دیواره های آتش در لینوکس

سید هاشم برادران قوامی

نکته

نصب یک فایر وال امن یک هنر است
این کار به درک درست از تکنولوژی نیازمند است
این کارگاه صرفا جنبه آشنایی با اینگونه ابزارها
میباشد وقویا به دوستان توصیه میگردد
برای درک فلسفه درست از این مقوله به
این اسلاید ها بسنده نکنند

یک توصیه

در موضوعات وابسته به امنیت به هیچکس اطمینان نکنید

آشنایی با شیوه های حمله

یک دیواره اتش
ip
در لینوکس از چه نوع حملاتی
شبکه ما رو حفظ میکند

حملات

دسترسی های غیر مجاز

بهره برداری از شکاف های امنیتی شناخته شده و ناشناخته در برنامه ها

ترافیک کاذب

Spoofing

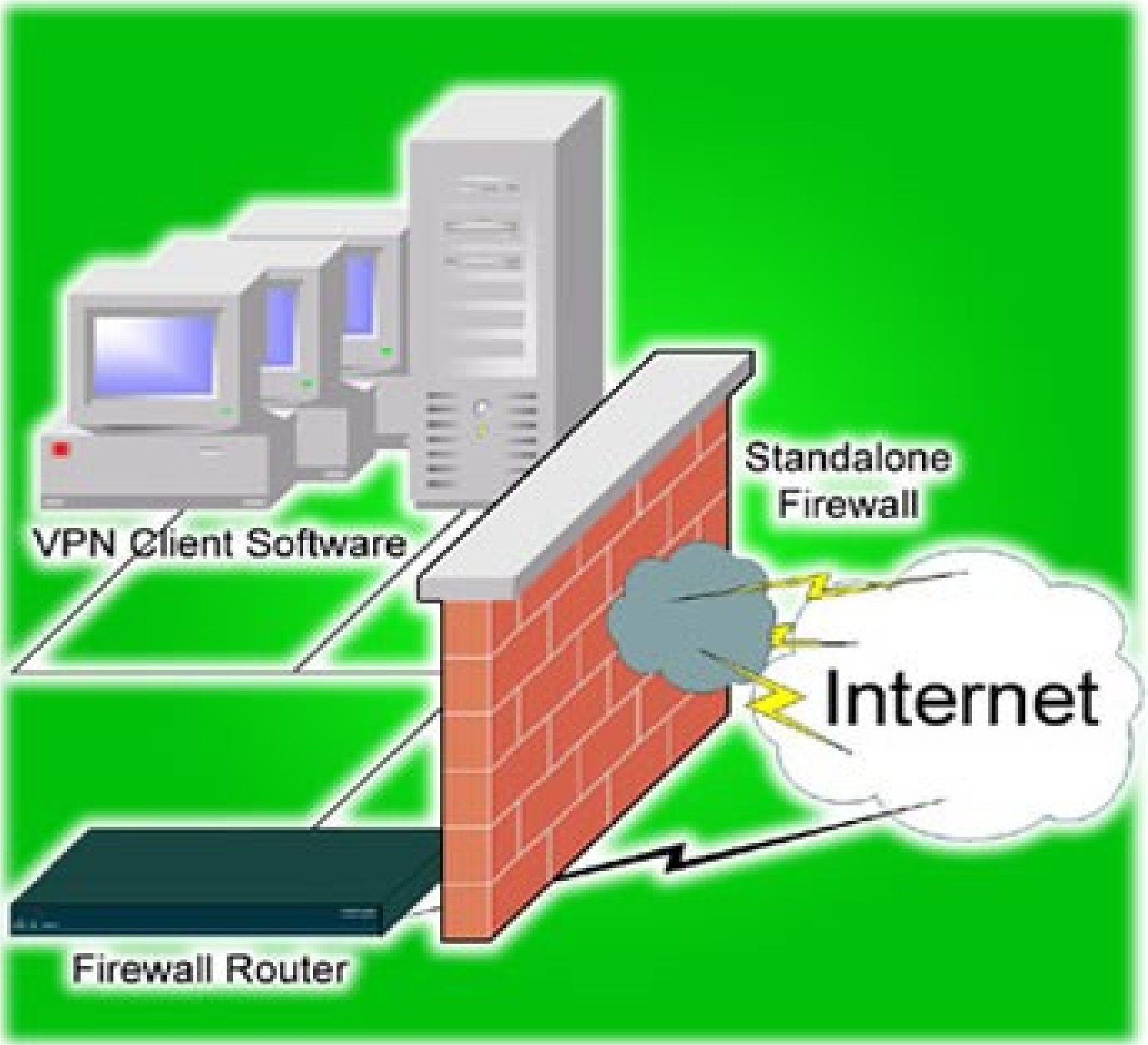
بدل سازی:معمولا یک حمله کننده یا تبعیت از آدرس ip
موجود در بسته ها ای اطلاعاتی شبکه میکوشد خود را به عنوان یک میزبان مجاز معرفی کند

Eavesdroping

یکی از شایع ترین و ساده ترین نوع حملات است
فایروال گذاری تاثیر بسیار زیادی در این گونه
حملات دارد

فایر وال چیست؟

دیواره آتش ماشین قابل اعتمادی است که بین یک شبکه خصوصی و یک شبکه عمومی قرار میگرد و با مجموعهای از قوانین و معیار های سنجشی تنظیم شده است که تعیین میکند کدام داده ها اجازه تردد بین ۲شبکه را دارند وکدام یک باید منع شود


VPN Client Software
Standalone
Firewall
Internet
Firewall Router

Perimeter network

روش های تنظیم دیواره های آتش نصبت به نوع شبکه و نوع شبکه متفاوت است که مشکل ترین آنها شبکه های محیطی است

Ip filtering

منظور این است که تعیین میکند کدام یک از بسته های اطلاعاتی باید طبق معمول بررسی شوند و کدام یک باید حدف و فراموش شود

معیار های فیلتر گذای

نوع قرار داد
TCP-udp-icmp
شماره درگاه و سوکت
نوع بسته اطلاعاتی
آدرس منبع
آدرس مقصد

نکته

فیلتر گذاری یکی از قابلیت های لایه شبکه هست
و تنها چیزی که در اینجا مهم است خود ارتباط است

exampel: Telnet on port 23

تنظیم لینوکس برای دیوار آتش

Kernel support:
kernel 2.2 =======>Ipfwad
kernel 2.2.X==========>ip chains
kernel 2.3.15=======>Net filter

kernel 2.X.X=========>IP tables

مثال برای IPFWADm

بیاید فرض کنیم شبکه ای در سازمانمان داریم که میخواهیم به کمک یک ماشین فایر وال مبتنی بر لینوکس ان را به اینترنت متصل کنیم.
ضمناا فرض کنید میخواهیم کاری کنیم که کاربران آن شبکه ضمن اینکه می توانند به سرورهای وب موجود در اینترنت دسترسی داشته باشند هیچ ترافیک دیگری اجازه عبور نداشته باشد

#Ipfwadm -F -f

F= Forwarding
f=flush

#ipfwadm -F -p deny

p=policy

ایجاد این سیاست برای تعیین تکلیف داده های که در حیطه قوانین گنجانده نشده لازم است

#ipfwadm -F -a accept -p tcp -S 172.16.1.0/24 -D 0/0 80

F=forwarding
-a accept = verfiy send packet
-p tcp= tcp not UDP
-s 172.16.1.0/24 24bit on ip 176.16.1.0
-D 0/0 80 ---------->evry evry things

Options:

-P protocol (either tcp, udp, icmp, or all)

-S address[/mask] [port ...]

source

-D address[/mask] [port ...]

destination specification

#ipfwadm -F -a accept -p tcp -S 0/0 80 -D 172.16.1.0/24

port WWW == 80 ---------->/etc/services
 -D 0/0 www

bidirectional

#ipfwadm -F -a accept -p tcp -S 172.16.1.0/24 -D 0/0 80 -b

One bug in this config

اضافه کردن سوکت ۸۰ به انتهای درخواست
از این نوع تنظیم دیوار آتش عبور میکند

```
#ipfwadm -F -a deny -p tcp -S 0/0 80 -D
172.16.10.0 /24 -y

#ipfwadm -F -a accept -p tcp -S
172.16.1.0/24 -D 0/0  80 -b
```

-V address network interface address
-W name network interface name
-b bidirectional match
-e extended output mode
-k match TCP packets only when ACK set
-m masquerade packets as coming from local host
-n numeric output of addresses and ports
-o turn on kernel logging for matching packets
-r [port] redirect packets to local port (transparent proxying)
-t and xor and/xor masks for TOS field
-v verbose mode
-x expand numbers (display exact values)
-y match TCP packets only when SYN set and ACK cleared

Default Mask

Class A

Network		Node	

11	11	11	11	00	00	00	00	00	00	00	00	00	00	00	00

Binary Dotted Decimal: 255 . 0 . 0 . 0

Class B

Network		Node	

11	11	11	11	11	11	11	11	00	00	00	00	00	00	00	00

Binary Dotted Decimal: 255 . 255 . Ø . Ø

Class C

	Network		Node

11	11	11	11	11	11	11	11	11	11	11	11	00	00	00	00

Binary Dotted Decimal: 255 . 255 . 255 . Ø