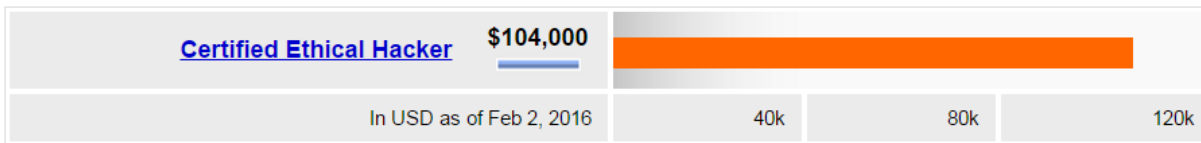


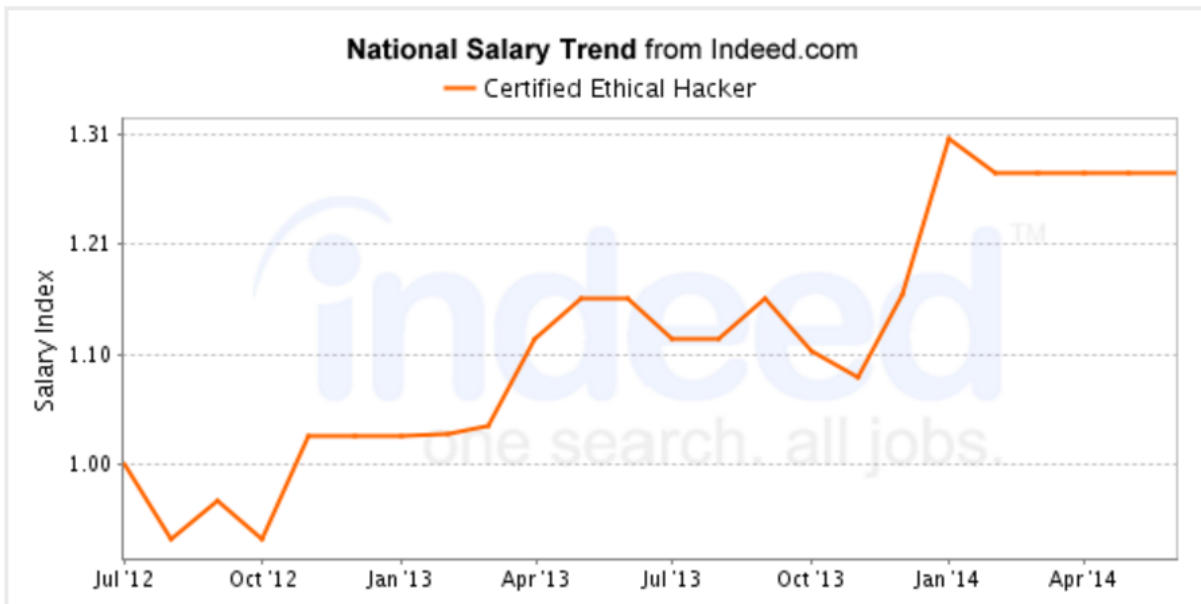


# Profissional Hacker Ético

Marcos Flávio Araújo Assunção  
Fundamentos de Ethical Hacking



Average Certified Ethical Hacker salaries for job postings nationwide are 81% higher than average salaries for all job postings nationwide.



Fonte: indeed.com





Para:

► [Jornalista](#)

Sobre:

► [Cidadania](#)

► [Ciência e Tecnologia](#)

## Ministério da Ciência, Tecnologia e Inovação convida movimento hacker para projeto de transparência

🕒 06/09/2011 17:07 - Portal Brasil

Uma iniciativa para aumentar o acesso às informações do Ministério da Ciência, Tecnologia e Inovação (MCTI) foi apresentada pelo ministro Aloizio Mercadante ao o movimento Transparência Hacker, a Plataforma Aquarius. Na reunião, o ministro convidou os ativistas digitais a ajudar no aperfeiçoamento do projeto.



# Cresce a busca pelo 'hacker ético', o que protege empresas

Após onda de invasões na rede, instituições apostam na prevenção

Os ataques recentes de hackers a sites de importância para a estratégia nacional — como os do Instituto Brasileiro de Geografia e Estatística (IBGE), do Ministério da Cultura e até da Presidência da República — reacenderam o alerta nas empresas contra os crimes virtuais. Para combater a ação dos criminosos, começa, então, a ganhar destaque no país a figura do "hacker ético" (ou *white hat hackers*, da expressão em inglês).

Os problemas de segurança, dizem os especialistas, tendem a tomar nova importância com as práticas de compu-

rus para proteger as empresas de ataques via internet, recrutou uma equipe de hackers de alto nível para descobrir formas de invadir equipamentos.

— A necessidade de verificação da própria segurança na rede aumentou muito nestes últimos anos. O mercado já percebeu a importância deste tipo de profissional — diz Bruno Salgado Guimarães, diretor-executivo da Clavis Segurança da Informação, que surgiu dentro do Departamento de Segu-

rança da Universidade Federal do Rio de Janeiro (UFRJ).

— É necessário garantir a segurança não só da página na web, mas também do cliente. Temos uma responsabilidade enorme nas mãos — diz Flávio Osso, diretor-executivo da WEBX, site especializado em e-commerce.

O analista de sistemas Diogo Mascarenhas explica por que foi contratado pela universidade Unisum para atuar como hacker ético:

— Um aluno hacker pode conseguir os dados de um professor e ter atitudes como trocar a própria nota para não ser reprovado. A manipulação de informações passa a ser fácil.

O mercado de trabalho para esses profissionais é maior em empresas como a Clavis, que trabalham no setor de segurança virtual. Seu trabalho é verificar a saúde de sistemas privados e tentar prever possíveis golpes na rede. A empresa também ministra treinamento para o público em geral.

## UMA PROFISSÃO EM ASCENSÃO

Formação, em tese, inclui graduação e certificações

Aneser de estar em cresci-





# As carreiras do futuro

Químico de alimentos, epidemiologista, hacker ético. Fobers revela lista com as profissões mais promissoras dos próximos anos



O Hacker ético é contratado para invadir sistemas de propósito para detectar problemas em medidas de segurança

FOTO: Thinkstock





# O papel do Hacker Ético

O que é um Penetration Test?



capacete destruído

Você usaria  
um produto  
que nunca foi  
testado na  
prática?





MULTICOLOR

capacete-moto

Teste de  
"stress" – Uma  
necessidade  
real







capacete  
Teste de  
"stress"  
Pressão

Teste de  
"stress"  
Temperatura



flame-test-helmet

# Penetration Test (Teste de Invasão)

## É a principal ferramenta de um Hacker Ético

Consiste em utilizar técnicas de Hackers em testes de stress da segurança de redes e sistemas

- Invadir para proteger
- Abordado pelo CEH (Certified Ethical Hacking)
- Uma **real** necessidade na atualidade.



# Níveis de um Pentester / Ethical Hacker

## Nível 1 – Júnior

### Tool based Penetration Tester:

Esse profissional é aquele que somente conhece as **ferramentas básicas para o pentest**, não sendo capaz de desenvolver suas próprias técnicas e ferramentas. Muitas vezes aprenderam as técnicas em treinamentos específicos. Esse é o nível exigido pela maioria das certificações de Pentest.

## Nível 2 - Pleno

### Coding based Penetration Tester:

Esse profissional é **aquele que desenvolve suas próprias ferramentas e scripts para a realização dos penetration tests**, mas ainda utiliza muitos recursos já “prontos” (como o **Metasploit**) para acelerar o processo de teste das vulnerabilidades. Necessita de conhecimentos pelo menos em **algoritmos e linguagens básicas de programação**.

## Nível 3 – Sênior

### Vulnerability Researcher:

Ao invés de realizarem PenTests, muitos hackers éticos com conhecimento mais avançado **preferem debugar o funcionamento de softwares e protocolos em busca de falhas do tipo 0-day**, e muitos são contratados por empresas com essa finalidade. O Google por exemplo costuma dar prêmios a quem descobre falhas no Chrome.





# Aspectos legais



## Artigo da “Lei Carolina Dieckmann”



Art. 154-A. Invadir **dispositivo informático alheio**, conectado ou não à rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de **obter, adulterar ou destruir dados** ou informações **sem autorização expressa ou tácita do titular do dispositivo** ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.



## Ataques de Denial of Service (Recusa de serviço)



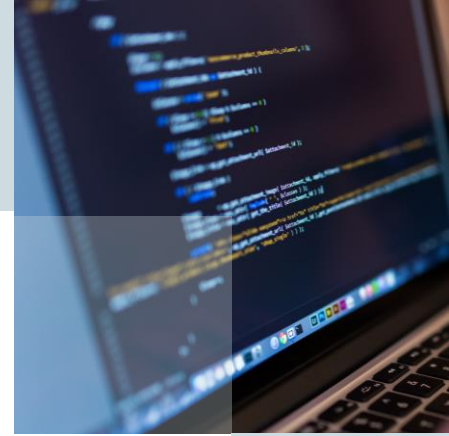
Art. 266.

§ 1º Incorre na mesma pena quem **interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.**



# Certificações de Ethical Hacking

# Certificações em Ethical Hacking / PenTest







# Tipos de Penetration Test

## BLACK BOX

Teste realizado em um sistema remoto, **sem nenhum conhecimento do alvo**. O invasor deve partir da estaca zero, sem informações sobre endereços IPs públicos, sistemas operacionais utilizados, tipos de roteadores e firewalls, etc. Esse teste visa demonstrar a visão de um atacante de fora da intranet da empresa.



## GRAY BOX

Teste realizado entre departamentos ou sub-redes de uma intranet, **com conhecimento parcial da estrutura**. O objetivo desse teste é demonstrar até que ponto um funcionário consegue chegar caso ele decida tentar acessar um sistema de outro departamento ao qual ele não tem acesso legítimo. Nesse tipo de PenTest, temos conhecimento parcial da rede, como a faixa de endereços IPs utilizada na sub-rede de origem, o endereço IP do gateway e do servidor DNS, etc.



## WHITE BOX

Teste realizado em uma intranet local, **com total conhecimento do alvo**. Nesse teste, temos o conhecimento total de como a rede opera, sabemos todos os dispositivos, endereços e sistemas operacionais utilizados. A visão de um teste White Box é a de um administrador de rede. Essa metodologia de testagem é utilizada quando desejamos conhecer até onde um administrador poderá ir caso deseje acessar dados ou obter informações, tais como conversar de MSN, senhas de usuários, e-mails alheios, etc.







# Fases de um Penetration Test



1

RECONHECIMENTO

2



VARREDURA

3



GANHANDO  
O ACESSO

4



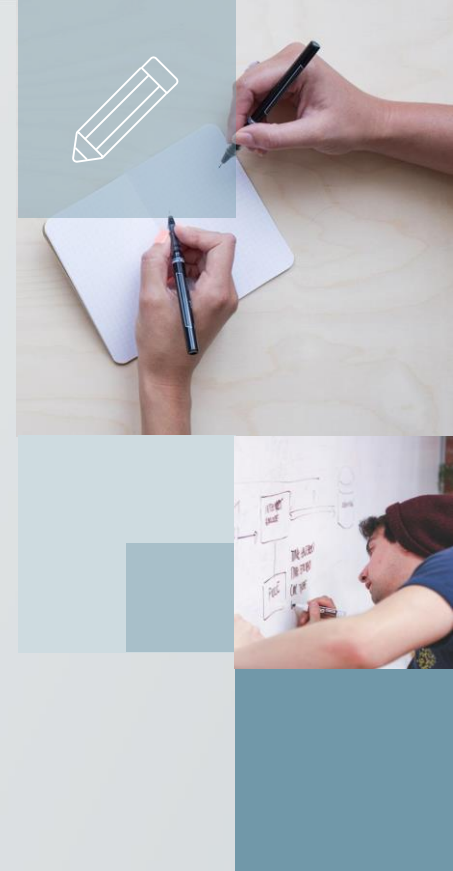
MANTENDO  
O ACESSO

5



COBRINDO  
RASTROS

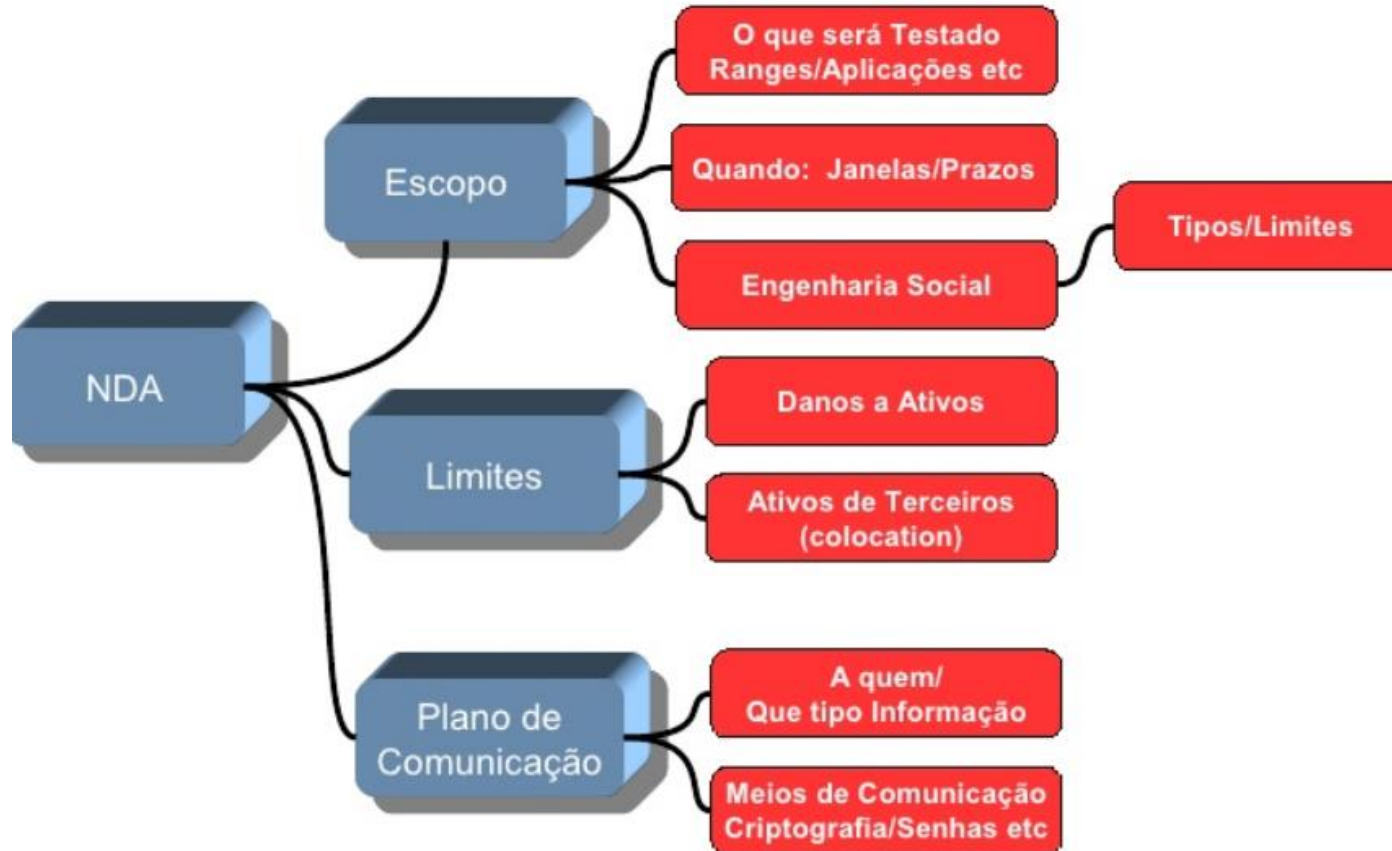
# Fases PENTEST



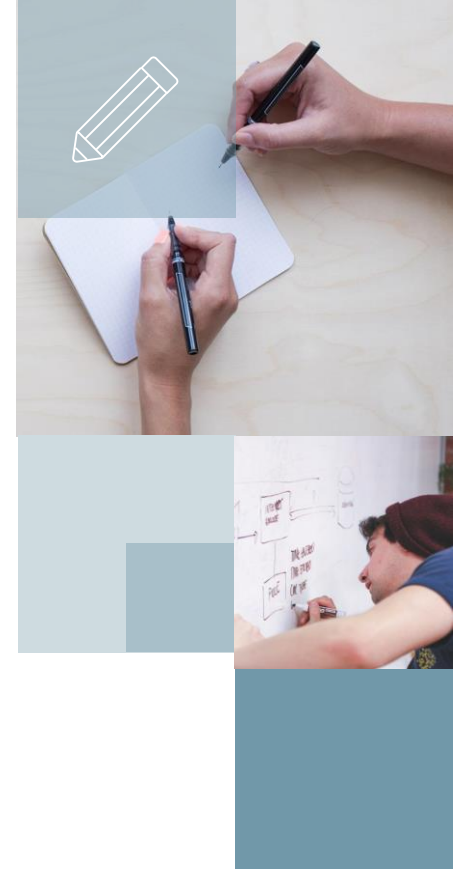


# Responsabilidade e confidencialidade

# NDA – Non Disclosure Agreement



*Mantenha artefatos comerciais, contratos etc separados do NDA*







# Relatório de um Penetration Test

# Tipos de relatório de Penetration Test

## Sumário executivo

Esse relatório é **preparado para os executivos da empresa**. Ele condensa todos os problemas de uma forma mais visual, utilizando gráficos e tabelas para sintetizar todas as vulnerabilidades detectadas e as sugestões para correção das mesmas. Não possui informações técnicas profundas.

## Relatório técnico

Esse relatório é **preparado para os profissionais de segurança da empresa**. Ele explica em detalhes todas as vulnerabilidades encontradas, mostrando tela a tela o resultado da exploração de cada problema, o impacto e uma sugestão de correção. É apresentado como se fosse um “tutorial” do que foi feito.



Mais informações  
em [www.pentest-standard.org](http://www.pentest-standard.org)

# Relatório PenTest – Sumário executivo

**Extreme**

13-15

- Extreme risk of security controls being compromised with the possibility of catastrophic financial losses occurring as a result

**High**

10-12

- High risk of security controls being compromised with the potential for significant financial losses occurring as a result

**Elevated**

7-9

- Elevated risk of security controls being compromised with the potential for material financial losses occurring as a result

**Moderate**

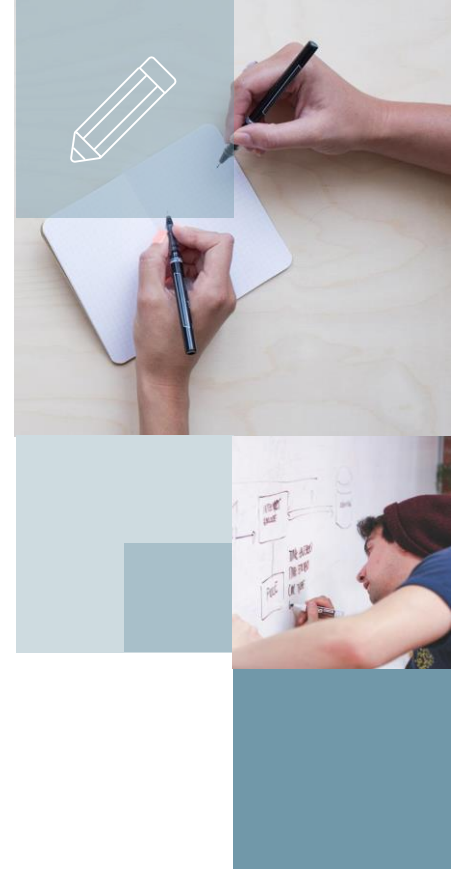
4-6

- Moderate risk of security controls being compromised with the possibility of limited financial losses occurring as a result

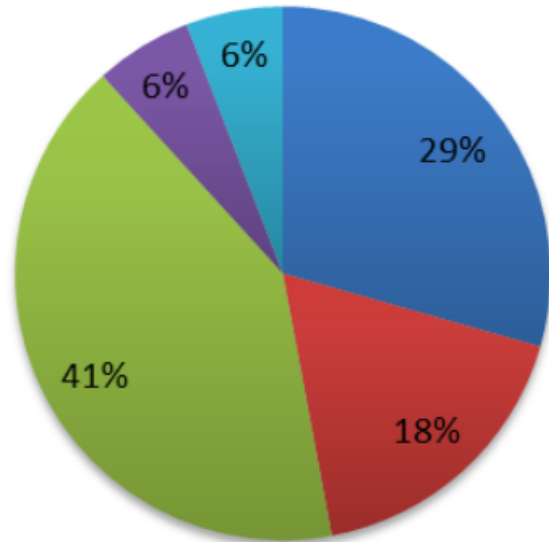
**Low**

1-3

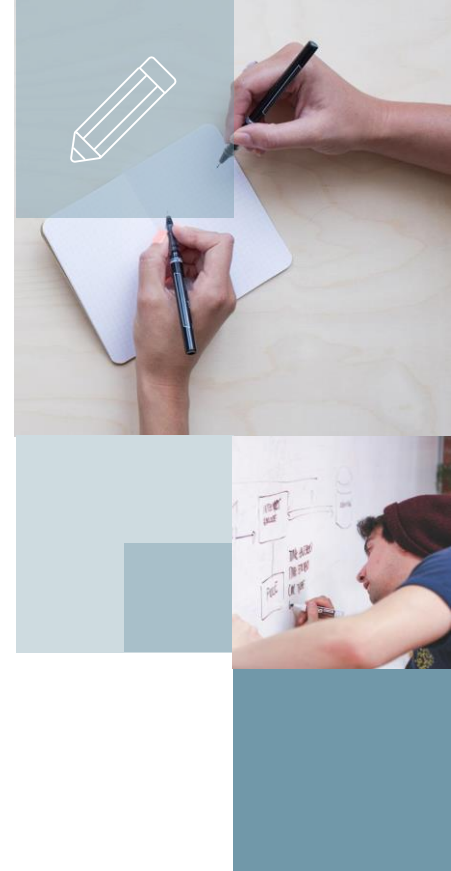
- Low risk of security controls being compromised with measurable negative impacts as a result



## Security Risk Origin/Category



- Missing Patch
- Lack of Application Hardening
- Lack of OS Hardening
- Easily guessable credentials
- Network Design Flaw



# Relatório PenTest – Sumário executivo

## One (1) to Three (3) Months

### Tasks

#### Create Remediation Strategy

- Leverage results found within the Penetration Test to create a full remediation strategy
- This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.

## Three (3) to Twelve (12) Months

### Tasks

#### Security Self Assessment

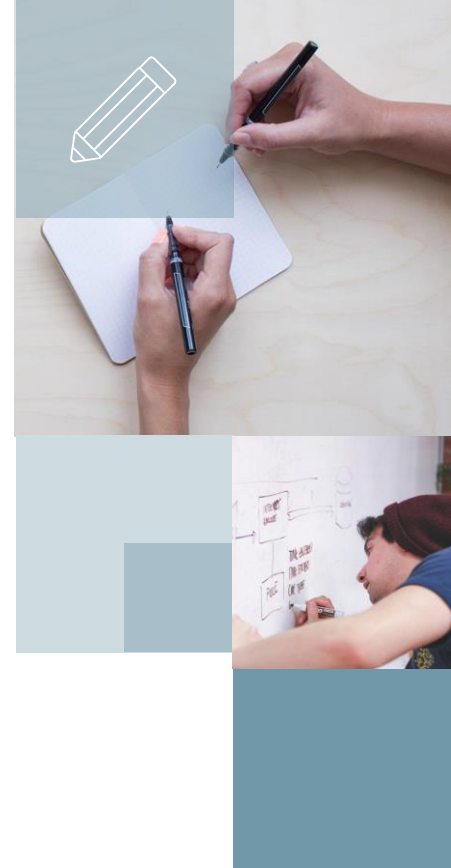
Adequate security of information and the systems that process it is a fundamental management responsibility. CLIENT officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for CLIENT officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. A good guide for this is **NIST SP 800-53a**, found at <http://csrc.nist.gov/publications/PubsDrafts.html>. Another approach would be to run the **Microsoft Security Assessment Tool** : found at <http://www.microsoft.com/technet/security/tools/msat/default.mspx>

## Twelve (12) Months+

### Tasks

#### Perform 3<sup>rd</sup> Party Assessment of Information Security and Compliance with 27001/2 (or any other compliance control set chosen).

- Perform a Corporate wide assessment of CLIENT's ability to defend against targeted & generic attacks
  - Identify the root cause of compliance gaps
  - Identify strategy for using the output of the assessment to facilitate a security baseline
- Begin remediation planning/budgeting

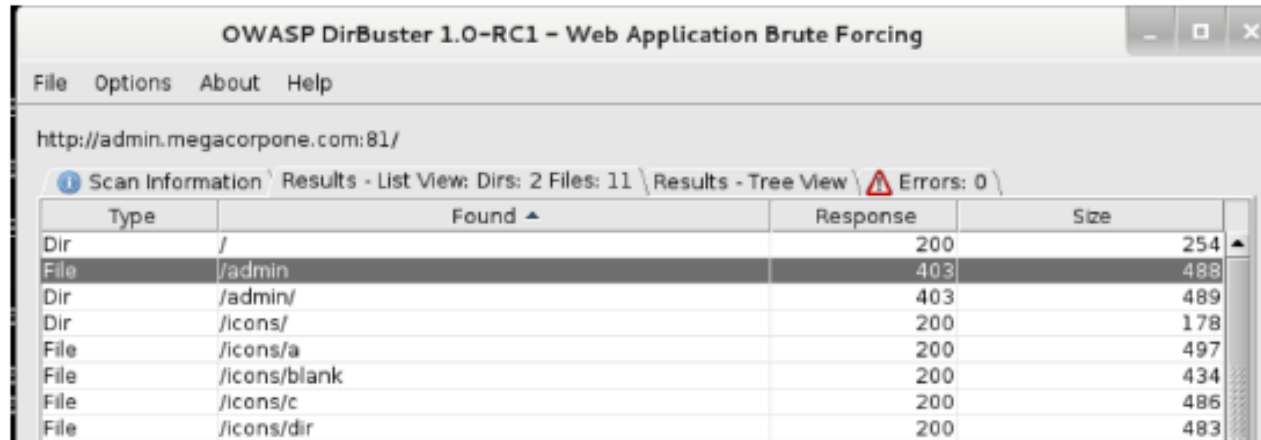




# Relatório PenTest – Relatório técnico

## Admin Webserver Interface Compromise

The `admin.megacorpone.com` webserver was found to be running an Apache webserver on port 81. Accessing the root URL of this site resulted in the display of a blank page. We next conducted a quick enumeration scan of the system looking for common directories and files (Figure 4).



Type	Found ▲	Response	Size
Dir	/	200	254
File	/admin	403	488
Dir	/admin/	403	489
Dir	/icons/	200	178
File	/icons/a	200	497
File	/icons/blank	200	434
File	/icons/c	200	486
File	/icons/dir	200	483

Figure 4 – Enumeration of the `admin.megacorpone.com` host partially discloses the webserver's folder structure.

The scan results revealed that along with common Apache default files (Please see Appendix A for more information), we identified an `"/admin"` directory that was only accessible after authentication. (Figure 5).



# Relatório PenTest – Relatório técnico

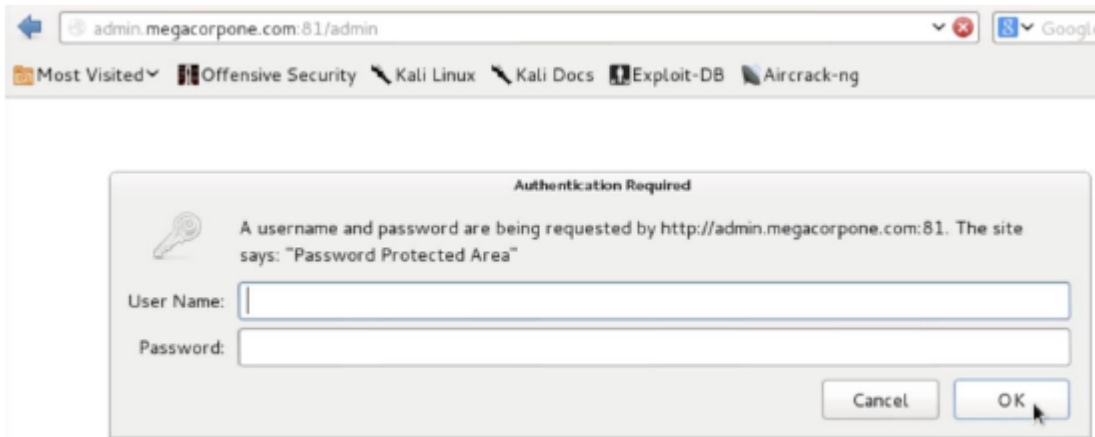


Figure 5 – Access to the “admin” folder is password-protected.

```
ACCOUNT CHECK: [http] Host: admin.megacorpone.com (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: assimilation1 (1020 of 16201 complete)
ACCOUNT CHECK: [http] Host: admin.megacorpone.com (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: created1 (1021 of 16201 complete)
ACCOUNT CHECK: [http] Host: admin.megacorpone.com (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: nanotechnology1 (1022 of 16201 complete)
ACCOUNT FOUND: [http] Host: admin.megacorpone.com User: admin Password: nanotechnology1 [SUCCESS]
root@kali:~#
```

Figure 6 – Using a custom word dictionary it is possible to discover the administrative password for the “admin” folder.

This brute-force attack uncovered a password of “nanotechnology1” for the admin user. We were able to leverage these credentials to successfully gain unauthorized access to the protected portion of the website (Figure 6). Please see Appendix A for more information on the exploited vulnerability.

