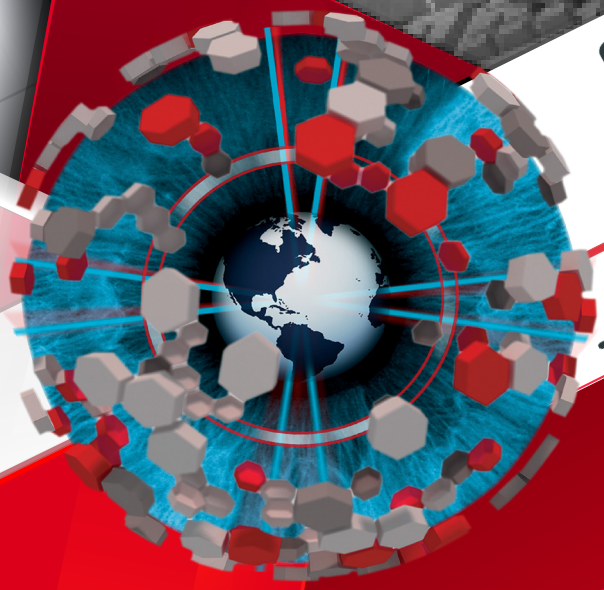
H2HC

HACKERS TO HACKERS CONFERENCE

MAGAZINE



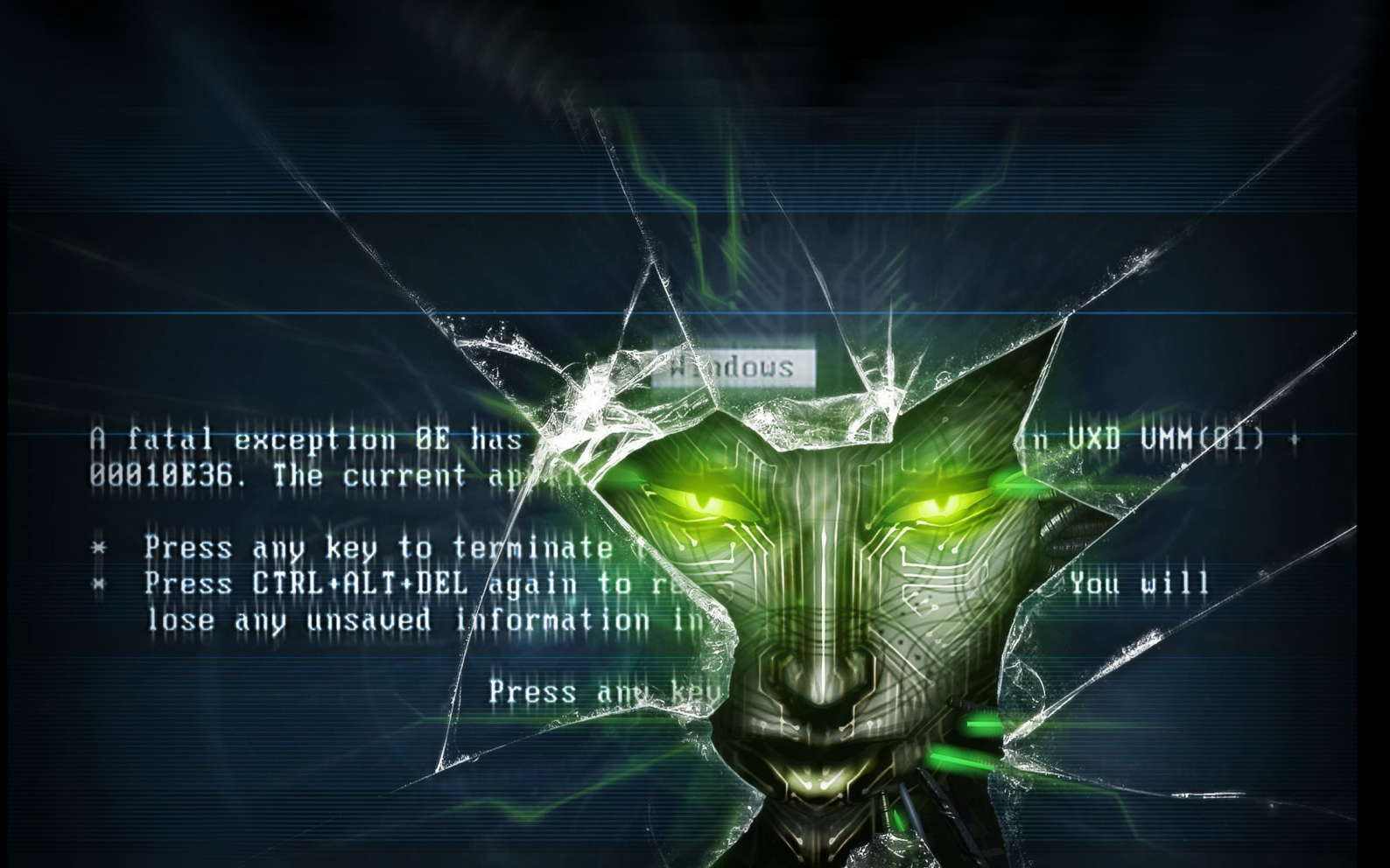
CFP COGUMELO BINARIO

CALL FOR PAPERS PARA COGUMELO BINARIO 2013 ESTÁ ABERTA!

H2HC EDIÇÃO 10 ANOS

EDIÇÃO DE 10 ANOS DA HACKERS TO HACKERS CONFERENCE JÁ ESTÁ COM AS INSCRIÇÕES ABERTAS!

ED. 4
Julho 2013



Call for Papers
E-zine Cogumelo Binário

Os 6 primeiros papers aprovados para o cogumelo binário terão palestra garantida no H2HC!

O staff do H2HC escolherá 3 possíveis tipos de palestras: principal, workshop ou auditório secundário.

Além disso, todos autores de papers aprovados terão sua entrada liberada no evento.

http://cogubin.ftp.sh/
http://www.secplus.com.br/cogubin/public/

Índice

Artigos

Artigos Universitários

Eventos

Inovando com Smartphones

Jordan M. Bonagura

No dia 12 do mês de setembro de 2012, Phil Schiller, executivo da Apple, anunciou ao mundo o novo iPhone 5, com muitas novas funcionalidades, entre elas, maior resolução *(1136x640)*, 18% mais fino e 20% mais leve do que o modelo anterior, porém a grande novidade que quero destacar é o chip A6. É um novo processador, que segundo a empresa, é duas vezes mais rápido que seu antecessor e possui dois núcleos de processamento.

Este novo modelo de processamento continua tendo suporte a multitarefa e com isto permite a navegação entre múltiplas aplicações, e diversas delas poderão ser executadas em background.

Partindo para o mercado de computação em geral, a previsão segundo o IDC, conforme *figura 1* na página seguinte, é de que os smartphones deverão continuar crescendo e cada vez mais substituindo os computadores, inclusive criando uma nova era chamada de Pós – PC, sejam eles portáteis ou não.

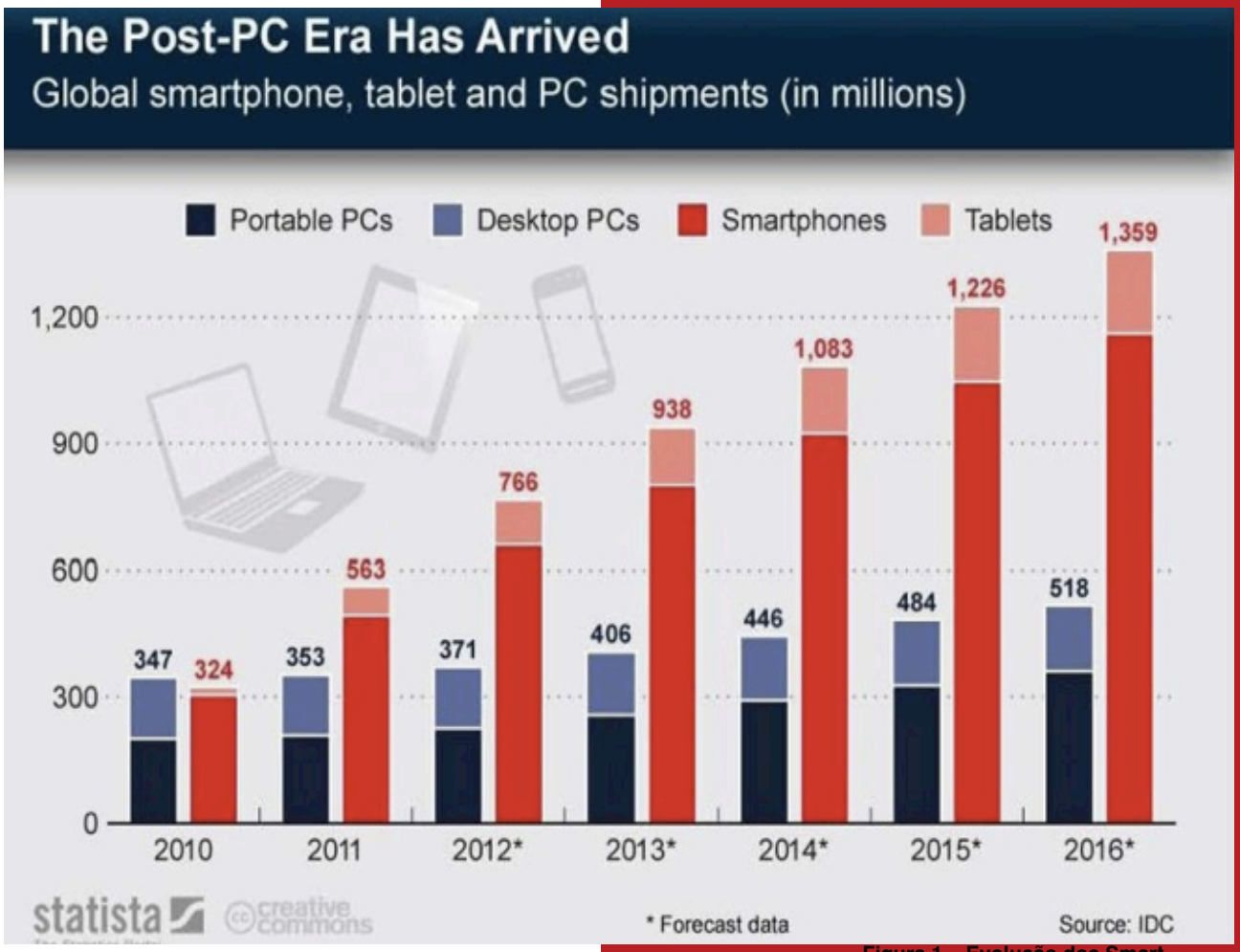


Figura 1 – Evolução dos Smartphones. Fonte: IDC

Ok, já sabemos o quanto este mercado de smartphones tem crescido, e que este deverá continuar sua trajetória de sucesso, obtendo diariamente novos usuários, seja para fins de uso pessoal ou empresarial.

Então você deve estar se questionando o porquê de um profissional, que normalmente fala sobre segurança da informação está tratando sobre o crescimento do mercado de smartphones.

Fácil! Você adivinhou! Este artigo demonstrará o quão importante é proteger minhas informações contidas no celular de um usuário mal intencionado, que poderá um dia invadir meu equipamento e roubar meus dados de contatos, e-mails e outras informações. Certo?

Não, não é sobre este ponto que quero tratar, pois isto não é mais novidade para ninguém, e nem mesmo a idéia de demonstrar a importância do crescimento deste mercado, e esta nova *"Era móvel"*, tudo isto foi só a base para o grande X da questão, ou devo dizer da Miopia do CSO...

O grande problema está novamente relacionado com questões que envolvem a política de segurança da informação de uma empresa e o meio pelo qual esta é gerida.

Refiro-me a este ponto, pois muitas vezes, principalmente em grandes corporações e até mesmo órgãos governamentais, onde o acesso a informação é, ou deveria ser, ainda mais restrita, profissionais tem literalmente seus notebooks barrados

no momento do acesso, ou então uma burocracia extrema para entrar com seu equipamento.

Se em algum momento você questionar o porquê desta atitude, certamente obterá a resposta: *"Por uma questão de segurança"*

É... Será que podemos passar a chamar a gestão relacionada à segurança como um todo de míope?

Literalmente existem menores computadores nas mãos de seus concorrentes ou crackers, e estes podem realizar com êxito todo o trabalho de um notebook em um processo de invasão e obtenção dos dados, aliás, as principais ferramentas para isto já estão disponíveis e podem até automatizar grande parte do processo, como você pode ver na figura 2, e ainda mais agora que são multitarefas e possuem grande poder computacional de processamento.

Atualmente chamamos isto de Smartphones!!!

Vocês concordam que no caso de espionagem industrial, é muito melhor um celular aparentemente inofensivo no bolso do terno em uma rápida visita ao banheiro, do que um notebook com o adesivo (figura 3) *"eu leio o seu e-mail ou meu outro computador é o seu computador".*

Figura 2 – Backtrack e Metasploit no Smartphone - Fonte: Backtrack-linux.org

Figura 3 – Notebook adesivado.
Fonte: Elaborado pelo autor

Jordan M. Bonagura

Pesquisador em Segurança da Informação / CEH.
Fundador do Projeto Stay Safe
Graduado em Ciências da Computação
Pós Graduado em Gestão Estratégica de Negócios, Docência e Estratégia para Empresas
Organizador da Vale Security Conference
Ex Membro Diretor do Cloud Security Alliance – Brasil. Membro da Comissão de Crimes de Alta Tecnologia da OAB.
Professor e Coordenador de Curso em TI.
Information Security Consultant – Regional Manager – Daryus.
Fundador do SJC Hacker Clube. Palestrante em eventos de segurança da informação (CNASI, H2HC, SegInfo, WebSecForum, ITA, entre outros)

Reflexões sobre os Impactos da Lei de Crimes Informáticos na Segurança da Informação

José Antônio Milagre

Fonte: http://jornalocotidiano.com

Entrou em vigor no Brasil, no dia 02 de abril de 2013, a *Lei Carolina Dieckmann*, número *12.737/2012*, que tipifica os crimes cibernéticos (crimes informáticos). A Lei, fruto de um casuísmo, em que o inquérito policial relativo a suposta invasão do computador da atriz sequer foi concluído, e nenhuma ação penal intentada (porém os acusados mais que pré-julgados), passa a punir determinados delitos, como a "invasão de dispositivos informátcos", assim dispondo especificamente: Art. 154-A.

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 meses a 1 ano, e multa.

Trata-se de crime em que basta a conduta, não se exigindo resultado. Invadir significa devassar, entrar a força. Esta “invasão” deve se dar em um dispositivo informático, que embora esteja associado a um “hardware” que armazena, trata ou processa informações ou dados, possa ter sua interpretação estendida por autoridades nos casos de invasão de ativos lógicos como um disco virtual, arquivo base de esteganografia, rede social, webmail de um serviço web ou ativos lógicos protegidos que armazenem informações (Embora tais interpretações devam ser freadas pelo principio da legalidade, é o que esperamos.)

Deve-se esclarecer que a invasão, para ser criminosa, deve se dar sem a autorização expressa ou tácita do titular do dispositivo ou dos dados (caso em que este usa um serviço Cloud SaaS, por exemplo) Logo, o agente que realiza teste de intrusão “pentest”, não pode ser punido, por não estarem reunidos os elementos do crime. Caberá, no entanto, às empresas de segurança e auditoria, adaptarem suas propostas, políticas e contratos de serviços e pesquisa neste sentido, prevendo expressamente a exclusão de eventual incidência criminosa nas atividades desenvolvidas.

Já as intrusões em sistemas cujo titular não autorizou, poderão ser consideradas condutas criminosas, desde que comprovado que o agente o fez com o objetivo de obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidade para obtenção de vantagem ilícita. Mas como “comprovar a finalidade” de uma intrusão?

A questão da finalidade de “obter dados” é também polêmica. Para um grupo de juristas, a “espiada” não seria crime, só se falando em objetivo de obtenção nos casos de cópia ou tentativa de cópia dos dados do dispositivo, ou quando o agente tentou entrar ou entrou na “posse dos dados”. Para outra corrente, o simples acesso a dados (um select em uma das tabelas da vítima, por exemplo) já agride o bem jurídico protegido pelo Direito Penal, e demonstra a “intenção em obter dados” eis que já permite ao cracker, em certos casos, se beneficiar das informações, de modo que tal “contato” com os dados estaria inserido no contexto do “obter dados”, previsto no tipo penal trazido pelo artigo 154-A da Lei Dieckmann.

É o Judiciário quem vai interpretar esta questão, porém ao contrário do que alegam alguns advogados, não é necessário a cópia dos dados para a prática do crime, pois trata-se de crime formal e de perigo abstrato, diga-se, basta a invasão com a “intenção da obtenção dos dados”. Tal fato poderá ser provado por perícia técnica. A perícia é capaz de, em se analisando os indícios deixados, ponderar sobre a intenção do cracker.

O agente que realiza o footprinting (levantamento de informações do alvo) com programas como nmap ou outro scanner, apenas para identificar se o alvo está ativo, as vulnerabilidades do sistema, portas abertas, serviços desnecessários rodando, sistema operacional, dentre outros, em tese não comete crime, pois atos preparatórios não são puníveis e o agente não chegou a dar início a invasão (ato executório).

Deste modo, quem encontra vulnerabilidade em sistema alheio, mesmo sem autorização para pesquisa, e comunica o administrador, está realizado a “revelação responsável”, não podendo incidir nas penas o art. 154-A, agora

previsto no Código Penal. Já a prova de conceito, desenvolvida por quem descobre falha em ativo, sem autorização do titular, dependerá da apreciação pericial para se verificar como afetava o dispositivo atingido e qual foi a extensão decorrente da PoC. É possível às empresas de pesquisa em segurança adaptar suas PoCs, para que não sejam consideradas ferramentas criminosas. Por exemplo, uma prova onde o payload é executar o notepad.exe, revela claramente a intenção do agente, que não pode ser considerada maliciosa, mesmo que não tenha autorização para testar determinado ativo.

É possível também se pensar na invasão tentada, onde o agente chega a executar a invasão, mas é impedido pelo time de resposta a incidentes, equipe de forense, ou IDS (Intrusion Detection System) que detecta o evento em tempo de execução. Caberá ao perito digital avaliar se os códigos executados tinham aptidão técnica para que o agente pudesse ter acesso às informações, manipulá-las ou para "instalar vulnerabilidades"(sic).

O agente que invade sistema, sem autorização, para tão somente demonstrar a insegurança e cooperar para o aprimoramento dos controles, em tese não responde pelo crime. Tal intenção poderá ser demostrada pelas fases da sua conduta (sempre menos ofensiva à empresa ou titular do dispositivo) ou mesmo pela atuação pericial ou depoimentos, no decorrer de eventual inquérito policial ou ação penal.

Outras formas de acesso indevido, onde não ocorre a "invasão", que é conduta comissiva/ativa, podem não se enquadrar no tipo penal. Assim, na engenharia social que faz com que a vitima forneça credenciais de acesso ou mesmo acesse voluntariamente determinado programa que libera o acesso a seu dispositivo, fica eliminada, em tese, a incidência do delito em comento, podendo o agente, diante do caso concreto, responder por outros delitos do Código Penal, de acordo com a extensão do dano.

Do mesmo modo, o acesso indevido feito por um agente através de protocolo RDP (Remote Desktop Protocol) ou tecnologias como Terminal Service, VNC, PCAnywhere, Logmein, dentre outras, não caracterizam invasão se o serviço de "assistência remota" foi habilitado pelo titular do dispositivo sem qualquer mecanismo de autenticação, o que equivaleria a uma "autorização tácita" do titular do dispositivo para acessos.

No que diz respeito a empresas de pesquisa e segurança da informação, a Lei tenta "imitar" os princípios da convenção de Budapeste, também punindo aquele que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da invasão. Temos que entender ou "ler", "no intuito de permitir a prática da invasão com fins ilícitos, tal como previsto no caput artigo 154-A" (A Convenção do Cibercrime de Budapeste recomenda até mesmo a punição de quem disponibiliza senhas para acesso a ativos de terceiros).

Assim, distribuições Linux como Backtrack, programas para invasão como sqlmap, havij, e frameworks como Metasploit, são amplamente utilizados por profissionais de segurança e empresas na consecução dos seu trabalhos, e não poderão ser confundidos, por autoridades, com por exemplo, códigos para coleta de dados de cartão de crédito, Keyloggers bancários desenvolvidos especificamente

para lesar correntistas, dentre outros códigos maliciosos ou para invasão que por sua natureza e diante do contexto do caso concreto, avaliada por perito digital, restar claro não se tratar de ferramentas usadas para “boas finalidades” ou “análises de segurança da informação”.

Porém repise-se. Não é a ferramenta que define a finalidade do agente, mas o próprio agente define como usar a ferramenta, para boas ou más finalidades. Infelizmente, o legislador não pensou nesta hipótese. Caberá dose extraordinária de bom-senso às autoridades e observância às conclusões da perícia em geral para constatar que não é porque alguém é encontrado distribuindo ferramentas ou códigos que permitam invasão que este alguém é um criminoso.

Para pesquisadores e profissionais que desenvolvem exploits, provas de conceito, códigos, frameworks, ferramentas de pentest, caberá a revisão das políticas de uso e distribuição dos referidos programas, fazendo menção expressa à ausência de responsabilidade do desenvolvedor diante do mau uso, consignando expressamente a finalidade lícita da criação da ferramenta.

Por fim, repise-se que a invasão, para caracterizar conduta criminosa, deve ocorrer em ativo protegido por mecanismo de segurança. Resistimos a simplicidade daqueles que entendem que basta uma senha no dispositivo para que ele esteja “protegido”, logo preenchendo os requisitos da lei. Poderemos ter a hipótese de um sistema operacional, por exemplo, Windows, com senha, mas que tem uma vulnerabilidade antiga no navegador nativo (MS11_003 por exemplo). Nestes casos a perícia deverá constatar que a despeito da senha, a máquina estava “desprotegida”, com patches desatualizados e que o titular, por sua conta e risco assim mantinha o serviço na rede em um sistema defasado. Em vários manuais de segurança da informação aprendemos que vulnerabilidade é a falha ou ausência de mecanismos de segurança. Deverá o perito também precisar se a invasão subverteu mecanismo de segurança instalado ou se não interagiu com ele, se consumando por outros meios desprotegidos. (Como por exemplo no caso do agente que coleta uma HD com Sistema operacional e senha e a monta como unidade “slave”, não rompendo mecanismo algum de segurança para acesso aos dados)

Logo, é preciso esclarecer que nem todo o dispositivo “com senha” está com efetivo “mecanismo de segurança” e, consequentemente, nem todo a invasão a dispositivo “com senha”, poderá ser considerada conduta criminosa, como muitos pensam. Cada caso é um caso. Por outro lado, a lei também veio para proteger usuários comuns, pessoas físicas, logo, não se pode engessar a aplicabilidade porque tal usuário não empreendeu o “melhor” mecanismo de segurança existente para proteger seu ativo. É preciso repetir, cada caso deverá ter suas características e circunstâncias avaliadas pelo Judiciário, não existindo solução pronta, e sendo indispensável a atividade pericial.

Seja como for, a segurança da informação, agora, passa a ser não apenas útil para impedir que o ato potencialmente criminoso ocorra, garantindo a disponibilidade, integridade e confidencialidade da informação, mas, em caso de invasão consumada, para que o

criminoso possa responder criminalmente.

Como visto, a não conformidade em segurança da informação, agora, pode representar claramente a impunidade e a responsabilidade civil em casos de invasão, pois não se pode invadir o que está “aberto” ou “desprotegido”, por nítida falha, negligência, imprudência ou imperícia dos contratados e profissionais que tinham o dever de garantir segurança do ativo de informação de alguém. Sobretudo agora, Segurança da Informação e Direito Digital, precisam caminhar juntos.

José Antônio Milagre

Vice-Presidente da Comissão Estadual de Informática da OAB/SP.
MCSO, CHFIc, SANS 508c, DSO, Profissional com mais de 12 anos de experiência área de Computação Forense e Direito da TI.
Advogado especializado em Direito da TI e Segurança da Informação.
MBA em Tecnologia da Informação.
Diretor da Consultoria Legaltech LATAM.
Perito Judicial em São Paulo em Informática e Telecom.
Palestrante de grandes eventos como Congresso de Crimes Eletrônicos FECOMERCIO, CNASI, BHACK, H2HC, WEBSECFORUM, SECURITYDAY, CPBR6, dentre outros.
E-mail: jose.milagre@legltech.com.br

Criando um Appliance Open Source para Mitigar Vulnerabilidades de Serviços e Aplicações

Alexos

A diversidade, descentralização administrativa e peculiaridades das aplicações são alguns dos fatores que dificultam a gestão das vulnerabilidades, principalmente devido ao alto custo de tempo/pessoas na manutenção, testes de correção, impacto das mudanças, sistemas órfãos, etc. Um provável cenário seria um datacenter hospedando aplicações heterogêneas (Wordpress [1], Joomla [2], Drupal [3], PHPBB [4] ou de desenvolvimento interno) com módulos de terceiros, ambientes sem administração interna e sistemas operacionais obsoletos. Cenário bastante hostil para Sysadmins que buscam seguir boas práticas de segurança como manter um ambiente atualizado por exemplo.

VULNERABILIDADES

Sistemas desatualizados são facilmente identificados na internet. Uma pesquisa por servidores com sistemas operacionais obsoletos (e.g Debian Sarge [5]) retorna milhares de serviços disponíveis.

Figura 1 - Resultado busca por Debian Sarge

A varredura de portas abaixo revela serviços com diversas vulnerabilidades, as versões do Proftpd [6], Apache [7] e PHP [8] possuem falhas que vão desde de negação de serviço à execução de código remoto.

```
Starting Nmap 6.25 ( http://nmap.org ) at 2012-12-17 22:10 Bahia Standard Time
Nmap scan report for [redacted]
Host is up (0.19s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        ProFTPD 1.2.10
80/tcp   open  http       Apache httpd 2.0.54 ((Debian GNU/Linux) PHP/5.0.5-Debi
an-0.8~sarge1)
554/tcp  open  tcpwrapped
2200/tcp open  tcpwrapped
3306/tcp open  tcpwrapped
7070/tcp open  tcpwrapped
Device type: media device|general purpose
Running (JUST GUESSING): Linux 2.6.X (86%)
```

Figura 2 – Identificando serviços vulneráveis usando varredura de portas

Falhas de aplicação também são facilmente identificadas, um exemplo é o uso de versões antigas do Wordpress ou plugins desatualizados.

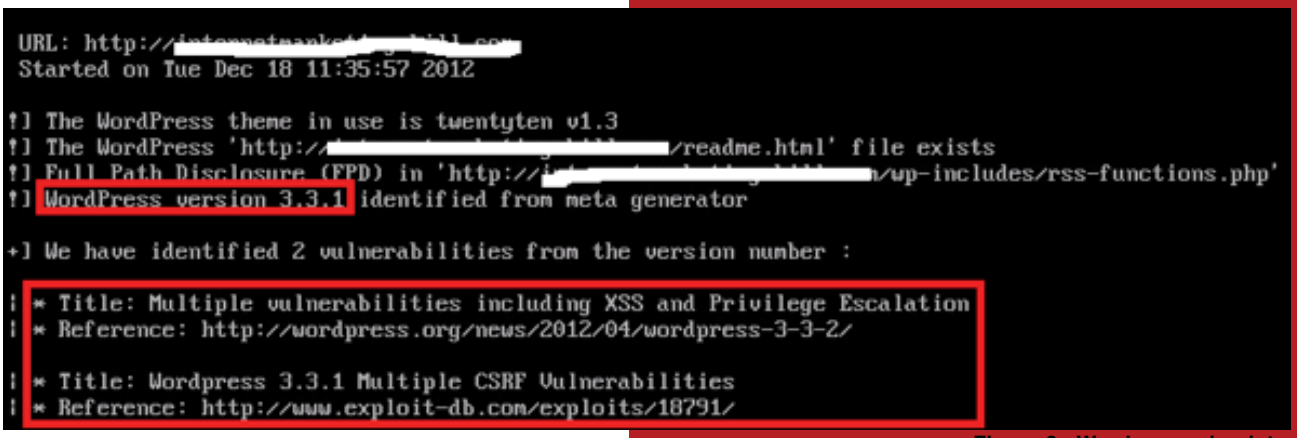


Figura 3 - Wordpress obsoleto

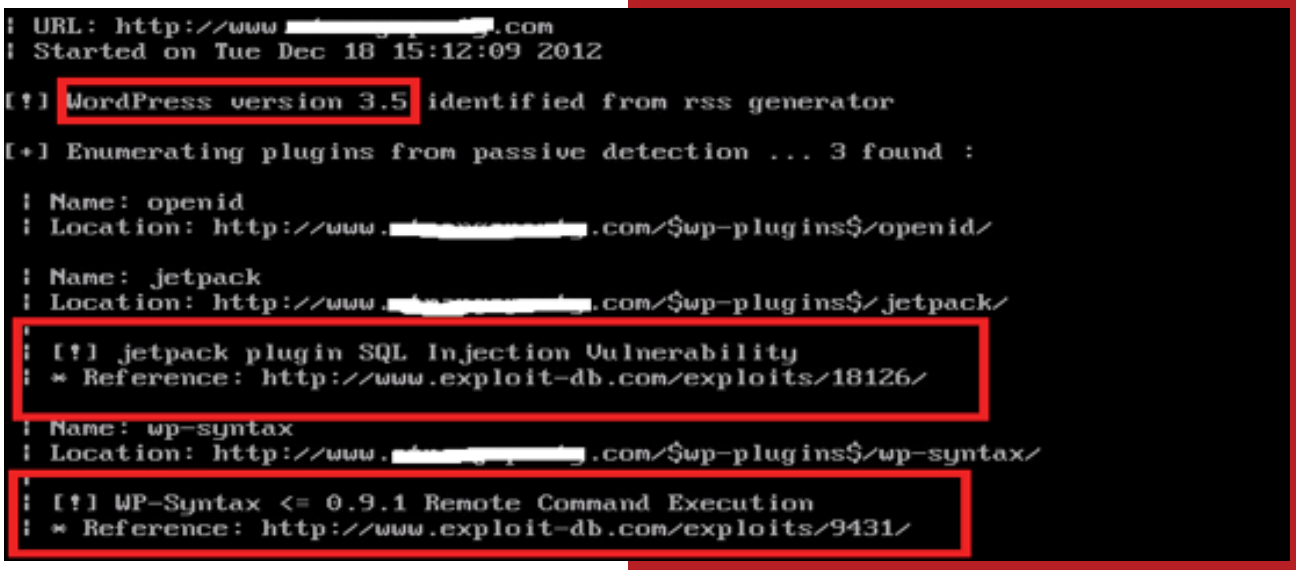


Figura 4 – Versão recente do Wordpress com plugins desatualizados

PROTEÇÃO

Baseado no conceito de Application Firewall [9] é possível criar uma camada de segurança unindo proxy reverso e ferramentas de proteção, prevenindo servidores e aplicações de diversos tipos de ataques (e.g. Vulnerability Scanning, brute force, SQL injection, XSS, etc).

O proxy reverso funciona como mediador, recebendo as requisições oriundas da Internet e redirecionando para múltiplos servidores, geralmente Web. Além disso, ele pode ser utilizado para balanceamento de carga, imap/pop3 proxy, caching e otimização de conteúdo.

As ferramentas de proteção Ossec HIDS [10] e Portsentry [11] irão analisar os logs das requisições, identificar atividades maliciosas e, quando necessário, bloqueá-las.

O Ossec Hids é por padrão capaz de identificar uma grande quantidade de ataques para vários tipos de servidores (e.g. Linux, Solaris, Windows), serviços (e.g. E-mail, Banco de dados, Web, FTP) e aplicações Web.

A arquitetura escalável e distribuída permite a integração com outras ferramentas de segurança (e.g. Firewall, SIEM, IPS) e a criação de novas regras são bastante simples.

O Portsentry integrado ao Ossec auxilia na detecção de portscans evitando a enumeração de portas e serviços.

Abaixo exemplos de identificação e bloqueio de scans de vulnerabilidades:

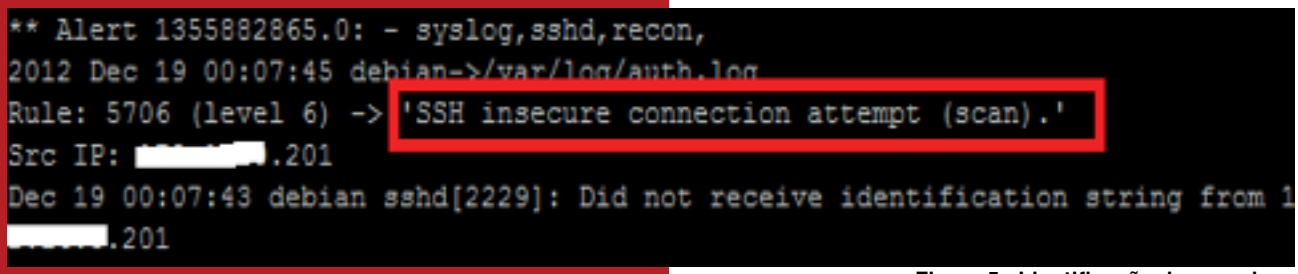


Figura 5 - Identificação de varredura

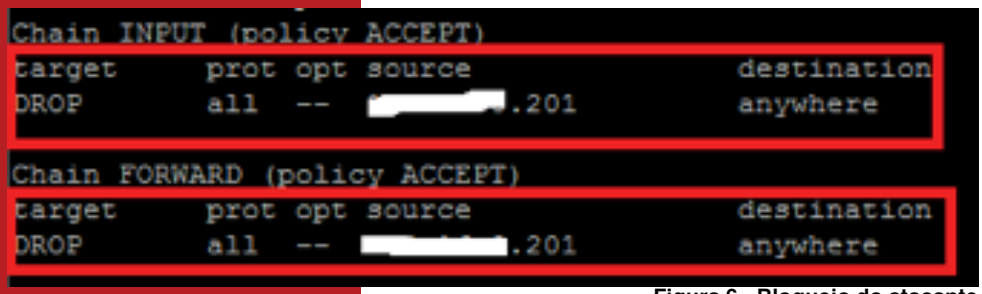


Figura 6 - Bloqueio do atacante

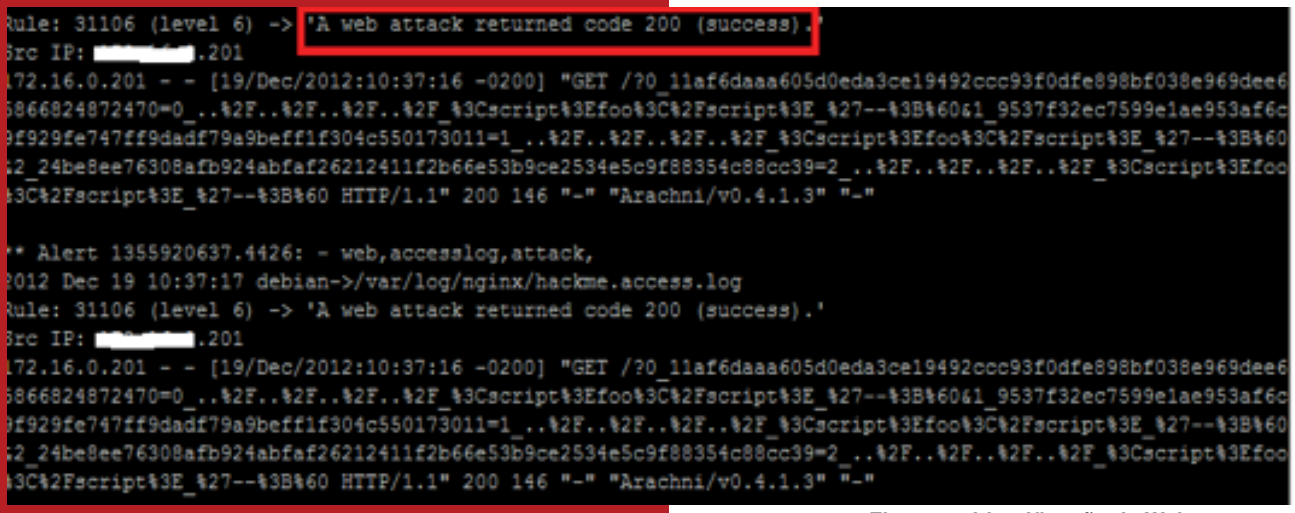


Figura 7 - Identificação de Web scanner

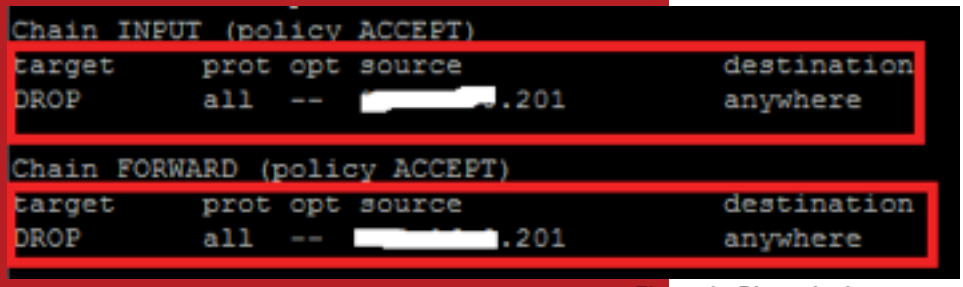


Figura 8 - Bloqueio do atacante

APPLICATION FIREWALL APPLIANCE VS WAF

A principal diferença entre esse appliance e um WAF é a integração com vários elementos dentro da infraestrutura, além de também prevenir contra ataques direcionados a serviços e sistema operacional.

Apesar de serem excelentes ferramentas os WAFs atendem prioritariamente contra ataques direcionados a aplicações Web. O ModSecurity [12] para Nginx , durante a criação deste artigo, ainda está em versão beta por exemplo.

Além dos pontos citados anteriormente, sabemos que a criação de novas regras não é muito intuitiva.

FUNCIONAMENTO

Depois de implantado o appliance passará a escutar todas as requisições, a figura abaixo demonstra a proteção de aplicações web, ftp, serviço de email e banco de dados. A instalação de agentes facilita a comunicação entre o appliance e outros ativos, mas ele também é capaz comunicar-se sem o uso de agente (agentless) com switches, firewalls e roteadores garantindo a proteção tanto do perímetro quanto em profundidade.

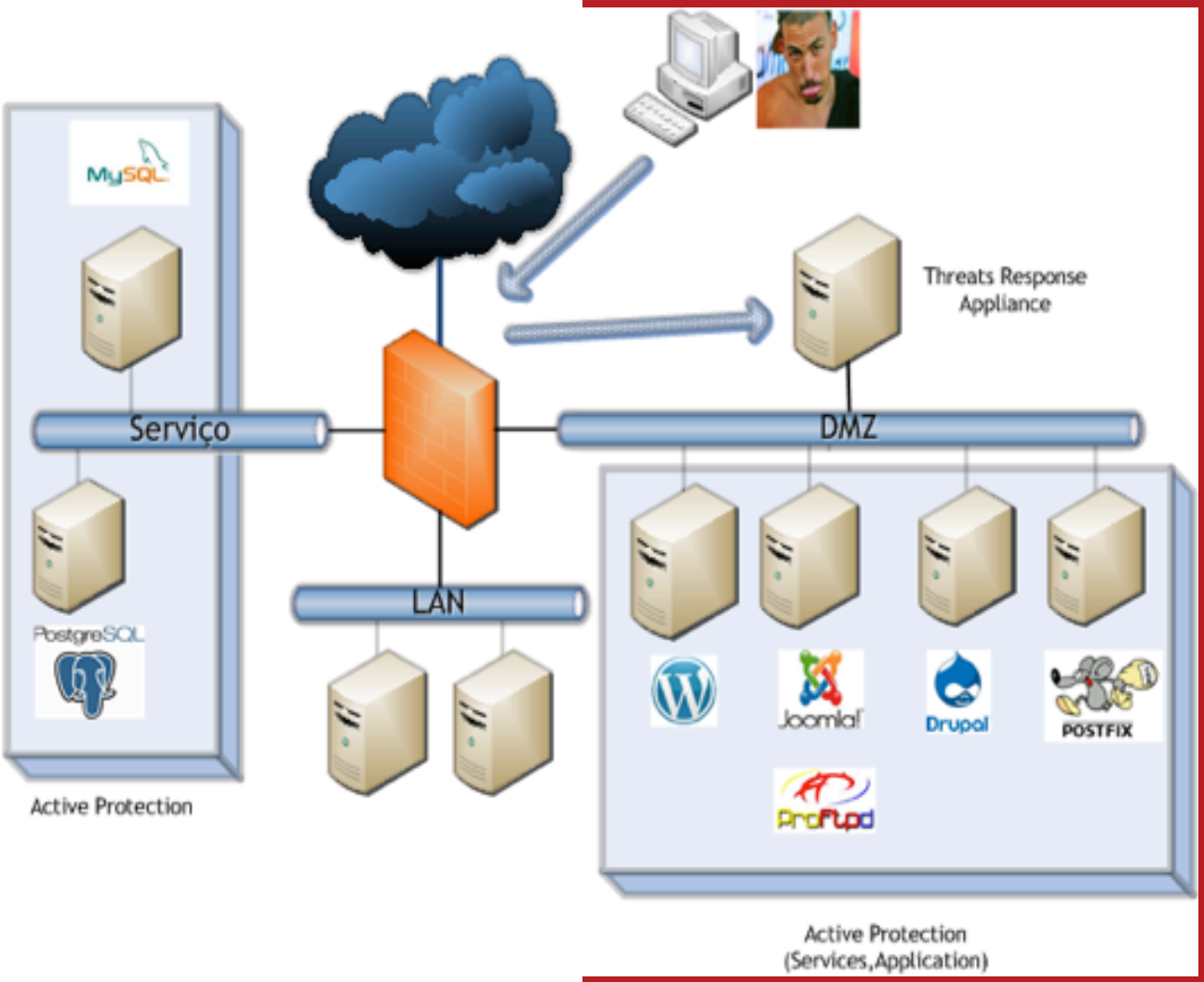


Figura 9 – Appliance protegendo diversos serviços e aplicações

COMPLEMENTOS

A capacidade de adicionar novos elementos permite ampliar proteção de diversos vetores de ataque, integração com o Snort [13] e SELinux [14] por exemplo. Alguns destes complementos podem suprir as limitações para identificar ataques direcionados ao sistema operacional como o acesso não autorizado e modificações no sistema de arquivos e kernel.

Tão importante quanto proteger é monitorar e acompanhar todos os eventos, neste caso pode-se utilizar o Analogi [15], Splunk [16] ou Elsa [17].

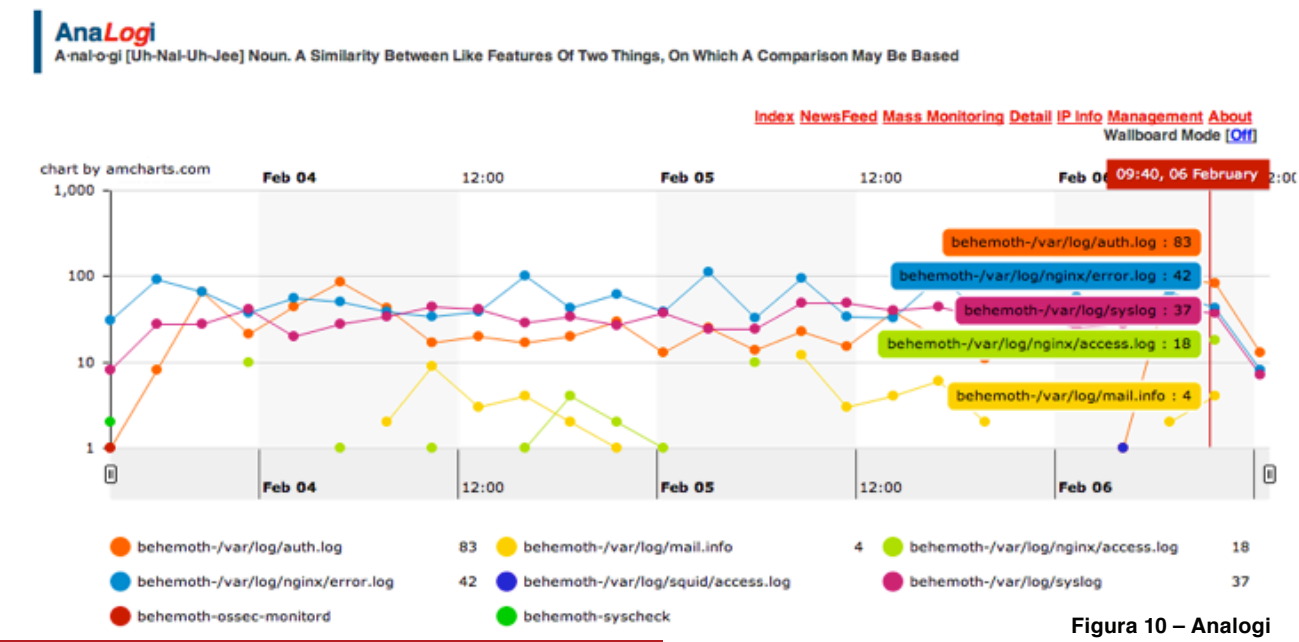


Figura 10 – Analogi

RESULTADOS

Os resultados obtidos durante a utilização do appliance em ambientes de produção foram bastante satisfatórios. Os vídeos abaixo demonstram a rapidez na identificação e bloqueio de alguns ataques usando técnicas evasivas.

Port Scanning [18]
SQL injection [19]
FTP Brute force backend [20]

CONCLUSÃO

Alguns ajustes em tempo de execução são necessários para evitar falsos positivos (e.g. aplicações enviando requisições SQL dentro do método GET).

Ele deve ser utilizado como ferramenta para mapear ameaças ajudando no processo de correção das vulnerabilidades.

As boas práticas de segurança (e.g. hardening e gestão de vulnerabilidades) devem ser seguidas, levando em conta que, qualquer solução de segurança está suscetível a técnicas evasivas durante a execução de um ataque.

Por ser baseado em blacklists e não possuir uma ferramenta gráfica de configuração exige-se um grande esforço técnico durante a implantação e tuning.

CRIANDO O NÚCLEO DO APPLIANCE

Um pequeno tutorial para a criação do appliance está disponível no link [21].

REFERÊNCIAS

[1] http://wordpress.org/
[2] http://www.joomla.org/
[3] http://drupal.org/
[4] http://phpbb.org/
[5] http://www.debian.org/releases/sarge/
[6] http://www.cvedetails.com/vulnerability-list/vendor_id-9520/product_id-16873/version_id-99601/Proftpd-Proftpd-1.2.10.html
[7] http://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-24084/Apache-Http-Server-2.0.54.html
[8] http://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/version_id-26452/PHP-PHP-5.0.5.html
[9] http://en.wikipedia.org/wiki/Application_firewall
[10] http://ossec.net
[11] http://sourceforge.net/projects/sentrytools/
[12] http://www.modsecurity.org/projects/modsecurity/nginx/index.html
[13] http://snort.org
[14] http://www.nsa.gov/research/selinux/
[15] https://github.com/ECSC/analogi
[16] http://splunk.com
[17] https://code.google.com/p/enterprise-log-search-and-archive/
[18] https://vimeo.com/67658208
[19] https://vimeo.com/67658591
[20] https://vimeo.com/67634359
[21] http://blog.alexos.com.br/nucleo-do-appliance/

Alexandro Silva é consultor na iBliss Segurança & Inteligência atuando no desenvolvimento e execução de projetos para detecção de vulnerabilidades de infraestrutura e aplicações, auditoria de segurança, criação e configuração de ambientes seguros (Hardening), também foi o responsável pelo projeto e execução da segurança da rede social Dilma na Rede, principal portal da campanha da presidente Dilma Rousseff, criado e mantido pela Colivre.

8 Vetores para Subverter Servidores Executando Citrix XenApp: da Calculadora ao Shell.

Crash

Esta é uma série de X artigos, em que irei falar sobre 8 vetores que encontrei para comprometer um servidor Citrix XenApp por meio das aplicações compartilhadas. O que é o Citrix XenApp? De acordo com a página oficial (*www.citrix.com.br/products/xenapp/overview.html*), o XenApp é um software que permite compartilhar um aplicação sob demanda ao usuário final, em qualquer dispositivo e lugar, desde que haja compatibilidade com o aplicativo cliente que viabiliza esse acesso. Esta tecnologia fornece acesso a programas de forma remota, como se estes estivessem instalados em seu equipamento, mas na realidade, estão em um ou mais servidores em locais e/ou redes diferentes.

Como funciona?

O Citrix XenApp trabalha com um conjunto de dois protocolos: o formato proprietário chamado ICA e o famoso RDP da Microsoft (Terminal Service).

No processo de execução de uma aplicação compartilhada, é criada uma instância de Terminal Service para o usuário autenticado e a aplicação é efetivamente executada nesta instancia, ou seja, qualquer interação da aplicação compartilhada irá interagir diretamente com servidor e não com máquina do usuário.

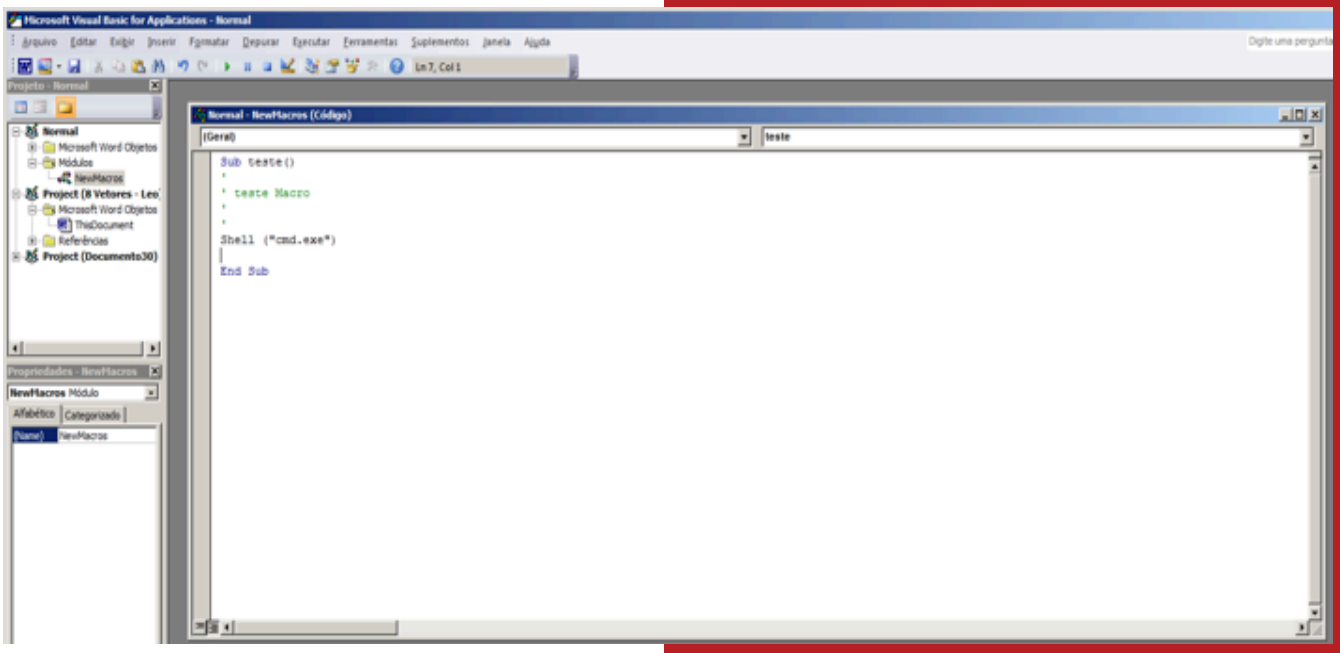
Pode-se observar essa característica claramente quando é necessário salvar ou abrir algum arquivo, na qual a estrutura de diretórios apresentada é a do servidor e não do dispositivo local.

Seguido este contexto, comecei a procurar vetores em aplicações comumente publicadas no Citrix como: Editores de texto, leitores de PDF, pacote MS Office, clientes de e-mail e navegadores. A seguir, irei relatar os 8 vetores que encontrei para comprometer o servidor Citrix XenApp.

Vetor 1: Macro do Microsoft Office

Considerando que o MS Excel é uma das aplicações que foram compartilhadas com meu usuário. Ao carregar o programa, eu criei uma macro com a seguinte linha: shell (“cmd.exe”)

Por conta da aplicação ser carregada a partir de um servidor remoto, evidentemente, foi aberto na minha máquina o prompt de comando do servidor, possibilitando executar qualquer comando diretamente no servidor, dentro do privilégio de acesso do meu usuário.



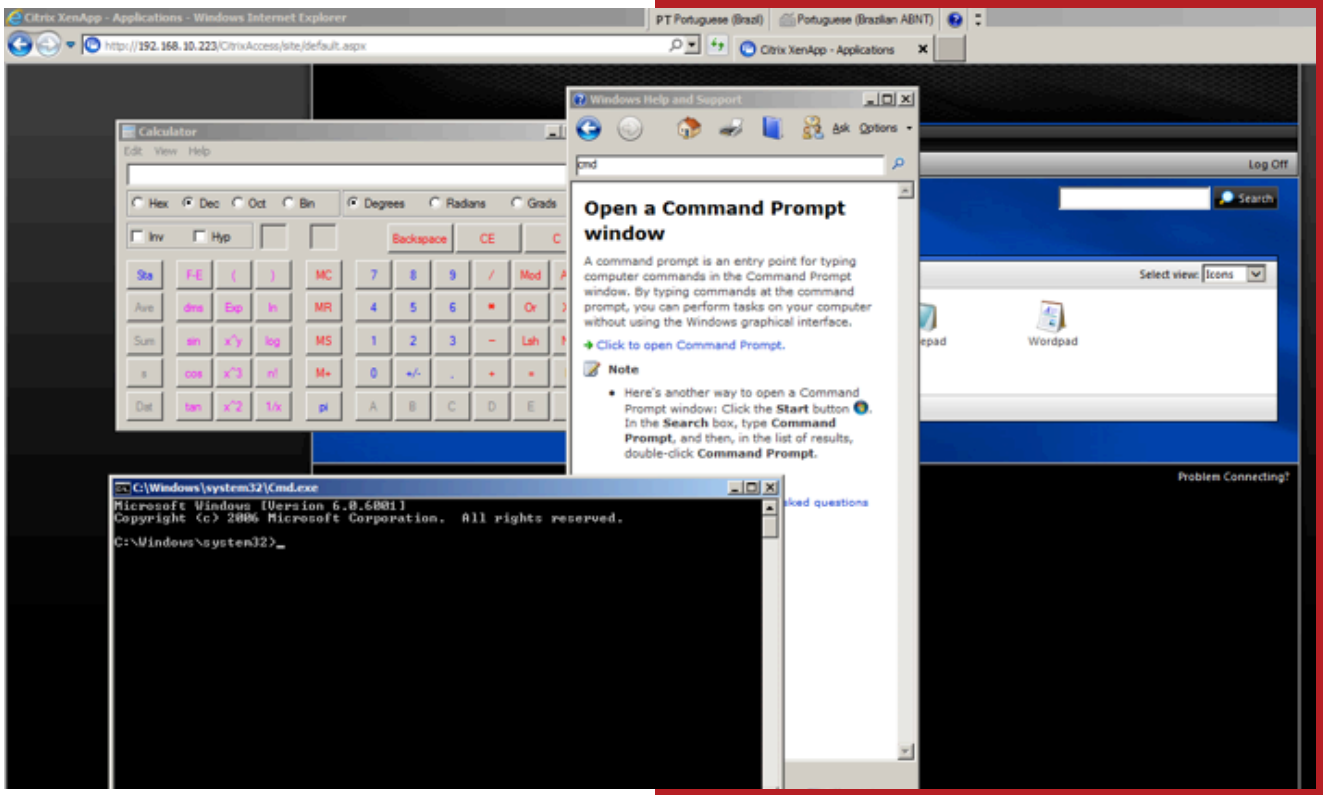
Vetor 2: Help do windows

Qual seria o perigo de uma simples calculadora publicada?

A resposta é simples:

Verificando os menus disponíveis na calculadora me deparei com o menu Help (F1), que quando é executado, claro, traz o help do servidor, que nos permite não só consultar a documentação da calculadora mas também de qualquer outro recurso do sistema operacional.

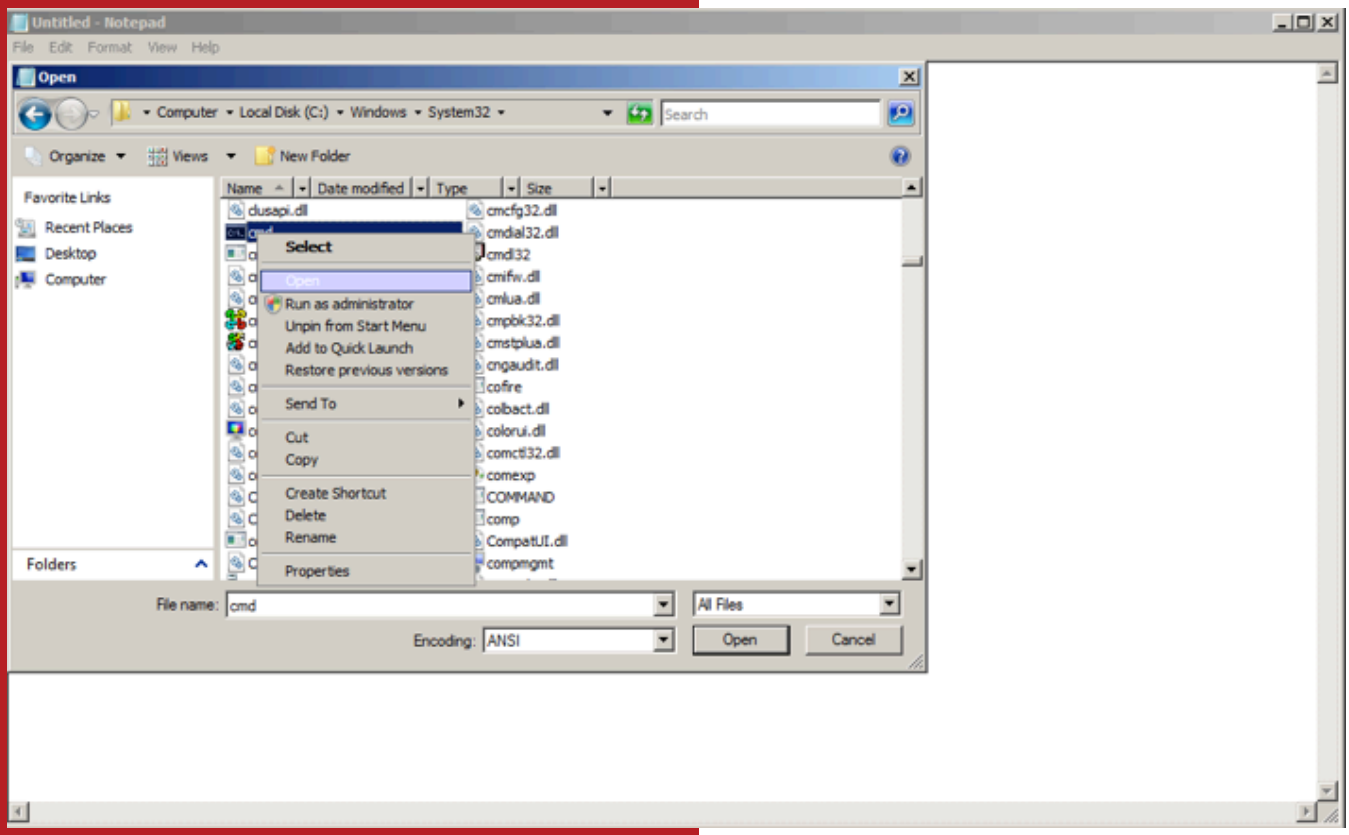
Na maioria dos casos, permite acessar recursos a partir do próprio Help. Logo, bastou uma pesquisa simples por "cmd" para conseguir um link de execução para o prompt de comando do servidor.



Isso se torna um grande problema, pois o help está disponível apenas pressionando a tecla F1, tornando-o praticamente um vetor universal, assim como a funções de abrir/ salvar arquivos.

Vetor 3: Funções de abertura e salvamento de arquivos.

A maioria esmagadora dos softwares permite interação com arquivos, seja para carrega-los no sistema, importar transferir ou salvar informações. Como vimos anteriormente todas essas funções interagem diretamente com o servidor Citrix, sendo assim, podemos usar ester recursos para mais um vetor universal. Neste exemplo foi usando o bloco de notas (notepad), o procedimento é trivial: com seu notepad virtualizado aberto clique em abrir, altere a extensão de TXT para todos os arquivos, na barra de endereços entre em c:\windows\system32, serão exibidos todos os arquivos do diretório, localize o cmd ou qualquer outro executável, clique com direto e finalmente em abrir.

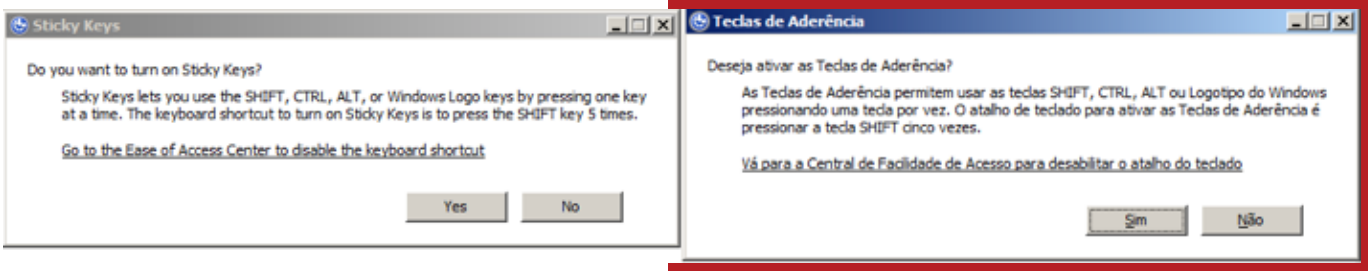


Este procedimento pode ser executado, como mencionado anteriormente, em qualquer sistema que tenham essas funções.

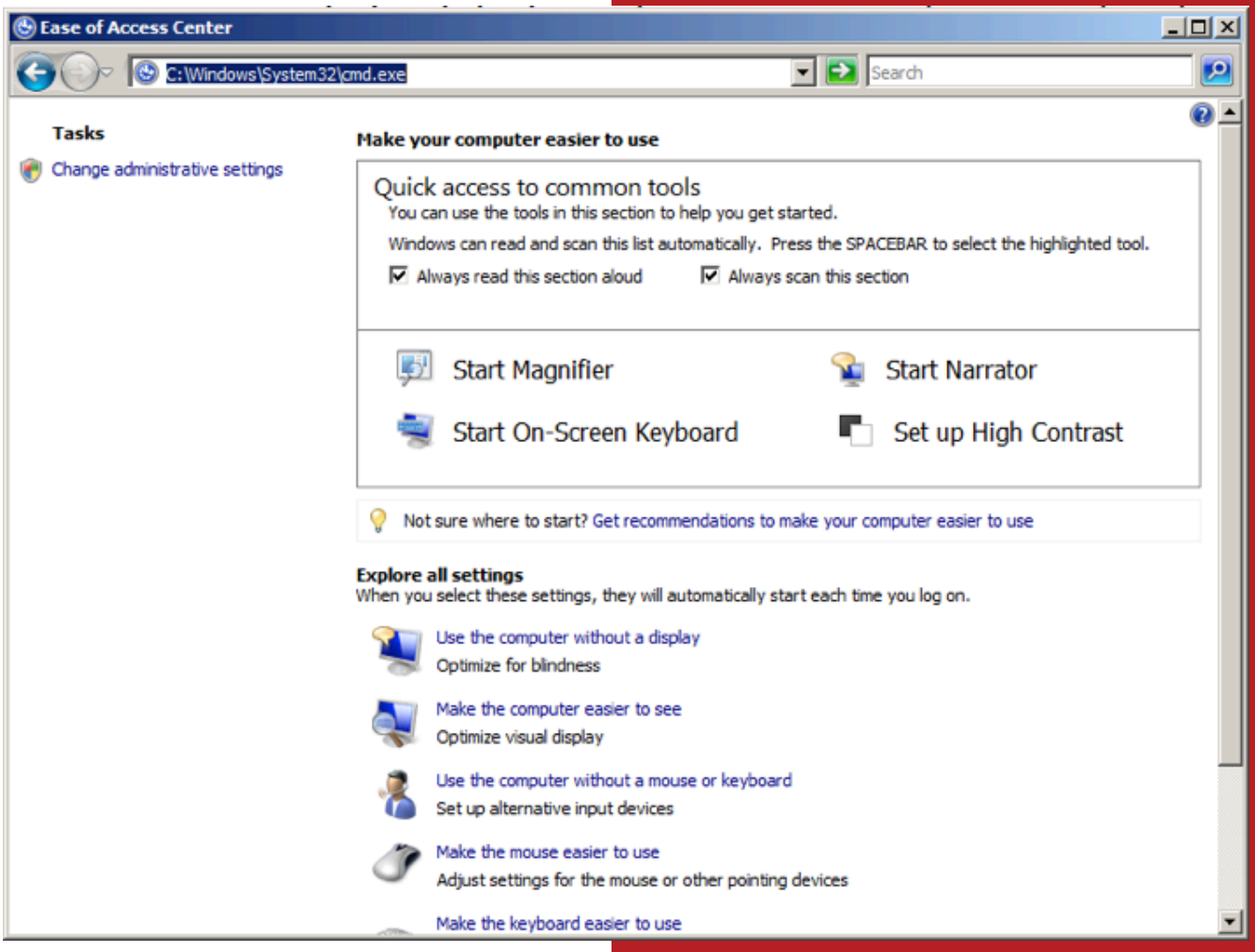
Vetor 4: Recursos de Acessibilidade

Continuando a pesquisa em torno de vetores universais, encontrei as teclas de aderência (recurso do Windows para pessoas que tem dificuldade em pressionar duas teclas ao mesmo tempo).

Como não há tratamento por parte do Citrix XenApp, ao pressionar 5 vezes a teclas shift será exibida a tela de configuração em ambos os ambientes, na estação de trabalho e servidor. Basta ignorar o alerta do computador local e clicar no link da tela do servidor, que o levará diretamente a central de configuração e permitirá a execução de qualquer binário.

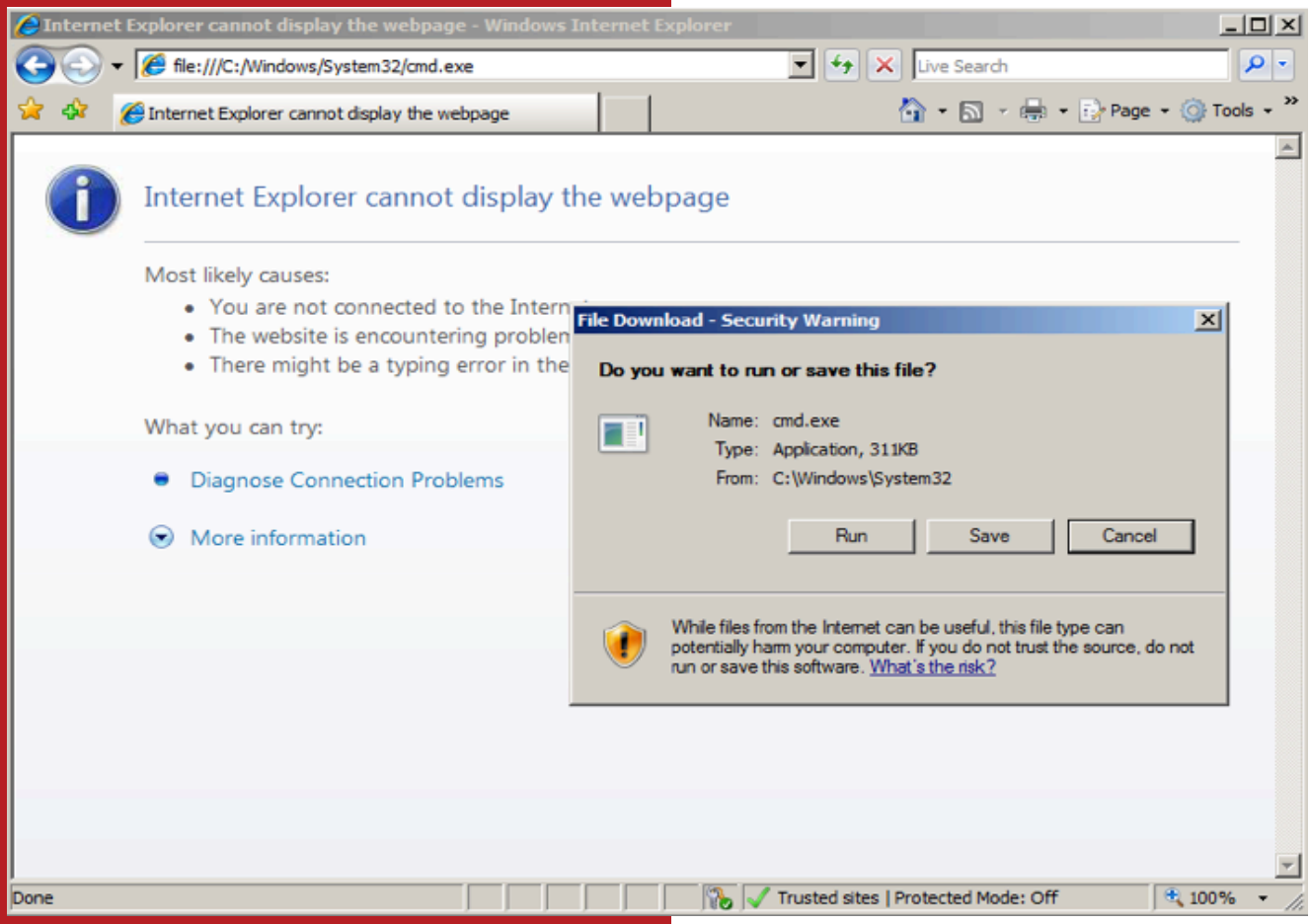


Ignoramos a mensagem local e exploramos a que veio do servidor Citrix clicando em Go to the Ease of Acess Center do disable the keyboard shortcut.



Vetor 5: Browser

Outros softwares comumente encontrados na gama de aplicações virtualizadas são os Browsers. Ester por sua vez permitem acesso ao servidor Citrix, além das funções de interação com arquivos citadas acima, podemos usar a barra de endereços para evocar um executável somente colocando seu endereço na barra ou usando o formato file:///endereço_do_binário.

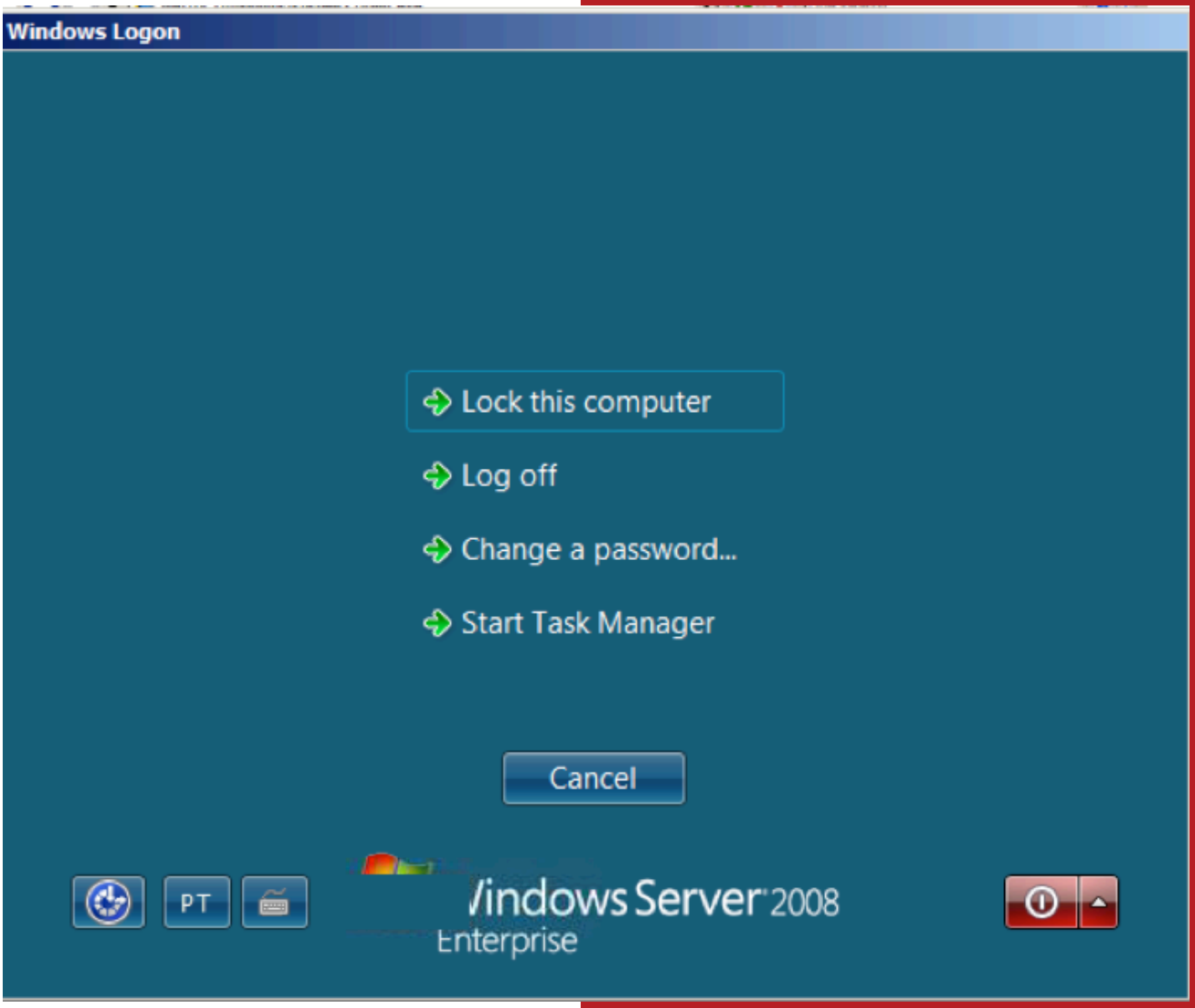


Basta clicar em Run e seu binário será executado.

Vetor 6 e 7: Citrix HotKeys

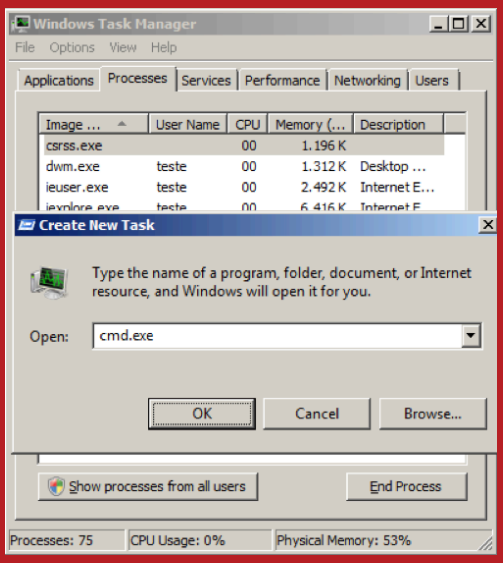
Curiosamente o XenApp disponibiliza duas HotKeys que nos permite usa-las como vetores para execução de comandos no servidor, são elas: Control + F1 e Control + F3 que nos permitem abrir gerenciador de tarefas e usar a opção Nova Tarefa (New Task).

Ao pressionar Control + F1 temos:



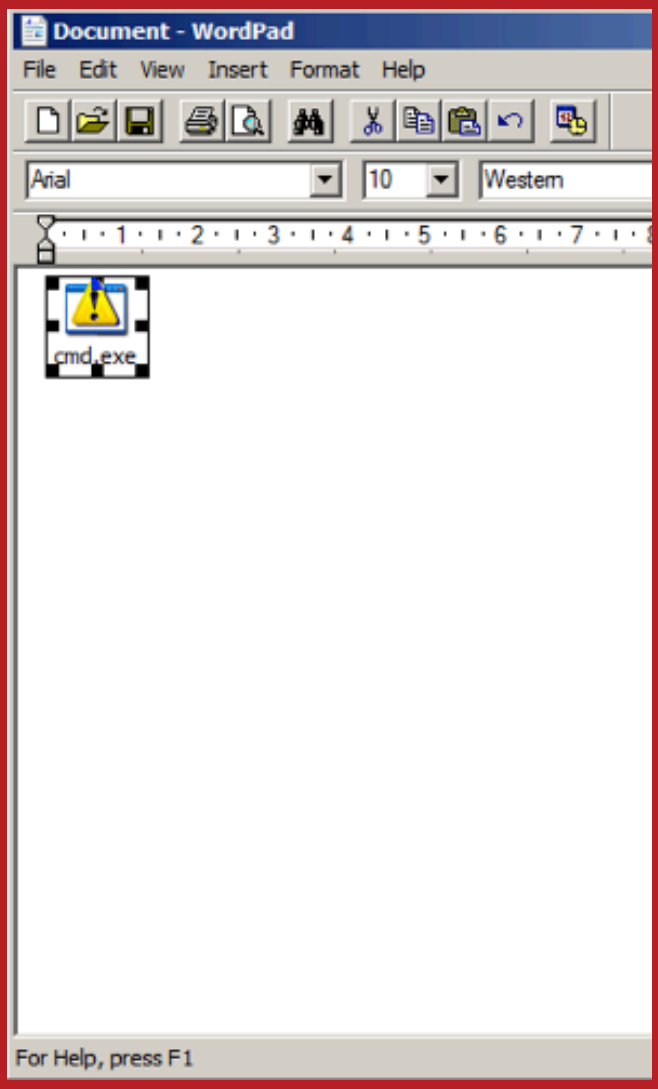
Start Task Manager assim como trocar a senha e desligar e máquina (se houver permissão para isso) é bem sugestivo não acha?

Já o Control +F3 poupa todo o seu trabalho, e abre diretamente o gerenciador de tarefas:



Vetor 8: Arquivos embutidos (Embedded files)

Por ultimo e não menos importante este vetor é sobre arquivos embutidos, que são aqueles que pode ser colocados dentro de outros arquivos. O exemplo básico para esse vetor será embutir o arquivo cmd.exe no wordpad. Há duas maneiras de ser fazer isso, usando o próprio cmd servidor Citrix ou enviando o arquivo com o binário embutido para o servidor, esta segunda forma, evidentemente você precisará de um cliente ftp, fazer download por um browser, cliente e email, ou seja, verificar quais recursos estão disponíveis para enviar/receber o arquivo craftado. Use sua imaginação!



Basta clicar no ícone do cmd.

Considerações finais

Apesar deste artigo ter sido focado na execução do cmd.exe gostaria de deixar claro que qualquer outro binário pode ser executado.

Outro ponto a ser observado é a importância de se manter um rigoroso plano de atualização do parque de servidores, ataques simples como estes poderiam comprometer a máquina como mostrado no vídeo abaixo. Como o servidor em questão não possuía os updates de segurança necessários, tornou-se um alvo fácil. O atacante conseguiu realizar uma escalação de privilégios locais, tornando-se administrador.

www.youtube.com/watch?v=2Mu0TiYOjhw

Além disso, foi possível escrever um "malware" que é ativado somente quando uma aplicação virtualizada é executada na máquina do cliente, no POC o malware grava um executável no servidor Citrix e o executa como finalização do ataque sem que haja interação do usuário final.

Ewerson Guimarães é formado em Ciência da Computação pela Universidade Fumec, Analista de Segurança na empresa Ibliss focado em pentest e pesquisa. Certificado pela Offensive Security (OSCP) como pentester, tem exploits publicados e alertas sobre vulnerabilidades de softwares de grandes empresas como Mcafee, IBM, TrendMicro, Citrix e Skype. Além disso, contribui para o desenvolvendo de módulos do projeto Metasploit Framework. Membro do grupo de pesquisa DcLabs e fundador da BHack Conference.

Tempos Modernos, Preconceitos Antigos.

Henrique Lima

Século XXI, o século da evolução humana, o século de grandes mudanças, o século do futuro. Tudo está mudando de forma acelerada - a tecnologia, os costumes, nossa rotina.

Atualmen te, estamos fadados a utilizar a tecnologia para tudo no dia a dia. Não é possível imaginar os dias atuais sem um computador, tablet ou mesmo um smartphone.

Os aparelhos eletrônicos hoje são utilizados para tudo - pesquisas científicas, exploração do universo, trabalho, locomoção, cura de doenças, entre outras coisas. No entanto, apesar de nossas vidas estarem totalmente ligadas a essa nova era e mudança de paradigmas, nós, em nossa grande maioria, ainda insistimos em ter alguns antigos preconceitos.

A palavra preconceito significa ter uma opinião ou pensamento acerca de algo ou de alguém, cujo teor é construído a partir de análises sem fundamentos, ou preconcebidas sem conhecimento e/ou até mesmo sem reflexão.

Sim, infelizmente ainda vivemos afundados em nosso preconceito, temos a conduta de julgar o que não conhecemos, seja para nos defendermos daquilo que um dia aprendemos ser prejudicial, ou para evitar uma possível decepção.

Estamos sempre julgando algo ou alguém, tomando como verdade um acontecimento, idéia ou notícia, sem ao menos analisar os fatos.

E nesses julgamentos falhos entra um conceito utilizado bastante recentemente na sociedade, com a efetivação da Lei 12.737/2012, apelidada de Lei Carolina Dieckmann, que é o uso do termo hacker. Mas, antes de falar sobre isso, vamos voltar ao nosso tempo de escola, lá no ensino fundamental. Você se lembra de quando frequentava as aulas e tinham aqueles alunos inteligentes, que se destacavam na sala de aula?

Todo mundo lembra-se deles, os "comedores de livros" que sabiam tudo, que passavam horas na biblioteca pesquisando, todos queriam fazer prova em dupla com eles, tiravam as melhores notas, as experiências nas aulas de ciências eram as melhores e por aí vai.

Este tipo de gente ainda existe, e ainda continuam afundados em bibliotecas e continuam buscando constantes conhecimentos, porém, e logicamente, em diferentes áreas. A palavra "Hacker" é a palavra que define essa categoria de pessoas, ou seja, pesquisadores natos em uma busca incessante pelo conhecimento. Todos aqueles equipamentos hospitalares super modernos, aquele trem extremamente rápido, o celular mais moderno com vários recursos, o computador mais fino, e mais aquela infinidade de aparelhos tecnológicos. Aquilo tudo não foi construído sozinho, o sistema operacional do seu computador não foi feito por robôs, aquela televisão 3D finíssima não foi feita por alienígenas.

Alguém precisou criar uma tecnologia para ela funcionar. E a sua facilidade ao usar o banco pela internet? Alguém precisou e precisa programar isso, não é? E também alguém precisa manter isso seguro. E sabe quem esta por trás de todas essas coisas que facilitam sua vida? Nós, os hackers.

Então, o seu pai ou alguém dos anos 80 lê esse texto aqui e fala: "Não, o hacker é o cara que invadiu o computador da fulana, que roubou a conta da beltrana, que invadiu e detonou todo o sistema" e todo esse papo sensacionalista que a mídia divulga. Mas não, não é isso, já que estamos lidando com conceitos mal formados, então vamos usar um pouco de ficção pra desenhar a realidade.

Sabe os gênios do mal de filmes que vocês assistem na sessão da tarde ou nos desenhos modernos? Pois é, eles também existem e a definição correta pra eles é Cracker e não Hacker. A principal diferença entre os dois tipos, e a mais importante de todas, é que o Cracker utiliza o conhecimento adquirido de forma ilícita, visando sempre o ganho próprio e/ou o prejuízo alheio e são frequentemente caracterizados como estelionatários, vândalos e "pichadores digitais".

A partir do que foi exposto acima, entendemos que o hacker é um pesquisador nato e, como todo pesquisador, ele precisa de um

espaço de estudos. Com isso, viu-se a necessidade de se criar espaços comunitários onde esse nicho de pessoas pudessem se encontrar em um local onde tivesse disponível uma infraestrutura adequada para desenvolvimento de pesquisas e que também pudessem servir de catalisador da difusão do conhecimento.

Assim, foram criados os Hackerspaces (ou Hacker Clubes), que nada mais são do que centros de convivência, locais onde buscadores de conhecimento se reúnem para aprender, com palestras, oficinas, entre outras atividades.

São ambientes abertos a todos que tenham interesse em aprender, desde coisas corriqueiras e básicas como realização de reparos simples em equipamentos eletrônicos ou introdução a programação Web, até participar de discussões complexas sobre programação, desenvolvimento de robôs, automação residencial, entre outra infinidade de assuntos.

No Brasil, nos últimos anos, foram criados vários destes espaços comunitários, entre eles o SJC Hacker Clube, em São José dos Campos, interior de São Paulo. Na cidade de São Paulo, o Garoa Hacker Clube, além do LHC, em Campinas, Kernel 40º, no Rio de Janeiro, entre outros.

Infelizmente, o hacker foi estigmatizado pela sociedade como sendo uma pessoa do mal, que comete crimes e prejudica pessoas, quando na verdade, como vimos acima, é exatamente o contrário. Temos a ética e a lei como valores, buscamos o conhecimento e o transmitimos, pois sentimos prazer em ajudar os outros.

E você, que depois de ler este artigo, ainda não se convenceu disso, visite qualquer um destes e tenho certeza que você se surpreenderá com o que pode aprender e repassar de conhecimento, e consequentemente reverá seus conceitos sobre nós.

Fica a dica!

Henrique de Oliveira Lima

Formando em Análise e Desenvovimento de Sistemas na ETEP

Sócio-fundador do SJC Hacker Clube.

Atual: Tier 2 Service Desk Analyst na Pilkington Brasil

Análise do Processo de Intrusão do Protocolo WEP

Jonas Barros

O processo de intrusão em redes Wi-Fi configuradas com o protocolo WEP utiliza-se de ataques do tipo Fluhrer, Mantin and Shamir (FMS). Segundo a documentação do aircrack-ng, ataques FMS baseiam-se na ideia de que o atacante recebe passivamente as mensagens enviadas por alguma rede, salvando esses pacotes criptografados com os vetores de inicialização usados por eles. Isso porque os primeiros bytes do corpo da maioria dos pacotes são facilmente previsíveis e o atacante pode conseguir usando alguma pouca matemática e analisando uma grande quantidade de pacotes, descobrir a senha de criptografia da rede.

Laboratório

O cenário proposto para o laboratório da análise foi composto por:

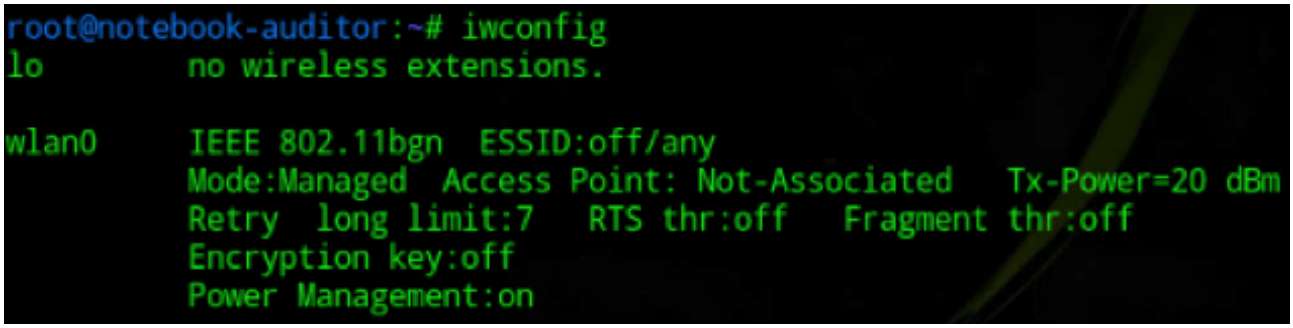
- 1 (um) notebook com Backtrack 5 R3 (notebook-auditor);
- 1 (um) roteador Wi-Fi Multilaser (Access Point - AP);
- 4 (quatro) dispositivos Wi-Fi (2 notebooks e 2 smartphones);
- 1 (um) computador desktop.

No AP foi configurado o protocolo de WEP e os 4 dispositivos Wi-Fi mais o computador desktop conectavam-se por meio deste, gerando tráfego de modo natural.

O notebook-auditor estava no alcance do sinal emitido pelo AP e foi simulado um ataque FMS (Fluhrer, Mantin, Shamir) para obter-se o acesso à rede.

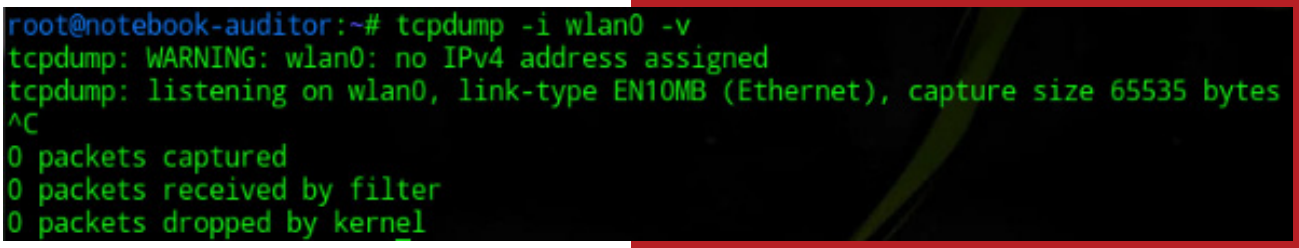
Placa de Rede em Modo Promíscuo

Um conceito que deve estar claro desde o inicio é o de interface de rede em modo promíscuo. Os seguintes passos demonstram a diferença entre uma interface de rede em modo padrão e uma interface de rede em modo promíscuo. Com o resultado do comando iwconfig, é possível identificar na figura abaixo uma interface Wi-Fi instalada ao sistema, sendo esta a wlan0.



Ela está em modo padrão, ou seja, só recebe pacotes destinados a ela além de precisar estar associada a um AP.

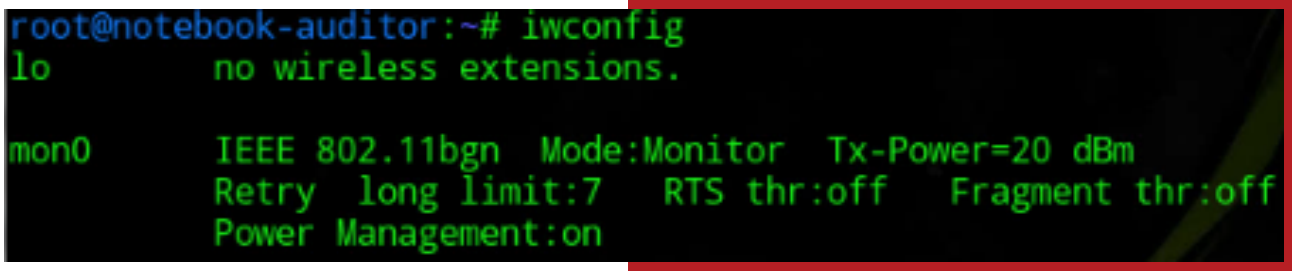
Com o comando tcpdump será possível visualizar todos os pacotes que trafegam pela wlan0. Conforme a figura abaixo, nenhum pacote é encontrado já que a wlan0 não está associada a nenhum AP.



-i : Define a interface.
-v: Modo verboso.

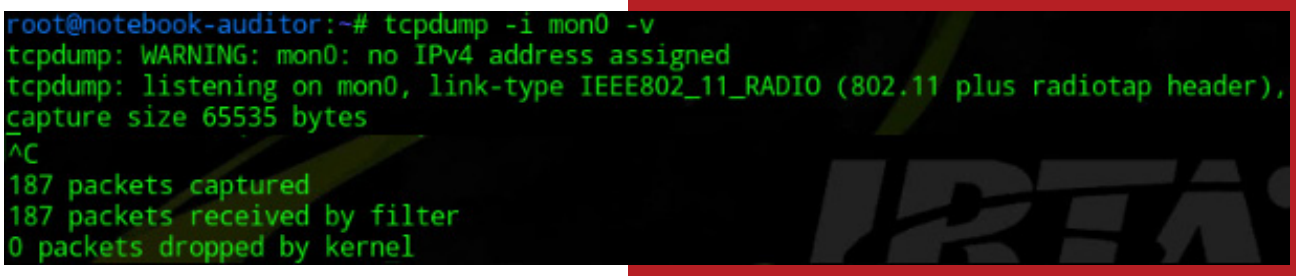
Já uma interface de rede em modo promíscuo, é capaz de capturar qualquer pacote ao seu alcance, mesmo sem estar associada a um AP. Com o comando airmon-ng ativa-se a interface de rede em modo promíscuo.

Conforme a figura abaixo, a interface mon0 foi ativada, outro detalhe é o campo “MODE: MONITOR”, ele indica que está interface está em modo de monitoramento, ou como antes dito, modo promíscuo.



O próximo comando tcpdump capturará os pacotes que estão trafegando pela interface mon0, mostrando a diferença entre o modo padrão (wlan0) e o modo promíscuo (mon0).

Conforme a figura abaixo, em poucos segundos quase 200 pacotes são capturados. Partindo deste princípio, apenas a interface mon0 será utilizada na intrusão, já que notebook-auditor não estará associado a um AP.



-i : Define a interface.
-v: Modo verboso.

O próximo comando tcpdump será responsável por coletar todos os pacotes durante o processo de intrusão e posteriormente uma análise mais detalhada será realizada partir dessa coleta. Outro detalhe é que conforme a figura abaixo todos os pacotes coletados

serão armazenados em um arquivo chamado lab.wep.analise.arp.

```
root@notebook-auditor:~# tcpdump -i mon0 -w lab.wep.analise.arp
tcpdump: WARNING: mon0: no IPv4 address assigned
tcpdump: listening on mon0, link-type IEEE802_11_RADIO (802.11 plus radiotap header),
capture size 65535 bytes
```

-i : Define a interface.
-w: Define o arquivo de saída.

Identificação da Rede Wi-Fi

Nesse segundo momento outro terminal é aberto e inicia-se o processo de intrusão. Primeiramente é necessária a identificação da rede. Com o comando airodump-ng, é possível visualizar todas as redes Wi-Fi ao alcance do notebook-auditor.

Conforme a figura abaixo, a rede usada para a intrusão será a lab-wep.

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
D8:5D:4C:FA:9A:98  -73        4        2    0   7  54e. WEP  WEP         lab-wep
```

Coleta de Vetores de Inicialização

Com a rede já identificada, inicia-se a coleta de vetores de inicialização, em um novo terminal utiliza-se novamente o comando airodump-ng, porem desta vez com a função especifica de coletar os vetores de inicialização unicamente da rede lab-wep. Outro detalhe é que conforme a figura abaixo todos os vetores de inicialização serão armazenados em um arquivo chamado lab.wep.analise.iv.

```
root@notebook-auditor:~# airodump-ng --ivs --bssid D8:5D:4C:FA:9A:98 --channel 7 --wri
te lab.wep.analise.iv mon0
```

--ivs: Salva somente os vetores de inicialização.
--bssid: Endereço MAC do AP.
--chanel: Número do canal configurado no AP.
--write: Define o arquivo de saída.

Injeção de Pacotes ARP

Enquanto a coleta ocorre em segundo plano, inicia-se o processo de injeção de pacotes ARP a fim de acelerar o processo da coleta de vetores de inicialização.

Para injetar pacotes é preciso antes estar associado ao AP, caso contrário, o AP simplesmente rejeitaria os pacotes. A partir do comando aireplay-ng é solicitado uma falsa associação ao AP, como mostra a figura abaixo, O notebook-auditor se passa por um cliente já associada ao AP para conseguir a associação.

```
root@notebook-auditor:~# aireplay-ng -1 0 -a D8:5D:4C:FA:9A:98 -h EC:55:F9:2E:3C:18 mo
n0
The interface MAC (00:87:11:02:C6:1C) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether EC:55:F9:2E:3C:18
03:46:10  Waiting for beacon frame (BSSID: D8:5D:4C:FA:9A:98) on channel 7

03:46:10  Sending Authentication Request (Open System) [ACK]

03:46:12  Sending Authentication Request (Open System) [ACK]
03:46:12  Authentication successful
03:46:12  Sending Association Request [ACK]
03:46:12  Association successful :-) (AID: 1)
```

-1: Falsa autenticação.
0: Período entre as tentativas.
-a: Endereço IP do AP.
-h: Endereço IP do cliente.

Conforme a figura abaixo, após o processo de falsa associação, utiliza-se novamente o comando aireplay-ng para ouvir pacotes ARP que trafegam pela rede Wi-Fi.

```
root@notebook-auditor:~# aireplay-ng -3 -b D8:5D:4C:FA:9A:98 -h EC:55:F9:2E:3C:18 mon0

The interface MAC (00:87:11:02:C6:1C) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether EC:55:F9:2E:3C:18
03:46:32  Waiting for beacon frame (BSSID: D8:5D:4C:FA:9A:98) on channel 7
Saving ARP requests in replay_arp-1020-034632.cap
You should also start airodump-ng to capture replies.
Read 4550 packets (got 937 ARP requests and 1023 ACKs), sent 1212 packets...(499 pps)
```

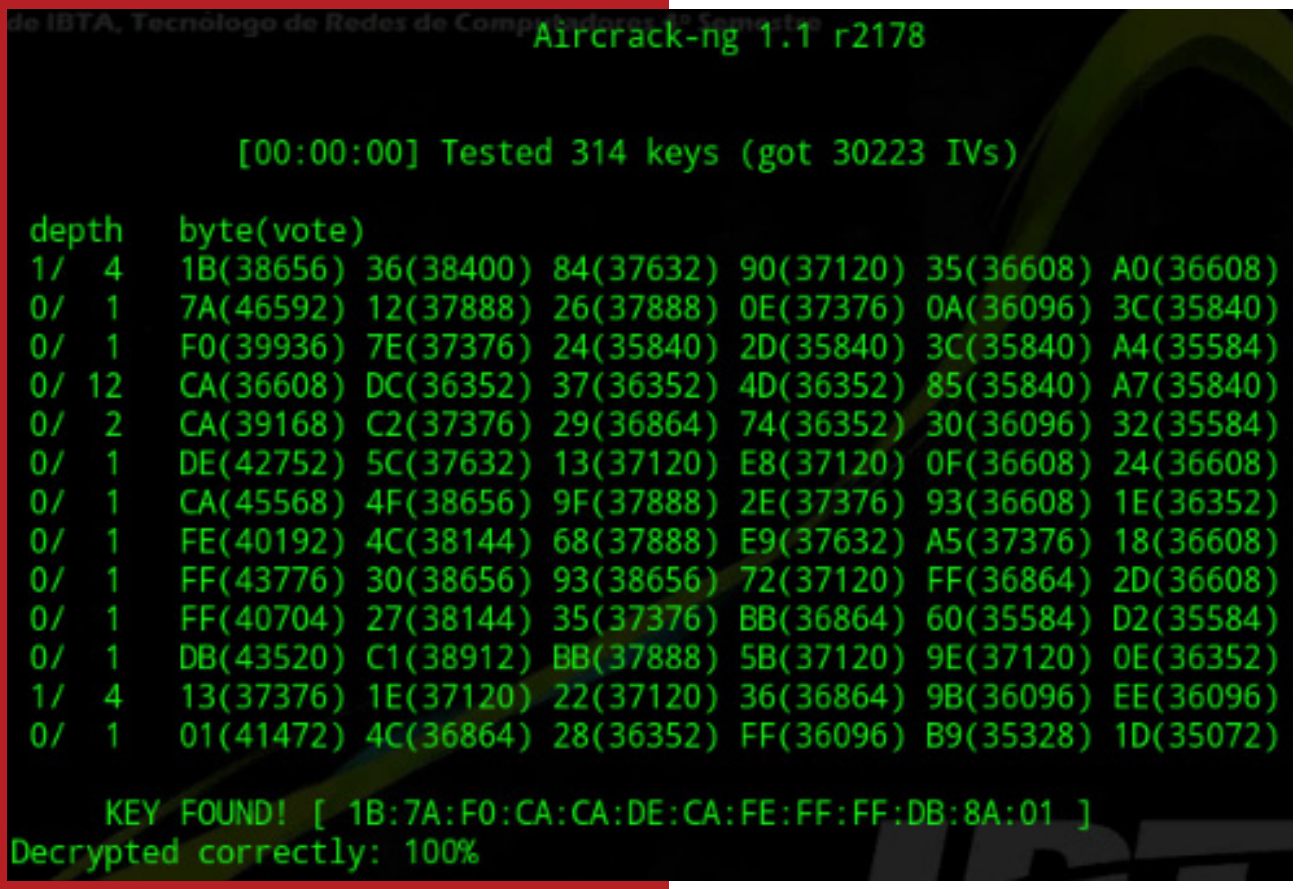
-3: Injeção de pacotes ARP.
-b: Endereço IP do AP.
-h: Endereço IP do cliente.

Assim que um pacote ARP é encontrado, o aireplay-ng responde instantaneamente com um broadcast ARP (ARP request replay). Este broadcast por sua vez é respondido pelo AP e consecutivamente respondido por outro broadcast ARP, gerando assim um laço repetitivo entre o aireplay-ng e o AP. Como antes dito, esta técnica tem como único objetivo criar novos vetores de inicialização para a coleta.

Quebra da Criptografia WEP

Enquanto a injeção de pacote ocorre em segundo plano, um novo terminal realiza a tentativa de quebra da criptografia WEP.

Ao se completar em média 4000 pacotes beacons capturados, o comando aircrack-ng executa um algoritmo estatístico baseado na coleta do arquivo lab.wep.analise.iv. Conforme a figura abaixo, a senha é encontrada em poucos segundos.



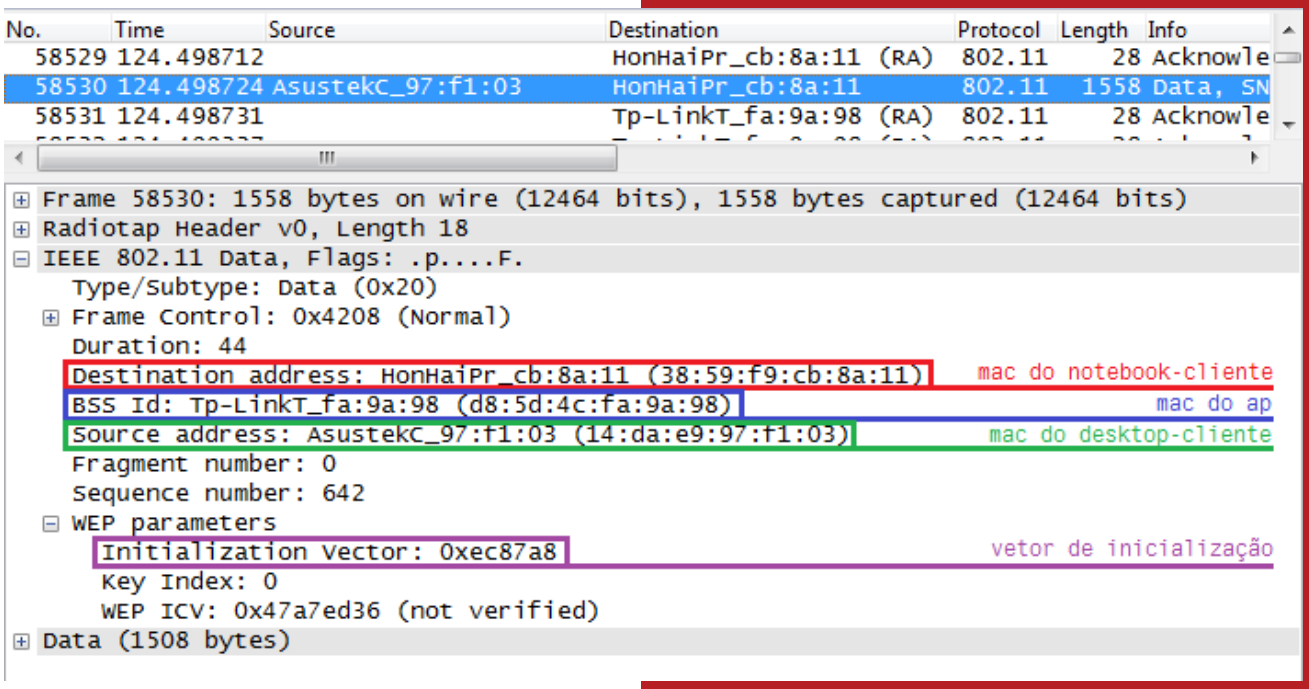
Command: ~# aircrack-ng -1 lab.wep.analise.iv-01.ivs

Resultados das Coletas

Após a intrusão foi extraído do notebook-auditor o arquivo lab.wep.analise.arp para análise. O mesmo continha em média 400.000 pacotes capturados. A partir da ferramenta Wireshark puderam ser identificados neste arquivo os pacotes que trafegavam entre os clientes do AP, os pacotes ARP injetados pelo aireplay-ng e os pacotes beacons.

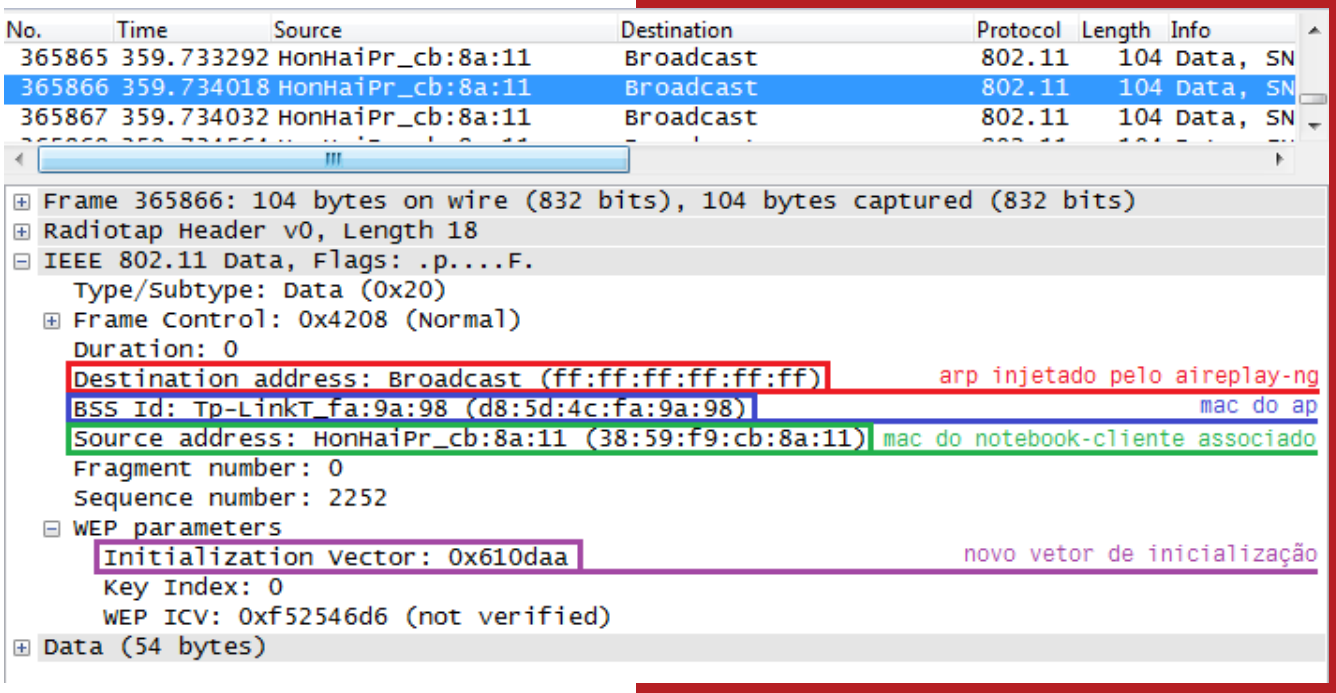
Pacotes Transmitidos Entre os Clientes

A figura abaixo representa uma troca de informação entre os clientes do AP. Outro detalhe é o vetor de inicialização, que foi capturado pelo airodump-ng antes da injeção de pacotes.



Pacotes ARP Injetados Pelo aireplay-ng

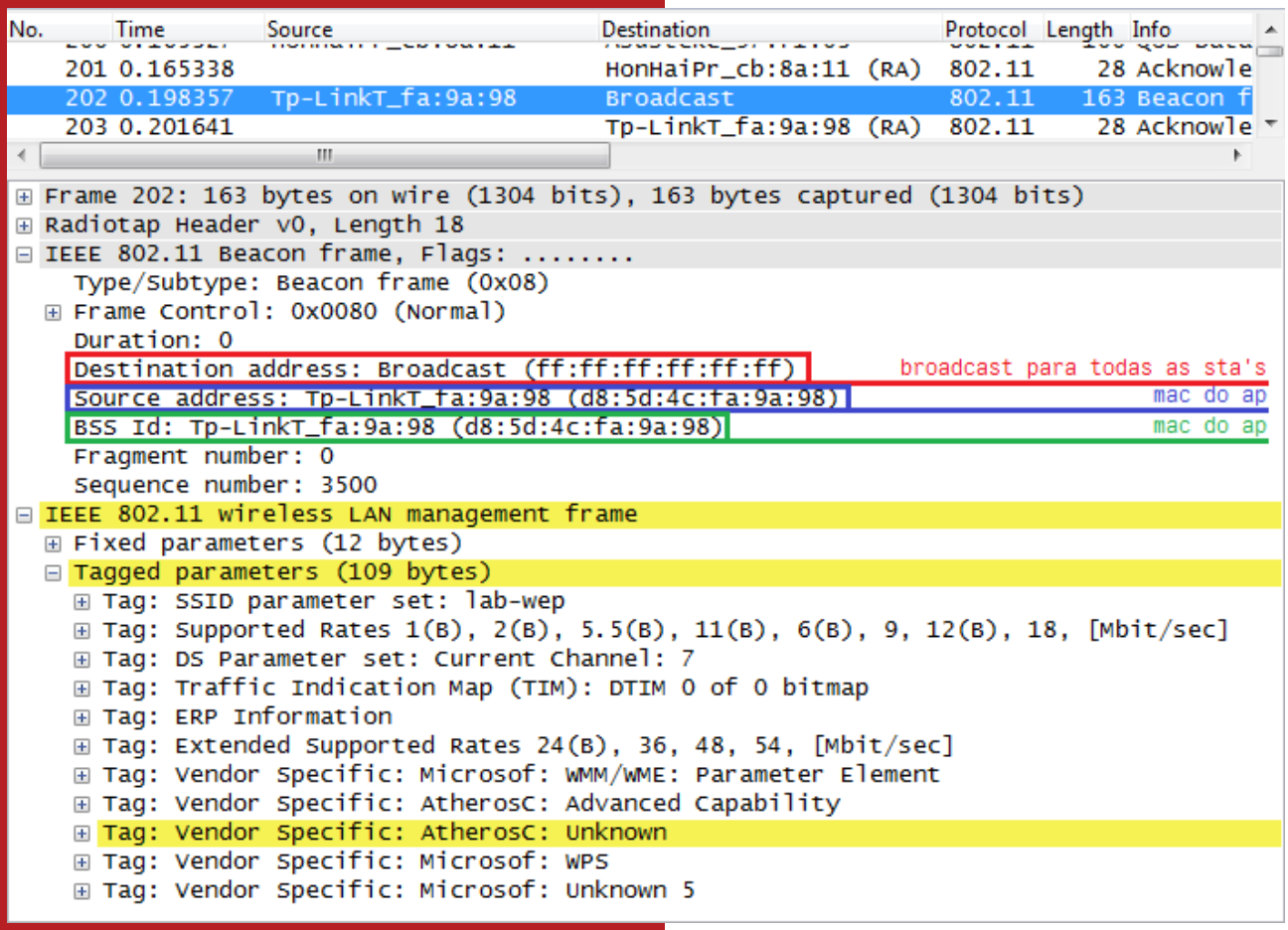
A figura abaixo representa um broadcast ARP enviado pelo aireplay-ng. Outro detalhe é o vetor de inicialização, que foi injetado pelo aireplay-ng e capturado pelo airodump-ng.



Pacotes Beacons

A figura abaixo representa um pacote beacon, ou seja, um pacote enviado do AP para todos os clientes com a função de dizer que o AP ainda está persistente, além de sincronizar informações como SSID, velocidades de transmissão suportadas, canais, dentre outras.

Outro detalhe é que este tipo de pacote não contém vetor de inicialização.



Considerações Finais

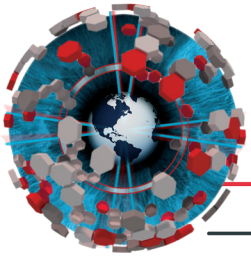
Após esse post pode-se concluir que apesar de existirem vários “tutoriais” de intrusão a redes Wi-Fi espalhados pela internet, estas técnicas vão muito além do que apenas se digitar comandos sequenciais em um terminal.

Na intrusão do protocolo WEP, por exemplo, são somadas duas técnicas para aumentar exponencialmente a eficácia na intrusão. Enquanto o método FMS captura os pacotes passivamente, o processo de injeção de pacotes ARP é realizado a fim de gerar mais vetores de inicialização para coleta. Neste processo aparentemente simples, deve ser levado em consideração alguns porquês, como exemplo, “por que usar apenas o protocolo ARP, e não todos os protocolos?”, isso se dá ao fato de o AP responder um pacote ARP com outro ARP e isso não acontece com outros protocolos. Ou seja, pode-se dizer que estas técnicas na verdade são soluções complexas, produzidas por “n” componentes.

Jonas Barros

Analista com mais de três anos de experiência em administração de redes e provisionamento de serviços. Atualmente responsável pela rede de dados e telefonia da Visiontec da Amazônia (empresa de médio porte, situada em Jacareí/SP), atua como projetista e mantenedor de soluções para a área de infraestrutura da tecnologia da informação.

BHACK CONFERENCE 2013



H2HC

HACKERS TO HACKERS CONFERENCE

H2HC MAGAZINE

Edição 04

Julho 2013

Direção Geral/ Editores:
Rodrigo Rubira Branco
Filipe Balestra

Diretora de Criação:
Amanda Vieira

Coordenadora Administrativa/ Mídias Sociais:
Laila Duelle

Captação de Artigos/ Redação:
Jordan M. Bonagura

Agradecimentos:

Jota Mossadihj

José Antônio Milagre

Alexandre Silva (Alexos)

Ewerson Guimarães (Crash)

Henrique Lima

Jonas Barros