

****

###### دانشگاه پیام نور

###### واحد رامسر

**عنوان:**

## سيستم هاي امنيتي شبكه

### استاد :

**دانشجو:**

**فهرست مطالب**

**عنوان صفحه**

1 مقدمه 1

فصل اول:

1-1 انواع حملات 1

1-1-1 حملات رد سرویس 1

1-1-2 حملاتی که به منظور بدست آوردن اطلاعات صورت مي‌گیرند 4

1-1-3 حملاتی که سرویسدهی روی شبکه را دچار مشکل مي‌کنند 4

1-2-امنیت پروتکلها 5

1-2-1 پیچیدگی سرویس 5

1-2-2 سوء استفاده از سرویس 6

1-2-3 اطلاعات ارائه شده توسط سرویس 6

1-2-4 میزان دیالوگ با سرویسگیر 6

1-2-5 قابلیت پیکر بندی سرویس 7

1-2-6 نوع مکانیزم احراز هویت استفاده توسط سرویس 7

فصل دوم:

2 فایروالهای packet- fkiter 9

2-1 فيلتر‌هاي stateless 9

2-1-1 کنترل بسته‌ها بر اساس نوع پروتکل 9

2-1-2 کنترل بسته‌ها بر اساس آدرس IP 9

2-1-3 کنترل بسته‌ها بر اساس پورتهای TCP/UDP 10

2-1-4 کنترل بسته‌ها از روی سایر اطلاعات موجود در سرآیند 11

2-1-5 مشکلات فیلتر‌های استاندارد 12

2-1-6 کنترل بسته‌ها توسط سیستم عامل 13

2-2 فیلترهای stateful 13

2-3 مشکلات فیلترها 14

فصل سوم:

3 NAT 15

3- انواع ترجمه آدرس در NAT 17

3-1-ترجمه پویا 17

3-1-2 ترجمه ایستا 18

3-1-3 توزیع بار 18

3-1-4 افزونگی (Redundancy) 19

3-2 مشکلات NAT 19

3-3 پراکسی 20

3-3-1 عملکردهای امنیتی پراکسی 21

3-3-2 پنهان کردن اطلاعات سرویسگیرها 22

3-3-3 بستن يک سري URL 22

3-3-4 کنترل کنترل محتویات بسته‌ها 22

3-3-5 اطمینان از سالم بودن بسته‌ها 23

3-3-6 کنترل روی دسترسی‌ها 23

3-4 تاثیر پراکسی در سرعت 23

3-4-1 cache کردن 23

3-4-2 توزيع بار 24

3-4-3 مشکلات پراکسی 24

3-5سیستم‌های تهاجم یاب 26

3-5-1 سیستم‌های تهاجم باب بر مبنای بازرسی 27

3-5-2 سیستم‌های تهاجم یاب طعمه 28

3-6 IP Filter 29

3-6-1 نصب IP Filter روی Solaris 30

3-6-2 پیاده سازی یک فیلتر با استفاده از IP filter 30

فصل چهارم:

4 Snort 36

4-1 مود Sniffer 37

4-2 مود Packet logger 38

4-3 مود تهاجم یاب شبکه 39

4-3-1 فیلترهای BPF 40

4-3-2 فایل پیکربندی Snort 42

4-3-3 Perprocessor‌ها 43

4-3-4 قوانین تهاجم یاب 45

4-3-5 ماجول‌های خروجی 45

4-4 SAINT 47

4-4-1 فایل پیکربندی 48

4-4-2 خط فرمان 52

4-4-3 فرمت بانک اطلاعاتی 55

4-4-4 بانک اطلاعاتی Facts 5

4-4-5 بانک اطلاعاتی all-hosts 557

4-4-6 بانک اطلاعاتی todo 57

4-4-7 بانک اطلاعاتی CVE 57

4-4-8 آنالیز خروجی 57

منابع و مآخذ 60

1 مقدمه

این متن به بررسی انواع سیستمهای امنیتی و بررسی نقاط ضعف و قوت هر کدام مي‌پردازد. در این بخش مقدماتی در مورد امنیت پروتکها و انواع حملات بیان مي‌شود و بخشهای بعدی به بررسی دقیق انواع فایروال (فیلتر[[1]](#footnote-1)، NAT [[2]](#footnote-2)و پراکسی[[3]](#footnote-3)) و سیستمهای تهاجم یاب[[4]](#footnote-4) مي‌پردازد. سپس سه نمونه از نرم افزارهای مفید امنیتی Snort, IPF) و SAINT) معرفی مي‌گردد.

1-1 انواع حملات

در این قسمت یک سری از روشهای متدول برای جمله به شبکه‌های کامپیوتری توضیح داده مي‌شود و در مورد هر کدام مشخصات و نحوه شناسایی آن حمله بیان شده است. این حملات در چهار دسته عمده تقسیم بندی شده اند:

* حملات رد سرویس یا DoS [[5]](#footnote-5)
* حملات استثماری[[6]](#footnote-6)
* حملاتی که به منظور بدست آوردن اطلاعات صورت مي‌گیرند.[[7]](#footnote-7)
* حملاتی که سرویسدهی روی شبکه را دچار مشکل مي‌کنند.[[8]](#footnote-8)

1-1-1 حملات رد سرویس

این نوع حملات با ایجاد یک بار زیاد و غیر عادی روی سرورها باعث از کار افتادن سرویسهای ارائه شده توسط آنها مي‌شوند. از آنجا که انجام دادن این نوع حمله ساده است. لذا بیشتر متداول مي‌باشد. این قسمت بيشتر این حملات را توضیح مي‌دهد:

**Ping of Death**

این حمله از طریق بسته‌های ICMP صورت مي‌گیرد. حجم بسته‌های ICMP به 64KB محدود مي‌شود و بسته‌هایی که در سر آیند آنها حجم بسته بیشتر از این مقدار بیان شده (در حالیکه نیست) ممکن است در سمت گیرنده مشکلاتی ایجاد کنند چون بسیاری از سیستم عاملها کنترل دقیقی روی بسته‌های معیوب ندارند. این نوع حمله نبستاً قدیمی است و امروزه تمام سیستم عامل‌ها قادر به تشخیص آن مي‌باشند.

**Teardrop**

این حمله از طریق Fragment‌های IP صورت مي‌گیرد. یک Fragment شامل اطلاعاتی است که بیان مي‌کند چه قسمتی از بسته داخل آن قرار دارد. بسیاری از سیستمها ممکن است با گرفتن Fragment‌هایی که متعلق به یک بسته بوده و با هم تناقض دارند (یک قسمت از بسته در دو Fragment قرار داشته باشد) دچار مشکل شوند. این نوع حمله نیز قدیمی است.

**UDP Flooding**

این حمله با استفاده از سرویسهای chargen , echo صورت مي‌گیرد. با فرستادن یک درخواست جعلی از طرف یک سرویس echo برای یک سرویس chargen مي‌توان به راحتی حجم زیادی از ترافیک را روی شبکه ایجاد کرد.

**SYN Fooding**

این حمله با فرستادن SYN پروتکل TCP صورت مي‌گیرد. برای یک سرور دریافت یک بسته SYN به معنی گرفتن فضایی از حافظه برای آن ارتباط و فرستادن یک بسته ACK در پاسخ مي‌باشد. فضای حافظه تخصیص داده شده تا زمان timeout یا بسته شدن ارتباط باقی مي‌ماند. اگر تعداد زیادی بسته SYN فرستاده شود موجب اتلاف قسمت عمده ای از حافظه مي‌شود، هر چند فرستادن بسته‌های ACK نیز زمان و پردازش زیادی لازم دارد. این حمله در نهایت سرور را به وضعیتی مي‌کشاند که قادر به قبول ارتباط جدید نمی باشد. از آنجا که فرستنده بسته SYN در این حمله منتظر پاسخ نمی ماند مي‌تواند بسته‌ها را قبل از فرستاندن تغییر دهد و هر بار یک آدرس تصادفی بجای آدرس فرستنده آنها قرار دهد. در این صورت تشخیص حمله بسیار مشکل مي‌شود.

**Land Attack**

این حمله شبیه SYN Fooding مي‌باشد. در این حمله یک بسته SYN برای سرور ارسال مي‌شود که آدرس فرستنده و گیرنده آن هر دو آدرس خود سرور است. سرور پس از دریافت این بسته پاسخ آن را برای خودش مي‌فرستد که نتیجه ای مشابه SYN Fooding به همراه دارد.

**Smurf Attack**

این حمله از طریق بسته‌های ICMP صورت مي‌گیرد. در این حمله یک بسته ICMP Reqest داخل شبکه فرستاده مي‌شود که آدرس reply آن آدرس broadcast شبکه مي‌باشد. چنین بسته‌هایی معمولاً ترافیک بالایی داخل شبکه ایجاد مي‌کنند.

**Fragle Atack**

این حمله شبیه Smurf Attack است ولی بجای بسته‌های ICMP از بسته‌های UDP استفاده مي‌کند.

**E-mail Bombs**

این نوع حمله شامل فرستادن نامه‌های بزرگ بطور مداوم برای یک سیستم است. از آنجا که سمت فرستنده و گیرنده دارای بار نسبتاً مساوی هستند از این روش کمتر مي‌توان بعنوان یک DoS واقعی استفاده کرد.

**Malfrmed Attacks**

بسیاری از سرویسها هنگام دریافت بسته‌هایی که دارای خطا مي‌باشند با مشکل مواجه مي‌شوند چون کنترل دقیق روی بسته‌های معیوب ندارند و این بسته‌ها باعث ایجاد مشکل در برنامه سرور مي‌شوند. یک تقسیم بر صفر یا سرریز بافر مي‌تواند سرور را از کار بیندازد یا سبب دسترسی افراد غیر مجاز به آن شود. هر سرویسی ممکن است در معرض این حمله قرار بگیرد چون در هر لحظه امکان پیدا شدن یک bug در برنامه مربوطه وجود دارد. بیشترین مواردی که از این حمله مشاهده شده بر روی سرویسهای وب و پست الکترونیکی بوده است.

**حملات استثماری**

این نوع حملات بیشتر برای بدست آوردن کنترل مستقیم روی یک ماشین انجام مي‌شود. مهمترین این حملات از قرار زیر مي‌باشند:

**حدس زدن Password**

بسیاری از سرورها برای ارائه سرویس نیاز به احراز هویت کاربران از طریق Password دارند. برنامه‌هایی وجود دارند که یک سری کلمات (اسامی، کلمات dictionary، اعداد، ...) را بطور اتوماتیک تست مي‌کنند تا به یک Password معتبر دسترسی پیدا کنند.

**Trojan Horse**

Trojan Horse به برنامه ای گفته مي‌شود که اغلب توسط یک مهاجم روی سیستم نصب مي‌شود و اطلاعاتی در مورد سیستم به خارج از شبکه مي‌فرستد یا راهی برای دسترسی غیر مجاز به سیستم فراهم مي‌کند که به آن backdoor مي‌گویند. Trojan Horse معمولاً برنامه کوچکی است که به سادگی نصب مي‌شود و از دید کاربر نیز پنهان مي‌ماند.

**Buffer Overrun**

اکثر سرورها برای رسیدگی به درخواستهایی که از شبکه دریافت مي‌کنند فضایی از حافظه را به عنوان بافر اختصاص مي‌دهند. اغلب برنامه‌ها حجم این بافر را به یک مقدار ثابت محدود مي‌کنند یا به بسته‌های رسیده اطمینان کرده و اندازه بسته‌ها را از روی اطلاعات سر آیند آنها استخراج مي‌کنند. این پدیده معمولاً زمانی اتفاق مي‌افتد که طول یک بسته از مقدار در نظر گرفته شده برای بافربیشتر باشد یا اطلاعات غلط در مورد طول خود به برنامه بدهد. برای مثال اگر طول یک بسته 256 بایت باشد ولی در اطلاعات غلط در مورد طول خود معرفی شده باشد 240 بایت بسته داخل بافر قرار مي‌گیرد و 16 بایت اضافی در یک مکان دیگر از حافظه نوشته مي‌شود و منجر به از بین رفتن اطلاعات آن قسمت حافظه مي‌شود. در این حالت با قرار دادن کد ماشین در 16 بایت آخر بسته ممکن است بتوان این کد را روی سرور اجرا کرده کنترل سرور را بدست آورد.

1. - Pachet Filter [↑](#footnote-ref-1)
2. - Nework Address Translation [↑](#footnote-ref-2)
3. - Proxy [↑](#footnote-ref-3)
4. - Inrusion Detection Systems [↑](#footnote-ref-4)
5. - Denial – of – service attacks [↑](#footnote-ref-5)
6. - Exploitation attacks [↑](#footnote-ref-6)
7. - Information gathering attacks [↑](#footnote-ref-7)
8. - Disinformation attacks. [↑](#footnote-ref-8)