Ataque de navegador da Web usando BeEF Framework

Apresentação · Janeiro 2018

CITAÇÕES
2

LER
21.008

1 autor:

Samuel Agaga
Universidade Tecnológica de Ontário
4 PUBLICAÇÕES 3 CITAÇÕES

VER PERFIL

Ataque de navegador da Web usando BeEF Framework

Harshil Sawant, Samuel Agaga

***Resumo*— O Web Browser é uma ferramenta que nos conecta à Internet. Nesta época, a Internet tornou-se um fator dependente para a maioria de nós. Portanto, é muito importante entendermos o que é um navegador da Web, a arquitetura e as ameaças que surgem ao usá-lo. Este artigo ilustra o lado teórico do que é um navegador da web, quais são seus componentes, como um navegador pode ser um risco e como proteger o usuário. Além disso, o artigo ilustra um laboratório que demonstra como explorar um ataque de navegador da Web usando o BeEF.**

I. INTRODUÇÃO

O navegador EB pode ser definido de várias maneiras. um comum
A definição de navegador da Web é que é um aplicativo de software que permite aos usuários visualizar e interagir com o conteúdo disponível de várias formas em uma página da Web, como texto, imagem, música, vídeo, jogos, etc. É o método mais popular para os usuários acessarem a Internet. Existem muitos exemplos de navegadores da web. Os cinco navegadores mais populares são Mozilla Firefox, Google Chrome, Internet Explorer, Safari e Opera. Além disso, add-ons estão disponíveis como aplicativos para estender a funcionalidade de tais navegadores. Alguns exemplos de add-ons incluem Flash Player, Java, Adobe Reader, QuickTime Player, etc. Dependendo de como os desenvolvedores projetaram a página da web, add-ons específicos são necessários para visualizar conteúdo específico. [1]

II. NAVEGADOR DA WEB EM PROFUNDIDADE

A principal função de um navegador da Web é apresentar os recursos da Web solicitados pelo usuário. O navegador solicita os recursos do servidor e os exibe na janela do navegador.
O recurso solicitado geralmente é um documento HTML, mas pode ser uma imagem, PDF ou qualquer outra forma de conteúdo. O usuário usa URL (Uniform Resource Identifier) para especificar a localização do recurso. Além disso, a especificação HTML e CSS define a maneira como um navegador interpretará e exibirá os arquivos HTML. Tais especificações são mantidas pela organização W3C (World Wide Web Consortium). W3C é uma organização padrão para a web. No passado, muitos navegadores seguiam uma parte das especificações e desenvolviam suas próprias extensões específicas para o navegador. Isso causava problemas de compatibilidade para autores da web. Agora, a maioria dos navegadores existentes segue as especificações comuns. [2]

III. SEMELHANÇA ENTRE NAVEGADORES DA WEB

Hoje, um usuário pode escolher entre vários tipos de navegadores. Cada um tem poucos elementos que são distintos um do outro.

Há, no entanto, um ponto em comum entre os navegadores que são os elementos da interface do usuário (IU). Os elementos da interface do usuário incluem barra de endereço para inserir um URL, botões de voltar/avançar, opções de favoritos, botões de atualização e parada para atualizar ou parar a página da Web e botão inicial que leva o usuário à página inicial. A especificação HTML5 usada hoje não define elementos de interface do usuário, mas inclui elementos comuns, como barra de endereços, barra de status e barra de ferramentas. [2]

4. COMPONENTES DO NAVEGADOR DA WEB

Existem sete componentes principais do navegador da web. Os componentes incluem interface do usuário, mecanismo do navegador, mecanismo de renderização, rede, back-end da interface do usuário, interpretador de JavaScript e armazenamento de dados. [2]

1. Interface do usuário: inclui todas as partes do navegador exibição, como a barra de endereço, botão voltar/avançar, menu de favoritos, etc., exceto a janela onde o usuário vê a página solicitada.
2. Mecanismo do navegador: organiza as ações entre a interface do usuário e o mecanismo de renderização.
3. Mecanismo de renderização: responsável por exibir conteúdo solicitado. Quando um usuário solicita conteúdo HTML, o mecanismo de renderização analisa os arquivos HTML e CSS e exibe o conteúdo analisado no tela.
4. Rede: inclui chamadas de rede, como solicitações HTTP.
5. UI Backend: é usado para desenhar widgets básicos como caixas de combinação e janelas. O back-end expõe uma interface genérica que não é específica da plataforma.
   Por baixo, tudo usa abordagens de interface de usuário do sistema operacional.
6. Interpretador JavaScript: é usado para analisar e executar Código JavaScript.
7. Armazenamento de Dados: É uma camada de persistência. O navegador precisa desse componente para salvar dados localmente, como cookies. Além disso, o navegador oferece suporte a mecanismos de armazenamento, como localStorage, IndexedDB, WebSQL e FileSystem.

A imagem a seguir ilustra como cada um dos componentes interagir dentro do sistema.

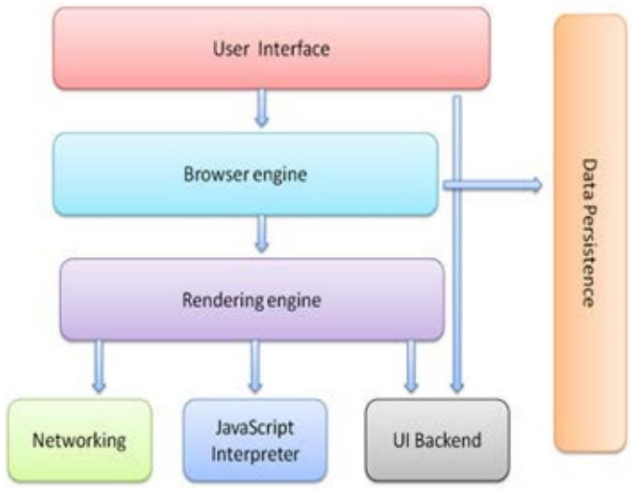

Figura 1: Componentes do navegador da Web [2]

V. RISCO DO NAVEGADOR DA WEB

De acordo com estudos anteriores, cerca de 45% das pessoas que navegam na Internet não estão utilizando a versão mais segura de seu navegador. Semelhante a muitos softwares, sem os patches de segurança adequados, os navegadores da Web ficam vulneráveis a ataques ou explorações. Além disso, mesmo um navegador da Web totalmente corrigido pode ser vulnerável a ataques se os complementos do navegador não estiverem totalmente corrigidos. Lembre-se, quando o usuário corrige o navegador, os complementos não são corrigidos automaticamente. [1]

Normalmente, os ataques baseados em navegador são originados de sites maliciosos. No entanto, uma programação de segurança deficiente de aplicativos da Web ou vulnerabilidades nos sites de suporte de software permitem que os invasores comprometam sites confiáveis para fornecer cargas maliciosas a visitantes desavisados. Os hackers adicionam scripts que não alteram a aparência de um site vulnerável. Esses scripts podem redirecionar silenciosamente o usuário para outro site sem que ele saiba. Esse redirecionamento para outro site pode fazer com que programas maliciosos sejam baixados para o seu computador. Esses programas geralmente são projetados para permitir o controle remoto do computador do usuário pelo invasor e para capturar informações pessoais, como informações de cartão de crédito, informações bancárias, etc. [1]

VI. PROTEJA O USUÁRIO CONTRA RISCOS DO NAVEGADOR

A seguir estão algumas das muitas práticas que um usuário deve aplicar para evitar riscos indesejados do navegador. [1]

- Mantenha seu(s) navegador(es) atualizado(s) e corrigido(s). • Mantenha seu sistema operacional atualizado e corrigido. • Use software antivírus e antispyware e mantenha eles atualizados.
- Mantenha seus aplicativos, como programas multimídia usados para assistir a vídeos, atualizados e corrigidos, especialmente se funcionarem com seu navegador.
- Verifique se o firewall do computador está ativado.
- Bloquear janelas pop-up, algumas das quais podem ser ataques maliciosos e ocultos. Isso pode impedir que softwares mal-intencionados sejam baixados para o seu computador. • Reforce as configurações de segurança em seus navegadores. Verifique as configurações nas seções de segurança, privacidade e conteúdo do seu navegador. O nível mínimo deve ser médio.
- Considere desativar os controles JavaScript, Java e ActiveX.

É importante observar que várias dessas dicas podem limitar o acesso dos usuários a parte do conteúdo do navegador. Por exemplo, o JavaScript é usado para controlar páginas da Web no lado do cliente do navegador, programas do lado do servidor e até mesmo aplicativos móveis. Se precisar usar JavaScript, configure seu navegador para avisá-lo antes de executar scripts. Reduza suas configurações de segurança temporariamente para ter acesso adequado e, em seguida, redefina-as. [1]

VII. O QUE É CARNE?

BeEF é a abreviação de The Browser Exploitation Framework. É uma ferramenta de teste de penetração que se concentra na exploração de vulnerabilidades do navegador da web. BeEF é um pacote de exploração baseado em navegador que “engancha” um ou mais navegadores como cabeças de praia, para que o invasor possa iniciar módulos de comando direcionados e outros ataques contra o sistema dentro do contexto do navegador. Um usuário pode ser fisgado ao abrir um URL personalizado e continuar a ver o tráfego típico da Web, enquanto um invasor tem acesso à sessão do usuário. O BeEF evita dispositivos de segurança de rede e aplicativos antivírus baseados em host, visando as vulnerabilidades encontradas em navegadores comuns. [4] O BeEF também permite que o testador de penetração profissional avalie a postura de segurança real de um ambiente de destino usando vetores de ataque do lado do cliente. Ao contrário de outras estruturas de segurança, o BeEF olha além do perímetro de rede e do sistema do cliente e examina a capacidade de exploração no contexto de uma porta aberta: o navegador da web. [3]

VIII. LAB

O experimento a seguir ilustra as etapas que seguimos para mostrar como executar um ataque bem-sucedido ao navegador da Web usando o BeEF e como é importante ter um antivírus atualizado em execução no seu computador para detectar um ataque ao navegador da Web usando a estrutura BeEF.

ATAQUE

Configure a VM da vítima e a VM do invasor. Certifique-se de que o adaptador de rede para ambas as VMs esteja definido como Adaptador em ponte.

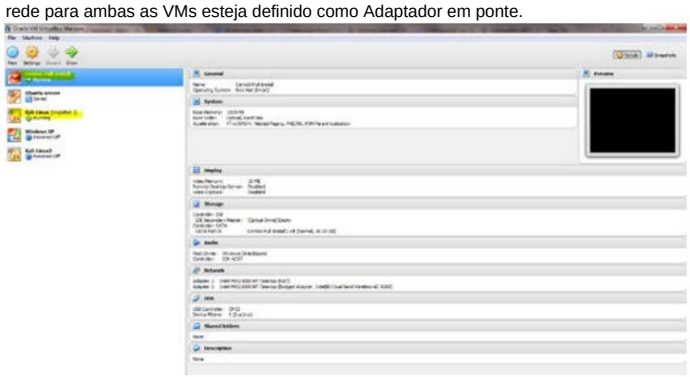

Figura 2: VMs [9]

As VMs destacadas são usadas para o experimento. A exploração foi realizada no Kali Linux enquanto o CentOS 7 era o sistema operacional vitimado.

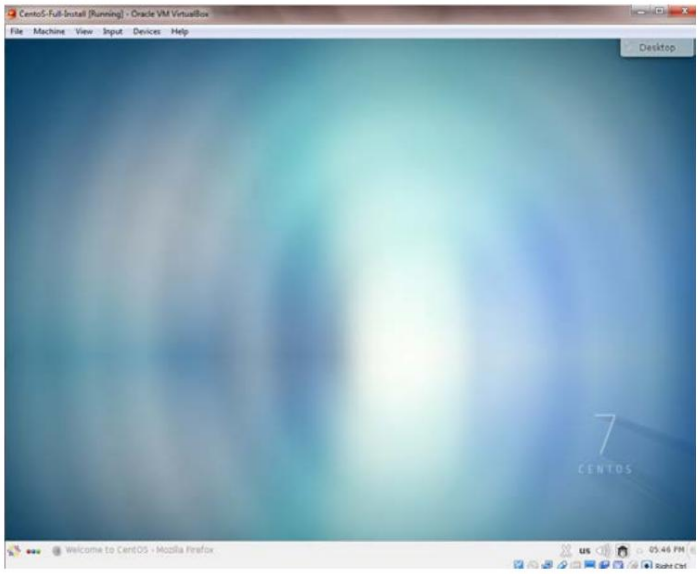

Figura 3: CentOS 7 da máquina da vítima [8]

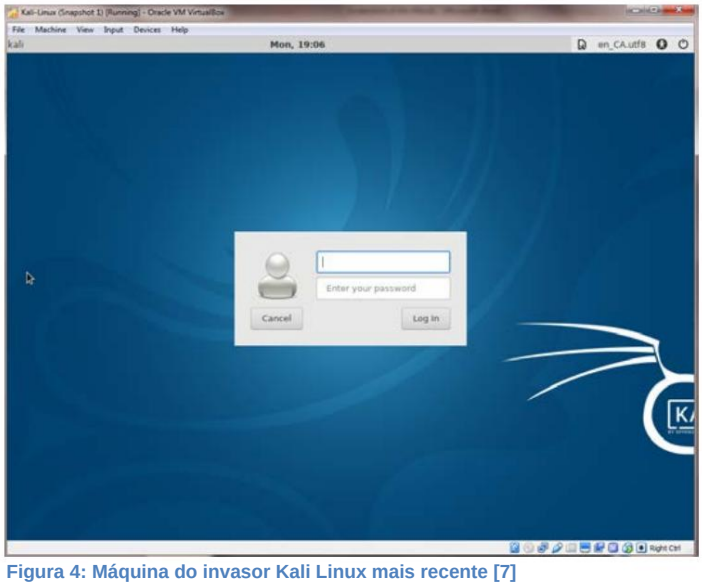

Figura 4: Máquina do invasor Kali Linux mais recente [7]

Acima está a página de login do Kali Linux. Observe que criamos os detalhes de login durante a instalação do sistema operacional.

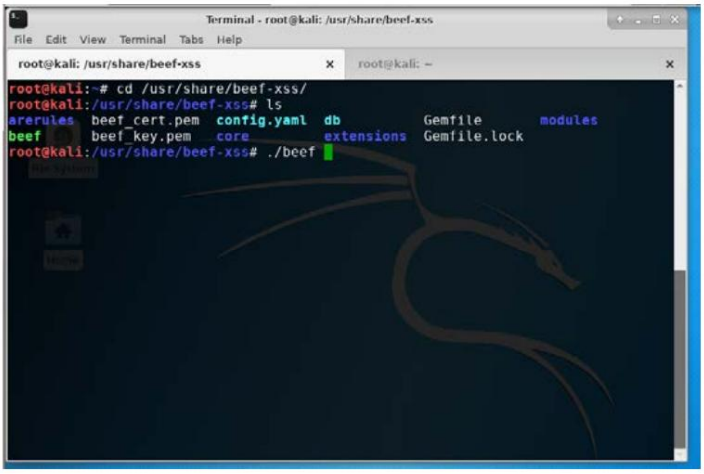

Figura 5: Diretório da Carne

Use o Terminal no Kali Linux para executar o framework beef, o invasor terá que fazer login no Kali Linux e, em seguida, navegar até o diretório “beef-xss” e executar o script “beef” conforme mostrado acima.

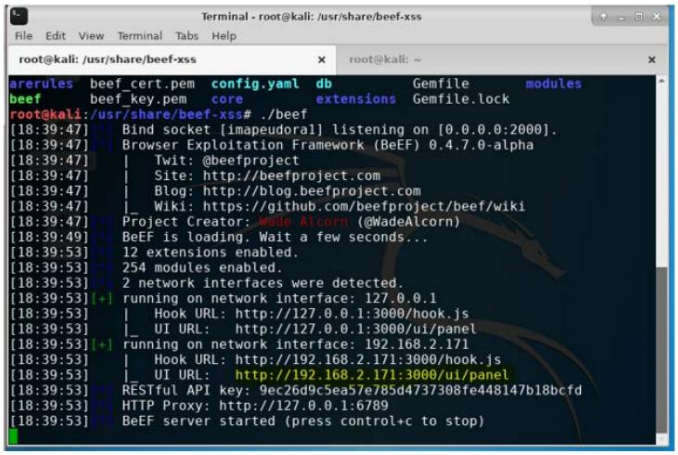

Figura 6: carne moída

Como pode ser visto na captura de tela acima, a carne bovina foi lançada com sucesso. Use a URL destacada para abrir a página de login do BeEF no navegador do invasor.

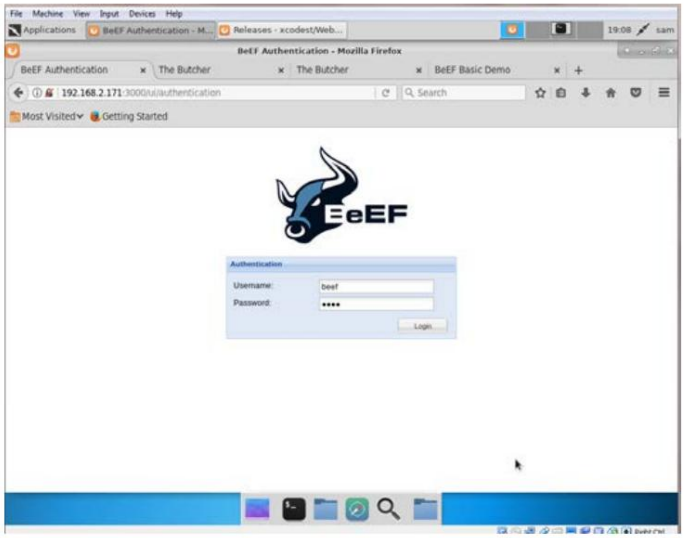

Figura 7: página de login do BeEF

Depois que o BeEF for lançado, o próximo passo será fazer login na interface do usuário, conforme visto acima. O nome de usuário e a senha são "bife".

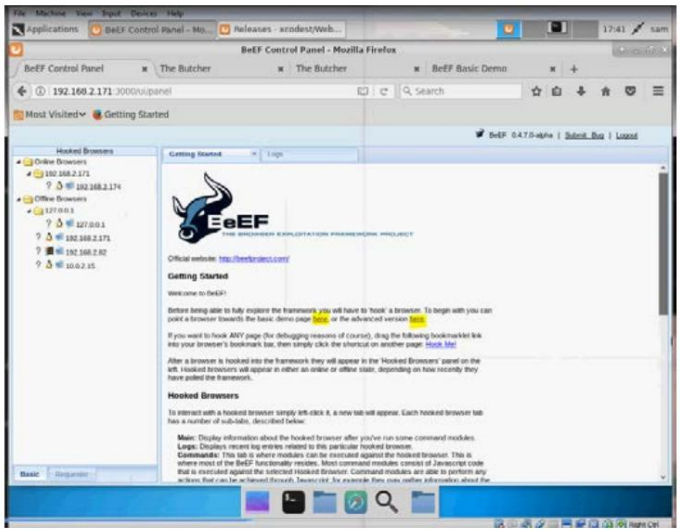

Figura 8: página inicial do BeEF

A imagem acima é a página inicial do BeEF com dois links destacados. Qualquer um dos links pode ser usado para conectar o navegador da vítima. Certifique-se de substituir o endereço IP do link de 127.0.0.1 pelo endereço IP do invasor (neste caso, 192.168.2.171). Você pode encontrar o endereço IP do invasor no terminal usando o comando “ifconfig”. Só por curiosidade, a imagem a seguir é um link chamado “versão avançada” da página html quando aberta na VM da vítima.

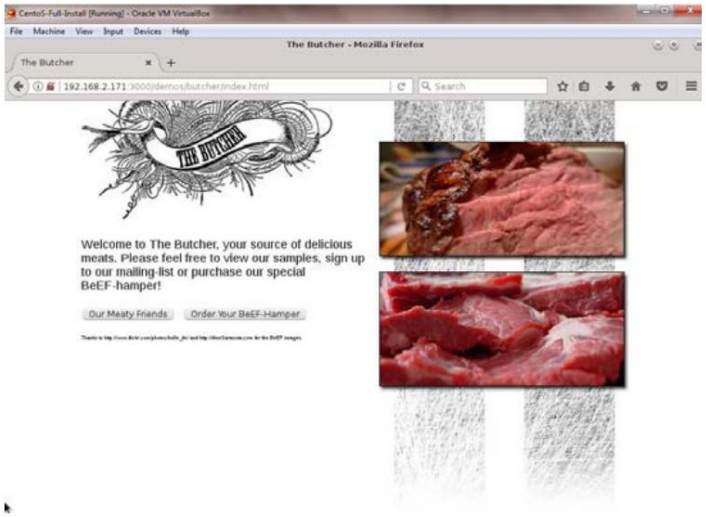

Figura 9: página de link malicioso

Neste ponto, do lado do invasor, você pode mascarar o link malicioso usando ferramentas como bitly.com, antes de atrair sua vítima para clicar em seu link malicioso usando engenharia social.

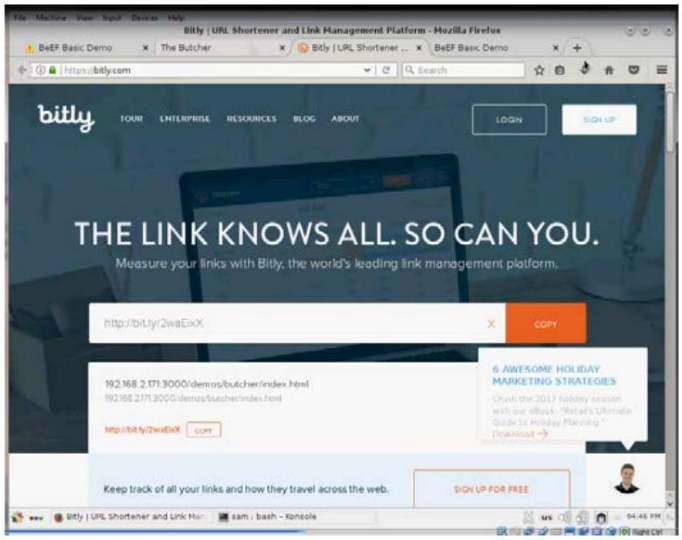

Figura 10: Bitly.com

Suponha que você tenha sucesso em convencer sua vítima a clicar em seu link usando e-mail ou outro método de engenharia social. O sistema da vítima ficará “fisgado” conforme ilustrado na imagem a seguir. Para esta experiência, abra o link da versão avançada na VM da vítima para mostrar que a engenharia social foi bem-sucedida.

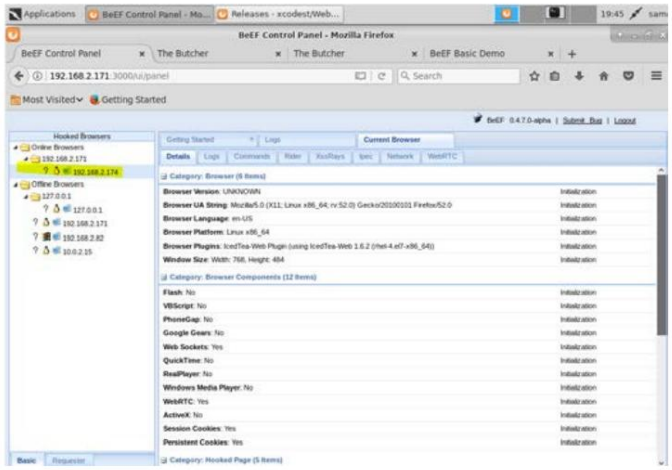

Figura 11: Navegador viciado

Como pode ser visto na captura de tela acima, o navegador em execução na máquina da vítima com o endereço IP 192.168.2.174 foi fisgado. A imagem acima é mostrada na VM do invasor.

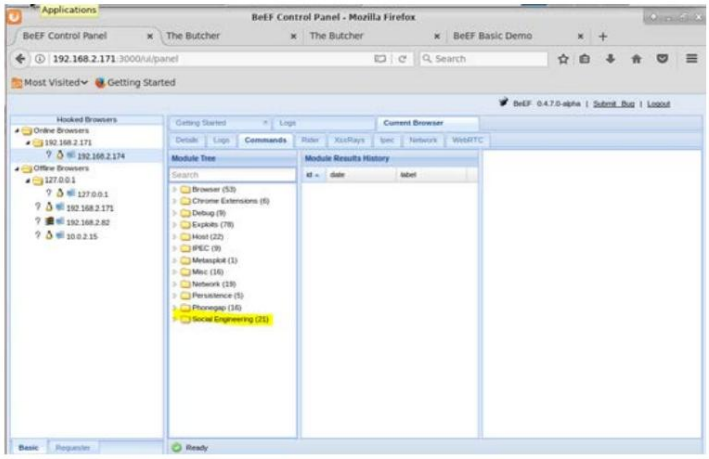

Figura 12: Ataque de Engenharia Social

Neste ataque, exploramos a máquina da vítima por meio de engenharia social, como pode ser visto acima. Na guia comandos, vá para engenharia social para testar o mesmo ataque que testamos.

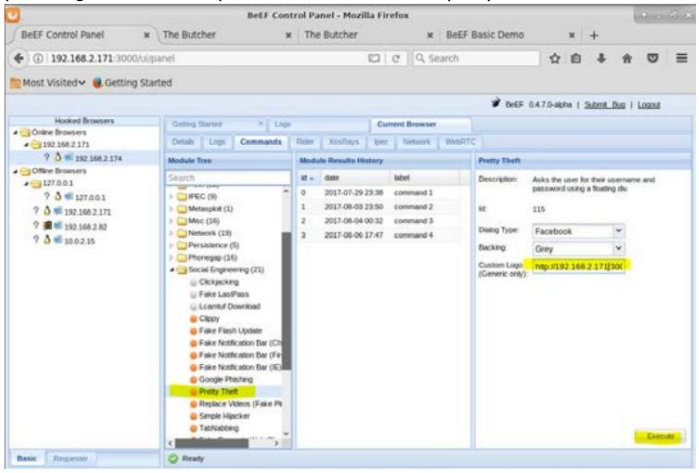

Figura 13: Selecionando Ataque

Estamos executando a "exploração Pretty Theft". Na Fig. 13 acima, à direita é onde inserimos as informações do atacante máquina executando o serviço de carne bovina. Certifique-se de substituir o endereço IP padrão no logotipo personalizado pelo endereço IP da VM do invasor (neste caso, 192.168.2.171) antes de executar.

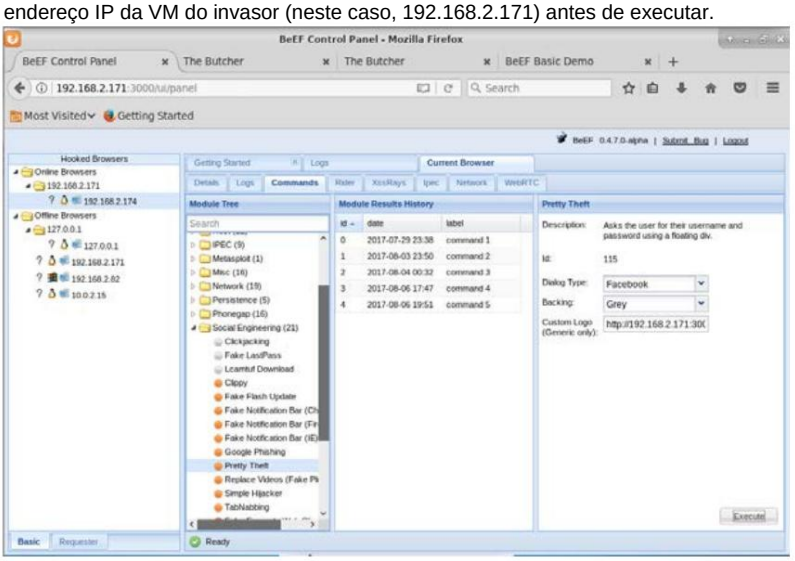

Figura 14: Lançando o ataque

Para executar o ataque, basta clicar em executar como mostrado na Fig. 14 acima.

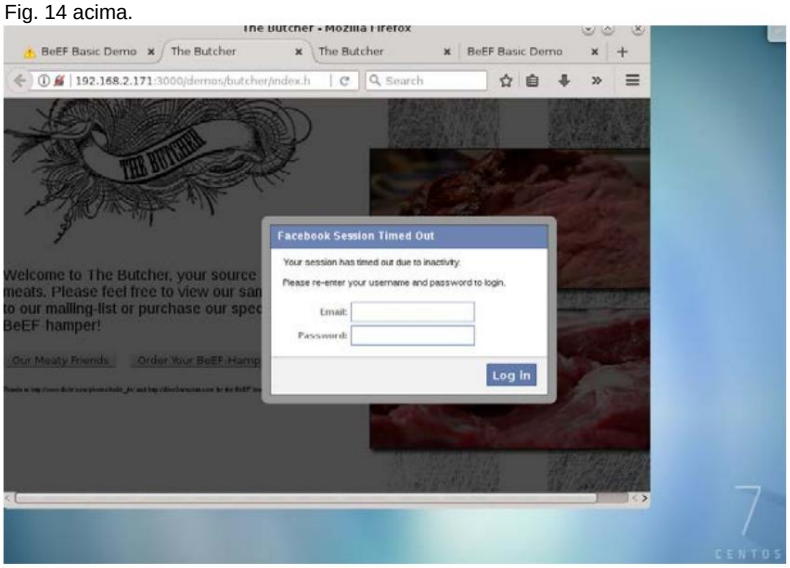

Figura 15: Login falso no Facebook

Depois de clicarmos em executar, a tela de autenticação Face Facebook será deslocada na máquina da vítima, como visto na Fig. 15 acima.

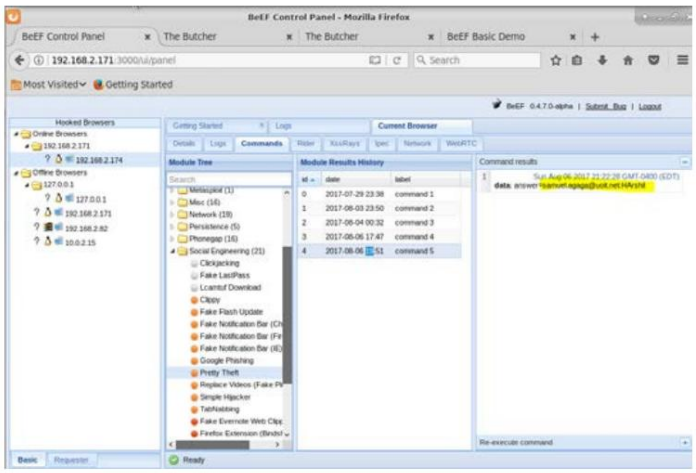

Figura 16: detalhes de login capturados

Observar a parte elevada à direita da captura de tela na Fig. 16 indica nossos detalhes de login capturados do nome de usuário e senha da vítima para o Facebook.

Observação. Seria mais autêntico para a vítima se o invasor executasse seu ataque no momento certo, por exemplo, quando a vítima está na página de login do Facebook.

Defesa

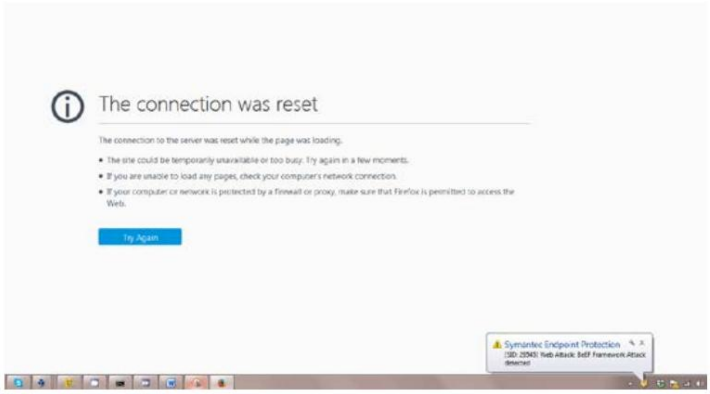

Figura 17: Defesa do Symantec Antivirus

Uma das maneiras de defender esse anexo é ter um programa antivírus atualizado em execução no seu computador. Na captura de tela acima, quando tentamos esta exploração contra uma máquina executando o antivírus Symantec, na verdade recebemos um aviso informando que houve um ataque BeEF framework, como pode ser visto na captura de tela da Fig. 17. Portanto, teste o mesmo processo, mas ative seu antivírus Symantec.

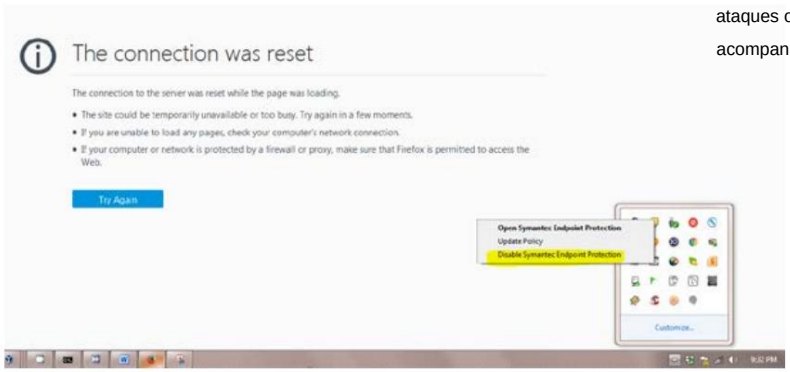

Figura 18: Desativando o Symantec Antivirus

No entanto, o ataque foi bem-sucedido depois que desativamos o programa antiferrugem, conforme mostrado acima.

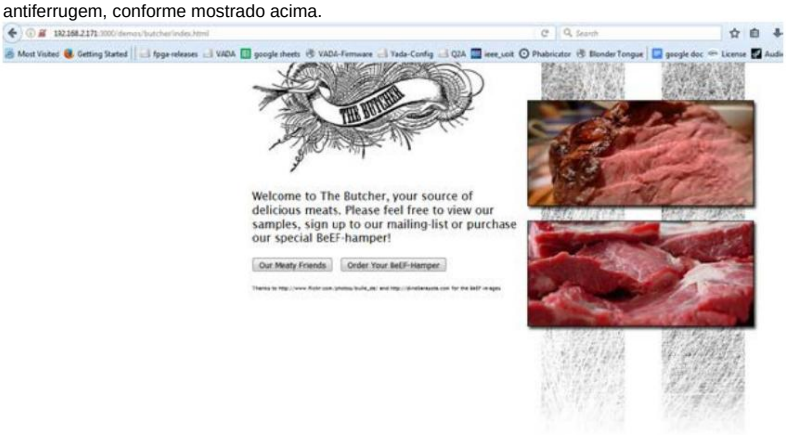

Figura 19: Login bem-sucedido após a desativação do antivírus

Depois que o programa antivírus foi desabilitado, a máquina da vítima ficou “viciada” veja a Fig. 18 acima.

IX. TRABALHO FUTURO

Em um artigo, é proposto que, após várias tentativas bem-sucedidas de roubar informações de cartão de crédito ou senhas bancárias, muitas empresas estão tentando avançar para navegadores baseados em nuvem, um navegador sem Java. Um navegador baseado em nuvem não armazena dados de cada sessão e evita que qualquer malware entre em rede com o computador do usuário. Um desses produtos é o Silo da Authentic8. Um navegador separado que é executado somente após inserir uma senha. Em seguida, ele é executado na nuvem e acessa uma lista de links que o usuário inseriu anteriormente e pode armazenar senhas para esses sites. Todo o código é executado em seus servidores remotos, fornecendo segurança contra malware e privacidade contra rastreamento. [5]

X. CONCLUSÃO

Em conclusão, agora sabemos como é ameaçador para todos navegar na web sem usar as práticas de segurança adequadas. Com o experimento, aprendemos que o ataque ao navegador da Web é um tópico amplo. Usuários mal-intencionados podem executar todos os tipos de ataques, de XSS a Buffer Overflow, se o usuário não estiver atualizando seu sistema regularmente. O BeEF é uma ferramenta simples de teste de penetração que pode ser usada por qualquer pessoa para testar alguns ataques ou hackear o sistema de alguém, por isso é necessário que todos acompanhem as atualizações e patches.

REFERÊNCIAS

[1] “Ataque do navegador da Web”, *Pvamus,* março de 2009. [On-line]. Disponível: https://www.pvamu.edu/Include/ITS/Vol3Issue2.pdf. [Acesso: 15 de julho de 2017].

[2] T. Garsiel e P. Irish, “How Browsers Work: Behind the scenes of navegadores da web modernos”, *html5rocks,* 05 de agosto de 2011. [On-line]. Disponível: https://www.html5rocks.com/en/tutorials/internals/howbrowserswork/. [Acesso: 15-jul-2017].

[3] “BeEF - O Projeto de Estrutura de Exploração de Navegador,” *BeEF - O Projeto de Estrutura de Exploração de Navegador.* [On-line]. Disponível: http://beefproject.com/. [Acesso: 15-jul-2017].

[4] J. Muniz e A. Lakhani, “Teste de penetração na Web com Kali Linux,” *Google Books.* [On-line]. Available: https://books.google.ca/books?id=4fD7AAAAQBAJ&pg=PT5&lpg=PT5&dq=countermeasure%2Bagainst%2Bbeef%2Bkali%2Blinux&source=bl&ots=qxPZaai Ff&sig=lyfWjc9AMfDcvjfLos9VpjVhRsA&hl=en&sa=X&ved=0ahUKEwihqdH98LzVAhWHz4MKHRwoDAAQ6AEIPzAE#v=snippet&q =ser ef&f=falso. [Acesso: 15-jul-2017].

[5] A. Tanner, “Por que os navegadores em nuvem são a onda do futuro”, *Forbes,* 10 de março de 2014. [On-line]. Disponível: https://www.forbes.com/sites/adamtanner/2014/03/10/why-cloud browsers-are-the-wave-of-the-future/#150af5b9305a. [Acesso: 15 de julho de 2017].

[6] “Hack Like a Pro: How to Hack Web Browsers with BeEF,” *WonderHowTo,* 02-fev-2015. [On-line]. Disponível: https://null byte.wonderhowto.com/how-to/hack-like-pro-hack-web-browsers-with beef-0159961/. [Acesso: 15-jul-2017].

[7] “Nossa distribuição de teste de penetração mais avançada de todos os tempos.”, *Kali Linux.* [On-line]. Disponível: https://www.kali.org/. [Acesso: 15 de julho de 2017].

[8] “O Projeto CentOS,” *Projeto CentOS.* [On-line]. Disponível: https://www.centos.org/. [Acesso: 15-jul-2017].

[9] “Oracle VM VirtualBox - Downloads | Rede de Tecnologia Oracle | Oracle,” *Oracle VM VirtualBox - Downloads | Rede de Tecnologia Oracle | Oráculo.* [On-line]. Disponível: http://www.oracle.com/technetwork/server storage/virtualbox/downloads/index.html. [Acesso: 15-jul-2017].