**Relatório de teste de penetração**

MegaCorp One

10 de agosto de 2013

**Serviços de segurança ofensiva, LLC**

19706 One Norman Blvd. Suíte B nº 253

Cornelius, NC 28031 Estados Unidos da América

Telefone: 1-402-608-1337

Fax: 1-704-625-3787

[E-mail: info@offsec.com](mailto:info@offsec.com)

[Site: http://www.offensive-security.com](http://www.offensive-security.com/)

Sumário

[Sumário executivo 3](#_Toc109103181)

[Resumo dos Resultados 3](#_Toc109103182)

[Narrativa de Ataque 3](#_Toc109103183)

[Descoberta remota do sistema 4](#_Toc109103184)

[Comprometimento da interface do servidor Web do administrador 5](#_Toc109103185)

[Shell interativo para servidor de administração 8](#_Toc109103186)

[Escalonamento de privilégios administrativos 9](#_Toc109103187)

[Ataques de cliente Java 10](#_Toc109103188)

[Encaminhamento para administrador local 11](#_Toc109103189)

[Bypass de inspeção profunda de pacotes 12](#_Toc109103190)

[Compromisso do Ambiente Citrix 15](#_Toc109103191)

[Encaminhamento para administrador de domínio 18](#_Toc109103192)

[Conclusão 20](#_Toc109103193)

[Recomendações 20](#_Toc109103194)

[Classificação de risco 21](#_Toc109103195)

[Apêndice A: Detalhe e mitigação da vulnerabilidade 21](#_Toc109103196)

[Escala de Classificação de Risco 21](#_Toc109103197)

[Credenciais padrão ou fracas 21](#_Toc109103198)

[Avaliação: Alto 21](#_Toc109103199)

[Reutilização de senha 21](#_Toc109103200)

[Avaliação: Alto 22](#_Toc109103201)

[Senha de administrador local compartilhada 22](#_Toc109103202)

[Avaliação: Alto 22](#_Toc109103203)

[Gerenciamento de patches 22](#_Toc109103204)

[Avaliação: Alto 22](#_Toc109103205)

[Transferência de zona DNS 23](#_Toc109103206)

[Avaliação: Baixo 23](#_Toc109103207)

[Arquivos padrão do Apache 23](#_Toc109103208)

[Avaliação: Baixo 23](#_Toc109103209)

[admin.megacorpone.com . 23](#_Toc109103210)

[Apêndice B: Sobre Segurança Ofensiva 23](#_Toc109103211)

# Sumário executivo

A Oﬀensive Security foi contratada pela MegaCorp One para realizar um teste de penetração a fim de determinar sua exposição a um ataque direcionado. Todas as atividades foram conduzidas de forma a simular um agente malicioso envolvido em um ataque direcionado contra a MegaCorp One com os objetivos de:

* Identificar se um invasor remoto pode penetrar nas defesas da BB Tecnologia e Serviços.
* Determinando o impacto de uma violação de segurança em:
  + Confidencialidade dos dados privados da empresa
  + Infraestrutura interna e disponibilidade dos sistemas de informação da MegaCorp One

Esforços foram feitos na identificação e exploração de pontos fracos de segurança que poderiam permitir que um invasor remoto obtivesse acesso não autorizado a dados organizacionais. Os ataques foram conduzidos com o nível de acesso que um usuário geral da Internet teria. A avaliação foi conduzida de acordo com as recomendações descritas no

NIST SP 800-115¹ com todos os testes e ações sendo realizados sob condições controladas.

1 <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

## Resumo dos Resultados

O reconhecimento inicial da rede MegaCorp One resultou na descoberta de um servidor DNS mal configurado que permitia uma transferência de zona DNS. Os resultados nos forneceram uma lista de hosts específicos a serem direcionados para esta avaliação. Um exame desses hosts revelou uma interface de servidor web administrativa protegida por senha. Depois de criar uma lista de palavras personalizada usando termos identificados no site da MegaCorp One, conseguimos acessar essa interface descobrindo a senha via força bruta.

Um exame da interface administrativa revelou que ela era vulnerável a uma vulnerabilidade de injeção remota de código, que era usada para obter acesso interativo ao sistema operacional subjacente. Esse comprometimento inicial foi escalado para acesso administrativo devido à falta de atualizações de sistema apropriadas no servidor web. Após uma análise mais detalhada, descobrimos que o servidor web comprometido utiliza um applet Java para usuários administrativos. Adicionamos uma carga maliciosa a este applet, que nos deu acesso interativo às estações de trabalho usadas pelos administradores da MegaCorp One.

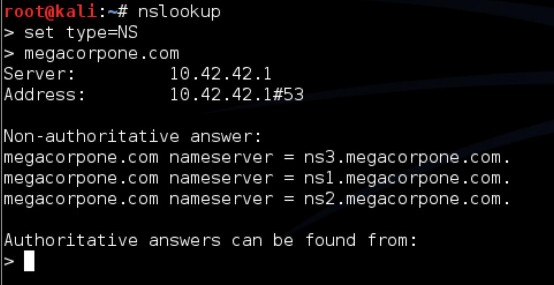
Usando o servidor web comprometido como um ponto de pivô junto com as senhas recuperadas dele, conseguimos direcionar recursos internos anteriormente inacessíveis. Isso resultou no acesso do Administrador Local a vários hosts internos do Windows, comprometimento total de um servidor Citrix e controle administrativo total da infraestrutura do Windows Active Directory. Os controles de tráfego de rede existentes foram ignorados por meio do encapsulamento de tráfego malicioso em protocolos permitidos.

# Narrativa de Ataque

## Descoberta remota do sistema

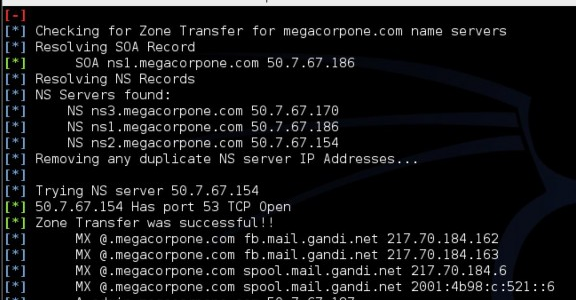
Para os fins desta avaliação, a MegaCorp One forneceu informações mínimas fora do nome de domínio organizacional: megacorpone.com. A intenção era simular de perto um adversário sem nenhuma informação interna. Para evitar direcionar sistemas que não eram de propriedade da MegaCorp One, todos os ativos identificados foram enviados para verificação de propriedade antes que qualquer ataque fosse realizado.

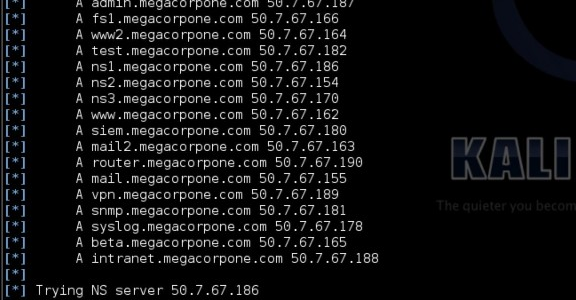
Na tentativa de identificar a possível superfície de ataque, examinamos os servidores de nomes do nome de domínio megacorpone.com (Figura 1).



**Figura 1 – A coleta de informações para megacorpone.com revela três servidores de nomes ativos.**

Com os servidores de nomes identificados, tentamos realizar uma transferência de zona. Descobrimos que **ns2.megacorpone.com** era vulnerável a uma configuração incorreta de transferência de zona DNS completa. Isso nos forneceu uma lista de nomes de host e endereços IP associados, que poderiam ser usados para direcionar ainda mais a organização. (Figura 2) As transferências de zona podem fornecer aos invasores informações detalhadas sobre os recursos da organização. Ele também pode vazar informações sobre os intervalos de rede de propriedade da organização. Consulte o Apêndice A para obter mais informações.





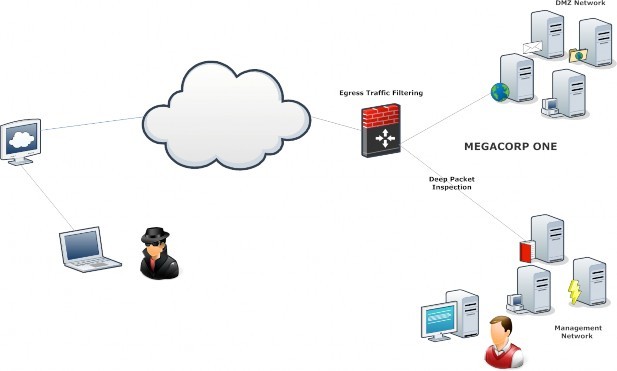
**Figura 2 – Um servidor de nomes mal conﬁgurado permite uma transferência de zona DNS completa e irrestrita.**

A lista de hosts identificados foi submetida à MegaCorp One para verificação, que verificou que toda a faixa de rede

50.7.67.x deveria ser incluída no escopo da avaliação. Esses sistemas foram então verificados para enumerar quaisquer serviços em execução. Todos os serviços identificados foram examinados em detalhes para determinar sua exposição potencial a um ataque direcionado.

Por meio de uma combinação de técnicas de enumeração de DNS e varredura de rede, conseguimos construir um composto que acreditamos reﬂetir a rede da MegaCorp One.

A rede de destino é mostrada abaixo na Figura 3. Detalhes adicionais sobre controles, como inspeção profunda de pacotes, foram descobertos posteriormente na avaliação, mas estão incluídos aqui para completar.

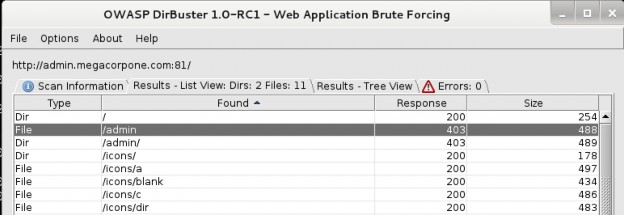


**Figura 3 - Rede de destino**

## Comprometimento da interface do servidor Web do administrador

Descobriu-se que o servidor web **admin.megacorpone.com** estava executando um servidor web Apache na porta 81. Acessar a URL raiz deste site resultou na exibição de uma página em branco. Em seguida, realizamos uma rápida

verificação de enumeração do sistema procurando por diretórios e arquivos comuns (Figura 4).



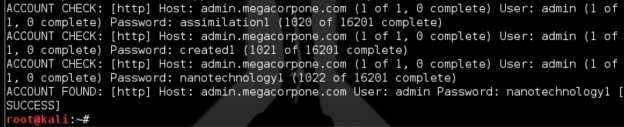
**Figura 4 – A enumeração do host admin.megacorpone.com divulga parcialmente a estrutura de pastas do servidor web.**

Os resultados da verificação revelaram que, juntamente com os arquivos padrão comuns do Apache (consulte o Apêndice A para obter mais informações), identificamos um diretório “ **/admin** ” que só era acessível após a autenticação. (Figura 5).



**Figura 5 – O acesso à pasta “admin” é protegido por senha.**

[Para preparar uma tentativa de força bruta direcionada contra esse sistema, compilamos um arquivo de dicionário personalizado com base no conteúdo do site www.megacorpone.com . O dicionário inicial consistia em 331 palavras](http://www.megacorpone.com/) personalizadas, que foram então submetidas a várias rodadas de permutações e substituições para produzir um arquivo de dicionário final de 16.201 palavras. Este arquivo de dicionário foi usado junto com o nome de usuário “ **admin** ” na seção protegida do site.



**Figura 6 – Usando um dicionário de palavras personalizado é possível descobrir a senha administrativa da pasta “admin”.**

Este ataque de força bruta descobriu uma senha de “nanotecnologia1” para o usuário administrador. Conseguimos aproveitar essas credenciais para obter acesso não autorizado à parte protegida do site (Figura 6). Consulte o Apêndice A para obter mais informações sobre a vulnerabilidade explorada.

A parte administrativa do site continha a interface da web do SQLite Manager (Figura 7), que era acessível sem nenhuma credencial adicional. Utilizando essa interface, encontramos o que parecia ser o banco de dados que

2

suportava uma instância do **phpSQLiteCMS** .



**Figura 7 – Uma instância do SQLite Manager está sendo executada no servidor web comprometido.**

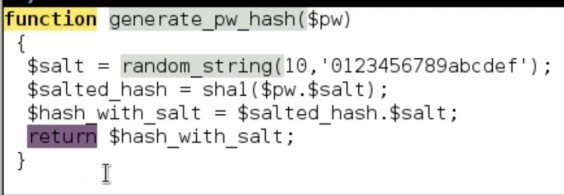
1. <http://phpsqlitecms.net/>

A interface nos deu acesso direto aos dados e a capacidade de extrair uma lista de usuários no sistema com os valores de hash de senha associados (Figura 8).



**Figura 8 – A falta de controles de acesso adicionais permite que um invasor recupere nomes de usuário e hashes de senha do banco de dados “userdata”.**

Após o exame dos valores, descobrimos que os hashes não estavam em conformidade com nenhum formato padrão. Usando uma cópia do software “ **phpselitecms** ”, examinamos o código-fonte para determinar exatamente como esse valor é produzido. Por meio desse processo conseguimos identificar a função responsável pelo hash das senhas das contas.



**Figura 9 – A revisão do código-fonte leva à descoberta do algoritmo de geração de hash de senha.**

Com o conhecimento recém-adquirido do formato de hash de senha e o uso de um valor de sal de 10 caracteres gerado aleatoriamente, conseguimos converter facilmente os hashes recuperados em seu equivalente SHA1 salgado e conduzir um ataque de força bruta.

Esse esforço resultou na recuperação de duas senhas de texto simples. Embora esses valores não fossem imediatamente úteis, eles foram mantidos na esperança de que pudessem ser reutilizados em outros sistemas dentro da organização.

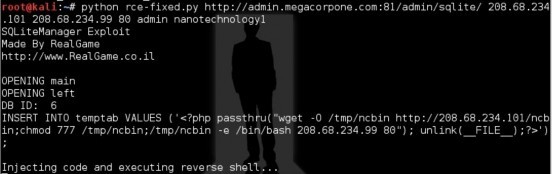
## Shell interativo para servidor de administração

O software SQLite Manager descoberto anteriormente era vulnerável a uma vulnerabilidade de injeção de código bem

3

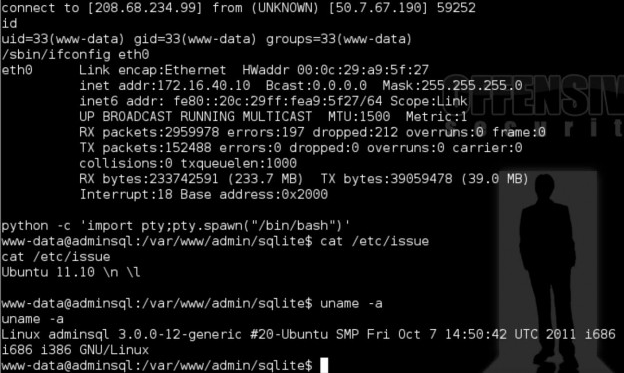
conhecida . A exploração bem-sucedida desta vulnerabilidade resulta em acesso shell ao sistema subjacente no

contexto do usuário do servidor web. Usando um exploit público modificado, conseguimos obter acesso interativo limitado ao servidor web **admin.megacorpone.com** . Consulte o Apêndice A para obter mais informações.



**Figura 10 – Uma exploração SQLite disponível publicamente é usada para obter acesso não autorizado no host admin.megacorpone.com.**

1. <http://www.exploit-db.com/exploits/24320/>

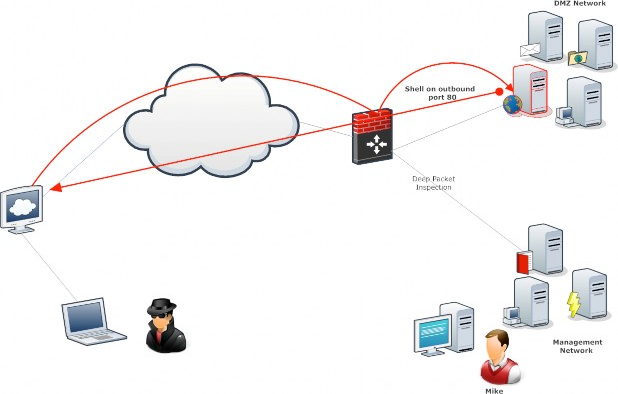


**Figura 11 – O controle do servidor vulnerável é limitado ao contexto do usuário www-data.**

A versão pública do exploit tem como alvo uma versão do SQLite Manager ligeiramente diferente daquela implantada pela MegaCorp One. Embora a versão implantada do software seja vulnerável aos mesmos problemas subjacentes, a

exploração não é executada com êxito sem modificação. Conseguimos estender o exploit original para oferecer suporte à autenticação HTTP e personalizá-lo para a versão atualizada. Uma cópia desta exploração atualizada será fornecida separadamente deste relatório.

A extensão do comprometimento neste ponto pode ser melhor visualizada na Figura 12.



**Figura 12 - Comprometimento do Servidor Web**

## Escalonamento de privilégios administrativos

Com o acesso interativo ao sistema operacional subjacente do servidor administrativo da Web obtido, continuamos com o exame do sistema em busca de maneiras de escalar privilégios para o nível administrativo. Descobrimos que o

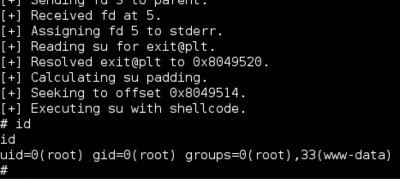
4

sistema estava vulnerável a uma exploração de escalonamento de privilégio local

Consulte o Apêndice A para obter mais informações.

, que pudemos utilizar com sucesso.





**Figura 13 – Uma exploração de escalonamento de privilégio local é usada para tirar proveito de um host sem patch e obter acesso no nível raiz.**

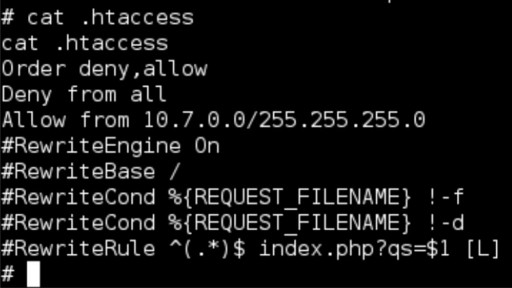
O uso deste exploit foi parcialmente possível devido à inclusão de ferramentas de desenvolvedor no sistema vulnerável. Se essas ferramentas não estivessem presentes no sistema, ainda seria possível explorar com sucesso, embora a dificuldade em fazê-lo fosse aumentada.

Em sua configuração atual, o servidor web representa uma plataforma de ataque interno para uma parte mal- intencionada. Com a capacidade de obter acesso administrativo total, uma parte mal-intencionada poderia utilizar esse sistema vulnerável para vários propósitos, desde ataques contra a própria MegaCorp One até ataques contra seus clientes. É altamente provável que os invasores aproveitem esse sistema para ambos os propósitos.

1. <http://www.exploit-db.com/exploits/18411/>

## Ataques de cliente Java

Utilizando o acesso administrativo ao sistema, realizamos uma análise do sistema explorado. Isso resultou na descoberta de uma seção privada do site que serve um applet Java apenas para estações de trabalho específicas. Essa faixa de rede em questão foi posteriormente descoberta como a rede de gerenciamento da MegaCorp One.



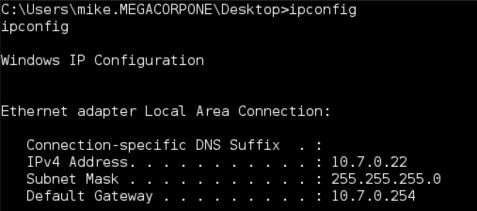
**Figura 14 - As regras Htaccess revelam uma sub-rede adicional na rede comprometida.**

Através do exame dos arquivos de log e do miniaplicativo Java presentes no sistema, descobrimos que o miniaplicativo fornecia funcionalidade administrativa a um subconjunto de usuários internos da MegaCorp One. Isso foi vantajoso para nós como invasores, pois nos forneceu um caminho potencial para sistemas internos que, de outra forma, não eram facilmente acessíveis.

Ao obter permissão da MegaCorp One, adicionamos um applet adicional para ser baixado pelos clientes. A teoria desse ataque era que os clientes acessariam o applet confiável, permitiriam sua execução e nos forneceriam acesso

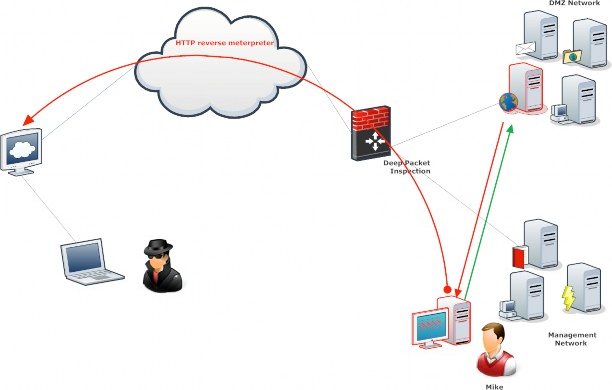
direto a hosts clientes adicionais. Este é um derivado de um ataque comum de engenharia social no qual a vítima é manipulada para executar um applet malicioso. Neste caso, no entanto, nenhum esforço foi necessário para enganar a vítima, pois o applet já é considerado confiável.

Este ataque funcionou como pretendido, fornecendo-nos acesso a um sistema cliente adicional.



**Figura 15 – Usando um applet java malicioso é possível explorar um host na sub-rede de gerenciamento.**

Com esse compromisso em vigor, obtivemos acesso aos sistemas na rede de gerenciamento, conforme indicado na Figura 16.



**Figura 16 – O ataque bem-sucedido do miniaplicativo java compromete a sub-rede de gerenciamento do MegaCorp One.**

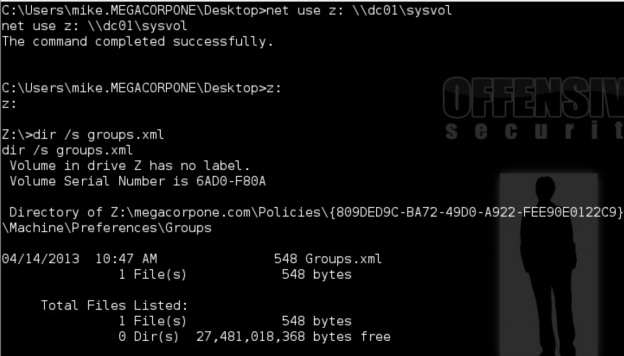
## Encaminhamento para administrador local

O acesso fornecido pelo ataque do applet Java foi limitado ao nível de um usuário padrão. Para maximizar o impacto do comprometimento, queríamos escalar o acesso ao nível de Administrador de Domínio. Como primeiro passo, precisávamos obter acesso administrativo local. Em um esforço para conseguir isso, examinamos o sistema comprometido para identificar como ele poderia ser aproveitado.

Usando essa abordagem, encontramos um arquivo de Preferências de Diretiva de Grupo no sistema que nos permitiu

56

descriptografar a senha administrativa local . Consulte o Apêndice A para obter mais informações.



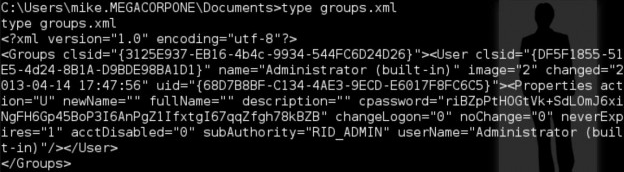
**Figura 17 – Usando o acesso recém-adquirido é possível recuperar o arquivo Groups.xml de um controlador de domínio.**

5

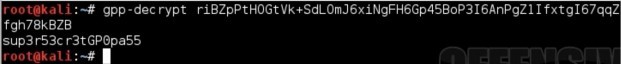
<http://msdn.microsoft.com/en-us/library/cc422924.aspx>

6

<http://blogs.technet.com/b/grouppolicy/archive/2009/04/22/passwords-in-group-policy-preferences-updated.aspx>



**Figura 18 – A senha do administrador local criptografada é encontrada no arquivo Groups.xml.**

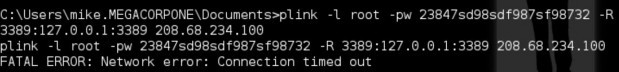


**Figura 19 – Usando a chave de criptograﬁa publicada pela Microsoft, a senha criptografada é facilmente descriptografada.**

Usando a senha de texto simples recuperada, conseguimos obter acesso administrativo local ao cliente comprometido.

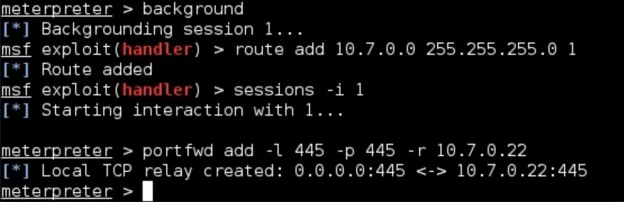
## Bypass de inspeção profunda de pacotes

Ao tentar estabelecer camadas adicionais de acesso ao sistema comprometido, encontramos uma filtragem de saída agressiva. Isso foi encontrado pela primeira vez ao tentar estabelecer um túnel de saída criptografado para o Microsoft Remote Desktop Protocol.

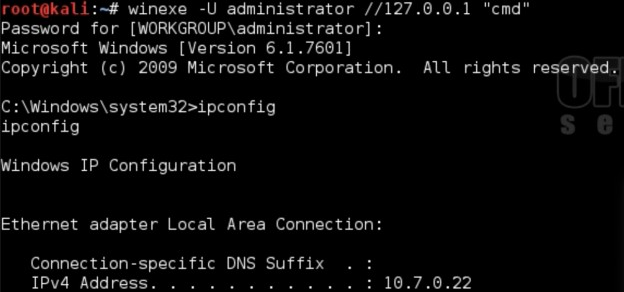


**Figura 20 – As tentativas iniciais de estabelecer um túnel de saída para RDP foram bloqueadas pelos sistemas de ﬁltragem de saída.**

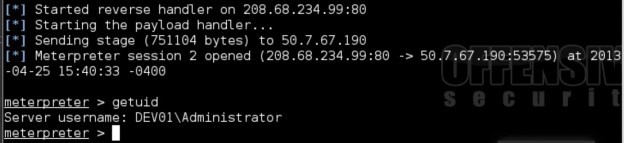
Além disso, descobrimos a aplicação do protocolo de rede ao tentarmos nos conectar ao servidor SSH do invasor na porta 80. Para contornar isso, criamos um túnel dentro da sessão do medidor existente para nos permitir acessar o compartilhamento de arquivos do Windows a partir do sistema do invasor. Isso foi utilizado para executar um shell de comando do Windows no host comprometido como o usuário administrativo local. Dentro desse shell, executamos uma carga útil adicional do meterpreter.



**Figura 21 – O encaminhamento de porta através da sessão inicial do meterpreter é estabelecido para obter acesso direto ao host de gerenciamento comprometido.**



**Figura 22 – A conexão recém-estabelecida é usada para obter um shell administrativo no host de gerenciamento comprometido.**



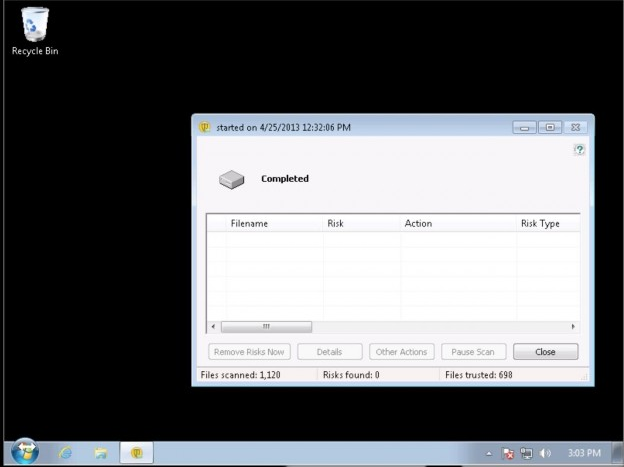
**Figura 23 - O acesso de Administrador Local é usado para estabelecer um shell meterpreter no host 10.7.0.22.**

Com o novo shell meterpreter instalado, usamos HTTP-Tunnel, um utilitário de código aberto

7

, que encapsula tráfego

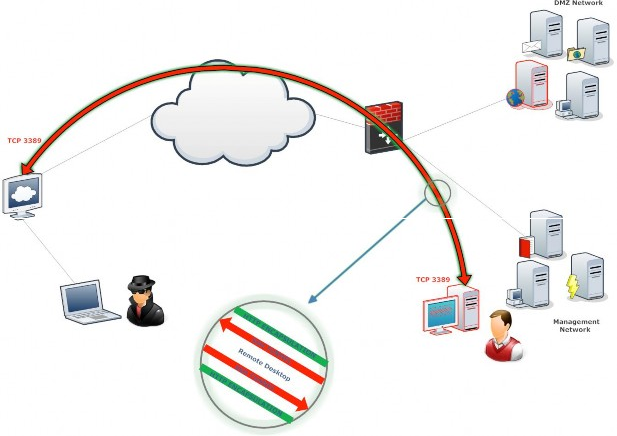
arbitrário dentro da carga HTTP. Usamos o recém-estabelecido “ **túnel http** ” para encapsular uma conexão de área de trabalho remota entre o invasor e o cliente comprometido. Isso nos permitiu obter acesso gráfico completo ao sistema cliente comprometido. A sessão de área de trabalho remota foi estabelecida usando a senha do usuário " **mike** ", que foi descoberta para ser reutilizada do aplicativo SQLite Manager comprometido. Consulte o Apêndice A para obter mais informações.



**Figura 24 - O acesso à Área de Trabalho Remota é estabelecido encapsulando o protocolo previamente ﬁltrado através de um túnel http.**

Nesse ponto, o perímetro externo da rede MegaCorp One estava totalmente comprometido, conforme mostrado na Figura 25. O equivalente virtual do acesso do console a um computador dentro do ambiente confiável do MegaCorp One havia sido obtido. Deve-se observar que o acesso atual à rede Windows estava limitado a uma conta de usuário de domínio sem privilégios e a uma conta de administrador local.

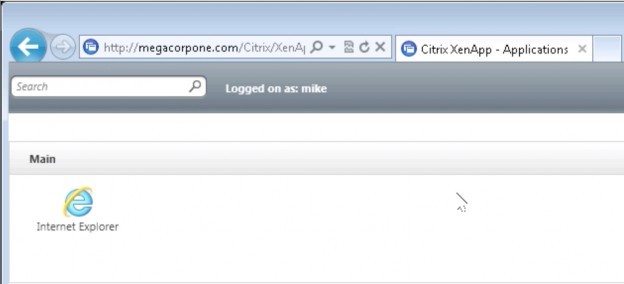
1. <http://http-tunnel.sourceforge.net/>



**Figura 25 – Comprometimento da rede MegaCorp One atingiu a sub-rede de gerenciamento de rede.**

## Compromisso do Ambiente Citrix

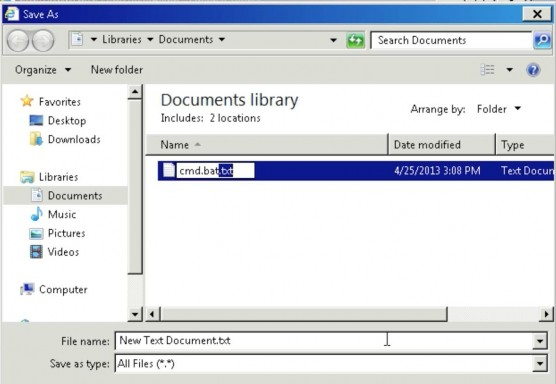
Usando o acesso remoto da área de trabalho à rede interna, passamos a explorar a rede em busca de alvos de alto valor. Um desses alvos parecia ser um servidor Citrix, que foi definido como a página inicial do host comprometido. Usando as mesmas credenciais que foram utilizadas para estabelecer a conexão de área de trabalho remota, conseguimos fazer login com sucesso neste ambiente Citrix.



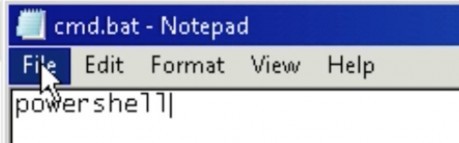
**Figura 26 – Um servidor Citrix que oferecia apenas o Internet Explorer foi descoberto na rede MegaCorp One.**

Esse ambiente Citrix expôs o “Internet Explorer” como o único aplicativo disponível. Esse é um método comumente utilizado por muitas organizações para limitar o acesso ao sistema operacional subjacente do servidor Citrix. É importante observar que existem muitos métodos para contornar essa configuração. Nesse caso, utilizamos a janela de diálogo “Salvar” para criar um arquivo em lote que nos forneceria uma interface Powershell.

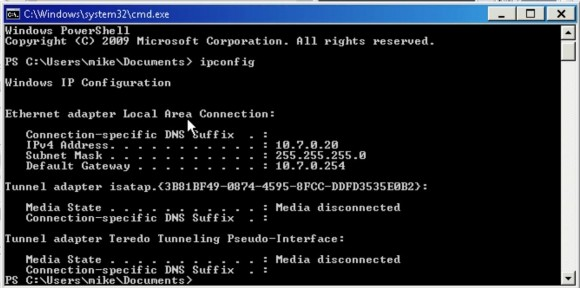
Isso é possível porque a caixa de diálogo "Salvar" funciona da mesma maneira que uma janela padrão de gerenciamento de arquivos "Windows Explorer".



**Figura 27 – Usando a caixa de diálogo Salvar, é possível contornar algumas restrições impostas pelo ambiente Citrix.**

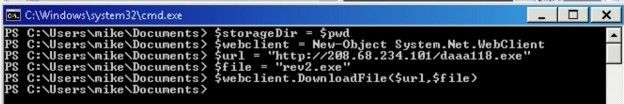


**Figura 28 – Um arquivo em lote invocando o aplicativo Powershell é criado no servidor Citrix.**



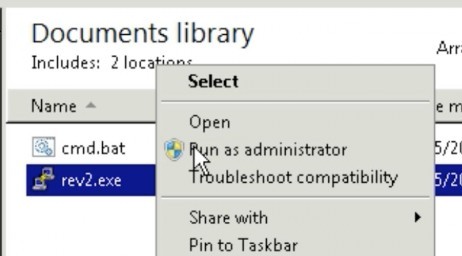
**Figura 29 – A restrição Citrix é ignorada resultando na execução do Powershell.**

A capacidade de usar o Powershell foi então utilizada para baixar uma carga maliciosa, que nos forneceria uma sessão de medidor para o servidor Citrix subjacente.

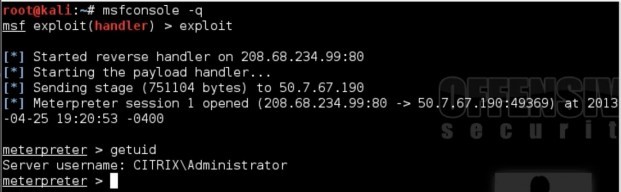


**Figura 30 - A funcionalidade do Powershell permite que um usuário ﬁnal recupere arquivos de fontes arbitrárias, incluindo locais remotos da Internet.**

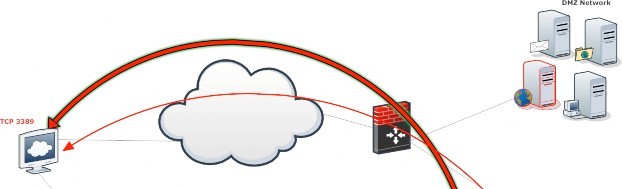
A capacidade de utilizar a caixa de diálogo “Salvar” para executar programas executáveis arbitrários foi combinada com a senha de administrador local descoberta anteriormente, permitindo-nos executar programas no contexto do administrador local. Isso nos permitiu obter controle administrativo total do sistema Citrix. Consulte o Apêndice A para obter mais informações.



**Figura 31 – A reutilização de senha permite que os invasores executem um executável malicioso com privilégios administrativos.**



**Figura 32 – O comprometimento completo do servidor Citrix é alcançado.**





**Figura 33 – Um host adicional na sub-rede de gerenciamento de rede foi comprometido.**

## Encaminhamento para administrador de domínio

Com o servidor Citrix comprometido, tentamos capturar senhas da memória. Um servidor Citrix é um candidato ideal para esse vetor de ataque, pois normalmente opera por longos períodos sem reinicializações e atende a um grande número de usuários.

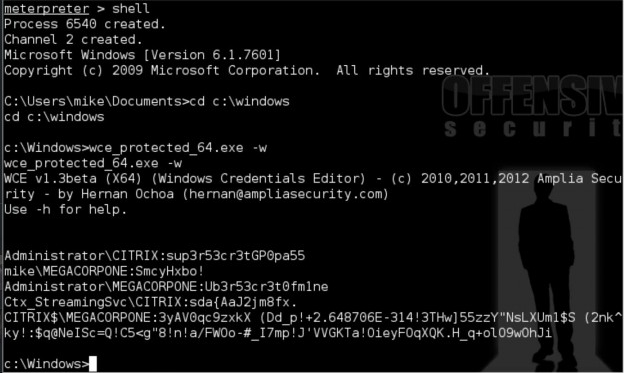
8

Para capturar senhas da memória, utilizamos a ferramenta Windows Credential Editor

rodar em sistemas de 64 bits sem causar efeitos adversos.

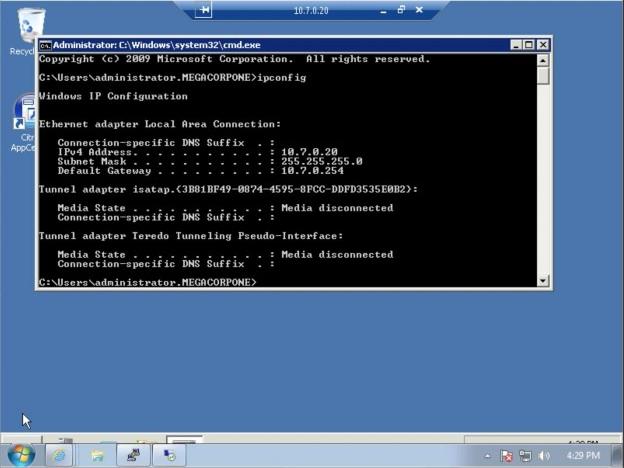
devido à sua capacidade de

1. <http://www.ampliasecurity.com/research/wcefaq.html>



**Figura 34 – O Windows Credentials Editor é usado para recuperar senhas de texto simples do servidor Citrix.**

Isso revelou várias senhas, incluindo uma conta de administrador de domínio do Windows. Consulte o Apêndice A para obter mais informações. Para validar as credenciais recém-recuperadas, criamos com sucesso uma nova sessão de área de trabalho remota para o servidor Citrix usando as credenciais do administrador do domínio.

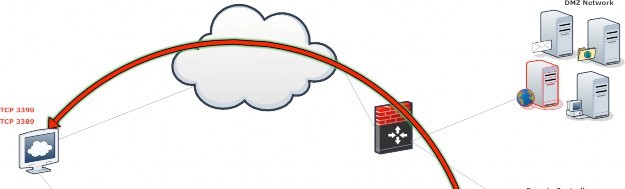


**Figura 35 - As credenciais do administrador de domínio são validadas em relação ao host Citrix.**

Neste ponto, o controle total do domínio do Windows foi obtido. Um invasor malicioso teria várias ferramentas à sua disposição, incluindo:

* Utilização da Diretiva de Grupo para implantar software backdoor em sistemas Windows.
* Exfiltração completa de todos os dados armazenados em qualquer sistema que use autenticação do Windows.
* Destruição de todo e qualquer recurso de rede.
* Ataques direcionados contra todo e qualquer funcionário da MegaCorp One, por meio do uso de ferramentas de coleta de informações, como keystroke loggers, para identificar informações pessoais.
* Aproveitando esse acesso sistêmico para realizar ataques contra fornecedores e parceiros da MegaCorp One que mantêm uma relação de confiança com a empresa.

Foi determinado que, embora essas etapas fossem possíveis, elas seriam consideradas fora do escopo do trabalho atual. Foi demonstrado que um comprometimento total do domínio MegaCorp One foi realizado com uma perda completa de integridade para todos os sistemas locais.





# Conclusão

**Figura 36 - Comprometimento total do domínio**

A MegaCorp One sofreu uma série de falhas de controle, o que levou ao comprometimento total dos ativos críticos da empresa. Essas falhas teriam um efeito dramático nas operações da MegaCorp One se uma parte mal-intencionada as explorasse. As políticas atuais relativas à reutilização de senhas e controles de acesso implantados não são adequadas para mitigar o impacto das vulnerabilidades descobertas.

Os objetivos específicos do teste de penetração foram declarados como:

* Identificando se um invasor remoto pode penetrar nas defesas da MegaCorp One
* Determinando o impacto de uma violação de segurança em:
  + Confidencialidade das informações da empresa
  + Infraestrutura interna e disponibilidade dos sistemas de informação da MegaCorp One

Esses objetivos do teste de penetração foram alcançados. Um ataque direcionado contra a MegaCorp One pode resultar em um comprometimento total dos ativos organizacionais. Vários problemas que normalmente seriam considerados menores foram aproveitados em conjunto, resultando em um comprometimento total dos sistemas de informação da MegaCorp One. É importante observar que esse colapso de toda a infraestrutura de segurança da MegaCorp One pode ser atribuído em grande parte a controles de acesso insuficientes nos limites da rede e nos níveis de host. Esforços apropriados devem ser realizados para introduzir segmentação de rede eficaz, o que pode ajudar a mitigar o efeito de falhas de segurança em cascata em toda a infraestrutura da MegaCorp One.

## Recomendações

Devido ao impacto para a organização geral, conforme descoberto por este teste de penetração, os recursos apropriados devem ser alocados para garantir que os esforços de remediação sejam realizados em tempo hábil. Embora uma lista abrangente de itens que devem ser implementados esteja além do escopo deste compromisso, alguns itens de alto nível são importantes de serem mencionados.

A Oﬀensive Security recomenda o seguinte:

* 1. **Certiﬁque-se de que credenciais fortes sejam usadas em todos os lugares da organização** . O comprometimento do sistema MegaCorp One foi drasticamente impactado pelo uso de senhas fracas, bem

9

como a reutilização de senhas em sistemas de diferentes níveis de segurança. O NIST SP 800-11 é

recomendado para diretrizes sobre como operar uma política de senha corporativa. Embora esse problema não tenha sido generalizado na MegaCorp One, ainda era um problema e deveria ser resolvido.

* 1. **Estabeleça limites de conﬁança** . Crie limites lógicos de confiança quando apropriado na rede interna. Cada segmento de confiança lógico deve poder ser comprometido sem que a violação se espalhe facilmente para outros segmentos. Isso deve incluir o uso de contas administrativas exclusivas para que um sistema comprometido em um segmento não possa ser usado em outros locais.
  2. **Implemente e imponha a implementação do controle de alterações em todos os sistemas** : problemas de configuração incorreta e implantação insegura foram descobertos em vários sistemas. As vulnerabilidades que surgiram podem ser mitigadas por meio do uso de processos de controle de alterações em todos os sistemas de servidor.
  3. **Implemente um programa de gerenciamento de patches** : A operação de um programa consistente de

10

gerenciamento de patches de acordo com as diretrizes descritas no NIST SP 800-40 é um componente

importante para manter uma boa postura de segurança. Isso ajudará a limitar a superfície de ataque resultante da execução de serviços internos não corrigidos.

* 1. **Conduza avaliações regulares de vulnerabilidade** . Como parte de uma estratégia de gerenciamento de risco organizacional eficaz, as avaliações de vulnerabilidade devem ser realizadas regularmente. Isso permitirá que a organização determine se os controles de segurança instalados estão devidamente instalados, operando

11

conforme o esperado e produzindo o resultado desejado. Consulte o NIST SP 800-30

sobre como operar um programa de gerenciamento de risco eficaz.

para obter orientações

1. <http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>

10 <http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf>

11 <http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-30-Rev.%201>

## Classificação de risco

O risco geral identificado para a MegaCorp One como resultado do teste de penetração é **Alto .** Foi descoberto um caminho direto do invasor externo para o comprometimento total do sistema. É razoável acreditar que uma entidade maliciosa seria capaz de executar com sucesso um ataque contra a MegaCorp One por meio de ataques direcionados.

# Apêndice A: Detalhe e mitigação da vulnerabilidade

## Escala de Classificação de Risco

De acordo com o NIST SP 800-30, as vulnerabilidades exploradas são classificadas com base na probabilidade e no impacto para determinar o risco geral.

## Credenciais padrão ou fracas

### Avaliação: Alto

**Descrição:** Uma interface administrativa exposta externamente só é protegida com um senha.

**Impacto:** Usando técnicas comuns de enumeração e força bruta, é possível recuperar a senha administrativa para a interface da Web do SQLite Manager. Devido à falta de mecanismos de autenticação adicionais, também é possível recuperar todos os hashes de senha do usuário no banco de dados subjacente. A recuperação bem-sucedida de senhas de texto simples pode permitir um comprometimento ainda maior do destino

ambiente se a reutilização de senha for encontrada.

**Remediação:** Garanta que todas as interfaces administrativas estejam protegidas com senhas complexas

ou senhas. Evite o uso de palavras comuns ou relacionadas a negócios, que podem ser encontradas ou facilmente construídas com a ajuda de um dicionário.

## Reutilização de senha

### Avaliação: Alto

**Descrição:** MegaCorp One usuário " **mike** " foi encontrado para reutilizar credenciais para o SQLite

Aplicativo Manager e seu acesso ao domínio Windows.

**Impacto:** A reutilização de senhas em geral é uma prática que deve ser altamente desencorajada e evitada na medida do possível. Nesse caso, o impacto da vulnerabilidade é amplificado pelo fato de um invasor externo ter comprometido indiretamente um conjunto válido de credenciais de domínio interno do Windows. Este compromisso permite potencialmente um

aumento substancial na superfície de ataque.

**Remediação:** Atualize as políticas de gerenciamento de senhas para impor o uso de senhas fortes e exclusivas para todos os serviços diferentes. O uso de gerenciadores de senhas deve ser incentivado para permitir mais facilmente que os funcionários utilizem senhas exclusivas em todos os

os vários sistemas.

## Senha de administrador local compartilhada

### Avaliação: Alto

**Descrição:** Vários hosts MegaCorp One são provisionados com o mesmo local senha do administrador.

**Impacto:** O MegaCorp One usa uma Diretiva de Grupo para definir uma senha de administrador local em todos os hosts dentro do escopo do GPO. Usar a mesma senha de administrador local em sistemas corporativos permite que um invasor com acesso apropriado utilize o conhecido vetor de ataque “pass-the-hash”. Ele permite que um invasor se autentique com sucesso em todos os hosts que compartilham a mesma senha, usando apenas o hash de senha recuperado.

Como tal, o ataque não depende da descriptografia bem-sucedida do hash e aumenta significativamente a pegada de violação de segurança.

**Remediação:** É altamente recomendável desabilitar todas as contas de administrador local. Nos casos em que uma conta administrativa local é necessária, deve ser atribuído a ela um único

nome e uma senha aleatória complexa.

## Gerenciamento de patches

### Avaliação: Alto

**Descrição:** Os ambientes externos e internos da MegaCorp One contêm uma série de sistemas e aplicativos não corrigidos.

**Impacto:** Uma combinação de autenticação fraca e hosts não corrigidos, que contêm vulnerabilidades conhecidas com exploits publicamente disponíveis, permite que um invasor obtenha acesso não autorizado a um grande número de ativos da MegaCorp One. Especificamente, a instância descoberta do SQLite Manager é vulnerável a uma vulnerabilidade de execução remota de código e o host subjacente também contém uma vulnerabilidade de escalonamento de privilégio local, que pode ser facilmente aproveitada para comprometer totalmente o host exposto externamente. Isso parece ser uma indicação de um patch insuficiente política de gestão e sua implementação.

**Remediação:** Todos os ativos corporativos devem ser mantidos atualizados com os patches de

segurança mais recentes fornecidos pelo fornecedor. Isso pode ser feito com ferramentas nativas do fornecedor ou aplicativos de terceiros, que podem fornecer uma visão geral de todos os patches ausentes. Em muitos casos, ferramentas de terceiros também podem ser usadas para implantação de patches em um

ambiente heterogêneo.

## Transferência de zona DNS

### Avaliação: Baixo

**Descrição:** Um servidor DNS mal configurado permite transferências de zona irrestritas.

**Impacto:** Um servidor DNS, configurado para permitir transferências de zona para qualquer servidor DNS, pode

fornecer informações confidenciais sobre ativos corporativos e layouts de rede.

**Remediação:** As transferências de zona DNS devem ser restritas apenas a servidores pré- aprovados.

## Arquivos padrão do Apache

### Avaliação: Baixo

**Descrição:** Os arquivos padrão do Apache foram descobertos no host

### admin.megacorpone.com .

**Impacto:** Um invasor pode adivinhar a versão exata do servidor Apache em execução inspecionando o conteúdo dos arquivos padrão. Informações confidenciais adicionais

também pode estar disponível.

**Remediação:** Remova todos os arquivos padrão de servidores da Web acessíveis publicamente.

# Apêndice B: Sobre Segurança Ofensiva

A Oﬀensive Security defende testes de penetração para impacto em oposição a testes de penetração para cobertura. O teste de penetração para cobertura ganhou popularidade nos últimos anos como um método simplificado de avaliação usado em situações em que o objetivo é atender às necessidades regulatórias. Como uma forma de verificação de vulnerabilidade, o teste de penetração para cobertura inclui a verificação seletiva de problemas descobertos por meio da exploração. Isso permite que os provedores de serviços realizem o trabalho em grande parte por meio do uso de conjuntos de ferramentas automatizados e mantenham a consistência do produto em vários compromissos.

O teste de penetração para impacto é uma forma de simulação de ataque sob condições controladas, que imita de perto o mundo real, ataques direcionados que as organizações enfrentam no dia-a-dia. O teste de penetração para impacto é uma avaliação baseada em metas, que cria mais do que um simples inventário de vulnerabilidades, fornecendo o verdadeiro impacto comercial de uma violação. Um teste de penetração baseado em impacto identifica áreas de melhoria que resultarão na maior taxa de retorno para o negócio.

O teste de penetração para impacto apresenta o desafio de exigir um alto conjunto de habilidades para ser concluído com sucesso. Conforme demonstrado neste relatório de amostra, a Oﬀensive Security acredita que está qualificada exclusivamente para fornecer resultados de classe mundial ao realizar testes de penetração para impacto, devido ao nível de experiência encontrado em nossa equipe de profissionais de segurança. A Oﬀensive Security não mantém uma equipe separada para testes de penetração e outras atividades nas quais a empresa está envolvida. , autores de livros mais vendidos, criadores de exploits de 0 dia,

A Oﬀensive Security oferece um produto que não pode ser igualado no mercado. No entanto, podemos não ser o ajuste certo para cada trabalho. A Oﬀensive Security normalmente realiza serviços de consultoria com baixo volume e

alta proporção de habilidades para permitir que a equipe da Oﬀensive Security imite mais de perto as situações do mundo real. Isso também permite que os clientes tenham maior acesso a conhecimentos reconhecidos no setor, mantendo os custos razoáveis. Como tal, compromissos de alto volume/retorno rápido geralmente não são uma boa opção para nossos serviços. A Oﬀensive Security está focada na realização de avaliações de alta qualidade e alto impacto e é ativamente procurada por clientes que precisam de serviços que não podem ser fornecidos por outros fornecedores.

[Se você gostaria de discutir suas necessidades de teste de penetração, entre em contato conosco em](mailto:info@offsec.com) info@oﬀsec.com

.