provê uma política de segurança sobre todos os processos e objetos do sistema baseando suas decisões em rótulos (labels) contendo uma variedade de informações relevantes à segurança (contextos de segurança). Mais informações sobre SELinux podem ser vistos em minha monografia de pós-graduação disponível em: http://jczucco.blogspot.com/2010/06/monografia-sobre-selinux.html

O sVirt utiliza o SELinux para proteger o sistema hypervisor e também implementa o MCS (Multi Category Securty) em máquinas virtualizadas. Cada máquina virtualizada no host pode ser classificada em uma categoria, que é completamente isolada das demais.

A rotulagem MCS é simples do ponto de vista do usuário e administrador do sistema. Ela é constituída por um conjunto de categorias, que são simplesmente rótulos de texto, tais como "Company_Confidential" ou "Medical_Records", e depois atribuir usuários a essas categorias. O administrador configura primeiro o sistema de categorias e depois as atribuí aos usuários, conforme necessário para a implementação específica.

Em um ambiente corporativo, as categorias poderiam ser usadas para identificar documentos confidenciais para departamentos específicos. Categorias poderiam ser estabelecidas para "Finanças", "Folha de Pagamento", "Marketing" e "Pessoal". Somente usuários atribuídos a essas categorias podem acessar os recursos marcados com a mesma categoria. Essas categorias podem ser expressas no contextos de seguranças utilizados no SELinux e atualmente é suportado até 1024 categorias no MCS.



O sVirt através do SELinux e do libvirt aplica uma política de segurança que impede qualquer interação entre as máquinas virtuais guests, pois cada guest roda em uma categoria diferente, reduzindo os riscos que surgem de falhas de ou configurações mal feitas em ambiente de máquina virtual.

Aumenta também o controle sobre o acesso a recursos de máquinas virtuais (imagens, partições, etc), garantindo que cada máquina virtual acesse somente os seus próprios recursos, além de controlar melhor o acesso a recursos compartilhados entre as máquinas virtuais (dispositivos diversos, rede virtual, imagens, etc). O controle discricionário (DAC) também é realizado, mas o MAC é muito mais eficiente. A integração entre a máquina virtual com o hypervisor também é melhor controlado através da aplicação da política do SELinux.

O sVirt, se for utilizado junto com com o software virt-manager, requer uma intervenção mínima de administração, pois já aplica os rótulos (labels) corretos MCS em cada máquina virtual gerenciada através dele. Desde o Linux Fedora 12, e a partir do Red Hat Enterprise Linux 6, esse mecanismo virá habilitado por padrão e não precisarão de configuração manual.

Esse é um grande passo para aumentar a segurança da virtualização, isolando as máquinas virtuais entre si e com o sistema hospedeiro. Essa proteção adicional dificulta ainda mais a exploração de vulnerabilidades na virtualização, e sua fácil administração torna mais acessível a sua utilização, aumentando a sua popularidade e tornando o pesadelo do administrador um sonho mais tranquilo.

Alguns outros controles além do sVirt também podem ser utilizados para aumentar a segurança no uso de virtualização, caso queira saber mais, recomendo o excelente blueprint de Klaus Kiwi, da IBM: Securing KVM Guests and the host system", disponível em: http://publib.boulder.ibm.com/infocenter/lnxinfo/v3r0m0/topic/liaai/kvmsec/kvmsecstart.htm .

Referências:

Página oficial do sVirt:
http://selinuxproject.org/page/SVirt

Artigo de Joe Hernick: "Sum of All Virtual Fears: The Breached Hypervisor":
http://www.scaleoutadvantage.techweb.com/news/hom_nwc20070903_sumoffears.jhtml

Vídeo: "sVirt: Hardening Linux Virtualization with Mandatory Access Control"-
http://video.google.com/videoplay?docid=5750618585157629496#

Multi-Category Security (MCS) -
http://centos.org/docs/5/html/Deployment_Guide-en-US/sec-mcs-ov.html

Vídeo: "Secure Virtualization with sVirt"-
http://jczucco.blogspot.com/2009/10/secure-virtualization-with-selinux.html

sVirt: Integrating SELinux and Linux-based virtualization -
https://www.redhat.com/archives/libvir-list/2008-August/msg00255.html

Securing KVM Guests and the host system -
http://publib.boulder.ibm.com/infocenter/lnxinfo/v3r0m0/topic/liaai/kvmsec/kvmsecstart.htm

Jerônimo Zucco

CISSP;

Bacharel em Ciências da Computação;

Pós Graduado em Gerência e Segurança de Redes de Computadores;

Experiência de mais de 15 anos em TI, sendo 10 relacionada a área de Segurança;

Já palestrou em diversos eventos no Brasil;

Especialista em Software Livre e de Código Aberto;

Membro do Projeto OWASP Capítulo Brasil e do #SecurityGuys.

Amigos Snorteiros,

Dando continuidade aos artigos sobre as regras que foram lançadas pelo Emerging-Threats faremos nossas sugestões e comentários sobre as regras. Sempre frisando que as sugestões não são baseadas em analise de performance, ou seja, use as com cuidado.

Devido ao delay entre o primeiro artigo e esse utilizarei 7 updates de Junho e Julho como base. Serão eles:

19 de Junho de 2010 http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-June/007907.html
26 de Junho de 2010 http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-June/007979.html
03 de Julho de 2010 http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-July/008091.html
10 de Julho de 2010 http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-July/008169.html
17 de Julho de 2010 http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-July/008274.html
24 de Julho de 2010 http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-July/008428.html
31 de Julho de 2010 http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-July/008509.html

Farei a avaliação de cada um separadamente deixando em negrito as regras que achei interessante e logo abaixo postarei os comentários, links para maiores informações.

Updates Emerging-Threats do dia 19 de Junho

10767 - ET WEB_SPECIFIC_APPS Avaya CallPilot Unified Messaging ActiveX InstallFrom Method Access Attempt (emerging-web_specific_apps.rules)
2011173 - ET CURRENT_EVENTS Windows Help Center Arbitrary Command Execution Exploit Attempt (emerging-current_events.rules)
2011672 - ET CURRENT_EVENTS Adobe Flash 0Day Exploit Attempt (emerging-current_events.rules)
2011673 - ET DOS Possible SolarWinds TFTP Server Read Request Denial Of Service Attempt (emerging-dos.rules)
2011674 - ET DOS SolarWinds TFTP Server Long Write Request Denial Of Service Attempt (emerging-dos.rules)
2011675 - ET CURRENT_EVENTS Possible NOS Microsystems Adobe Reader/Acrobat getPlus Get_atlcom Helper ActiveX Control Multiple Stack Overflows Remote Code Execution Attempt (emerging-current_events.rules)
2011676 - ET WEB_SPECIFIC_APPS Cisco Collaboration Server LoginPage.jhtml Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011677 - ET TROJAN MSIL.Amiricil.gen HTTP Checkin (emerging-virus.rules)
2011678 - ET USER_AGENTS Suspicious User-Agent (HTTP_Query) (emerging-user_agents.rules)
2011679 - ET USER_AGENTS Suspicious User Agent (dbcount) (emerging-user_agents.rules)
2011680 - ET CURRENT_EVENTS Skype Easybits Extras Manager - Exploit (emerging-current_events.rules)
2011681 - ET WEB_SPECIFIC_APPS Avaya CallPilot Unified Messaging ActiveX Function Call (emerging-web_specific_apps.rules)

2011682 - ET WEB_SPECIFIC_APPS AnNoText AdvoMahn IDAutomation Barcode SaveBarCode Method Buffer Overflow Attempt(1) (emerging-web_specific_apps.rules)
2011683 - ET WEB_SPECIFIC_APPS AnNoText AdvoMahn IDAutomation Barcode SaveEnhWMF Method Buffer Overflow Attempt(1) (emerging-web_specific_apps.rules)
2011684 - ET WEB_SPECIFIC_APPS AnNoText AdvoMahn IDAutomation Barcode SaveBarCode Method B0F Attempt(2) (emerging-web_specific_apps.rules)
2011685 - ET WEB_SPECIFIC_APPS AnNoText AdvoMahn IDAutomation Barcode SaveEnhWMF Method BOF Attempt(2) (emerging-web_specific_apps.rules)
2011686 - ET WEB_SPECIFIC_APPS AnNoText AdvoAkte KeyHelp ActiveX JumpMappedID Method Buffer Overflow Attempt (emerging-web_specific_apps.rules)
2011687 - ET WEB_SPECIFIC_APPS AnNoText AdvoAkte KeyHelp ActiveX JumpURL Method Buffer Overflow Attempt (emerging-web_specific_apps.rules)
2011688 - ET WEB_SPECIFIC_APPS AnNoText AdvoAkte KeyHelp ActiveX Buffer Overflow Function Call (emerging-web_specific_apps.rules)
2011690 - ET WEB_CLIENT Possible Sygate Personal Firewall ActiveX SetRegString Method Stack Overflow Attempt (emerging-web_client.rules)
2011691 - ET USER_AGENTS Hotbar Agent Activity (emerging-user_agents.rules)

Updates Emerging-Threats do dia 26 de Junho

2011174 - ET WEB_SERVER SQL Injection Attempt (Agent CZxt2s) (emerging-web_server.rules)
2011692 - ET WEB_SPECIFIC_APPS Avaya CallPilot Unified Messaging ActiveX InstallFrom Method Access Attempt (emerging-web_specific_apps.rules)
2011693 - ET TROJAN Fragus Exploit Kit Landing (emerging-virus.rules) 2011694 - ET POLICY Windows 3.1 User-Agent Detected - Possible Malware or Non-Updated System (emerging-policy.rules)

Updates Emerging-Threats do dia 03 de Julho

2011695 - ET WEB_CLIENT Possible Microsoft Internet Explorer Dynamic Object Tag/URLMON Sniffing Cross Domain Information Disclosure Attempt (emerging-web_client.rules)
2011696 - ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt (emerging-web_specific_apps.rules)
2011697 - ET WEB_SPECIFIC_APPS JBoss JMX Console Beanshell Deployer .WAR File Upload and Deployment Cross Site Request Forgery Attempt (emerging-web_specific_apps.rules)
2011698 - ET CURRENT_EVENTS Java Web Start Command Injection (.jar) (emerging-current_events.rules)
2011699 - ET P2P Bittorrent P2P Client User-Agent (Transmission/1.x) (emerging-p2p.rules)
2011700 - ET P2P Bittorrent P2P Client User-Agent (KTorrent/3.x.x) (emerging-p2p.rules)
2011701 - ET P2P Bittorrent P2P Client User-Agent (Opera/10.x) (emerging-p2p.rules)
2011702 - ET P2P Bittorrent P2P Client User-Agent (BitTornado) (emerging-p2p.rules)
2011703 - ET P2P Bittorrent P2P Client User-Agent (Enhanced CTorrent 3.x) (emerging-p2p.rules)
2011704 - ET P2P Bittorrent P2P Client User-Agent (Deluge 1.x.x) (emerging-p2p.rules)
2011705 - ET P2P Bittorrent P2P Client User-Agent (rTorrent) (emerging-p2p.rules)
2011706 - ET P2P Bittorrent P2P Client User-Agent (uTorrent) (emerging-p2p.rules)
2011707 - ET P2P Client User-Agent (Shareaza 2.x) (emerging-p2p.rules)
2011708 - ET P2P Bittorrent P2P Client User-Agent (Blizzard Downloader 2.x) (emerging-p2p.rules)
2011710 - ET P2P Bittorrent P2P Client User-Agent (BitComet) (emerging-p2p.rules)
2011711 - ET P2P Bittorrent P2P Client User-Agent (KTorrent 2.x) (emerging-p2p.rules)
2011712 - ET P2P Bittorrent P2P Client User-Agent (FDM 3.x) (emerging-p2p.rules)
2011713 - ET P2P Bittorrent P2P Client User-Agent (BTSP) (emerging-p2p.rules)
2011714 - ET CURRENT_EVENTS Hidden iframe Served by nginx - Likely Hostile Code (emerging-current_events.rules)
2011715 - ET CURRENT_EVENTS MALVERTISING Adobe Exploited Check-In (emerging-current_events.rules)
2011716 - ET SCAN Sipvicious User-Agent Detected (friendly-scanner) (emerging-scan.rules)
2011718 - ET USER_AGENTS Suspicious User-Agent (RangeCheck/0.1) (emerging-user_agents.rules)
2011719 - ET USER_AGENTS Suspicious User-Agent (SOGOU_UPDATER) (emerging-user_agents.rules)
2011720 - ET SCAN Possible WafWoof Web Application Firewall Detection Scan (emerging-scan.rules)
2011721 - ET SCAN Possible Fast-Track Tool Spidering User-Agent Detected (emerging-scan.rules)
2011722 - ET WEB_SPECIFIC_APPS Axis Media Controller ActiveX SetImage Method Remote Code Execution Attempt (emerging-web_specific_apps.rules)

2011723 - ET WEB_SPECIFIC_APPS Webmoney Advisor ActiveX Redirect Method Remote DoS Attempt (emerging-web_specific_apps.rules)
2011724 - ET WEB_SPECIFIC_APPS Webmoney Advisor ActiveX Control DoS Function Call (emerging-web_specific_apps.rules)
2011725 - ET WEB_SPECIFIC_APPS EZPX photoblog tpl_base_dir Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011726 - ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter SELECT FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011727 - ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter DELETE FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011728 - ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter UNION SELECT SQL Injection Attempt (emerging-web_specific_apps.rules)
2011729 - ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter INSERT INTO SQL Injection Attempt (emerging-web_specific_apps.rules)
2011730 - ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter UPDATE SET SQL Injection Attempt (emerging-web_specific_apps.rules)
2011731 - ET WEB_SPECIFIC_APPS SchoolMation studentmain.php session Parameter Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011732 - ET DOS Possible VNC ClientCutText Message Denial of Service/Memory Corruption Attempt (emerging-dos.rules)
2011733 - ET GAMES TeamSpeak3 Connect (emerging-game.rules)
2011734 - ET GAMES TeamSpeak2 Connection/Login (emerging-game.rules)
2011735 - ET GAMES TeamSpeak2 Connection/Login Replay (emerging-game.rules)
2011736 - ET GAMES TeamSpeak2 Connection/Ping (emerging-game.rules)
2011737 - ET GAMES TeamSpeak2 Connection/Ping Reply (emerging-game.rules)
2011738 - ET GAMES TeamSpeak2 Standard/Login Part 2 (emerging-game.rules)
2011739 - ET GAMES TeamSpeak2 Standard/Channel List (emerging-game.rules)
2011740 - ET GAMES TeamSpeak2 Standard/Player List (emerging-game.rules)
2011741 - ET GAMES TeamSpeak2 Standard/Login End (emerging-game.rules)
2011742 - ET GAMES TeamSpeak2 Standard/New Player Joined (emerging-game.rules)
2011743 - ET GAMES TeamSpeak2 Standard/Player Left (emerging-game.rules)
2011744 - ET GAMES TeamSpeak2 Standard/Change Status (emerging-game.rules)
2011745 - ET GAMES TeamSpeak2 Standard/Known Player Update (emerging-game.rules)
2011746 - ET GAMES TeamSpeak2 Standard/Disconnect (emerging-game.rules)
2011747 - ET GAMES TeamSpeak2 ACK (emerging-game.rules)
2011748 - ET GAMES TrackMania Game Launch (emerging-game.rules)
2011749 - ET GAMES TrackMania Game Check for Patch (emerging-game.rules)
2011750 - ET GAMES TrackMania Request GetConnectionAndGameParams (emerging-game.rules)
2011751 - ET GAMES TrackMania Request OpenSession (emerging-game.rules)
2011752 - ET GAMES TrackMania Request Connect (emerging-game.rules)
2011753 - ET GAMES TrackMania Request Disconnect (emerging-game.rules)
2011754 - ET GAMES TrackMania Request GetOnlineProfile (emerging-game.rules)
2011755 - ET GAMES TrackMania Request GetBuddies (emerging-game.rules)
2011756 - ET GAMES TrackMania Request SearchNew (emerging-game.rules)
2011757 - ET GAMES TrackMania Request LiveUpdate (emerging-game.rules)
2011758 - ET GAMES TrackMania Ad Report (emerging-game.rules)

Updates Emerging-Threats do dia 10 de Julho

2007880 - ET USER_AGENTS Suspicious User Agent (single dash) (emerging-user_agents.rules)
2011175 - ET USER_AGENTS Casper Bot Search RFI Scan (emerging-user_agents.rules)
2011176 - ET USER_AGENTS MaMa CaSpEr RFI Scan (emerging-user_agents.rules)
2011178 - ET CURRENT_EVENTS FakeAV Download with Cookie WinSec (emerging-current_events.rules)
2011179 - ET TROJAN Generic Checkin - MSCommonInfoEx (emerging-virus.rules)
2011180 - ET TROJAN Phoenix Exploit Kit - pdfopen.pdf (emerging-virus.rules)
2011181 - ET TROJAN Phoenix Exploit Kit - pdfswf.pdf (emerging-virus.rules)
2011182 - ET TROJAN Phoenix Exploit Kit - libtiff.pdf (emerging-virus.rules)
2011183 - ET TROJAN Phoenix Exploit Kit malware payload download (emerging-virus.rules)
2011184 - ET TROJAN Phoenix Exploit Kit VBscript download (emerging-virus.rules)
2011759 - ET WEB_SERVER TIEHTTP User-Agent (emerging-web_server.rules)

Updates Emerging-Threats do dia 17 de Julho

2011185 - ET TROJAN Nine Ball Infection Ping Outbound (emerging-virus.rules)
2011186 - ET TROJAN Nine Ball Infection ya.ru Post (emerging-virus.rules)
2011187 - ET TROJAN Nine Ball Infection Posting Data (emerging-virus.rules)
2011188 - ET TROJAN Nine Ball User-Agent Detected (NQX315) (emerging-virus.rules)
2011189 - ET WEB_SPECIFIC_APPS Possible Cisco IOS HTTP Server Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011190 - ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module cindefn.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011191 - ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module power_management_policy_options.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011192 - ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module pm_temp.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011193 - ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module power_module.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011194 - ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module blade_leds.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011195 - ET WEB_SPECIFIC_APPS Possible IBM BladeCenter Management Module ipmi_bladestatus.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011196 - ET WEB_SPECIFIC_APPS Possible HP OpenView Network Node Manager Getnnmdata.exe Invalid ICount Remote Code Execution Attempt (emerging-web_specific_apps.rules)
2011197 - ET WEB_SPECIFIC_APPS Possible HP OpenView Network Node Manager Getnnmdata.exe Invalid MaxAge Remote Code Execution Attempt (emerging-web_specific_apps.rules)
2011198 - ET WEB_SPECIFIC_APPS Possible HP OpenView Network Node Manager Getnnmdata.exe Invalid Hostname Remote Code Execution Attempt (emerging-web_specific_apps.rules)
2011199 - ET TROJAN Outbound AVISOSVB MSSQL Request (emerging-virus.rules)
2011200 - ET WEB_SPECIFIC_APPS AVTECH Software ActiveX SendCommand Method Buffer Overflow Attempt (emerging-web_specific_apps.rules)
2011201 - ET WEB_SPECIFIC_APPS AVTECH Software ActiveX Login Method Buffer Oveflow Attempt (emerging-web_specific_apps.rules)
2011202 - ET WEB_SPECIFIC_APPS AVTECH Software ActiveX Snapshot Method Buffr Overflow Attempt (emerging-web_specific_apps.rules)
2011203 - ET WEB_SPECIFIC_APPS AVTECH Software ActiveX _DownloadPBOpen Metod Buffer Overflow Attempt (emerging-web_specific_apps.rules)
2011204 - ET WEB_SPECIFIC_APPS AVTECH Software ActiveX _DownloadPBClose Method Buffer Overflow Attempt (emerging-web_specific_apps.rules)
2011205 - ET WEB_SPECIFIC_APPS AVTECH Software ActiveX _DownloadPBControl Method Buffer Overflow Attempt (emerging-web_specific_apps.rules)
2011206 - ET WEB_SPECIFIC_APPS AVTECH Software ActiveX Buffer Overflow Function Call (emerging-web_specific_apps.rules)
2011207 - ET WEB_SPECIFIC_APPS SaschArt SasCam Webcam Server ActiveX Control Head Method Buffer Overflow Attempt (emerging-web_specific_apps.rules)
2011208 - ET WEB_SPECIFIC_APPS SaschArt SasCam Webcam Server ActiveX Buffer Overflow Function Call (emerging-web_specific_apps.rules)
2011209 - ET WEB_SPECIFIC_APPS ClearSite device_admin.php cs_base_path Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011210 - ET WEB_CLIENT ComponentOne VSFlexGrid ActiveX Control Archive Method Buffer Overflow Attempt (emerging-web_client.rules)
2011211 - ET WEB_CLIENT AtHocGov IWSAlerts ActiveX Control Buffer Overflow Function Call Attempt (emerging-web_client.rules)
2011212 - ET WEB_CLIENT Consona Products SdcUser.TgConCtl ActiveX Control Buffer Overflow Attempt (emerging-web_client.rules)
2011213 - ET WEB_CLIENT Consona Products SdcUser.TgConCtl ActiveX Control BOF Function Call (emerging-web_client.rules)
2011214 - ET WEB_SPECIFIC_APPS ArdeaCore pathForArdeaCore Parameter Remote File Inclusion Attempt (emerging-web_client.rules)
2011215 - ET WEB_SPECIFIC_APPS Campsite article_id Parameter SELECT FROM SQL Injection Attempt (emerging-web_client.rules)
2011216 - ET WEB_SPECIFIC_APPS Campsite article_id Parameter DELETE FROM SQL Injection Attempt (emerging-web_client.rules)

2011217 - ET WEB_SPECIFIC_APPS Campsite article_id Parameter UNION SELECT SQL Injection Attempt (emerging-web_client.rules)
2011218 - ET WEB_SPECIFIC_APPS Campsite article_id Parameter INSERT INTO SQL Injection Attempt (emerging-web_client.rules)
2011219 - ET WEB_SPECIFIC_APPS Campsite article_id Parameter UPDATE SET SQL Injection Attempt (emerging-web_client.rules)
2011220 - ET CURRENT_EVENTS Executable requested from /wp-content/languages (emerging-current_events.rules)
2011221 - ET TROJAN FakeAV Served To Client (emerging-virus.rules)
2011222 - ET CURRENT_EVENTS Malvertising drive by kit encountered - bmb cookie (emerging-current_events.rules)
2011223 - ET CURRENT_EVENTS Malvertising drive by kit encountered - Loading... (emerging-current_events.rules)
2011224 - ET CURRENT_EVENTS Malvertising drive by kit collecting browser info (emerging-current_events.rules)
2011225 - ET USER_AGENTS Suspicious User Agent (AskInstallChecker) (emerging-user_agents.rules)
2011226 - ET USER_AGENTS Suspicious User-Agent (SeFastSetup) (emerging-user_agents.rules)
2011227 - ET USER_AGENTS Suspicious User-Agent (NSIS_Inetc (Mozilla)) (emerging-user_agents.rules)
2011228 - ET TROJAN Trojan.StartPage activity (emerging-virus.rules)
2011760 - ET CURRENT_EVENTS Likely FAKEAV scanner page encountered - i1000000.gif (emerging-current_events.rules)
2011761 - ET DOS Possible MySQL ALTER DATABASE Denial Of Service Attempt (emerging-dos.rules)
2011762 - ET WEB_CLIENT Arguments.callee.toString Javascript Obfuscation - Likely Hostile (emerging-current_events.rules)
2011763 - ET WEB_SERVER Possible Cisco PIX/ASA HTTP Web Interface HTTP Response Splitting Attempt (emerging-web_specific_apps.rules)
2011764 - ET WEB_CLIENT Possible Microsoft Internet Explorer mshtml.dll Timer ID Memory Pointer Information Disclosure Attempt (emerging-web_client.rules)
2011765 - ET MALWARE eval(function(p,a,c,k,e,d) JavaScript from ngix Detected - Likely Hostile (emerging-malware.rules)
2011766 - ET SCAN Sipvicious User-Agent Detected (sundayddr) (emerging-scan.rules)

Updates Emerging-Threats do dia 24 de Julho

2011229 - ET USER_AGENTS Suspicious User Agent (Suggestion) (emerging-user_agents.rules)
2011230 - ET CURRENT_EVENTS MALVERTISING client requesting drive by - /x/?src= (emerging-current_events.rules)
2011231 - ET CURRENT_EVENTS MALVERTISING client requesting redirect to drive by - .php?n=cust (emerging-current_events.rules)
2011232 - ET P2P Related User Agent (eChanblard) (emerging-policy.rules)
2011233 - ET TROJAN Troxen GetSpeed Request (emerging-virus.rules)
2011234 - ET TROJAN Cosmu Process Dump Report (emerging-virus.rules)
2011235 - ET EXPLOIT Possible Novell Groupwise Internet Agent CREATE Verb Stack Overflow Attempt (emerging-exploit.rules)

Updates Emerging-Threats do dia 31 de Julho

2003925 - ET USER_AGENTS WebHack Control Center User-Agent Outbound (WHCC/) (emerging-user_agents.rules)
2010343 - ET SCAN pangolin SQL injection tool (emerging-scan.rules)
2010715 - ET SCAN ZmEu exploit scanner (emerging-scan.rules)
2010768 - ET SCAN Open-Proxy ScannerBot (webcollage-UA) (emerging-scan.rules)
2011175 - ET WEB_SERVER Casper Bot Search RFI Scan (emerging-web_server.rules)
2011176 - ET WEB_SERVER MaMa CaSpEr RFI Scan (emerging-web_server.rules)
2011236 - ET TROJAN Trojan-Downloader Win32.Genome.avan (emerging-virus.rules)
2011237 - ET TROJAN General Proxy.Agent (emerging-virus.rules)
2011238 - ET USER_AGENTS Suspicious User-Agent (Mozilla/4.0 (SP3 WINLD)) (emerging-user_agents.rules)
2011239 - ET CURRENT_EVENTS Possible Microsoft Windows Shortcut LNK File Automatic File Execution Attempt Via WebDAV (emerging-current_events.rules)
2011240 - ET WEB_CLIENT Mozilla Firefox Window.Open Document URI Spoofing Attempt (emerging-web_client.rules)
2011241 - ET EXPLOIT M3U File Request Flowbit Set (emerging-exploit.rules)
2011242 - ET EXPLOIT Possible VLC Medial Player M3U File FTP URL Processing Stack Buffer Overflow Attempt (emerging-exploit.rules)
2011243 - ET WEB_SERVER Bot Search RFI Scan (ByroeNet/Casper-Like, planetwork) (emerging-web_server.rules)
2011244 - ET WEB_SERVER Bot Search RFI Scan (ByroeNet/Casper-Like, sun4u) (emerging-web_server.rules)

2011245 - ET WEB_CLIENT PDF Containing Windows Commands Downloaded (emerging-web_client.rules)
2011246 - ET WEB_CLIENT Likely Malicious PDF Containing StrReverse (emerging-web_client.rules)
2011247 - ET USER_AGENTS Forthgoer User Agent - Likely Hostile (emerging-user_agents.rules)
2011248 - ET USER_AGENTS Suspicious User Agent (XieHongWei-HttpDown/2.0) (emerging-user_agents.rules)
2011249 - ET WEB_CLIENT RSP MP3 Player OCX ActiveX OpenFile Method Buffer Overflow Attempt (emerging-web_client.rules)
2011250 - ET WEB_CLIENT Image22 ActiveX DrawIcon Method Buffer Overflow Attempt (emerging-web_client.rules)
2011251 - ET WEB_CLIENT FathFTP ActiveX Control GetFromURL Method Buffer Overflow Attempt (emerging-web_client.rules)
2011252 - ET WEB_CLIENT FathFTP ActiveX Control RasIsConnected Method Buffer Overflow Attempt (emerging-web_client.rules)
2011253 - ET WEB_CLIENT Registry OCX ActiveX FullPath Method Buffer Overflow Attempt (emerging-web_client.rules)
2011254 - ET WEB_SPECIFIC_APPS Redaxo CMS index.inc.php Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011255 - ET WEB_SPECIFIC_APPS Redaxo CMS specials.inc.php Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011256 - ET WEB_SPECIFIC_APPS FireStats window-add-excluded-ip.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011257 - ET WEB_SPECIFIC_APPS FireStats window-add-excluded-url.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011258 - ET WEB_SPECIFIC_APPS FireStats window-new-edit-site.php Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011259 - ET WEB_SPECIFIC_APPS MAXcms fm_includes_special Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011260 - ET WEB_SPECIFIC_APPS TVUPlayer ActiveX LangFileName method File overwrite Attempt (emerging-web_specific_apps.rules)
2011261 - ET WEB_SPECIFIC_APPS TVUPlayer ActiveX LangFileName method File overwrite Function Call (emerging-web_specific_apps.rules)
2011262 - ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter SELECT FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011263 - ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter DELETE FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011264 - ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter UNION SELECT SQL Injection Attempt (emerging-web_specific_apps.rules)
2011265 - ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter INSERT INTO SQL Injection Attempt (emerging-web_specific_apps.rules)
2011266 - ET WEB_SPECIFIC_APPS Group-Office comment_id Parameter UPDATE SET SQL Injection Attempt (emerging-web_specific_apps.rules)
2011268 - ET WEB_SPECIFIC_APPS Oracle Business Process Management context Parameter Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011269 - ET TROJAN Downloader.Win32.Small (emerging-virus.rules)
2011270 - ET CURRENT_EVENTS Possible Microsoft Windows .lnk File Processing WebDAV Arbitrary Code Execution Attempt (emerging-current_events.rules)
2011271 - ET USER_AGENTS Suspicious User-Agent (CustomSpy) (emerging-user_agents.rules)
2011272 - ET TROJAN Win32/Chekafe.A or Related Infection Checkin (emerging-virus.rules)
2011273 - ET USER_AGENTS Suspicious User-Agent (GM Login) (emerging-user_agents.rules)
2011274 - ET WEB_SPECIFIC_APPS OpenX phpAdsNew phpAds_geoPlugin Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011275 - ET POLICY Akamai Redswoosh CLIOnlineManager Connection Detected (emerging-policy.rules)
2011276 - ET USER_AGENTS Suspicious User-Agent (InfoBot) GET (emerging-user_agents.rules)
2011277 - ET TROJAN Generic Trojan HTTP Get (emerging-virus.rules)
2011285 - ET WEB_SERVER Bot Search RFI Scan (Casper-Like, Jcomers Bot scan) (emerging-web_server.rules)
2011286 - ET WEB_SERVER Bot Search RFI Scan (Casper-Like, MaMa Cyber/ebes) (emerging-web_server.rules)

As atualizações de RBN, Compromised Hosts, Dshield não foram postadas, pois como citado antes acho de suma importância sempre utilizá-las, mas sempre fazendo updates diários da mesma visto constante mudanças e melhorias desses rulesets.

Baseado nas regras em negrito que são as sugestões vemos bastante ataques para cliente side especialmente com alvo IE, Acrobat reader, JavaScript maliciosos, exploit kits e os Trojans/botnets on the wild.

Logicamente esses nomes e métodos de comunicação se modificam bastante, ou seja, não adianta utilizar essas regras para sempre, eu sugiro que a grande maioria por um prazo de 30 a 60 dias, pois na sua grande maioria apos isso possivelmente perdera a capacidade de detecção bem como ficara consumindo recursos desnecessários do seu sensor.

As regras relacionadas a User-Agents estranhos são interessantes, mas consume muito CPU, sugiro utilizá-las caso queira fazer um enforcement de uso de versões especificas de browsers e realmente te interessa uso de CPU com as mesmas. E por final as regras de Aplicações especificas que caso você as possuas certamente você DEVE habilitá-las.

A Sourcefire fez o release do Projeto RazorBack na Defcon 18 que você poderá ver em http://labs.snort.org/razorback que certamente cobrira maioria dos ataques que as regras sugeridas detectam, mas infelizmente ainda na versão 0.1 .

Vale lembrar que as sugestões são de minha inteira autoria não tendo relações com a opinião da empresa que trabalho.

A continuação da coluna abordaremos assuntos relacionados a IDS/IPS/HIDS no geral especialmente focando Snort, OSSEC e Razorback com dicas, atualidades, técnicas, possivelmente será chamada de “Mundo IDS”.

Entendemos que o release de sugestão de regras precisa ser mais dinâmico e por isso retornarei com o Snort Rules Week semanal em meu blog e/ou no http://www.snort.org.br

Happy Snorting!

Rodrigo “Sp0oKeR” Montoro

Rodrigo “Sp0oKeR” Montoro tem mais de 12 anos de experiência na área de T.I especialmente com Segurança Open Source com Pentesting, Firewalls, IDS/IPS , já tendo atuando e trabalhado com grandes empresas do mercado. Possui certificações LPI ,RHCE , SnortCP e MCSO. Atualmente é coordenador e evangelizador do snort IDS na comunidade snort-br (http://www.snort.org.br) , membro do OWASP entre outros projetos Open source que gosta. Trabalha no time de pesquisas do Spiderlabs na Trustwave (http://www.trustwave.com/spiderlabs) onde cria assinaturas para IDS/IPS da empresa, analisa malwares e tem focado principalmente em PDF maliciosos.

CSA BR Brazil Chapter

cloud security alliance SM

A Associação, sem fins lucrativos, CSA (Cloud Security Alliance) foi criada em 2008 na cidade de Las Vegas, e tem como principal objetvo tratar sobre assuntos relacionados a Segurança em Cloud Computing.

Em 2010 a CSA decidiu lançar a iniciativa para a criação de Chapter locais, então países fora dos EUA, puderam começar a colaborar com a disseminação das informações em outros idiomas.

O Chapter Brasileiro foi o segundo a ser reconhecido oficialmente pela CSA e com isso está trabalhando atualmente para poder alcançar as seguintes metas:

* Traduzir o guia de boas práticas para Segurança em Cloud Computing para o Português Brasil e
* Desenvolver um guia para auxiliar os fornecedores e consumidores na melhor forma de adoção de Cloud Computing.

Board Brasil

Presidente:
Leonardo Goldim

Diretores:
Anchises Moraes
Jaime Orts Y Lugo
Jordan M. Bonagura
Olympio Renno

www.cloudsecurityalliance.org
presidencia@br.cloudsecurityalliance.org

SEGURANÇA NO DESENVOLVIMENTO DE SW

Por Renato Salatiel

1. Introdução

Segurança no desenvolvimento de Software é um tema que vem ganhando força à medida que o Brasil, cada vez mais vai ingressando no mercado de exportação de software.

De acordo com estimativas do presidente da Brascom (Brasilian Association of Information Technology and Communication Companies) a exportação de software alcançará US$ 2 bilhões neste ano.

Novos padrões são impostos pelo mercado internacional e conceitos como SOA (Service Oriented Architeture), desenvolvimento Orientado a Objetos e ERP (Enterprise Resource Planning) vêm se solidificando cada vez mais no mercado de desenvolvimento de software.

Sistemas integrados, reutilização de componentes, reutilização de serviços, exigência de alta disponibilidade dos sistemas críticos, exigem das organizações maior responsabilidade com relação à segurança no desenvolvimento desses recursos.

Outro importante fator, que reforça essa exigência é a necessidade de adoção de padrões reconhecidos internacionalmente e requerimentos legais como a lei americana Sarbanes-Oxley de 2002 (que apresenta diversas regras com o objetivo de transformar os princípios de uma boa governança corporativa em leis), normas ISO 27001 e 27002 (que trata de questões de segurança da informação), a norma ISO 15.408 (que tratam questões de segurança no desenvolvimento de software) e frameworks como o COBIT (padrões e procedimentos para TI) e o COSO (que trata questões de analise e gerenciamento de riscos na organização).

O desenvolvimento de sistemas, dessa forma, passou a ter grande importância para o negócio das empresas e governos.

Até o início da década de 1990, a maior parte dos sistemas era dedicada a áreas-meio das empresas e eles possuíam funcionalidades limitadas, com processamento dedicado e uso restrito.

O advento da internet e o desenvolvimento dos computadores e telecomunicações trouxeram uma nova posição para os sistemas (e novos riscos), que passaram a automatizar aplicações de negócios alem de serem integrados a outros sistemas e parceiros.

Esse novo cenário permitiu que o desenvolvimento de sistemas passasse a uma posição estratégica nas organizações fazendo que as empresas começassem a depender cada vez mais dos mesmos. Além disso, a automatização de processos trouxe para os sistemas o negócio da organização e, dessa forma, as informações passaram a ser o maior patrimônio de uma organização, tornando possível a difusão quase que instantânea da informação.

O aumento do número de pessoas envolvidas em produção e processamento de dados e o baixo custo da coleta fizeram disparar a velocidade de produção da informação. Atualmente, a quantidade de informação disponível dobra a cada cinco anos, em breve estará duplicando a cada dois anos.

Hoje, no desenvolvimento de nossas atividades profissionais e para sobrevivermos no mercado de trabalho ou até para atuarmos na sociedade em geral, somos forçados a assimilar um corpo de conhecimento que se amplia a cada minuto.

2. Riscos no desenvolvimento de novas aplicações em TI

Com o surgimento de aplicações complexas e com alto grau de interação entre usuários e sistemas, o desenvolvimento de sistema apresenta novos riscos.

O risco é definido com sendo a exposição às seguintes conseqüências: falhas em obter benefícios antecipados, custos de implementação acima das expectativas e incompatibilidade do sistema com o hardware e software escolhidos.

Contudo, caso a empresa não assuma projetos de risco elevado, ela pode não ocupar um nicho de mercado e deixá-lo livre para a concorrência.

A avaliação do risco dá-se após a aplicação das ferramentas e abordagens gerenciais. Segundo McFarlan (1981) três fatores têm maiores influência no risco de um projeto de TI:

- o tamanho do projeto, sendo que quanto maior a quantidade de recursos despedido maior é o risco;
- a familiaridade com a tecnologia , sendo que quanto maior a familiaridade com a tecnologia, maior é o risco;
- a estrutura do projeto, sendo que quanto mais estruturado for o projeto, menor é o risco.

Figura 1 – Riscos em projetos de TI (baseado em McFarlan, 1981)

3. Conceitos

Apresento alguns conceitos relacionados ao tema como:

- Software (Pressman, 1995): instruções (programas de computador) que, quando executadas, produzem a função e o desempenho desejados;
- Desenvolvimento de Software: ato de elaborar e implementar instruções que, quando executadas, produzem a função e o desempenho desejados, transformando a necessidade de um usuário em um produto técnico;
- Segurança em desenvolvimento de software: a preocupação quando falamos em segurança no desenvolvimento de software são:
  - Segurança no ambiente de desenvolvimento: o foco é manter os códigos-fonte seguros e evitar roubos;
  - Segurança da aplicação desenvolvida: o foco é desenvolver uma aplicação que seja segura, siga corretamente as especificações de segurança, não contenha códigos maliciosos ou falhas que comprometam a segurança;
  - Garantia de segurança da aplicação desenvolvida: garantir ao cliente que a aplicação que está em desenvolvimento é segura, permitindo que o cliente se assegure que o sistema é seguro.
- Confidencialidade (ISO 17799:2001): garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- Integridade (ISO 17799:2001): salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- Disponibilidade (ISO 17799:2001): garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

4. Como desenvolver SW com segurança?

A norma ISO 15.408 apresenta uma série de requisitos e práticas como, por exemplo, controle de acesso, trilha de auditoria, autenticação, uso de criptografia dentre outras, que podem ser adotadas para o desenvolvimento de uma aplicação tornando-a mais segura. Além disso, a norma sugere níveis de maturidade para a aplicação desenvolvida que é conhecida como EAL (Evaluation Assurance Level).

Esses níveis variam de 1 (um) a 7 (sete) e são atribuídos à aplicação após uma avaliação do produto. Essa avaliação deve ser realizada por rede de laboratórios credenciados e reconhecidos mundialmente como reguladores do mercado.

Contudo, a adoção de segurança no desenvolvimento de software não exige um alto nível de investimento para seu desenvolvimento e implantação desde que, seja pensado logo nas primeiras fases do desenvolvimento de um software. É importante que nesse momento exista a interação do analista de sistemas, usuário e o analista de segurança para que, requisitos de segurança sejam definidos e planejados juntamente com todos os demais requisitos do sistema.

Papel	Principal Responsabilidade
Usuário	Expor seu problema, suas necessidades; Verificar se o produto entregue atende a suas necessidades;
Analista de Sistema	Capturar a necessidade do usuário e transformar essa necessidade em requisitos de software;
Analista de Segurança	Conhecer as normas de segurança (como por exemplo, ISO 15.408); Apresentar requisitos relacionados à segurança da informação tendo em vista o negócio;

Tabela 1 – Visão geral dos papeis e responsabilidades no desenvolvimento de um SW

O analista de segurança deve fazer uma leitura da ISO 15.408 e procurar extrair os procedimentos e controles que se adéquam a realidade da sua organização. Segundo Albuquerque e Ribeiro (Albuquerque e Ribeiro, 2002) essa leitura é muito importante e deve ser feita pela equipe de sistemas em conjunto com a equipe de segurança.

Deve-se tomar cuidado para não "engessar" o processo de desenvolvimento de sistemas, comprometendo os prazos e custos do projeto.

Alem da avaliação de segurança a empresa deve possuir uma metodologia de desenvolvimento aderente as boas práticas de mercado com processos de engenharia de software e papeis da equipe do projeto previamente definidos.

A norma ISO 15.408 pode ser usada como parte do processo de testes, que ocorrem durante o desenvolvimento, para dessa forma verificar se não somente os requisitos de sistema (usuário) estão sendo atendidos, mas também os requisitos de segurança.

Conforme apresentado anteriormente, requisitos de segurança foram definidos nas primeiras fases do desenvolvimento do software.

Essa especificação de segurança precisa ser validada, ou seja, o analista de segurança deve verificar se a segurança implementada na aplicação está aderente com a especificação de segurança.

Conforme Albuquerque e Ribeiro (Albuquerque e Ribeiro, 2002) há duas alternativas para essa verificação:

- Bater a especificação da aplicação com a especificação da segurança necessária para aquela aplicação.
- Verificar, através de testes, qual a segurança implementada na aplicação e compará-la com a especificação de segurança;

Os testes de segurança podem ser feitos de forma cíclica no projeto, testando componentes individualmente ou mesmo todo o sistema em pontos diferente do desenvolvimento ou apenas ao final do mesmo.

5. Por que desenvolver com segurança?

Alem dos requerimentos legais como, por exemplo, legislação e padrões de mercado e a necessidade de padronização das aplicações desenvolvidas, citadas anteriormente, adotar a segurança no desenvolvimento de software contribui para:

- Redução de riscos: aplicações desenvolvidas de forma estrutura e baseada na norma ISSO 15.408 podem passar por um processo de certificação que irá atestar a segurança no aplicativo. Garantir a segurança dos sistemas minimiza os riscos de fraude, invasões, perda e roubo de informações e indisponibilidade que impactam direta ou indiretamente na imagem da organização;

- Exigências legais: cada vez mais existe a necessidade de comunicação e troca de informações entre as organizações. Alem dos riscos de vazamento nessa integração, legislações (como a SOX) impõem padrões e exige controles em diversas atividades e processos;

- Redução de custos: a adoção de padrões de desenvolvimento e segurança na aplicação diminui a manutenção nos sistemas e correções de falhas de segurança que minimizam os impactos da mudança conforme mostra o gráfico 4.1 sobre impactos da mudança do software. Segundo Pressman (Pressman, 1995), se uma séria atenção for dada à definição inicial, os primeiros pedidos de mudança podem ser acomodados facilmente. O cliente pode rever as exigências e recomendar modificações em causar grande impacto sobre os custos. Porém, quando são exigidas mudanças durante o projeto do software, o impacto sobre os custos eleva-se rapidamente. Recursos foram comprometidos e uma estrutura de projeto foi estabelecida. A mudança pode causar sublevações que exijam recursos adicionais e grandes modificações de projeto, isto é, custo adicional. Mudanças na função, desempenho, interfaces e outras características durante a implementação (código e teste) exercem um forte impacto sobre o custo.

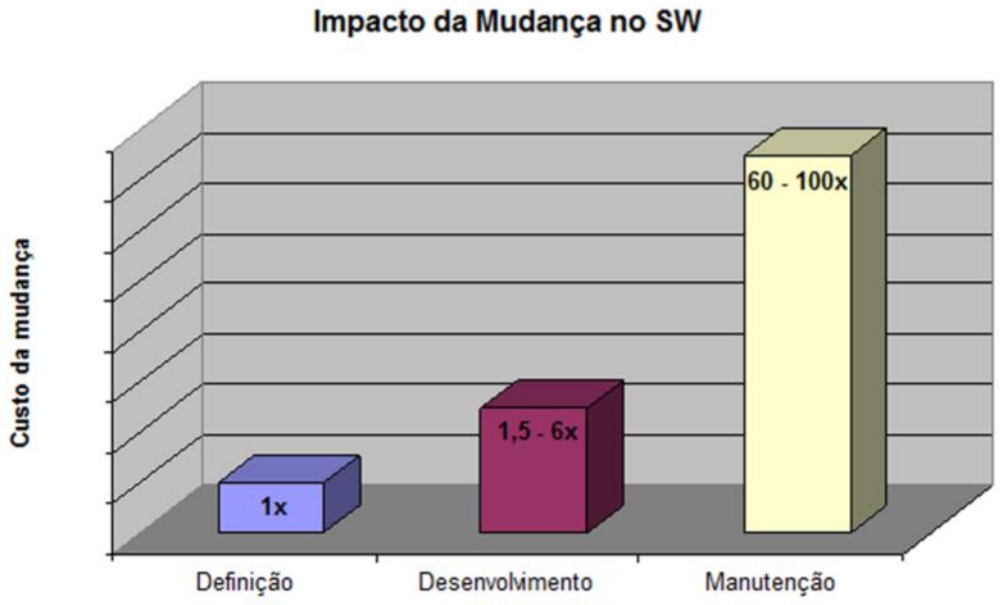


Gráfico 4.1. Impacto na mudança de requisitos em software
Adaptado de Pressman (Pressman, 1995)

6. Conclusão

Conforme apresentado, as empresas podem desenvolver aplicações com segurança sem que esse processo impacte de forma considerável nos custos e prazos do projeto.

Podemos observar uma crescente preocupação com segurança desde as primeiras fazes do projeto para que os impactos financeiros com mudanças e correções sejam minimizados e riscos mitigados.

Ressalto que as equipes envolvidas no desenvolvimento de software devem estar atentas as normas e procedimentos legais para que as informações, que são o maior patrimônio das organizações, estejam seguras, confiáveis e integras para que garantam a eficácia aos objetivos e metas organizacionais.

7. Referências

• Ribeiro, Bruno e Albuquerque, Ricardo – Segurança no Desenvolvimento de Software – Editora Campus – 2002;

• S. Pressman, Roger – Engenharia de Software – Editora Makron Books – 1995;

• Prof. Rodrigues, Ramiro – Desenvolvimento de software seguro para as organizações – Centro de Pós Graduação – FIAP;

• Araújo Santos, Luciana de Almeida – A lei Sarbanes-Oxley: uma tentativa de recuperar a credibilidade do mercado de capitais norte-americano – Disponível em: <http://www.congressousp.fipecafi.org/artigos12004/299.pdf> Acesso em 15 de jun 2009;

• Angrisano, Carlos Augusto e Barbin Laurindo, Fernando José – Gestão da Tecnologia da Informação em empresas industriais e de serviços: estudo de casos – Disponível em <http://www.abepro.org.br/biblioteca /ENEGEP2003_TR0702_1075.pdf> Acessado em 12 de jul 2009;

• Estimativa de exportação de software – http://www.agrosoft.org.br/agropag/210115.htm Acessado em 23 de jul 2009

• NBR ISO/IEC 17799:2001 – Tecnologia da informação – Código de prática para a gestão da segurança da informação, Rio de Janeiro, 2001;

Renato Salatiel

Formado em Análise e desenvolvimento de sistemas pela FMU;

MBA em Gestão de Segurança da Informação pela FIAP;

Atua como analista de segurança da informação no Itaú Unibanco.

LIXO ELETRÔNICO

Cuidado ele pode ser um risco a sua privacidade

Por Gilberto Sudré

O lançamento de novos produtos acontece de forma cada vez mais rápida. Isto faz com que muitos usuários troquem seus equipamentos eletrônicos frequentemente. O que as empresas e pessoas não se dão conta é que ao doar, vender ou jogar fora um computador ou celular usado e até mesmo um disco rígido (HD) danificado podem estar colocando sua privacidade em risco.

Todos estes equipamentos armazenam muitas informações classificadas como particulares (e confidenciais) mas que imaginamos estarem inacessíveis. Isto é verdade para pessoas comuns mas não para hackers e espiões à caça de munição para praticarem algum delito eletrônico. No caso dos computadores, um dos procedimentos mais utilizados é a formatação do HD e a exclusão da partição. Apesar de interessantes, estas ações não são suficientes para impedir o acesso aos dados armazenados.

Hoje já existem diversos aplicativos, com download gratuito através da Internet, que não necessitam de prática ou habilidade para recuperação de arquivos e informações em HDs que foram formatados. Assim todo cuidado é pouco.

Para dificultar o acesso as informações "descartadas" você deve gravar novas informações sobre as existentes no HD .

Só para se ter uma ideia o governo americano sugere que o conteúdo de um HD a ser descartado deve ser sobrescrito no mínimo 6 vezes para alcançar uma segurança média (norma DoD 5220.22-M).

Este é um procedimento demorado que pode levar até 1 minuto por Giga. Parece pouco mas pense em uma empresa que possua centenas de discos rígidos de grande capacidade para serem descartados. Por desconhecimento ou falta de recursos a maioria das empresas não executam este procedimento. Assim fica fácil entender porque alguns hackers estão de olho no lixo eletrônico corporativo.

No caso dos celulares alguns cuidados também devem ser tomados. Apague todas as atividades executadas como ligações efetuadas e recebidas, torpedos enviados e recebidos e qualquer outra informação armazenada no celular.

Uma última dica. Fique de bem com a natureza dando uma destinação adequada para as baterias de seu celular ou Notebook. Não as descarte no lixo comum. A doação de equipamentos é muito importante e pode ajudar a várias pessoas mas tenha cuidado com suas informações. Neste tempo da Vida virtual lembre-se que os riscos são muito reais.

Gilberto Sudré

Consultor em Segurança da Informação;
Comentarista de Tecnologia da Rádio CBN;
Articulista do Jornal A Gazeta e Portal iMasters;
Redator e apresentador do quadro Tecnodicas na TV Gazeta;
Palestrante sobre Segurança da Informação, privacidade e infra-estrutura de redes.
Professor de Graduação e Pós-Graduação;
Instrutor da Academia Cisco;
Membro do comitê técnico CB21/CE27 da ABNT sobre Segurança da Informação;
Coordenador do ISSA Brasil – ES.
Co-Autor do livro "Internet: O Encontro de 2 Mundos";
Autor dos livros "Antenado na Tecnologia" e "Rede de Computadores".

Stay Safe Podcast

O Stay Safe tem como principal objetivo divulgar a área de Segurança da Informação entre os profissionais e não profissionais desta área, bem como discutir o mercado, trazendo notícias, novidades e eventos em geral.

Sempre traremos profissionais da área para discutirmos temas relevantes que estão ocorrendo no mercado. Pretendemos sempre discutir os assuntos relacionados de forma simples e descontraída, tornando o PodCast mais interativo e interessante para os nossos ouvintes.

Agradecemos a todos os nossos convidados que voluntariamente participaram do Stay Safe Podcast, bem como a toda comunidade da Segurança da Informação que nos motiva cada dia mais a continuarmos com este trabalho sério que acreditamos contribuir de alguma maneira para o mercado brasileiro de TI.

Stay Safe Podcast

Fundadores:
Jordan M. Bonagura
Thiago Bordini

www.staysafepodcast.com.br
contato@staysafepodcast.com.br

SELECIONADAS STAY SAFE

Com Tony Rodrigues

Qual o sistema de arquivos mais simples e o mais difícil para se fazer recovery?
(Por Alessandro de Souza)

Como foi comentado no podcast, a maioria dos sistemas de arquivos realiza a deleção de um arquivo marcando-o na tabela de alocações, que o arquivo está logicamente deletado.

Para recuperar esses arquivos, basta procurar pela entrada dele na tabela de alocações e reverter o tal flag/marca de arquivo apagado. Todas as suas estruturas, que estavam intocadas, estarão de volta.

Há alguns sistemas, como o ext3, que além de registrar a marca de arquivo apagado, destrói todos os ponteiros da tabela para os blocos do disco que contém conteúdo desse arquivo. Nesse caso, a recuperação envolve retornar todos os ponteiros e o flag/marca de arquivo apagado. Como não há referencias guardadas dos ponteiros, essa recuperação é extremamente complicada.

Também é possível acontecer de uma entrada na tabela de alocações, referente a um arquivo apagado, ser parcial/totalmente sobreposta. Nesse caso, o dado pode ainda estar no HD, mas as referencias que indicavam onde estão cada pedaço do arquivo foram perdidas. Acaba sendo uma situação semelhante ao que sempre acontece no ext3.

Nesses casos, o arquivo ainda poderia ser recuperado:

- Por análise de conteúdo: Essa técnica é extremamente complicada, pois requer que o arquivo tenha características bem marcantes em termos de conteúdo, de forma a permitir que os blocos que fazem parte dele sejam reconhecidos no disco.
- Por Carving: É uma técnica que, de certa forma, automatiza a técnica que citei acima. Os arquivos são recuperados diretamente na mídia, sem qualquer ajuda das referencias e ponteiros do sistema de arquivos.

Normalmente, o conteúdo é identificado por magic numbers nos cabeçalhos. Apresenta ainda alguns problemas, principalmente quando os blocos com as informações estão não contíguos ou estão fora de ordem.

Qual utilidade de capturar dados na RAM e qual o melhor software?
(Por Alessandro de Souza)

Os dados capturados na RAM permitem análises e conclusões mais diretas sobre os artefatos que estavam sendo executados.

Em combinação com a já tradicional Forense de Disco e a Forense de Rede, será fundamental nas análises forenses. Além da análise dos dados da RAM, as mesmas técnicas podem ser usadas para analisar o conteúdo de arquivos de hibernação e de memória virtual.

Há vários softwares muito bons nessa área. HBGary, Memorizer, mdd, Win32DD, Win64DD e Volatility são exemplos de excelentes utilitários com essa finalidade.

A Polícia Federal ainda é a melhor maneira de entrar nessa área aqui Brasil (como perito em informática)?
(Por Magno Logan)

É uma das melhores. Mas há outras, o mercado está crescendo e as empresas estão percebendo que ter uma área interna que verifique casos de fraudes, problemas de conformidade ou ainda investiguem incidentes, tem grande valor agregado.

Imagine que, na maioria das vezes, não será possível determinar a real causa de um incidente sem alguém que tenha as qualificações de um perito em Computação Forense. Com isso, o incidente poderá ocorrer novamente, causando mais perdas à corporação.

"Navegacao Privativa" (ie, ff) é REALMENTE privativa? Isso não pode estar gerando falsa expectativa para usuários?"
(Por Geraldo Fonseca)

No âmbito do usuário, a maioria vai oferecer alguns mecanismos que apagam os vestígios criados pelos browsers.

Ainda assim, um profissional de Forense Computacional poderá recuperar alguns desses vestígios, mas reconheço que não será tão fácil para um usuário comum, desprovido das ferramentas e técnicas que conhecemos. Nesse caso, podemos dizer que é relativamente "privativa".

Porém, esse conceito vale somente para os vestígios deixados no computador cliente. Se a navegação não for criptografada, o usuário pode estar com todas essas configurações ligadas e ainda ser alvo de um ataque MITM.

Como evitar que o processo de ligar/desligar de um computador suspeito corrompa/altere provas/dados?
(Por Jorge Moura)

Conforme falamos no podcast, esse tema já foi muito polêmico no passado. Estou convicto de que não podemos basear um caso ou uma conclusão em apenas um vestígio. Dessa forma, não acredito que o desligamento do computador pelos meios normais do sistema operacional possa ser tão problemática quanto acusavam. Além disso, simplesmente retirar o plugue da tomada pode trazer riscos à mídia, e nesse caso, a ementa é bem pior que o soneto ...

Pergunta para o Tony: comente sobre o caso TrueCrypt + Daniel Dantas + FBI. No ano passado vimos ser possivel quebrar esta crypt no H2HC!
(Por Nelson Brito)

Como falamos no podcast, nem sempre uma técnica de quebra de criptografia funciona em todas as versões.

É preciso analisar com mais detalhes qual versão do TrueCrypt está em uso no famoso HD do Daniel Dantas e verificar se a técnica apresentada no H2HC se aplicaria.

Para todos os efeitos, acredito que há medidas mais eficientes do que quebras de algoritmos ou chaves criptográficas. Uma delas é planejar uma campana digital, monitorando 100% do tráfego de rede, através de ordem judicial, diretamente nos pontos de acesso à Internet do suspeito.

QUER SABER MAIS???

ESCUTE O STAY SAFE PODCAST COM TONY RODRIGUES

Tony Rodrigues

Certificado CISSP, CFCP e Security+ ;

Mais de 20 anos de experiência em TI e 8 anos em Gestão de Segurança de Informações;

Já liderou várias investigações, perícias e pesquisas sobre Computação Forense;

Consultor em Segurança de Informações;

Palestrante em importantes conferências (CNASI, H2HC,YSTS);

É criador do blog forcomp.blogspot.com, sobre Resposta a Incidentes e Forense Computacional;

Colabora com artigos no blog de Computer Forensics da SANS

ISSA™

Information Systems Security Association

Porque ser ISSA ?

A ISSA, Associação dos Profissionais da Segurança da Informação, é uma associação sem fins lucrativos. Nos últimos 8 anos, temos participado ativamente de campanhas para divulgar e conscientizar o mercado em relação à necessidade de se fomentar e praticar a Segurança da Informação.

Estas atividades entre outras, tem nos agraciado com a honra da ISSA ser conhecida como "A Voz da Segurança da Informação no Brasil".

Nossa presença, se estende de Norte a Sul, de Leste a Oeste, e nossa rede de associados se estende por todo o território brasileiro. Nosso quadro de associados congrega profissionais de importância nacional e internacional.

Venha conhecer e trocar idéias com seus pares, participe de nossos Congressos, Seminários, Palestras, Treinamentos e muito mais, tudo planejado para integrar os associados e gerar novas oportunidades.

Conhecendo a ISSA você estará participando da maior comunidade de Segurança da Informação no Brasil. Na ISSA costumamos resumir nossa missão com a seguinte frase. "A ISSA será tão forte quanto forem os laços entre seus associados", por isso investimos tudo no nosso associado.

Associe-se no link abaixo e venha compartilhar conosco todo seu potencial criativo.

https://www.issa.org/page/?p=Join_Online_8

ISSA Brasil

Presidente:
Jaime Orts Y Lugo

http://www.issabrasil.org

ANÁLISE DE SESSÃO COM AFTERGLOW

Por Michel Barbosa

No manejo de incidentes envolvendo segurança perimetral, principalmente DoS nos devices de frontend é muito comum que a primeira etapa da análise de um incidente passe pelos indicadores básicos de performance como utilização das interfaces, utilização de CPU e memória e o mais interessante (para o estudo deste artigo) a análise de sessões estabelecidas.

Este último indicador é como uma foto dos fluxos que estão passando pela sua rede no momento do problema e geralmente traz informações dos ofensores, tipo de ataque (SYN Flood, UDP Flood, etc) e também é uma fonte que pode ser analisada para otimizar o ambiente a partir da distribuição de tráfegos em determinados momentos.

Um ambiente médio pode ter milhares de sessões legítimas estabelecidas em dado momento e deixar para conhecer como sua rede se comporta no momento do ataque é a pior coisa que qualquer administrador de firewalls pode fazer, outra dificuldade desta abordagem é que a informação gerada por um dump de sessões geralmente é tão vasta que torna-se impossível analisar o log em sua forma "crua".

A comunidade já sinalizou em diversos momentos a necessidade de facilitar a análise de logs e muitas ferramentas vêm sendo desenvolvidas para suprir esta necessidade [1], scripts, analisadores de logs, SIEMs tem seu espaço no sentido de facilitar a análise de grandes quantidades de informação como é o caso exposto.

Uma iniciativa Open Source muito interessante para tornar gráfica a informação existente nos extensos arquivos de logs coletados em diversos momentos da vida útil da informação é o Afterglow [2], que é descrito por seus criadores como "uma coleção de scripts que facilitam o processo de geração de gráficos".

Sua configuração é bem minimalista e basicamente basta definir as regras de criação do seu gráfico em um arquivo de configuração consumido na chamada do script de geração do gráfico para obter de forma gráfica a informação existente em um dump de sessões por exemplo.

Um dos primeiros problemas enfrentados ao utilizar esta ferramenta estava na concentração de informação exibida, como dito anteriormente um firewall tem facilmente milhares de sessões estabelecidas e ao exibir isto graficamente a quantidade de informação concentrada no desenho pode facilmente se tornar um impecílio para qualquer análise de tendência ou utilização indevida.

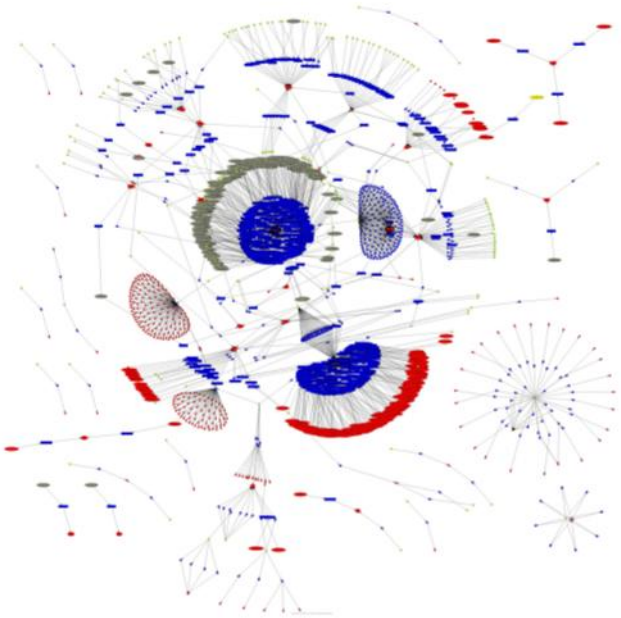
Uma saída encontrada foi a de suprimir a exibição de logs abaixo de um determinado threshold, desta maneira apenas hosts anômalos ou especialmente "ocupados" seriam exibidos, tornando a análise muito mais eficiente e relevante.

Abaixo segue um arquivo de configuração utilizado para exibir somente hosts que estão com mais de 100 sessões abertas (a linha importante é "label=field() if ($fields[0] > 100)"), as outras linhas servem para colorir o gráfico de acordo com o endereçamento e número da porta utilizada.

```
##############################################################################
# AfterGlow Color Property File
#
# @fields is the array containing the parsed values
# color.source is the color for source nodes
# color.event is the color for event nodes
# color.target is the color for target nodes

color.source="yellow" if ($fields[0]=~/^192\.168\..*/);
color.source="greenyellow" if ($fields[0]=~/^10\..*/);
color.source="lightyellow4" if ($fields[0]=~/^172\..*/);
color.source="red"
color.event="blue" if ($fields[1]<1024)
color.event="lightblue"
color.target="yellow" if ($fields[2]=~/^192\.168\..*/);
color.target="greenyellow" if ($fields[2]=~/^10\..*/);
color.target="lightyellow4" if ($fields[2]=~/^172\..*/);
color.target="red"

# Changing node labels:
label=field() if ($fields[0] > 100)
##############################################################################
```



Outras variações de chamada do programa e de configurações podem trazer ainda mais informações da sua rede do que você poderia esperar do árido dump de sessões do seu firewall.

[1] http://www.loganalysis.org/ e [2] http://afterglow.sourceforge.net/

Michel Barbosa

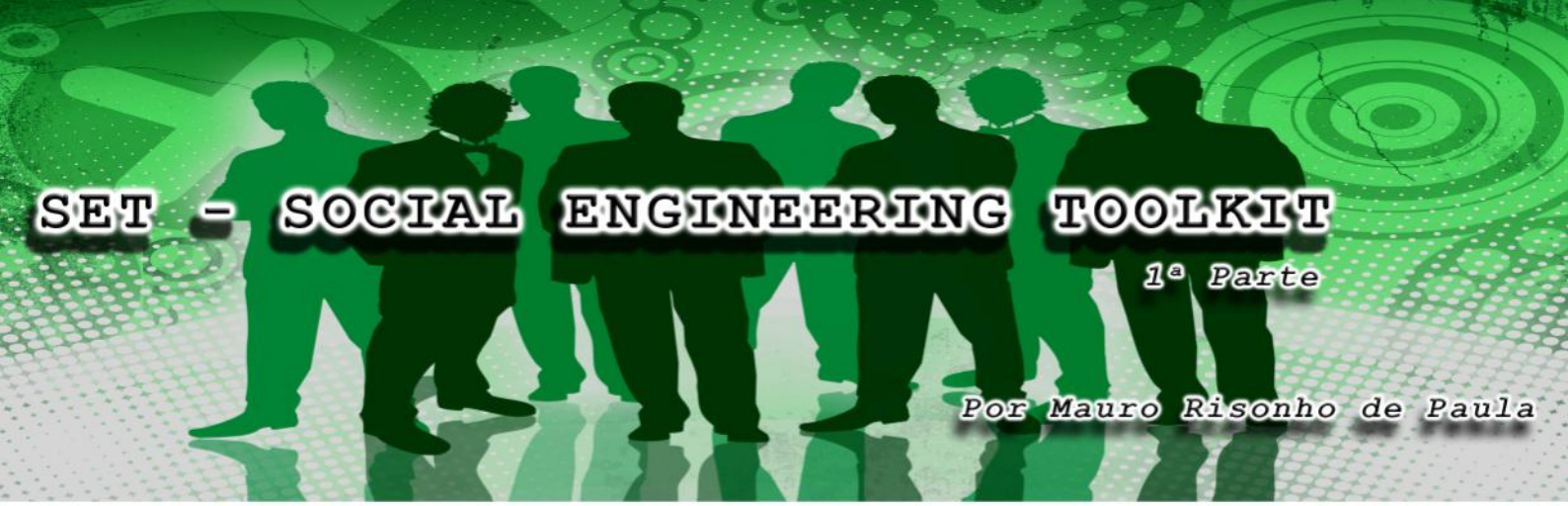
Formado em Engenharia Elétrica;

Trabalha há 3 anos com InfoSec lidando diariamente com tecnologias como firewalls e IPS;

Certificações nas tecnologias Juniper e Cisco;

Integra o time de especialistas em segurança da Global Crossing.

Possui um blog onde divulga técnicas de troubleshooting e ferramentas para facilitar a vida dos administradores de firewall (deadpackets.wordpress.com)



1. Introdução

Em Pentest (teste de invasão) há uma etapa onde testamos também a segurança social das pessoas e podemos comprovar se o "proxy mental", "firewall intelectual" e os IDS e IPS psicologicos das mentes da pessoas em geral, deixam passar desapercebidos que se trata de uma "idéia falsa".

Em Pentest (teste de invasão) há uma etapa onde testamos também a segurança social das pessoas e podemos comprovar se o "proxy mental", "firewall intelectual" e os IDS e IPS psicologicos das mentes da pessoas em geral, deixam passar desapercebidos que se tratam de uma "idéia falsa". Mesmo com um grande nível de segurança e tecnologia, há ainda pessoas que clicam nos sites e emails, do tipo "você acaba de ganhar 1 milhão de dolares, clique aqui." Esta ferramenta, é interessante para testar até que ponto seus usuários a serem testados são "ingênuos" ou não. A Engenharia Social é uma idéia antiga na humanidade. Dos tempos dos reis ou até antes, quando a comunicação era feita por mensageiros, se o rei inimigo soubesse daquele mensageiros, ele poderia mandar matar o verdadeiro mensageiro e substituir por um de seus guerreiros. Ao chegar a mensagem ao rei (que recebeu o falso mensageiro), haveria uma grande chance do falso mensageiro, por estar relativamente próximo ao entregar a mensagem, a grande chance de matar este rei (se o guerreiro fosse do tipo "Chuck Norris", é claro).

Tudo é uma questão de oportunidade!

Bom voltando para nosso tempo, hoje não é diferente. Invasores esperam a oportunidade de invadir seus alvos, mas muitas vezes há uma grande segurança (ou não) cercando e protegendo o alvo.

Mas dizem que não há cura para ignorância humana e uma ferramenta dessas pode fazer bem este trabalho.

O que o Social-Engineering Toolkit (SET)?

O Social-Engineering Toolkit (SET) foi desenvolvido por David Kennedy (ReL1K) e incorpora muitos ataques úteis de Engenharia Social e tudo em uma interface simples. O objetivo principal do SET é automatizar e melhorar em muitos dos ataques de engenharia social. Pentests em engenharia social muitas vezes é uma prática que muitas pessoas não executam.

O SET, assim vamos chamá-lo daqui em diante, é focado na técnica que em Pentest e Security chamado de Client Side Attacks ou melhor, Ataques no Lado do Cliente, isso devido a idéia de Client-Server ou Cliente-Servidor, que é por exemplo, um site hospedado no Servidor de um Hosting e o Cliente você acessando esta página via Browser (firefox, IE e outros).

Praticamente o SET é construido em cima do metasploit, mas com scripts automatizados e resultantes nas sequencias de ataque. Seria o equivalente a codificar scripts que acionam os comandos via msfcli do metasploit, mas há muitos comandos que não são do metasploit e que em conjunto, formam o SET.

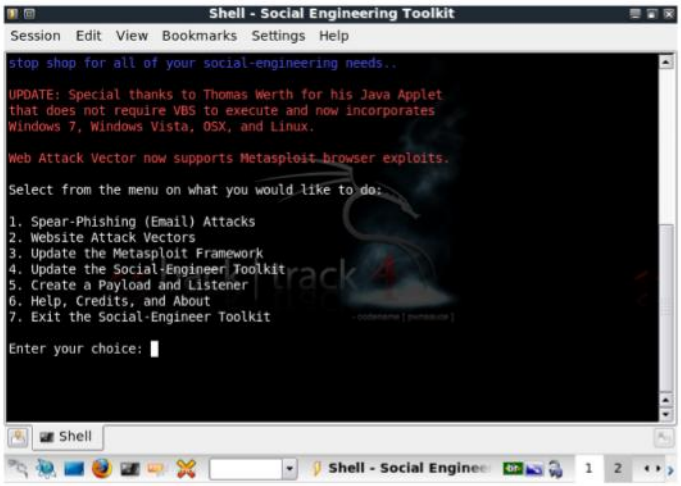
Bom vamos lá!

Estarei continuando este artigo em vários outros, por isso estou divindo em parte pois a ferramenta é um pouco grande para um artigo só.

Aguardem.

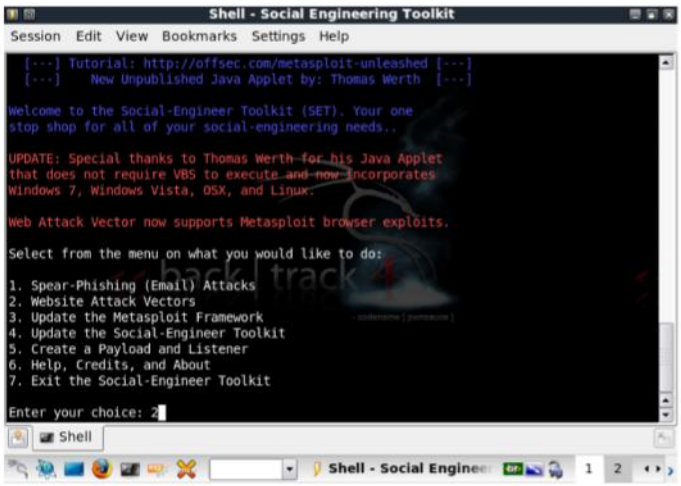
Passo 1

Iniciado o framework do SET, você irá ver um menu como este:



Passo 2

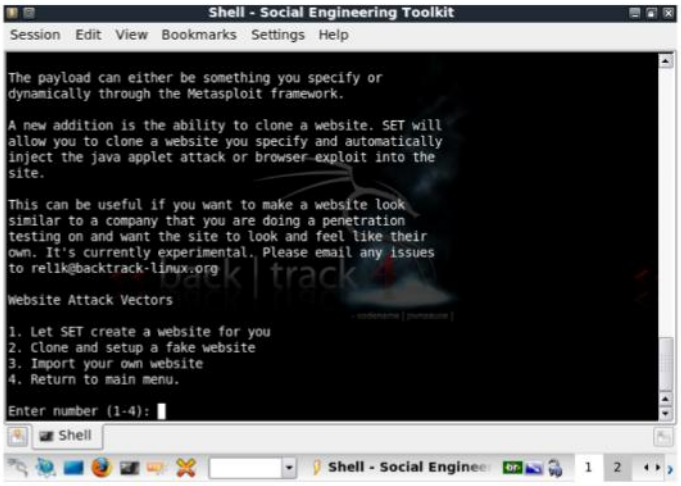
Escolha a opção 2 - "Web Attacks Vectors", ou seja, Vetores de Ataque para Web, digitando 2 e enter



OBS: "Web Attacks Vectors" ou Vetores de Ataque para Web, são equivalentes a combos de ataques ou vários ataques diferentes sobre alvo(s), que resultando em um ataque mais poderoso, do que 1 ataque por vez, sendo então melhor definido com uma sequencia de ataques simultãneos e diferentes entre si.

Passo 3

Em seguida, escolha a opção 1 "Let SET create a website for you", ou "Deixe o SET criar um site para você", sendo esta opção, uma escolha para quem quer criar um site automatizado do zero. Lembrando que após este passo será criado um Payload via Metasploit em conjunto com seu site falso.



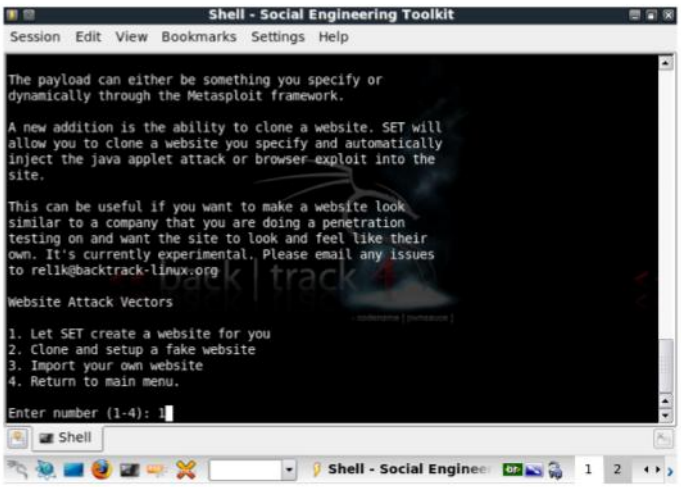
OBS: As outras opções dentro desse menu são:

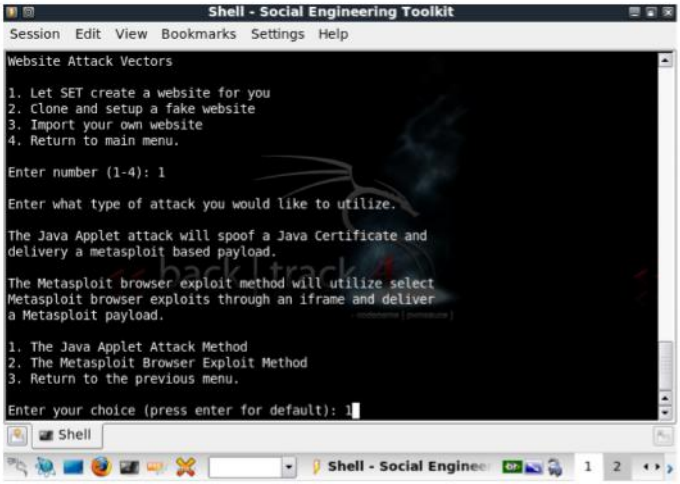
2- Clone and setup a fake website (Clone e configure um site falso) - ou seja, você copiará um site autêntico e verdadeiro da web, que o SET irá gerar um falso site, baseado no verdadeiro (falarei em outro artigo em breve).

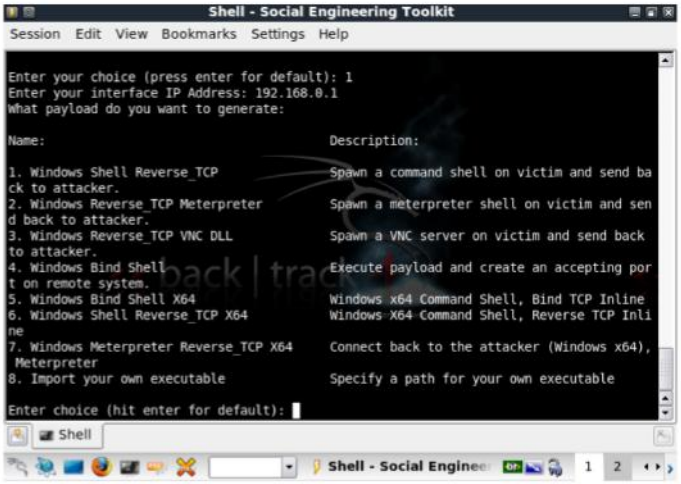
3. Import your own website - Irá importar um site que você mesmo fez (falarei em outro artigo em breve, também) 4-Return to main menu. - Voltar ao menu anterior, caso você queira trocar de opção anterior ou algo assim.

Passo 4

Depois, escolha a opção 1 "The Java Applet Attack Method", ou "Método de Ataque através de Applet Java" que será usado no alvo com uma "isca" para o usuário que acessar seu site falso. Afinal de contas, hoje em dia alguns bancos tem seu componente de acesso ao banco em java e muitos usuários apenas "aceitam" sem entender muito tecnicamente, pois apenas querem acessar suas contas. Nem imaginam que pode ser um componente falso, podendo ser usado para estes fins.







ALTAMENTE IMPORTANTE:

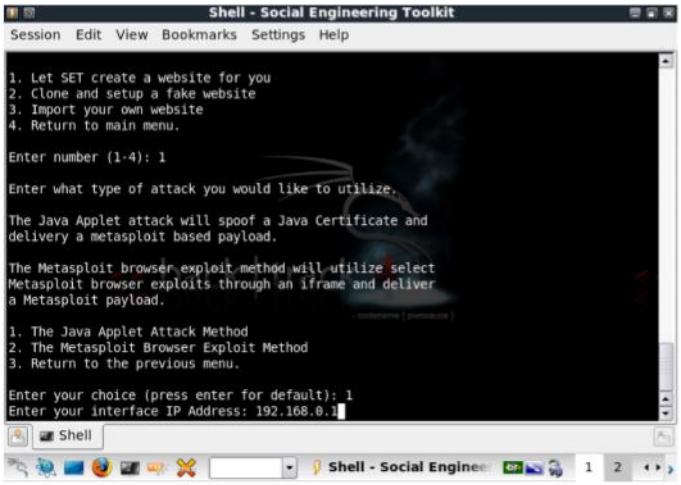
Não seja um grande idiota que será possivelmente preso tentando fazer essa técnica para fins que não sejam educacionais, de pesquisa ou para a área profissional de segurança (pentest ético).

Utilize uma máquina virtual para seus testes.

O autor deste artigo não se responsabiliza pelos atos expressos neste artigo para fins criminais e/ou que possam lesar terceiros.

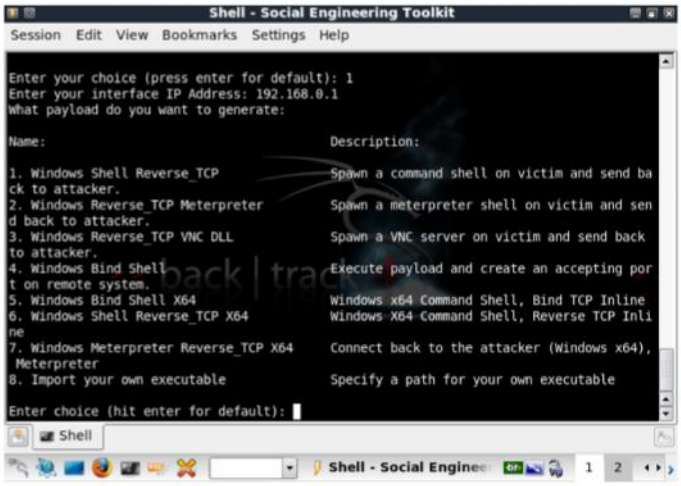
Passo 5

Confirmado com a opção opção 1 "The Java Applet Attack Method", ou "Método de Ataque através de Applet Java", o SET irá te perguntar em qual IP(ORIGEM), você deseja que seja o Servidor do seu site falso. Aproveitem a idéia de IP SPOOFING aqui. No nosso exemplo, será 192.168.0.1 por ser um exemplo de Lab Penetration Testing.



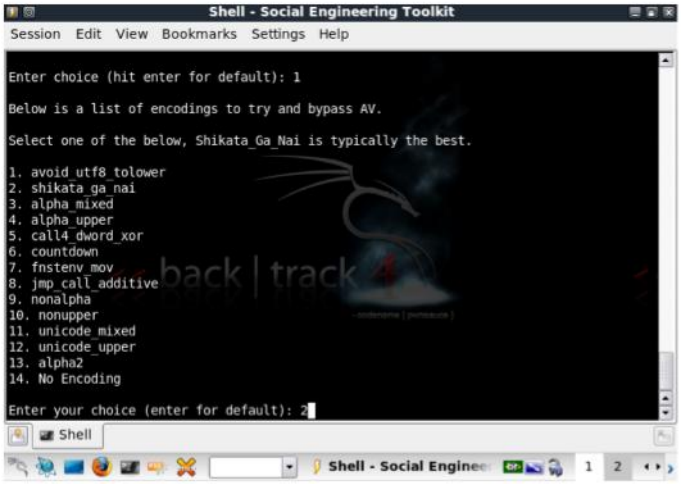
Passo 6

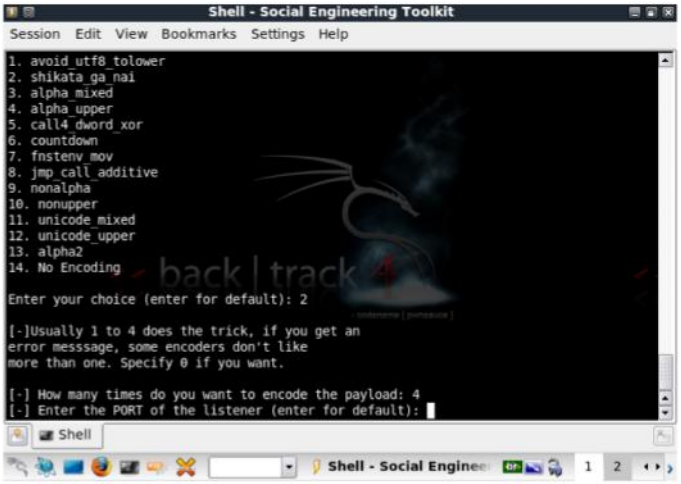
Agora escolhemos o Payload, que no caso será usado do metasploit. Escolhemos a opção 1 que é "Windows Shell TCP Reverse" para enviar um payload a vitima por TCP e voltar com a conexão do alvo para você (reverse). Há vários payloads, para escolher, cada cenário ao alvo, um é mais indicado que outro, mas você também, se for um "writer payload na unha", pode codificar seu próprio payload ou usar de algum outra pessoa desta área, que será adicionado ao site falso.



Passo 7

Agora você vai escolher o encoder, no exemplo, a opção 2 "shikata_ga_nai" "(deve ser algum oriental que fez este encoder:). O que seria o encoder aqui neste passo? Seria uma forma de compatibilizar seu exploit com seu alvo e ao mesmo tempo codificar de tal maneira que passe sem ser percebido pelas assinaturas de vírus do AntiVirus, então passando livremente. Essa técnica é chamado de Bypass AV. Há vários tipos de Bypass para SQUID, IPTABLES, BIOS, Logins e outros.



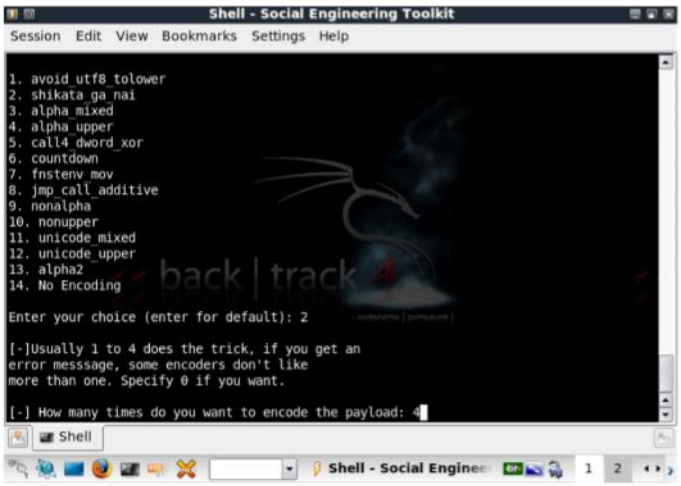


Passo 8

Agora será perguntado, quantas vezes você deseja que seja recodificado via o encoder. Sendo 1 = 1 vez e até 4 = 4 vezes (é lógico que quantos mais vezes, sendo codificado, menos chances do Antivirus detectar seu exploit), mas lembre-se, dependendo do SO ou aplicativo, você poderá ter resultados estranhos. Para testar se seu exploit está sendo detectado pelos Antivirus mais conhecidos no mercado, envie à este sites:

http://www.virustotal.com/
http://www.jotti.org/

Quantos mais antivírus detectarem na lista, menos chances você terá de estabelecer conexão com alvo e executar plenamente seu exploit, se seu alvo tiver algum deles.



Passo 9

Escolha a porta que seu alvo irá comunicar com você digitando e confirmando com Enter: Por padrão a porta que será transmitida pelo servidor do site falso será por exemplo:80 que é tradicional na maioria das vezes para Servidores Web.

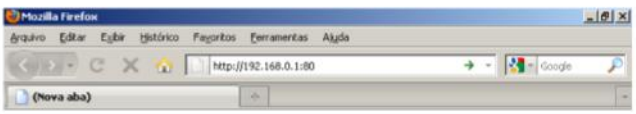
A partir deste momento estamos simulando a máquina do usuário (alvo)

Passo 10

Pulamos o passo, onde o usuário (alvo) acessou um email phishing veja mais em http://pt.wikipedia.org/wiki/Phishing (é aquele e-mail que fala que você ganhou na loteria, uma garota modelo quer te conhecer, fotos proibidas das mulheres do BBB, bom acho que você entendeu...) e o usuário alvo clicou no link e acessou o site

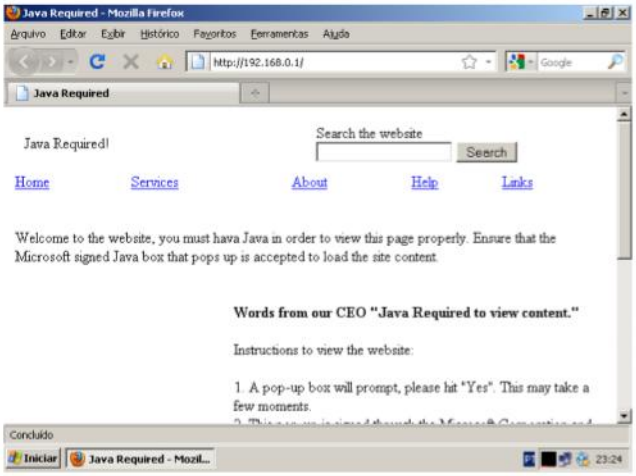
Passo 11

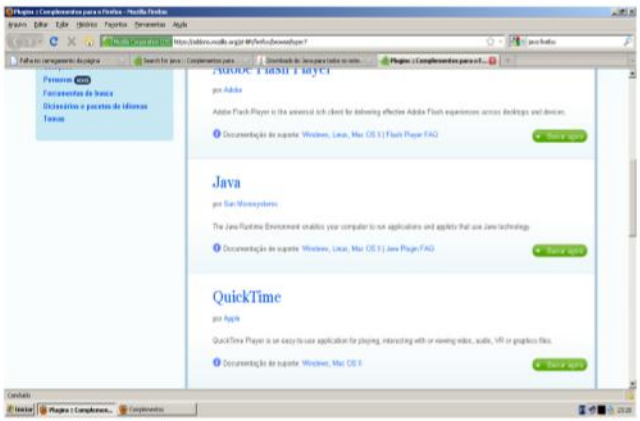
(no caso usamos o IP 192.168.0.1 e na porta 80, por ser um VM, mas poderia ser um funcionário interno da empresa praticando MITM (man-in-the-middle attack)).



No caso o site no está modelado o suficientemente para convencer alguns usuários a clicar, pois dá impressão que está em construção ou é "suspeito", mas você pode desenvolver de tal maneira, que seja convincente.

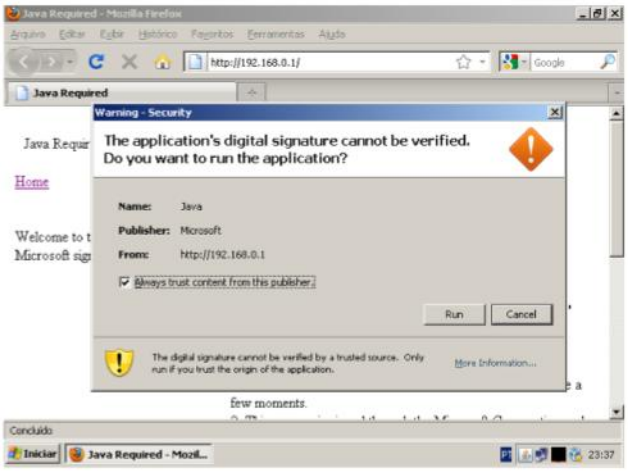
Ao acessar o site, será requisitado a instalação do JAVA, caso não tenha. Acessando o site de Add-ons do firefox há um add-ons para JAVA em https://addons.mozilla.org/pt-BR/firefox/search/?q=java&cat=all&lver=any&pid=1&sort=&pp=20&lup=&advanced=





Já para usuários windows ou IE o download em outro local

Instalado o JAVA, uma janela alerta se deseja executar o aplicativo JAVA, então o usuário(alvo) irá clicar em "RUN"



Pronto!

Você já tem o se alvo, conectado ao seu payload, com um exploit e pode ter uma sessão de meterpreter, etc, etc, etc.

O Resto, fica por conta da sua imaginação, ou melhor, do seu "expertise".

Mais informações em:

http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29

Até o próximo artigo.

Mauro Risonho de Paula Assumpção

Diretor Firebits;

Consultor de Segurança Independente;

Pentester da NSEC Security Systems;

Realiza projetos de segurança/palestras em empresas do ramo de obras, petrolífero, cosmético, atacado e outros;

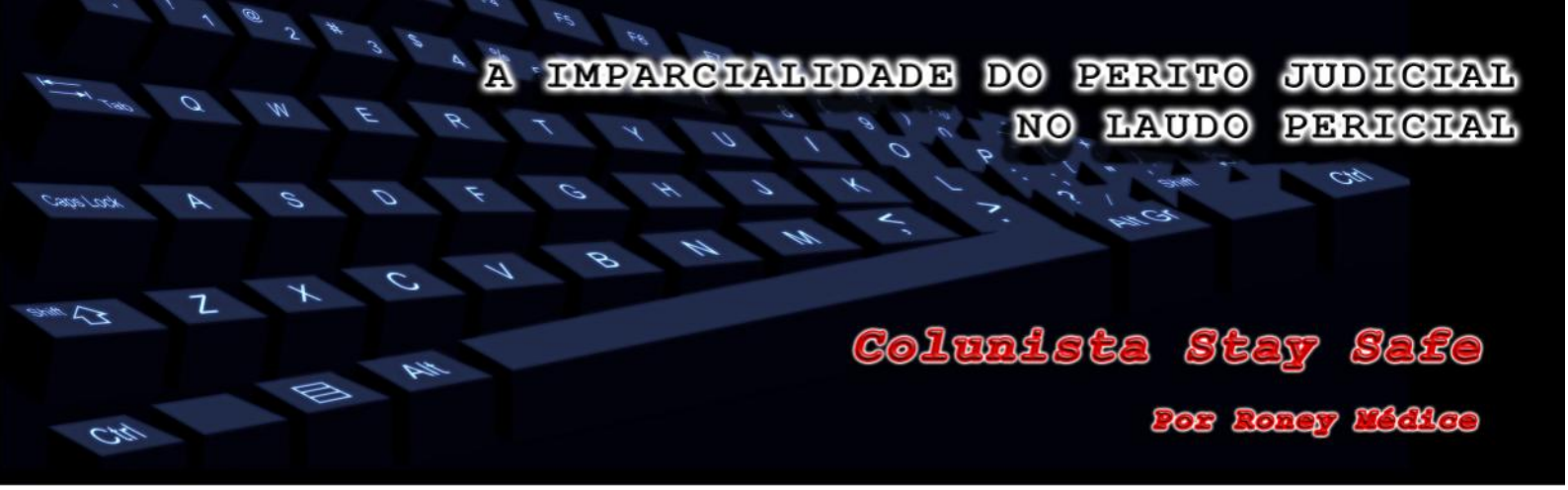
Líder/Fundador do "Backtrack Brasil" e Moderador do Backtrack EUA;

Palestrante da c0c0n 2010(India).

Você quer a sua empresa em contato com os melhores profissionais de Segurança da Informação???

Então a sua logomarca deveria estar aqui.

contato@staysafepodcast.com.br



A IMPARCIALIDADE DO PERITO JUDICIAL NO LAUDO PERICIAL

Colunista Stay Safe

Por Roney Médice

Um experiente profissional em computação acaba de concluir um curso de perícia digital e obtêm o seu primeiro certificado, qualificando-o para conduzir um processo de investigação para resolver um caso que necessite conhecimento aprofundado. Entretanto, existe o medo natural desse profissional que em seu primeiro trabalho, o seu lado pericial seja rejeitado pela Justiça ou desqualificado pelo advogado da defesa.

Conhecer os preceitos dos Códigos Penal e Civil, assim como os Códigos Processuais vigentes é de fundamental importância para que o perito faça o seu trabalho da melhor maneira possível e dentro da legalidade, evitando que todo o seu trabalho de investigação e confecção do laudo pericial não seja invalidado.

No artigo 332 do Código de Processo Civil Brasileiro conceitua que "Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos...". Entretanto, o perito judicial não pode fazer a busca por provas ou indícios para responder aos quesitos do juiz (que são perguntas previamente levantadas pelas partes interessadas da lide e do próprio magistrado) e tecer a sua opinião pessoal no laudo pericial ou mesmo durante o processo de investigação, posicionando a favor do autor da ação ou da defesa.

Caso ocorra, por parte do perito, algum tipo de manifestação de opinião ou julgamento prévio sobre o investigado, o perito poderá ser desqualificado pela parte prejudicada conforme o artigo 138, inciso III do Código de Processo Civil que é motivo de impedimento ou suspeição do perito, ocasionando em descaracterizar o perito que foi nomeado para responder aos quesitos do magistrado.

O Perito Judicial é um excelente auxiliar da justiça pois a sua nomeação é parar dirimir dúvidas ou buscar por provas quando o juiz não possui conhecimento específico para opinar sobre as questões técnicas. Seu dever é reunir todos os seus esforços para honrar a sua nomeação e fazer jus à sua atividade, trabalhando de forma imparcial e com fidelidade dos fatos apurados, não deixando que razões de ordem pessoal interfiram no resultado.

A elaboração do laudo pericial deverá ser constituída de termos técnicos sem excesso, evitando ao máximo expressões complexas, informando a metodologia de trabalho utilizada, técnicas, softwares e hardwares empregados. Em hipótese alguma o Perito Judicial colocará a sua opinião em decorrência das provas constituídas. Lembre-se que o juiz não tem o conhecimento específico e portanto, tem que entender o laudo pericial para que possa se um documento de auxílio na decisão do magistrado e não um documento com posição pessoal do perito, pois quem decide a lide é o juiz.

Conforme o artigo 429 do Código de Processo Civil, o Perito possui ampla liberdade em seu trabalho, podendo ouvir testemunhas, obter informações, solicitar documentos que estejam em poder da parte ou em repartições públicas, bem como instruir o laudo com desenhos e fotografias. Entretanto, o profissional deve lembrar que o seu papel é de relatar as provas obtidas e responder as questões que lhe foram submetidas, sem expressar sua convicção sobre o caso. As vezes, muitos peritos terão acesso à informações confidenciais que incriminam o autor do processo em outros crimes previstos pelo Código Penal, porém, a sua investigação tem que ficar limitada a responder as perguntas sobre o crime tipificado no processo atual, que ensejará o laudo pericial.

Na sociedade, devido à formação, hábitos e referências, é normal tomarmos partido aos eventos que acontecem a nossa volta, de uma forma ou de outra, influenciados por diferentes motivações. Por exemplo, nos últimos acontecimentos que estamos vendo nos noticiários sobre a suporte morte de uma jovem por uma pessoa bem sucedida financeiramente, é normal ficarmos contra ou a favor do acusado conforme as informações vão sendo noticiadas na imprensa. Entretanto, o Perito Judicial não pode ter opinião, e sim, somente respostas baseadas nas provas levantadas.

Obviamente que o Perito carrega uma grande carga emocional forte em cada caso que ele é nomeado, pois o simples fato de se instaurar um processo, já estabelece um situação de conflito entre as partes, que pode eventualmente a conduzi-lo a uma tomada de posição, a um juízo de valor. O Perito está sujeito a cair nessa armadilha.

Um problema que o perito judicial pode ter é sentir-se responsabilizado por "decidir" o processo com base nas provas que ele levantar, ou seja, dependendo do resultado do seu esforço, o réu poderá ser absolvido ou condenado. Outros fatores preocupantes é envolver-se emocionalmente na questão, preocupar-se em fazer um laudo com preciosismo técnico, duvidar se tem conhecimento suficiente para aceitar a perícia, etc.

Contudo, o Perito Judicial deve-se abster de manifestar sobre a lide em questão, não fazendo conclusões que podem induzir em erro o juiz, levantando todas as provas necessárias e indícios para responder aos quesitos de forma objetiva e que o seu laudo pericial seja o mais completo possível para evitar que seja desqualificado ou questionado o seu trabalho pericial.

Roney Médice

Coordenador de Segurança da Informação do Terminal Retroportuário Hiper Export S/A;

Consultor de Segurança da Informação do Grupo Otto Andrade;

Membro da Diretoria do CSA – Cloud Security Alliance, do Comitê ABNT/CB-21;

Presidente da APECOMFES – Associação de Peritos em Computação Forense do ES;

Graduado em Ciência da Computação e Direito;

MBA em Gestão de Segurança da Informação e

Presidente da Comissão de Fomento e Desenvolvimento do ISSA nas Regiões Sudeste/Centro-Oeste.

MURPHY

Por Glaysson dos Santos Tomaz

Suponha que bem na hora de sair de casa, você não encontre as suas chaves e inicie uma busca frenética pela mesma. Quando enfim as encontra, você para e pensa, mas como fui encontrar as chaves no último lugar onde procurei?

Não é obvio que uma vez encontrada as chaves a busca se torna desnecessária? Ou faria algum sentido encontrar as chaves e continuar procurando por elas?

Portanto, onde as chaves estiverem, será o último lugar onde você irá procurá-las.

Ignorando essa breve elucidação, vamos à fórmula:

$$P_M = K_M \left(e^{\frac{-I*C*U+F}{F_M}} - 1 \right)$$

A fórmula usa uma constante igual a 1, um fator inconstante e algumas variáveis. Nessa fórmula Joel Pel [1] usa a importância do evento (I), a complexidade do sistema envolvido (C), a urgência da necessidade do sistema funcionar (U) e a freqüência com que o sistema é usado (F).

Não parece familiar?

No dia em que você mais precisar de um backup, ele não terá sido feito, ou estará corrompido. Será a lei de Murphy? Sim, e ao quadrado, pois dentre as medidas de segurança adotadas por uma organização, que preza pelos seus dados, o backup deve receber especial atenção, uma vez que o perito forense investiga a cena do crime em busca de indícios que levem a identificação do criminoso, e dos atos realizados, mas, caso haja um "cadáver", cabe ao backup a tarefa de ressuscitar.

No entanto, a checagem da integridade dos mesmos é tão importante quanto os mecanismos para realizá-los, pois de nada adiantam backups zerados ou corrompidos. Dessa ótica, qualquer que fosse o dia em que um backup se fizesse necessário, ele não serviria, e surgiria o enigma: "Justo quando preciso de um backup ele não funciona."

```
-rw-r--r-- 1 root root 0 2010-05-06 20:05 BACKUP-MYSQL-SERVER-20100505.tar.gz
-rw-r--r-- 1 root root 0 2010-05-06 20:05 BACKUP-DATABASE-SERVER-20100505.tar.gz
-rw-r--r-- 1 root root 0 2010-05-06 20:05 CONFIG_FILES-20100505.tar.gz
-rw-r--r-- 1 root root 0 2010-05-06 20:05 DADOS_CLIENTES-20100504.tar.gz
-rw-r--r-- 1 root root 0 2010-05-06 20:05 EMPRESAS_CLIENTES-20100503.tar.gz
-rw-r--r-- 1 root root 0 2010-05-06 20:05 EMPRESAS_CLIENTES-20100504.tar.gz
-rw-r--r-- 1 root root 0 2010-05-06 20:05 SERVER_CONFIG_FILES-20100505.tar.gz
```

Figura 1 - Backups zerados e irregulares

A situação dos backups é semelhante a dos logs. O administrador implanta todo tipo de solução, mas nunca verifica os logs gerados pelos mesmos, então para que servem os logs? Serão meros arquivos inconvenientes que ficam lotando o HD? “Não seja leigo, leia os logs!”.

É surpreendente como a simples leitura de /var/log/secure, /var/log/httpd/access_log pode evitar problemas em ambientes *n*x. Possíveis invasões por alguns sistemas de bruteforce podem ser evitadas dessa forma; pois, por se tratar de uma técnica indiscreta que gera grande volume de log no alvo pode ser facilmente detectado com a verificação dos arquivos de log dos serviços correspondentes.

Figura 2 - SSH Automated bruteforce

O mesmo se aplica a outros ataques baseados em tentativa e erro, que passam instruções via browser, ou automatizados, que passam instruções via métodos GET/POST, como mostra a figura 3.

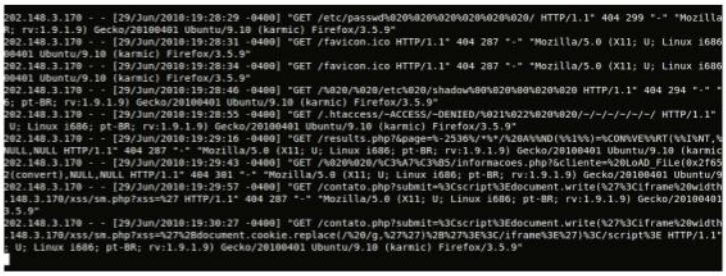
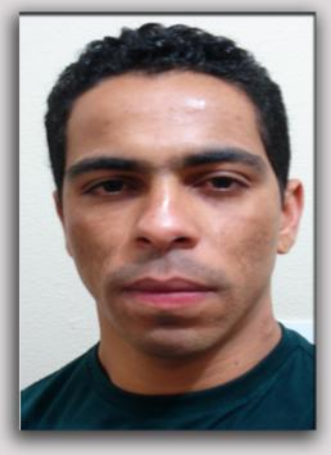


Figura 3 - SQLi, XSS,TransPath,RFI

Contudo, se ler logs não é um hábito, e não existe uma boa política de senhas e de acesso, o que permite que as senhas sejam criadas indiscriminadamente, e que qualquer um de posse da mesma possa se conectar é só uma questão de tempo para que o servidor seja shared with the world.

Tenha sempre em mente a formula de Joel Pel[1], dando especial atenção às variáveis (U) e (F), que representam a urgência do sistema funcionar e a freqüência com que o sistema é usado, respectivamente, pois, quando você mais precisar dos backups e dos logs, eles podem não estar tão confiáveis, íntegros ou disponíveis como deveriam.

1 - Joel Pel, engenheiro biológico da University of British.



Glaysson dos Santos Tomaz

Cursando 3º período de Ciências da Computação pela PUC;

Pesquisador de segurança independente;

Atua como analista de segurança e administrador de redes Linux;

Seus interesses incluem Forense Digital, Pentest, Python, Linux, Literatura, PNL e estudos relacionados à aplicação desta na segurança da informação e hacking