Iniciação Científica **CESUMAR**
Jul.Dez. 2005, Vol. 07, n.02, pp. 147 - 156

UM ESTUDO SOBRE OS MÉTODOS DE VARREDURA UTILIZADOS EM PORTSCANS

Fabrício Ricardo Lazilha[1]
Márcia Cristina Dadalto Pascutti[2]
Edson Yanaga[2]
Clayton Kendy Nakahara Passos[3]

RESUMO: É apresentado neste artigo um estudo feito diante da pilha de protocolos TCP/IP, afim de encontrar assinaturas de diversos métodos utilizados para detectar quais portas estão abertas em um determinado host. Para tanto, são utilizados duas ferramentas públicas, o Nmap e o Tcpdump. Desta forma foi possível captar e analisar diversos pacotes não convencionais, que são simplesmente ignorados pela maioria, por serem considerados meros erros causados pela própria rede. Esta análise é importante quando torna se necessário evitar que pessoas mal intencionadas adquiram informações sobre determinado host.

PALAVRAS-CHAVE: redes; segurança; varredor de portas; sistema de detecção de intrusos.

A STUDY ABOUT SCANNING METHODS USED IN PORTSCANS

ABSTRACT: É apresentado neste artigo um estudo feito diante da pilha de protocolos TCP/IP, afim de encontrar assinaturas de diversos métodos utilizados para detectar quais portas estão abertas em um determinado host. Para tanto, são utilizados duas ferramentas públicas, o Nmap e o Tcpdump. Desta forma foi possível captar e analisar diversos pacotes não convencionais, que são simplesmente ignorados pela maioria, por serem considerados meros erros causados pela própria rede. Esta análise é importante quando torna se necessário evitar que pessoas mal intencionadas adquiram informações sobre determinado host.

KEYWORKS: network; security; portscan; intrusion detection system.

INTRODUÇÃO

Na última estatística do NBSO (NIC BR Security Office), janeiro a março de 2004, é mostrado que de todos os tipos de ataques (externos), 49% deles são ataques de varreduras de portas. Este tipo de investida muitas vezes antecede uma real invasão de um sistema interligado à Internet. De posse desta informação fica claro a necessidade de bloquear a ação destes portscans (varredores de portas), não autorizados. Para tanto, deve se catalogar os métodos utilizados para realizar a varredura, afim de documentar e possibilitar a criação de uma ferramenta que identifique e bloqueie em tempo real, de acordo com as exigências do administrador de se-

[1] Orientador da Pesquisa. Docente do Curso de Processamento de Dados do CESUMAR
[2] Co-orientadores da Pesquisa. DocenteS do Curso de Processamento de Dados do CESUMAR
[3] Acadêmico do Curso de Processamento de Dados do CESUMAR, bolsista do Programa de Bolsas de Iniciação Científica do Cesumar (PROBIC)

gurança. Este estudo se faz necessário, pois, sem esta base é impossível desenvolver um "anti-portscan". A falta desta solução facilita a ação dos chamados crackers, cuja ação podem acabar em perda de dados, tempo e dinheiro.

O portscan ou varredor de portas é o processo de conectar a portas TCP ou UDP de um sistema - alvo, com o intuito de identificar a existência ou não de um serviço atrelado àquela porta. Ou seja, varrer uma porta é a arte de identificar, externamente, os serviços disponíveis para cada interface. Se tais serviços estiverem mal conFigurados ou com falhas de segurança, estes podem comprometer toda a rede deste sistema, permitindo a um usuário não autorizado ter acesso a informações restritas. Em boas mãos, os programas de varredura podem simplificar o trabalho de um administrador de segurança. Em mãos irresponsáveis, estes programas podem tornar-se uma ameaça legitima. (ANÔNIMO, 2000)

Inicialmente os varredores de portas eram ferramentas de poucos e utilizada pelos administradores no intuito de visualizar os serviços de sua rede. Isto é, através de um varredor de portas em uma de suas maquinas, o administrador era capaz de descobrir quais eram as portas que sua máquina disponibilizava para o resto da rede. (FREISS, 1998)

Com o advento da Internet e do conceito de rede pública, o varredor de portas popularizou-se, desde então adolescentes e curiosos apontam seus varredores para determinado alvo e após alguns minutos tem-se um relatório de todas as "portas abertas". Este era o objetivo principal do varredor de portas chamado SATAN (D.Farmer e W.Wenema), um dos primeiros a se popularizar. (FREISS, 1998).

Também conhecido como detect-scan, o anti-portscan tem o papel de evitar que pessoas estranhas conheçam quais serviços seus servidores disponibilizam. Para isto coloca-se escuta em portas TCP e/ou UDP especificas, quando é detectado algo semelhante a um varredor é possível executar diversas funções, tais como: gravar um registro de log; bloquear ou executar comandos externos pré-estabelecidos. Mas então pode surgir a seguinte dúvida: Monitorando as portas, como distinguir a ação de um varredor de portas de uma conexão válidas?

Levando em conta que um varredor de portas está sendo direcionado a um determinado IP, como autor não tem nenhuma informação sobre o alvo ele irá selecionar um grande intervalo de portas, dentre as quais estarão com certeza algumas que não disponibilizam nenhum serviço, é neste ponto que se consegue descobrir a ação destes varredores, pois o nosso anti-varredor-de-portas escuta apenas portas que não rodam serviços válidos. (MCCLURE, 2000).

Outra técnica utilizada por alguns anti-varredor-de-portas, consiste em monitorar portas mesmo com serviços válidos, diferenciando uma conexão válida do varredor pelo tempo de conexões em portas diferentes, vindas de um mesmo endereço

Para o bom entendimento do funcionamento destes programas de varreduras de portas faz-se necessário o conhecimento da pilha de protocolos TCP/IP, principalmente a camada de transporte e seus protocolos TCP e UDP. (WILLSEY)

Este artigo está organizado da seguinte forma: a seção 2 apresenta as ferramentas utilizadas neste estudo. A seção 3 descreve os tipos de varreduras existentes. A seção 4 descreve o funcionamento de uma das técnicas utilizadas para implementar uma varredura de portas distribuída. A seção 5 apresenta possíveis soluções. Por fim, na seção 6 são apresentadas as conclusões.

1. FERRAMENTAS UTILIZADAS

Para o levantamento das informações foi utilizado o Sistema Operacional Linux, juntamente com o programa Nmap, utilizado para gerar as assinaturas durante a análise dos pacotes TCP/IP. Este programa é um dos mais populares varredores de portas, e pode ser adquirido em http://www.insecure.org/nmap. Outra ferramenta não menos importante é o Tcpdump, utilizado para coletar dados em nossa rede, decifrar os bits e exibir a saída de uma maneira mais amigável.

1.1. NMAP

Nmap é um programa que permite aos administradores de sistemas e curiosos a explorar grandes redes para determinar quais computadores estão ativos e quais serviços são fornecidos. O Nmap, também oferece um número grande de características avançadas, que estão fora do contexto deste trabalho. (MCCLURE, 2000)

Segundo Dostoyevsky (DOSTOYEVSKY, 2000) o resultado da execução do Nmap é uma lista de portas, acompanhada do nome do serviço, o número, estado, e o protocolo das "portas bem conhecidas". O estado pode ser tanto aberto, filtrado ou não filtrado. Quando um estado é dito aberto, a máquina alvo aceita (accept()) conexões na porta. O estado filtrado significa que o firewall, filtro ou outro obstáculo da rede está cobrindo a porta e prevenindo o Nmap de determinar quando a porta está em estado aberto. Não filtrado é o estado em que a porta é conhecida pelo Nmap para estar fechada e nenhum firewall ou filtro parece estar interferindo na investigação do Nmap. Portas não filtradas são um caso comum e são mostradas, somente, quando a maioria das portas exploradas estão no estado filtrado.

1.2. TCPDUMP

O Tcpdump é um programa que, como próprio nome diz, mostra na tela os cabeçalhos dos pacotes que estão trafegando na rede e que satisfazem (operação boleana) as opções de comandos entradas pelo usuário. Vale lembrar que o "payload" ou os dados propriamente dito não serão mostrados pelo Tcpdump, visto que o mesmo foi programado para analisar somente os cabeçalhos dos pacotes IP, TCP, UDP, ICMP etc. Desenvolvido por Van Jacobson, Craig Leres e Steven McCanne. (JACOBSON, 2003 e BEJTLICH, 2003)

```
1) 16:11:51.567529 evil.1163 > vict.www-http: S
3659299645:3659299645(0) win 32767 <mss
16396,sackOK,timestamp 350860 0,nop,wscale 0> (DF)
[tos 0x10]

2) 16:11:51.567648 vict.www-http > evil.1163: S
3662367214:3662367214(0) ack 3659299646 win 32767
<mss 16396,sackOK,timestamp 350860
350860,nop,wscale 0> (DF)

3) 16:11:51.567748 evil.1163 > vict.www-http:. ack 1 win 32767
<nop,nop,timestamp 350860 350860> (DF) [tos 0x10]
```

Figura 1 – Apresenta o código de uma conexão TCP na porta 80 (http)

No exemplo da Figura 1 pode-se observar diversas informações geradas pelas partes envolvidas em um conexão TCP na porta 80, neste estudo, apenas alguns campos são necessários para a compreensão das análises feitas, tais informações serão simplificadas de acordo com a Figura 2:

```
evil -> SYN
vict -> SYN|ACK
evil -> ACK
```

Figura 2 – Apresenta as informações mais importantes

Da maneira exemplificada na Figura 2, pode-se observar melhor toda a transação, onde o host evil envia uma requisição de conexão (SYN), o host vict responde dizendo que recebeu sua requisição (ACK) e quer iniciar uma conexão com o host evil (SYN), então a conexão é estabelecida com o envio de uma confirmação do pedido de vict (ACK). Na seção 3 serão apresentadas as saídas completas geradas pelo Tcpdump em seguida de um resumo no mesmo formato da Figura 2.

Uma conexão TCP normal possui um ou mais flags definidos (POSTEL, 1981). Estas flags são utilizadas para indicar a finalidade da conexão, o Tcpdump representa estas flags como mostra a tabela 1:

Tabela 1 – Equivalência entre o nome das flags e suas representações no Tcpdump

Flag TCP	Representação no Tcpdump
SYN	S
ACK	Ack
FIN	F
RESET	R
PUSH	P
URGENT	Urg

Nas saídas do Tcpdump pode-se encontrar um marcador de lugar (um ponto "**.**") indicando a falta das flags, SYN, FIN, RESET ou PUSH. (JACOBSON, 2003)

2. CLASSIFICAÇÃO VARREDURAS DE PORTAS

Foram feitos vários testes em ataques simulados e obtiveram-se várias assinaturas das principais formas de varredura de portas executadas pelo Nmap.

Existem três métodos utilizados para efetuar a varredora de portas: os de conexão completa (open scanning); os de meia conexão (half-open scanning); e os stealth (stealth scanning). (ARKIN , 2003)

2.1. Open Scan

As técnicas pertencentes a este grupo são fáceis de detectar e filtrar, pois envolve uma conexão completa, tipicamente conhecida como "three way handshake". A seção 3.1.1 descreve um exemplo de varredura de portas do tipo TCP Connect, capturado pelo Tcpdump e gerado pelo Nmap. (NORTHCUTT, 2001)

2.1.1. TCP connect

Esta é a mais básica forma de TCP scanning. Esta técnica utiliza-se de chamadas de sistema, connect(), provida pelo seu sistema operacional para abrir uma conexão com todas as portas

interessadas. Se a porta estiver esperando por uma conexão, connect() irá ter sucesso. A maior vantagem desta técnica é que não é necessário nenhum privilégio especial. Qualquer usuário está livre para usar esta chamada. (DOSTOYEVSKY, 2003).

Este tipo de varredura de portas é facilmente detectável além de gerar log no host alvo, o qual mostrará um grupo de conexões e mensagens de erro. O TCP connect é mais rápido dentre todo os métodos, porem, o mais fácil de detectar, pois envolve uma conexão completa, utilizando um típico "three way handshake" que é "logado" pelos "daemons".

No próximo exemplo esta técnica é disparada sobre a porta 21 do computador chamado vict utilizando a seguinte linha de comando:

nmap -sT localhost -p 21

Com este comando será realizado uma varredura na porta 21 utilizando a técnica chamada de "TCP connect", caso a porta 21 esteja aberta obtém -se uma assinatura semelhante ao da Figura 3:

1) 16:02:40.671179 evil > vict: icmp: echo request

2) 16:02:40.671287 vict > evil: icmp: echo replv

3) 16:02:40.672007 evil.60713 > vict.www-http: . ack 1086941624 win 1024

4)16:02:40.672079 vict.www-http > evil.60713: R 1086941624:1086941624(0) win 0 (DF)

5)16:02:40.985319 evil.1159 > vict.ftp: S 3083896052:3083896052(0) win 32767 <mss 16396,sackOK,timestamp 295802 0,nop,wscale 0> (DF)

6)16:02:40.985429 vict.ftp > evil.1159: S 3075970073:3075970073(0) ack 3083896053 win 32767 <mss 16396,sackOK,timestamp 295802 295802,nop,wscale 0> (DF)

7) 16:02:40.985518 evil.1159 > vict.ftp: . ack 1 win 32767 <nop,nop,timestamp 295802 295802> (DF)

Figura 3 – Assinatura de uma varredura de portas do tipo TCP Connect, com a porta 21 aberta

A Figura 3 mostra a saída do Tcpdump diante desta varredura de portas. Desconsidere os números em negrito, pois estes servem apenas para enumerar as diversas linhas.

Analisando a saída do Tcpdump encontra-se nas linhas um e dois um pacote ICMP fazendo um echo request e a estação vict fazendo um reply, ou seja, está ocorrendo o famoso ping. O Nmap começa a varredura testando o host alvo com o ping para verificar se ele está "vivo", ou se o ICMP está sendo filtrado por um firewall. Em seguida (linha três e quatro) encontra-se uma tentativa frustrada de conexão na porta 80, este meio é utilizado pelo Nmap para ludibriar possíveis anti-varredores-de-portas. Hoje este meio não é mais tão eficiente como antes. Somente nas linhas seis, sete e oito é que começa realmente a varredura de portas. Observe ainda que está é uma conexão completa na porta 21(ftp).

Simplificando a saída do Tcpdump acima, encontra-se exatamente as mesmas "flags" envolvidas em uma conexão TCP à porta 80 exemplificada na seção 2.2, a única diferença aqui é que a conexão é feita na porta 21, compare a Figura 1 com a Figura 3:´

evil -> SYN
vict -> SYN|ACK
evil -> ACK

Figura 5 – Assinatura de uma conexão à porta 21, gerada por uma varredura de portas do tipo TCP Connect

Caso a porta esteja fechada é encontrada a seguinte assinatura:

1) 16:10:34.497795 evil > vict: icmp: echo request

2) 16:10:34.497899 vict > evil: icmp: echo reply

3) 16:10:34.498511 evil.48203 > vict.www-http: . ack 1852692527 win 3072

4)16:10:34.498576 vict.www-http > evil.48203: R 1852692527:1852692527(0) win 0 (DF)

5) 16:10:34.807645 evil.iad3 > vict.ftp: S 2389699502:2389699502(0) win 32767 <mss 16396,sackOK,timestamp 294584 0,nop,wscale 0> (DF)

6) 16:10:34.807722 vict.ftp > evil.iad3: R 0:0(0) ack 2389699503 win 0 (DF)

Figura 6 – Assinatura de uma varredura de portas do tipo TCP Connect, com a porta 21 fechada

```
evil -> SYN
vict -> RST| ACK
```

Figura 7– Resumo da figura 6

Observe que a varredura ocorre nas linhas 5 e 6 da Figura 6, observe também que o host vict responde a tentativa de conexão com um RST e um ACK, onde a mensagem RST indica que a porta está fechada e o ACK confirma o recebimento do SYN enviado pelo host evil.

2.2 Half Open

Técnicas pertencentes a este grupo são chamadas de meia conexão por abortarem no meio o "Three Way Handshake" de uma conexão.

2.2.1 Syn Scan

O SYN Scan envia um pacote com a flag SYN, como se fosse abrir uma conexão real e é esperado pela resposta. Uma resposta SYN/ACK indica que a porta está no estado listening e a flag RST é uma indicação de estado não listening. Se o flag SYN/ACK é recebido, o flag RST é imediatamente enviado para encerrar a conexão (atualmente o núcleo do SO faz isso por nós). Desafortunadamente é necessário privilégio de super usuário para construir estes pacotes SYN customizados. (DOSTOYEVSKY, 2000).

A Figura 8 mostra a assinatura gerada pelo SYN Scan, utilizando o comando: nmap -sS vict -p 21

1) 16:08:39.245412 evil > vict: icmp: echo reques

2) 16:08:39.245528 vict > evil: icmp: echo reply

3) 16:08:39.246023 evil.34364 > vict.www-http: . ack 1152477231 win 4096

4) 16:08:39.246086 vict.www-http > evil.34364: R 1152477231:1152477231(0) win 0 (DF)

5) 16:08:39.555370 evil.34344 > vict.ftp: S 1448059797:1448059797(0) win 4096

6) 16:08:39.559571 vict.ftp > evil.34344: S 2270944276:2270944276(0) ack 1448059798 win 32767 <mss 16396> (DF)

7) 16:08:39.559631 evil.34344 > vict.ftp: R 1448059798:1448059798(0) win 0 (DF)

Figura 8 – Assinatura de uma varredura de portas utilizando a técnica SYN scan, com a porta 21 aberta

```
evil -> SYN
vict -> SYN|ACK
evil -> RST
```

Figura 9 – Resumo da figura 8

A Figura 10 ilustra a assinatura desta técnica no caso da porta 21 estar fechada.

1) 16:05:45.249565 evil > vict: icmp: echo request

2) 16:05:45.253823 vict > evil: icmp: echo reply

3) 16:05:45.256057 evil.34189 > vict.www-http: . ack 904563989 win 1024

4) 16:05:45.256145 vict.www-http > evil.34189: R 904563989:904563989(0) win 0 (DF)

5) 16:05:45.565043 evil.34169 > vict.ftp: S 397308297:397308297(0) win 1024

6) 16:05:45.565123 vict.ftp > evil.34169: R 0:0(0) ack 397308298 win 0 (DF)

Figura 10 – Assinatura de uma varredura de portas utilizando a técnica SYN scan, com a porta 21 fechada

```
evil -> SYN
vict -> RST| ACK
```

Figura 11– Resumo da figura 10

A varredura ocorre na linha cinco e seis, Uma atenção maior à linha seis deve ser dada pois é onde o host vict responde a tentativa de conexão com um RST e um ACK, onde o RST indica que a porta está fechada e o ACK confirma o recebimento do SYN enviado pelo host evil. Analisando mais atentamente, é possível observar que esta reação é exatamente igual ao do método "TCP connect". Onde a porta 21 encontra-se fechada.

2.3 Stealth Scan

Quando a técnica SYN Scan não é intrusiva o suficiente para passar desapercebido, podemos utilizar uma das técnicas descritas nas subseções abaixo.

Stealth FIN (Figura 12 e 14), Xmas Tree (Figura 20 e 22), ou Null Scan (Figura 16 e 18) são técnicas utilizadas para realizar a varredura de portas, onde vários firewalls e filtros de pacotes obser-

vam por pacotes contendo a mensagem syn direcionadas a portas restritas. (DOSTOYEVSKY, 2000).

O principio destas técnicas é que portas fechadas são exigidas por responder aos pacotes de teste com um RST, enquanto portas abertas precisam ignorar os pacotes em questão (POSTEL, 1981). Desafortunadamente a Microsoft (como usual) decidiu completamente ignorar o padrão e faz as coisas do seu próprio jeito. Então estas técnicas de varredura podem não funcionar contra sistemas executando Windows95/NT.

2.3.1 Fin Scan

A técnica chamada de FIN Scan utiliza o limitado pacote FIN como objeto de teste. (DOSTOYEVSKY, 2000). Observando a Figura 12 é possível verificar à assinatura de uma varredura obtendo a informação de que aporta 21 está aberta, na linha cinco o nmap envia a mensagem FIN, e na linha seis a vítima responde também com uma mensagem FIN. Este comportamento nunca deveria existir, afinal, não havia nenhuma comunicação anterior entre as partes envolvidas.

1) 16:22:03.289633 evil > vict: icmp: echo request

2) 16:22:03.289743 vict > evil: icmp: echo reply

3) 16:22:03.290376 evil.61823 > vict.www-http: . ack 877979370 win 3072

4) 16:22:03.290446 vict.www-http > evil.61823: R 877979370:877979370(0) win 0 (DF)

5) 16:22:03.599551 evil.61803 > vict.ftp: F 0:0(0) win 3072

6) 16:22:03.900829 evil.61804 > vict.ftp: F 0:0(0) win 3072

Figura 12 – Assinatura de uma varredura de portas utilizando a técnica FIN Scan, com a porta 21 aberta

evil -> FIN
evil -> FIN

Figura 13 – Resumo da figura 12

Caso a porta 21 esteja fechada, a vitima responde a esta técnica com uma mensagem de RESET (RST) como é exemplificado na Figura 14 e 15.

1) 16:21:35.980283 evil > vict: icmp: echo request

2) 16:21:35.980418 vict > evil: icmp: echo reply

3) 16:21:35.981083 evil.53060 > vict.www-http: . ack 4200874383 win 4096

4) 16:21:35.981155 vict.www-http > evil.53060: R 4200874383:4200874383(0) win 0 (DF)

5) 16:21:36.290331 evil.53040 > vict.ftp: F 0:0(0) win 4096

6) 16:21:36.290416 vict.ftp > evil.53040: R 0:0(0) ack 1 win 0 (DF)

Figura 14 – Assinatura de uma varredura de portas utilizando a técnica FIN Scan, com a porta 21 fechada

evil -> FIN
vict -> RST|ACK

Figura 15 – Resumo da figura 14

2.3.2 Null Sscan

Null Scan é emelhante ao FIN Scan, porém usa pacotes sem flag alguma para realizar o teste. Nas Figuras 16, 17, 18 e 19 é exemplificada toda a comunicação que ocorre durante as parte envolvidas em uma varredura de portas utilizando a técnica Null Scan. Na Figura 16 e 17 a porta 21 está aberta, enquanto que no exemplo da Figura 18 e 19 a porta está fechada. (DOSTOYEVSKY, 2003)

1) 16:34:34.142269 evil > vict: icmp: echo request

2) 16:34:34.142378 vict > evil: icmp: echo reply

3) 16:34:34.142988 evil.41447 > vict.www-http: . ack 4285663756 win 1024

4) 16:34:34.143091 vict.www-http > evil.41447: R 4285663756:4285663756(0) win 0 (DF)

5) 16:34:34.464644 evil.41427 > vict.ftp: . win 1024

6) 16:34:34.770841 evil.41428 > vict.ftp: . win 1024

Figura 16 – Assinatura de uma varredura de portas utilizando a técnica NULL Scan, com a porta 21 aberta

evil -> NULL (nenhuma flag)
evil -> NULL (nenhuma flag)

Figura 17 – Resumo da figura 14

1) 16:35:38.686467 evil > vict: icmp: echo reques

2) 16:35:38.686582 vict > evil: icmp: echo reply

3) 16:35:38.687213 evil.54543 > vict.www-http: . ack 2162260688 win 3072

4) 16:35:38.687281 vict.www-http > evil.54543: R 2162260688:2162260688(0) win 0 (DF)

5) 16:35:38.996464 evil.54523 > vict.ftp: . win 3072

6) 16:35:38.996545 vict.ftp > evil.54523: R 0:0(0) ack 0 win 0 (DF)

Figura 18 – Assinatura de uma varredura de portas utilizando a técnica NULL Scan, com a porta 21 fechada

evil -> NULL (nenhuma flag)
vict -> RST|ACK

Figura 19 – Resumo da figura 18

2.3.3 XMAS Scan

Varredura Xmas Tree. Da mesma forma que a varredura FIN, utiliza um pacote com um conjunto de flags mal formados com FIN, URG e PUSH como teste. (ARKIN, 2003)

1) 16:36:33.637350 evil > vict: icmp: echo request

2) 16:36:33.637465 vict > evil: icmp: echo reply

3) 16:36:33.638076 evil.40129 > vict.www-http: . ack 3649128894 win 2048

4)16:36:33.638145 vict.www-http > evil.40129: R 3649128894:3649128894(0) win 0 (DF)

5) 16:36:33.950285 evil.40109 > vict.ftp: FP 0:0(0) win 2048 urg 0

6) 16:36:34.260821 evil.40110 > vict.ftp: FP 0:0(0) win 2048 urg 0

Figura 20 – Assinatura de uma varredura de portas utilizando a técnica XMAS Scan, com a porta 21 aberta

evil -> XMAS (Todas as flags)

Figura 21 – Resumo da figura 20

Abaixo é exemplificada na Figura 22 uma varredura de portas utilizando a técnica Xmas Scan, porém neste caso a porta 21 está fechada.

1) 16:35:57.368850 evil > vict: icmp: echo request

2) 16:35:57.368968 vict > evil: icmp: echo reply

3) 16:35:57.369581 evil.53336 > vict.www-http: . ack 3409757699 win 1024

4) 16:35:57.369649 vict.www-http > evil.53336: R 3409757699:3409757699(0) win 0 (DF)

5) 16:35:57.678866 evil.53316 > vict.ftp: FP 0:0(0) win 1024 urg 0

6) 16:35:57.678944 vict.ftp > evil.53316: R 0:0(0) ack 1 win 0 (DF)

Figura 22 – Assinatura de uma varredura de portas utilizando a técnica XMAS Scan, com a porta 21 fechada

evil -> XMAS (Todas as flags)
vict -> RST

Figura 23 – Resumo da figura 22

3. VARREDURA DE PORTAS DISTRIBUIDA

Todas os métodos descritos até aqui podem ser utilizados em uma nova implementação, mesclando o conceito de varredura de portas com o conceito de sistema distribuído. Erroneamente muitos acreditam ser necessário acesso a diversos computadores para efetuar a varredura distribuída. Uma das técnicas que não se utiliza de diversos computadores vem correndo no "lado negro da internet", e vem sendo chamada de Varredura de portas ld (Port Scanning LD).

A varredura de portas ld, consiste em utilizar qualquer um dos métodos já descritos, em conjunto com técnicas chamadas de IP spoof e sniff. Com acesso a uma maquina da rede vitima, o atacante instala o sniffer e envia diversos pacotes com os endereços IP do resto da rede para seu alvo, com o sniffer consegue-se capturar a resposta do alvo aos computadores "spoofados".

"Com isto a regra mais utilizada por firewalls e ferramentas de segurança seria quebrada e com acesso a apenas um único computador o atacante poderia varrer as portas de qualquer rede sem problemas". (Autor conhecido na internet como: Jerry Slater).

4. SOLUÇÕES

Para usuários domésticos que utilizam o Sistema Operacional Linux (no qual este trabalho foi desenvolvido), o seguinte comando pode ser o suficiente para evitar problemas com os portscans baseados em pacotes que utilizam a flag syn:

/sbin/iptables -A INPUT -p tcp —syn -j DROP

Isto permite aos usuários executar todas as atividades normais de Internet. Permitirá navegar na Internet, conectar-se para fora usando o ssh, ou conversar com um colega usando o ICQ. Por outro lado, o mundo externo, quando tentar se conectar a seu computador Linux via TCP/IP será simplesmente ignorado.

Infelizmente, impedir que pessoas consigam conectar ao computador não impedirá a ação dos varredores de portas que utilizam os metidos stealth, afinal estes não utilizam a flag SYN para vasculhar todo o computador. O ideal seria construir um anti-varredor-de-portas que identifique a ação destes programas, isto é possível uma vez que temos as assinaturas dos métodos utilizados.

Analisando os pacotes recebidos, torna possível verificar de onde vem e para onde vai cada informação, de modo que seja possível encontrar um host enviando pacotes para várias portas diferentes em um intervalo de tempo muito pequeno, esta atividade pode ser considerada a de um varredor de portas, claro que se esta atividade estiver ocorrendo somente em portas válidas, ou seja, em portas que estão sendo oferecidos serviços, uma conexão válida pode ser confundida com a que queremos evitar. Para não haver confusão, deve-se determinar quais portas estão atualmente em uso e monitorar todas que não estão, de forma que se houver atividade em portas variadas em um intervalo de tempo pequeno, podemos considera-lo uma varredora de portas.

CONCLUSÃO

Nestas análises foram encontradas reações interessantes e curiosas sobre o comportamento do protocolo TCP, que levou a identificação de diversas assinaturas, ou seja, foram identificados e documentados diversos comportamentos que podem ser utilizados para a detectar e bloquear a ação de ferramentas como o Nmap.

Como foi possível observar, dezenas de "pacotes" não convencionais chegam aos servidores diariamente, sendo ignorados por muitos administradores por serem considerados erros causados pela própria rede. Hoje em dia tais pacotes são reconhecidos como tentativas de varredura de portas ou exploração de vulnerabilidades. Alguns tipos de varreduras de portas não são detectados e podem levantar as informações necessárias para uma futura invasão, sem nem mesmo deixar rastro. Por isto é necessário o desenvolvimento de uma ferramenta que possa detectar e possibilitar ao administrador agir de acordo.

Não basta apenas detectar uma simples assinatura, pois este método detecta apenas ataques já documentados (conhecidos), deve-se criar uma ferramenta que possa prevenir ataques ainda não existentes, isto só será possível com o auxílio da inteligência artificial. As assinaturas aqui estudadas podem ser utilizadas para "alimentar" tal sistema, ensinando o básico sobre varreduras de portas.

REFERÊNCIA

FREISS, M., Protecting Networks with SATAN. Ed. O'Reilly: 1998

MCCLURE, S., SCAMBRAY, J., GEORGE, K. **Hacker Expostos – Segredos e Soluções Para a Segurança de Redes.** São Paulo: Ed. Makron Books: 2000.

POSTEL, J., **Transmission Control Protocol - DARPA Internet Program Protocol Specification,** USC/Information Sciences Institute, RFC 793, September 1981.

NORTHCUTT, S., COOPER, M., FEARNOW, M., FREDERICK, K., **Intrusion Signatures and Analysis.** Indiana: Ed. New Riders: January 2001.

MANDIA, K., PROSISE, C. **Hackers Resposta e Contra-Ataque.** Rio de Janeiro: Ed. Campus: 2001.

COMER, D.E., **Interligação em Redes com TCP/IP,** Volume I, Princípio, protocolos e arquitetura

DOSTOYEVSKY, F., **Nmap network security scanner man page.** 2000

WILLSEY, B., CASAD, J., **Aprenda em 24horas TCP/IP**

ANÔNIMO, **Segurança Máxima – O guia de um hacker para proteger seu site na Internet e sua rede.** Rio de Janeiro: Ed. Campus: 2000.

ARKIN, O., **Network Scanning Techniques.** <http://www.sys-security.com/archive/papers/Network_Scanning_Techniques.pdf>. Acesso em 10, Agosto de 2003

STANIFORD, S., HOAGAND, J. A., McALERNEY, J. M., **Practical Automated Detection of Stealthy Portscans** <http://www.silicondefense.com/papers/Spice-JCS.pdf>. Acesso em 15, Agosto de 2003

DOSTOYEVSKY, F., **The Art of Port Scanning.** <http://www.phrack.org/phrack/51/P51-11>. Acesso em Outubro de 2003

BEJTLICH, R., **Interpreting Network Traffic: A Network Intrusion Detector's Look at Suspicious Event.** <http://www.taosecurity.com/intv2-8.pdf>. Acesso em 09, setembro de 2003

BEJTLICH, R., **Network Intrusion Detection of Third Party Effects.** <http://www.taosecurity.com/nid_3pe_v101.pdf>. Acesso em 15, setembro de 2003

NBSO (NIC BR Security Office), <http://www.nbso.nic.br/stats/incidentes/>. Acesso em abril de 2004

JACOBSON, V., LERES, C., MCCANNE, S., tcpdump - dump traffic on a network <http://www.tcpdump.org/tcpdump_man.html>. Acesso em Setembro de 2003