

基于虚拟网络的入侵防御系统实验设计与实现

曹雪峰, 尚宇辉, 傅冬颖

(河北民族师范学院 数学与计算机系, 河北 承德 067000)

摘要: 利用模拟软件 GNS3 中的 IPS 模拟器、VirtualBox 虚拟机以及 Nmap 软件的扫描功能, 设计了虚拟网络入侵防御系统的实验内容和实验方案, 实现了对利用 Nmap 发起的多种端口扫描方式入侵的防御仿真实验。验证了在虚拟网络环境下网络安全实验的可行性, 提高了学生综合运用网络安全技术的能力, 同时也加深了学生对相关理论知识的理解, 为网络安全实践教学提供了切实可行的解决方案。

关键词: 入侵防御系统; 网络安全; 虚拟网络

中图分类号: TP393.08; TP391.9 **文献标识码:** A **文章编号:** 1002-4956(2017)5-0109-06

Design and realization of intrusion prevention system based on virtual network

Cao Xuefeng, Shang Yuhui, Fu Dongying

(Department of Mathematics and Computer, Hebei Normal University for Nationalities, Chengde 067000, China)

Abstract: By using IPS simulator and VirtualBox virtual machine in the GNS3 and Nmap software scanning function, the experimental contents and experimental scheme were designed, the devices such as IPS, router, switch and virtual machine were configured. This paper realizes the intrusion prevention simulation experiment by using multiple port scanning methods initiated by Nmap. It proves the feasibility of network security experiment under the virtual network environment, improves the students' ability of using the network security technology synthetically, at the same time, it also deepens the understanding of theory knowledge and provides practical solution for network security practice teaching.

Key words: intrusion prevention system; network security; virtual network

随着信息技术的快速发展,网络服务越来越多地融入各行各业以及人们的日常生活中,计算机网络安全问题变得越来越重要。计算机网络安全课程是高校网络工程、通信工程和信息安全等专业的重要基础课程,网络安全实践教学在加深学生理解计算机网络安全理论、培养学生实践动手能力方面有重要作用。但在现实中,由于防火墙和入侵防御系统等实验教学设备价格昂贵,高校在实验室搭建网络安全实践环境存在一定困难^[1-2]。笔者利用开源的网络模拟软件 GNS3 上的 IPS 模拟器和 VirtualBox 虚拟机,开发了防御利用 Nmap 发起的端口扫描入侵的仿真实验^[3-5],

达到与真实设备同样的实验效果,弥补了由于实验设备缺乏而影响网络安全实践教学的缺憾。

1 入侵防御系统工作原理

入侵防御系统(intrusion prevention system, IPS)是指主动检测企图入侵或者正在入侵的行为,并且能够根据安全策略和通过一定的响应方式(如报警、丢弃、阻断等),实时监测和中断入侵行为的发生和发展,保护系统和网络不受攻击的安全体系^[6-7]。IPS 不仅具有防火墙拦截攻击和阻断攻击的能力,而且具有检测攻击行为的能力,是防火墙与入侵检测系统结合的产物。

入侵防御系统采用串联方式接入网络,侧重于主动防御,其目的是预先对入侵网络的数据流进行拦截,避免网络遭到破坏。当数据包从一个网络接口到达入侵防御系统后,按照包首部的信息进行分类,根据分类结果将数据包送往相应的过滤器中。过滤器利用协议分析、特征匹配、流量分析等技术对数据包进行深层检

收稿日期:2016-11-20

基金项目:国家民委高等教育教学改革研究项目(15114);河北省高等学校科学技术研究项目(ZC2016116);河北民族师范学院科研项目(201406)

作者简介:曹雪峰(1967—),男,河北隆化,硕士,副教授,主要研究方向为计算机网络技术。

E-mail: cxf_cd@163.com

测分析。分析结果按安全策略进行具体的防御响应,决定让数据包通过或丢弃。如果数据包符合过滤规则,则将数据包发送到的另一个网络接口,传送到网络中;如果数据包不符合过滤规则,含有入侵或攻击特征,则将该数据包丢弃,并将其相关的数据流状态更新,删除该数据流的信息,将同一数据流的后续数据包丢弃。

IPS 将策略和采取的防御措施提交给日志系统,将工作状态信息提交给管理控制台。管理员可以通过它了解系统的状态以及可能存在的入侵行为。

2 入侵防御系统实验设计

2.1 软件介绍

GNS3 是一款开源、免费的思科网络模拟软件^[8],适用于多种操作系统,能够仿真路由器、交换机、入侵防御、入侵检测和防火墙等设备,集成了 VirtualBox 和 VMware 虚拟机接口,配合虚拟机能够完成一些复杂网络环境的仿真配置,还可以利用 Wireshark 来捕获虚拟网络中通过的报文^[9],分析网络协议原理或者网络入侵、攻击过程。

Nmap 是一款开源、免费的网络发现和安全审计工具^[10],它包含 4 项基本功能:主机发现、端口扫描、应用与版本探测和操作系统探测。端口扫描是其核心的功能,提供了多种探测方式,包括 TCP SYN scanning、TCP connect 和 TCP FIN/Xmas/NULL scanning 等。另外 Nmap 还提供了多种规避防火墙与 IDS 的技巧,如分片、IP 诱骗和扫描延时等。

2.2 实验场景设计

思科 IPS 设备支持在线和杂合两种工作模式^[11-12]。

采用在线模式时,有 2 种流量转发方式——VLAN 对模式和接口对模式。在接口对模式中,数据包从接口对中的第一个接口进入,从接口对中的第二个接口出去。如果没有特征要拒绝或修改此数据包,它就会被发送到接口对中的第二个接口。需要注意的是,在线模式需要二层网络分段,也就是说第一个接口和第二个接口在两个不同的 VLAN 中,而三层网络保持不变。

本实验把 IPS 配置成在线接口对模式,网络流量从 e1 端口进入,从 e2 端口流出,在主机 PC2 上运行 Nmap 对服务器 Server 所在网络中主机进行端口扫描,当 IPS 检测到进行 TCP SYN 端口扫描的流量时,就触发告警并阻塞攻击源的网络流量。实验拓扑结构如图 1 所示。

R1、R2 是 2 台 C3640 路由器,再用 1 台 C3640 路由器添加 NM-16ESW 模块后模拟交换机 SW,f0/3 和

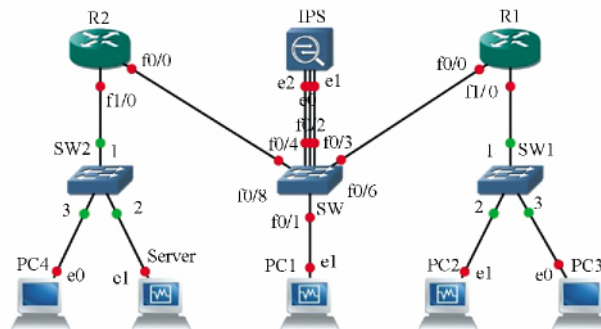


图 1 入侵防御系统实验网络拓扑结构

f0/6 划分到 vlan10,f0/4 和 f0/8 划分到 vlan20。SW1 和 SW2 是接入交换机。PC1 和 PC2 是安装了 Windows XP 操作系统的 VirtualBox 虚拟机,其中 PC1 安装 JAVA 运行环境,用 IDM 图形化配置 IPS,PC2 安装 Nmap 用来进行端口扫描。PC3 和 PC4 是 VPCS 虚拟机。Server 是安装了 Windows 2003 server 操作系统的 VirtualBox 虚拟机,安装并配置了 WWW 服务器。各设备端口 IP 地址分配见表 1。

表 1 虚拟机及路由器端口 IP 地址分配表

设备	端口	IP 地址	默认网关
R1	f0/0	192.168.0.2/24	-
R1	f1/0	192.168.2.1/24	-
R1	Loopback 0	172.16.0.1/24	-
R1	Loopback 1	172.16.1.1/24	-
R1	Loopback 2	172.16.2.1/24	-
R1	Loopback 3	172.16.3.1/24	-
R2	f0/0	192.168.0.1/24	-
R2	f1/0	192.168.3.1/24	-
IPS	e0	192.168.1.8/24	192.168.1.1/24
PC1	e1	192.168.1.10/24	192.168.1.1/24
PC2	e1	192.168.2.20/24	192.168.2.1/24
PC3	e0	192.168.2.30/24	192.168.2.1/24
PC4	e0	192.168.3.40/24	192.168.3.1/24
Server	e1	192.168.3.10/24	192.168.3.1/24

3 实验环境配置

3.1 配置路由器

R1 路由器主要配置如下^[13-14]:

```

R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config)# interface fastEthernet 1/0
R1(config-if)# ip address 192.168.3.1 255.255.255.0

```

```
R1(config-if) # no shutdown
R1(config) # interface lookback 0
R1(config-if) # ip address 172.16.0.1 255.255.255.0
R1(config) # interface lookback 1
R1(config-if) # ip address 172.16.1.1 255.255.255.0
R1(config) # interface lookback 2
R1(config-if) # ip address 172.16.2.1 255.255.255.0
R1(config) # interface lookback 3
R1(config-if) # ip address 172.16.3.1 255.255.255.0
R1(config) # ip route 0.0.0.0 0.0.0.0 192.168.0.2
```

R2 路由器主要配置如下:

```
R2(config) # interface fastEthernet 0/0
R2(config-if) # ip address 192.168.0.2 255.255.255.0
R2(config-if) # no shutdown
R2(config) # interface fastEthernet 1/0
R2(config-if) # ip address 192.168.2.1 255.255.255.0
R2(config-if) # no shutdown
R2(config) # ip route 0.0.0.0 0.0.0.0 192.168.0.1
```

3.2 配置交换机

SW 交换机主要配置如下:

```
SW # vlan database
SW(vlan) # vlan 10
SW(vlan) # vlan 20
SW # configure terminal
SW(config) # interface range f0/3 ,f0/6
SW(config-if-range) # switchport access vlan 10
SW(config-if-range) # no shutdown
SW(config-if-range) # exit
SW(config) # interface range f0/4 ,f0/8
SW(config-if-range) # switchport access vlan 20
SW(config-if-range) # no shutdown
SW(config-if-range) # exit
```

3.3 初始化配置 IPS

IPS 主要初始化配置如下:

```
IPS# setup
Current Configuration:
host-ip 192.168.1.8/24,192.168.1.1 ! 配置管理接口地址和网关
host-name IPS
access-list 192.168.1.0/24 ! 允许 192.168.1.0/24 网络内主机访问 IPS
time-zone-settings
offset 480
standard-time-zone-name GMT+08:00
service web-server
port 443 ! 安全 web 访问的默认端口
```

```
:
```

```
IPS#
```

4 实验内容

4.1 基本端口扫描防御

在 PC2 上运行 Nmap, 执行命令“nmap -sS -v -F 192.168.3.10,40,60”。此命令采用快速模式对 IP 地址为 192.168.3.10、192.168.3.40 和 192.168.3.60 的目标主机进行主机发现扫描和 TCP SYN 扫描, 并输出详细信息, 运行结果如下:

```
Starting Nmap 7.11 ( https://nmap.org ) at 2016-11-15 09:36 ?
Initiating Ping Scan at 09:36
Scanning 3 hosts [4 ports/host]
Completed Ping Scan at 09:36, 1.76s elapsed (3 total hosts)
Nmap scan report for 192.168.3.60 [host down]
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 09:36
Scanning 2 hosts [100 ports/host]
Discovered open port 445/tcp on 192.168.3.10
Discovered open port 139/tcp on 192.168.3.10
Discovered open port 80/tcp on 192.168.3.10
Discovered open port 1025/tcp on 192.168.3.10
Discovered open port 135/tcp on 192.168.3.10
Completed SYN Stealth Scan against 192.168.3.10 in 0.52s (1 host left)
Completed SYN Stealth Scan at 09:36, 3.02s elapsed (200 total ports)
Nmap scan report for 192.168.3.10
Host is up (0.10s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
Nmap scan report for 192.168.3.40
Host is up (0.040s latency).
All 100 scanned ports on 192.168.3.40 are filtered
Read data files from: C:\Program Files\Nmap
Nmap done: 3 IP addresses (2 hosts up) scanned in 5.35 seconds
Raw packets sent: 314 (13.728KB) | Rcvd: 106 (4.236KB)
```

从以上内容可以看到正在运行的主机 Server 和 PC4。在 Server 上开放了 80、135、139、445 和 1025 号端口,其他端口被过滤;而 PC4 上所有端口都被过滤。

在执行扫描命令的同时,在 R1-SW 链路上运行 Wireshark 捕获报文。从捕获的报文中可以看到:所有打开的端口都返回了 SYN 和 ACK 比特置 1 的 TCP 报文,如图 2 所示。

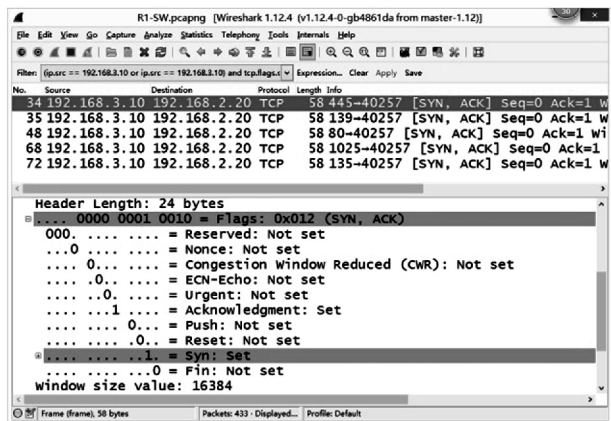


图 2 R1-SW 链路上捕获的 TCP 报文

这说明在 TCP SYN 扫描中判断端口是否打开的依据,是看对应端口是否返回了 SYN 和 ACK 比特置 1 的 TCP 报文。如果收到 SYN/ACK 回复,可以判断端口是开放的。接下来,在 PC1 上调整 IPS 特征集中 Sig ID 为 3002 的行为,增加“Deny Attacker Inline”,如图 3 所示。

应用 3002 特征对流量进行监控,当检测到在相同的攻击源和被攻击目标之间每秒有 5 个以上的 SYN 比特置 1 而 ACK 和 FIN 比特置 0 的 TCP 报文时,就发出警告信息并拒绝所有攻击源的网络流量。然后在 PC2 上再次执行命令“nmap -sS -v -F 192.168.3.10,40,60”,结果如下:

Starting Nmap 7.11 (<https://nmap.org>) at 2016-11-15 10:27 ?

Initiating Ping Scan at 10:27

Scanning 3 hosts [4 ports/host]

Completed Ping Scan at 10:27, 1.70s elapsed (3 total hosts)

Nmap scan report for 192.168.3.60 [host down]

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Initiating SYN Stealth Scan at 10:27

Scanning 2 hosts [100 ports/host]

Completed SYN Stealth Scan against 192.168.3.40 in 7.03s (1 host left)

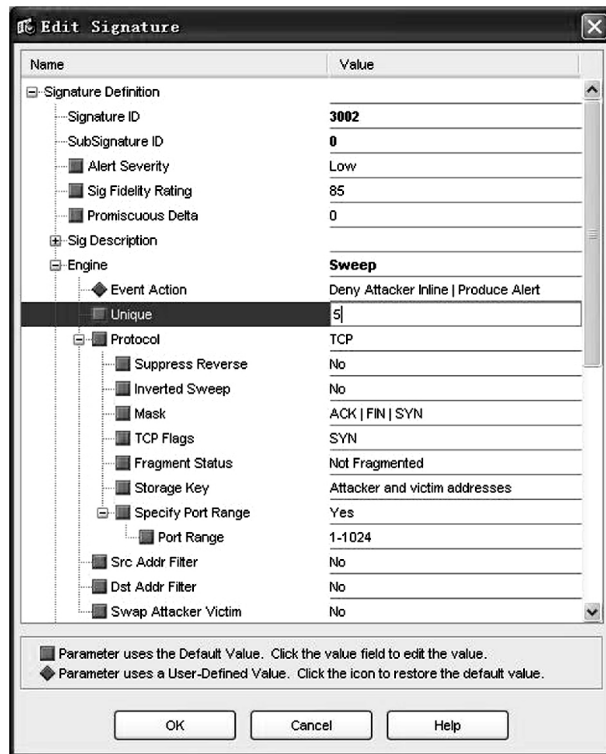


图 3 调整特征的行为参数

Increasing send delay for 192.168.3.10 from 0 to 5 due to 11 out of 15 dropped probes since last increase.

Completed SYN Stealth Scan at 10:29, 106.35s elapsed (200 total ports)

Nmap scan report for 192.168.3.10

Host is up (0.13s latency).

Not shown: 96 filtered ports

PORT STATE SERVICE

53/tcp closed domain

111/tcp closed rpcbind

143/tcp closed imap

993/tcp closed imaps

Nmap scan report for 192.168.3.40

Host is up (0.040s latency).

All 100 scanned ports on 192.168.3.40 are filtered

Read data files from: C:\Program Files\Nmap

Nmap done: 3 IP addresses (2 hosts up) scanned in 109.41 seconds

Raw packets sent: 429 (18,780KB) | Rcvd: 9 (336B)

可以看到:发现主机 Server 和 PC4(因为没有限制 ICMP 扫描),但是在 Server 上 53、111、143 和 993 号端口被关闭,其他端口被过滤,而 PC4 上所有端口都被过滤。

在 IPS 上收到了 2 个警告信息,其中一个警告信息的内容如下:

```

evIdsAlert: eventId = 1299876074698385058  vendor =
Cisco  severity=low
originator:
hostId: IPS
appName: sensorApp
appInstanceId: 399
time: 2016 年 11 月 15 日 上午 02 时 24 分 34 秒  offset
=480  timeZone=GMT+08:00
signature:  description=TCP SYN Port Sweep  id =
3002  version = S2  type = anomaly  created =
20010202
subsigId: 0
marsCategory: Probe/PortSweep/Non-stealth
interfaceGroup: vs0
vlan: 0
participants:
attacker:
addr: 192.168.2.20  locality=OUT
port: 42815
target:
addr: 192.168.3.10  locality=OUT
port: 443
port: 113
port: 22
port: 80
port: 23
port: 139
os:  idSource=unknown  type=unknown  relevance
=relevant
actions:
deniedAttacker: true
riskRatingValue: 52  targetValueRating=medium  at-
tackRelevanceRating=relevant
threatRatingValue: 7
interface: ge0_0
protocol: tcp

```

同时在 IPS 的被拒绝的攻击源主机列表中增加了 PC2。这说明 IPS 不但可以检测到 Nmap 的 TCP SYN 扫描,还执行了拒绝攻击源为 192.168.2.20 的主机的所有流量。而此时正常的 WWW 访问服务并没有受到影响,在 PC2 上能够访问 Server 的 WWW 服务器。

4.2 高级端口扫描防御

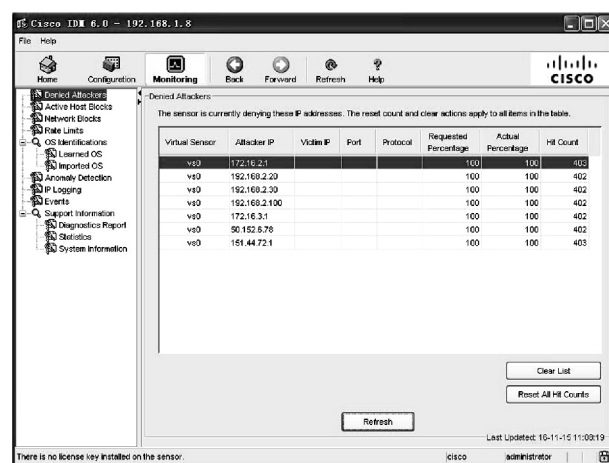
在 PC2 的 Nmap 上执行命令“nmap-sS-v-F-D 172.16.2.1,172.16.3.1,RND:2,ME,192.168.2.30,192.168.2.100 192.168.3.10,40,60”,此命令采用 IP 诱骗方式对 IP 地址为 192.168.3.10、192.168.3.40 和 192.168.3.60 的目标主机进行主机发现扫描和 TCP SYN 快速扫描并输出详细信息,结果如下:

```

Starting Nmap 7.11 ( https://nmap.org ) at 2016-11-15
10:51 ?
Initiating Ping Scan at 10:51
Scanning 3 hosts [4 ports/host]
Completed Ping Scan at 10:51, 2.30s elapsed (3 total
hosts)
Nmap scan report for 192.168.3.60 [host down]
:
Completed SYN Stealth Scan at 10:55, 240.26s elapsed
(200 total ports)
Nmap scan report for 192.168.3.10
Host is up (0.29s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
23/tcp    closed telnet
587/tcp   closed submission
993/tcp   closed imaps
995/tcp   closed pop3s
8080/tcp  closed http-proxy
Nmap scan report for 192.168.3.40
Host is up (0.12s latency).
All 100 scanned ports on 192.168.3.40 are filtered
:

```

可以看到:主机 Server 和 PC4,在 Server 上 5 个端口被关闭,其他端口被过滤,而 PC4 上还是所有端口都被过滤。在 IPS 上看到了多个警告信息,并在 IPS 的被拒绝的攻击源主机列表中增加了多个主机,如图 4 所示



Virtual Sensor	Attacker IP	Victim IP	Port	Protocol	Requested Percentage	Actual Percentage	Hit Count
vs0	172.16.2.1				100	100	402
vs0	192.168.2.20				100	100	402
vs0	192.168.2.30				100	100	402
vs0	192.168.2.100				100	100	402
vs0	172.16.3.1				100	100	402
vs0	50.152.8.78				100	100	402
vs0	191.44.72.1				100	100	403

图 4 多个攻击源主机被加入列表

这说明 IPS 不但可以检测到 Nmap 的 IP 诱骗 TCP SYN 扫描,还可以及时作出相应的反应。

继续在 PC2 上运行 Nmap,执行命令“nmap-sS-v-F-scan-delay 300ms -D 172.16.2.1,172.16.3.1,RND:2,ME,192.168.2.30,192.168.2.100 192.

168.3.10, 40, 60”,此命令功能只是针对每一个目标主机发送探测报文的时间间隔设置为 300 ms,其他不变。

可以看到:Nmap 通过扫描延时发现了主机 Server 的部分开放端口,但是在 IPS 上还是看到了多个警告信息,并拒绝了所有攻击源主机的网络流量,起到了入侵防御的作用,同时也说明要真正拒绝所有的端口扫描是很困难的。

5 结语

利用 GNS3 模拟软件中的 IPS 模拟器和 Virtual-Box 虚拟机搭建的虚拟网络入侵防御系统,实现了对利用 Nmap 发起的多种端口扫描方式的入侵防御仿真实验,达到与真实设备同样的实验效果,验证了在虚拟网络环境下进行网络安全实验的可行性。该系统的使用,提高了学生动手能力,同时也加深了学生对相关理论知识理解。

参考文献(References)

- [1] 周敏. 计算机网络安全实验教学改革[J]. 实验技术与管理, 2013, 30(6): 113-117.
- [2] 张旭珍, 黄成玉, 张志波. 基于 Snort 的入侵检测系统教学实验设计与实现[J]. 实验室研究与探索, 2014, 33(4): 159-163.
- [3] 唐灯平, 朱艳琴, 杨哲, 等. 计算机网络管理仿真平台防火墙实验设

计[J]. 实验技术与管理, 2015, 32(4): 156-160.

- [4] 张玲丽. 基于 GNS3 虚拟机的 PIX 防火墙配置实例[J]. 数字通信, 2014, 41(5): 78-80.
- [5] 曾刚. GNS3 在网络安全实践教学中的应用[J]. 网络安全, 2014(4): 11-12.
- [6] 薛静锋, 祝烈煌. 入侵检测技术[M]. 2 版. 北京: 人民邮电出版社, 2016.
- [7] 李剑. 入侵检测技术[M]. 北京: 高等教育出版社, 2008.
- [8] Welsh C. GNS3 Network Simulation Guide[M]. Birmingham: Packt Publishing Ltd, 2013.
- [9] Orebaugh A, Ramirez G, Burke J, et al. Wireshark & Ethereal Network Protocol Analyzer Toolkit[M]. Rockland: Syngress Publishing Inc, 2007.
- [10] Lyon G F. Nmap Network Scanning[M]. Sunnyvale: Insecure. Com LLC, 2008.
- [11] Cisco Systems Inc. Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 6. 0 [EB/OL]. <http://www.cisco.com/c/en/us/td/docs/security/ips/6-0/configuration/guide/idm/idmguide/dmIntro.html>. 2016.
- [12] Frahm J, Santos O, Ossipov A. Cisco ASA All-in-One Next-Generation Firewall, IPS, and VPN Services[M]. 3rd ed. Indianapolis: Cisco Press, 2014.
- [13] Lammle T. CCNA 学习指南(第 7 卷)[M]. 袁国忠, 徐宏, 译. 北京: 人民邮电出版社, 2012.
- [14] Yusuf Bhajji. 网络安全技术与解决方案[M]. 修订版. 田果, 刘丹宁, 译. 北京: 人民邮电出版社, 2009.

(上接第 108 页)

(5) 稳态轧制过程中, 电机定子侧电压的 3、5、7、9 次谐波都增加到原来的 2~3 倍; 电机侧电流的 9 次谐波有一些; 电网的谐波电流几乎为 0;

(6) 精轧机轧制完成, 机组降速, 此时电网电流的 3、5、7、9 次谐波都急剧增大, 但对电机的电压和电流谐波没什么影响。

5 结语

交-交变频同步电机调速系统将仿真系统的电机转速、力矩电流与实际值进行对比, 证明由 PSIM 建立的同步电机调速系统有很好的稳定性, 并可以很好地接收精轧机仿真模型输出的转速。

参考文献(References)

- [1] Wang Zhangyuan, Liu Yilu. Modeling and Simulation of a Cyclo-converter Drive System for Harmonic Studies[J]. IEEE Transactions on Industrial Electronics, 2000, 47(3): 533-541.
- [2] 干永革, 王文, 李发海, 等. 交交变频同步电机矢量控制系统供电电网谐波分析[J]. 中国电机工程学报, 1999, 19(6): 21-25, 32.

- [3] 马小亮. 大功率交-交变频调速及矢量控制技术[M]. 3 版. 北京: 机械工业出版社, 2003.
- [4] 薛丽英, 齐蓉, 梅亮. 永磁同步电动机矢量控制系统在 PSIM 下的仿真分析[J]. 电力系统及自动化学报, 2006, 18(5): 46-48.
- [5] 纪志成, 周震, 李三东. 基于 PSIM 永磁同步电机矢量控制系统的仿真建模[J]. 系统仿真学报, 2004, 16(5): 898-901.
- [6] 李林泉. 双馈电机调速系统的仿真[D]. 北京: 北京科技大学, 2008.
- [7] 赵晓坦, 李崇坚, 王云鹏, 等. 磁场定向控制同步电机稳态特性分析[C]//全国自动化新技术学术交流会会议论文集. 南京, 2005.
- [8] 吴轩钦, 谭国俊, 宋金梅, 等. 基于混合磁链观测器电励磁同步电机矢量控制[J]. 电机与控制学报, 2010, 14(3): 62-68.
- [9] Hu Jun, Wu Bin. New integration algorithms for estimating motor flux over a wide speed range[J]. IEEE Transactions on Power Electronics, 1997, 13(5): 1075-1081.
- [10] 李崇坚. 交流同步电机调速系统[M]. 北京: 科学出版社, 2006.
- [11] 张勇军, 王京, 李静, 等. 轧机主传动交流变频传动技术的发展及应用[J]. 电机与控制应用, 2008, 35(8): 1-5.
- [12] 杜少通, 高庆华. 基于双变量六脉波交-交变频器的变压变频控制方法研究[J]. 工矿自动化, 2010, 36(8): 89-92.
- [13] 张进之, 王文瑞. 热连轧张力复合控制系统的探讨[J]. 冶金自动化, 1997(3): 10-13.