Computer Networks project phase 0

Mohamad Hosein Hoseinee 9712762670

در ابتدا گزارشی به زبان انگلیسی و سپس به زبان فارسی آمده است

Packet sniffing vs Packet analyzing

What is packet sniffing?

Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass through a computer network, regardless of how the packet is addressed. In this way, every packet, or a defined subset of packets, may be gathered for further analysis. You as a network administrators can use the collected data for a wide variety of purposes like monitoring bandwidth and traffic.

A packet sniffer, sometimes called a packet analyzer, is composed of two main parts. First, a network adapter that connects the sniffer to the existing network. Second, software that provides a way to log, see, or analyze the data collected by the device.

How does packet sniffing work?

A network is a collection of nodes, such as personal computers, servers, and networking hardware that are connected. The

network connection allows data to be transferred between these devices. The connections can be physical with cables, or wireless with radio signals. Networks can also be a combination of both types.

As nodes send data across the network, each transmission is broken down into smaller pieces called packets. The defined length and shape allows the data packets to be checked for completeness and usability. Because a network's infrastructure is common to many nodes, packets destined for different nodes will pass through numerous other nodes on the way to their destination. To ensure data is not mixed up, each packet is assigned an address that represents the intended destination of that packet.

A packet's address is examined by each network adapter and connected device to determine what node the packet is destined for. Under normal operating conditions, if a node sees a packet that is not addressed to it, the node ignores that packet and its data.

Packet sniffing ignores this standard practice and collects all, or some of the packets, regardless of how they are addressed.

There are two main types of packet sniffers:

- Hardware Packet Sniffers A hardware packet sniffer is designed to be plugged into a network and to examine it. A hardware packet sniffer is particularly useful when attempting to see traffic of a specific network segment. By plugging directly into the physical network at the appropriate location, a hardware packet sniffer can ensure that no packets are lost due to filtering, routing, or other deliberate or inadvertent causes. A hardware packet sniffer either stores the collected packets or forwards

them on to a collector that logs the data collected by the hardware packet sniffer for further analysis.

- Software Packet Sniffers Most packet sniffers these days are of the software variety. While any network interface attached to a network can receive every bit of network traffic that flows by, most are configured not to do so. A software packet sniffer changes this configuration so that the network interface passes all network traffic up the stack. This configuration is known as *promiscuous mode* for most network adapters. Once in promiscuous mode, the functionality of a packet sniffer becomes a matter of separating, reassembling, and logging all software packets that pass the interface, regardless of their destination addresses. Software packet sniffers collect all the traffic that flows through the physical network interface. That traffic is then logged and used according to the packet sniffing requirements of the software.
  Capturing data on an entire network may take multiple packet sniffers. Because each collector can only collect the network traffic that is received by the network adapter, it may not be able to see traffic that exists on the other side of routers or switches. On wireless networks, most adapters are capable of connecting to only one channel at a time. In order to capture data on multiple network segments, or multiple wireless channels, a packet sniffer is needed on each segment of the network. Most network monitoring solutions provide packet sniffing as one of the functions of their monitoring agents.

What kind of information does packet sniffing gather?

Packet sniffing collects the entire packet of each network transmission. Packets that are not encrypted can be reassembled and read in their entirety. For example, intercepted packets from a user accessing a website would include the HTML and CSS of the web pages. Most notoriously, users logging in to network resources across unencrypted transmissions expose their username and password as plain text that can be seen in captured packets.

When should I consider using packet sniffing?

Packet sniffing has many practical uses. Typically, packet sniffing is used for network troubleshooting. Packets detected on a network they are not supposed to be in might suggest improper routing or switching. Packets marked for ports that do not match their protocol might also suggest a misconfiguration of one or more nodes. You can also analyze traffic and the responses received for requests. Does the node query the correct DHCP server? Does the correct DNS request get routed to the correct location? Is traffic encrypted with SSL or HTTPS when it should be, or are unencrypted responses being sent? Is the routing path taken by the packet the most efficient route to its final destination?

Packets can also be analyzed to see if a specific application is using too much bandwidth or if authentication is requiring numerous back-and-forth calls. Based on the data provided, you might upgrade communications, or troubleshoot applications to enhance the software performance.

You may use packet sniffing to monitor consumption trends on a network. Analysis of collected packets may show that a large amount of traffic is being used by a certain in-house application,

or video transmissions. Also, a decline in traffic may suggest that specific resources are being used less.
Packet sniffing may be useful in increasing network security. When monitoring traffic for clear-text usernames and passwords, for example, you could notice possible security issues before any hacker. In addition, monitoring remote traffic can help ensure that all traffic is properly encrypted and not being sent out onto the open internet without encryption.

What is a packet analyzer?

Packet analyzers, also known as packet sniffers or network analyzers, are a network monitoring tool that examines data traffic moving in and out of the network. These tools analyze network performance issues that can lead to traffic bottlenecks, network downtime, and other common performance issues that ultimately effect end-user experience and a companies productivity.

Continuing with our shipping analogy, you can think of packet analyzers as the gate agents and security scanners in the data transportation process. They work behind the scenes to ensure everything runs smoothly on your network.

Packet sniffers are a go-to tool for everything from making sure network traffic is routed correctly, to ensuring employees aren’t using company internet time for inappropriate websites. Packet analyzers also help detect potential network intrusion by looking for network access patterns inconsistent with standard usage.

In a process known as packet capture (PCAP), analyzers snag packet data as it moves over your network. It saves a copy of this data as a file on your monitoring device. You can analyze these copies of your packet data, to detect usage spikes, suspicious data transfer, and inconsistent network performance.

What are the advantages of packet sniffing?

Aside from achieving network visibility by having all your data on hand, there are a handful of other huge benefits you can achieve through packet sniffing.

Find the root cause of various issues to secure your network

When you have access to your packet data, you can dig into the root cause of network issues. Thinking like a good threat hunter, you can familiarize yourself with typical traffic patterns and use your knowledge to identify inconsistencies.

When you understand your standard network performance, you can also use packet analyzer data to detect network vulnerabilities. When you know where you can improve, you can bolster your network security to prevent future threats, issues, or attacks.

Better understand your network speed

Armed with your PCAP analysis, you can figure out the average time it takes for a packet to travel across your network. Using these numbers, you can more quickly and easily figure out the

source of any network slowdowns. When you understand the source, you can determine which applications are impacted and take action to fix any issues.

Identify inefficient network usage

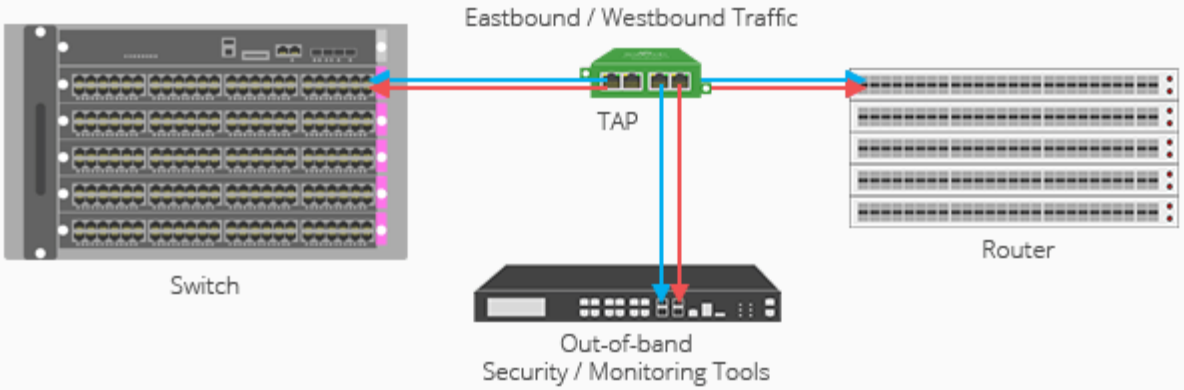
Packet analyzers can help you categorize the traffic on your network. With this data, you can identify non-business uses of your network, like visits to social media sites, that might slow your network performance.

How do Packet Sniffers access the Packets?

There are two different methods you can use to access packet data: network TAPs (test access points) and port mirroring or switch port analyzers (SPAN).

We've already covered the differences between network TAPs and SPANs; but to recap how each functions to perform PCAP analysis.

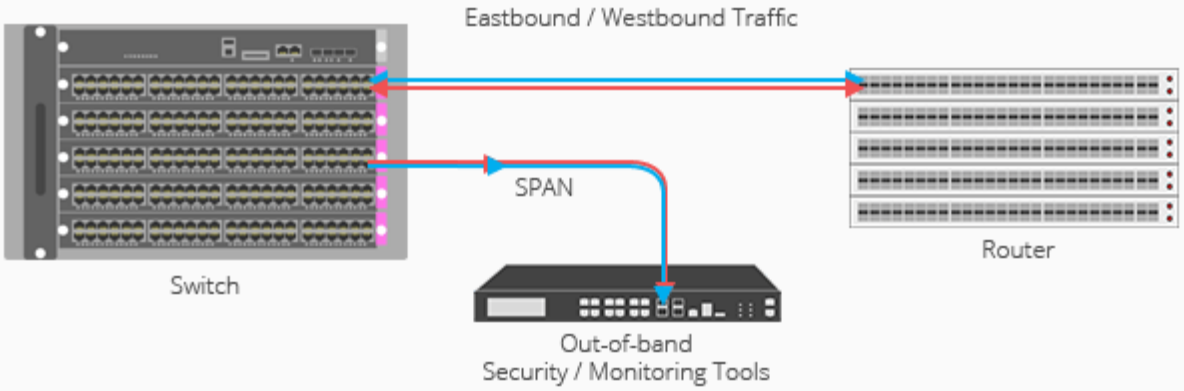
Network TAPs



Network TAPs sit between devices in a network and send complete copies of data packets to your analyzer device in real time. Unlike SPAN, TAPs don't alter data when they make copies to send to your monitoring device. This lack of alteration means TAPs can provide accurate timestamps and errors, which makes analysis and auditing much easier.

Considered the industry best practice for packet visibility, “EMA recommends that enterprises use TAPs as much as possible in the access layer to avoid network performance impacts and assure packet fidelity.” -*EMA [Enterprise Management Associates]*

SPAN Ports



The SPAN method also creates a copy of data sent from one port

to another of a network segment. However, SPAN is not recommended for networks with high throughput, as it was designed for lower volume spot checks. If your designated SPAN port is overutilized, it can drop and duplicate packets. These dropped and duplicate packets can make thorough, accurate analysis difficult or impossible.

Looking to add network TAP visibility to your packet analysis, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it’s what we love to do.

Packet sniffing و Packet analyzing چیست؟

از ابتدای بروز مسائل امنیتی و حملات به سرویس های اینترنتی و کامپیوتری استفاده از فرآیندی موسوم به packet sniffing مورد استفاده قرار گرفته است. هکرها از روش هایی جهت افزایش بسته های اطلاعاتی محرک در طول شبکه استفاده نموده و با آنالیز بسته های افزایش یافته از وجود اطلاعات حساس در یک شبکه مطلع میشوند، پروتکلی نظیر IPSec به منظور پیشگیری این فرآیند طراحی شده است که رمزنگاری بسته های اطلاعاتی را برعهده دارد. حال با استفاده از تکنولوژی IPSec بخش کوچکی از داده ها و بسته های اطلاعاتی رمزنگاری میگردند و همین امر باعث شده است که packet sniffing همچنان یکی از روش های متداول به منظور سرقت اطلاعات باشد. مدیران و ادمین های شبکه به منظور عیب یابی و مشاهده مشکلات ترافیکی به کمک packet sniffer که به عنوان network monitor یا network analyzerنیز یاد میشود، بسته های اطلاعاتی خطاگونه و گلوگاه های حساس شبکه را شناسایی کرده و بستر امن به منظور انتقال داده ها را فراهم می آورند. با این تعاریف میتوان گفت packet sniffer تمامی بسته های اطلاعاتی ارسال شده از طریق یک اینترفیس مشخص را جمع آوری مینماید تا بررسی و آنالیز آن بسته ها در فرصت مقتضی فراهم گردد، پس برنامه های packet sniffer به منظور جمع آوری بسته های اطلاعاتی مقصدی خاص و یا صرف نظر از مقصد ، مورد استفاده قرار می گیرند.

هکر از طریق تولید یک packet sniffer در شبکه مورد نظر به جمع آوری و آنالیز تمامی ترافیک شبکه میپردازد، باتوجه به اینکه اطلاعات مربوط به نام و رمز عبور به

صورت متن معمولی و رمز نشده در شبکه ارسال می گردد با آنالیز ترافیک شبکه امکان مشاهده اطلاعات حساس از این دست برای مهاجمان وجود خواهد داشت. این ترفند تنها قابلیت جمع آوری اطلاعات مربوط به بسته های اطلاعاتی درون یک subnet شبکه را دارد یعنی مهاجم با ایجاد packet sniffer در شبکه خود نمیتواند دسترسی به شبکه میزبان برای جمع آوری اطلاعات و سوء استفاده از آن را داشته باشد، پس این افراد اهداف مخرب خود را با نصب بدافزار ایجاد بسته اضافی برروی یک کامپیوتر موجود در شبکه میزبان عملی مینمایند .با این توضیحات متوجه خواهیم شد که packet sniffing با روش اترنت شبکه موازی کار میکند، به این صورت که هر زمان کامپیوتری یک بسته اطلاعاتی را ارسال می نماید آن بسته به عنوان یک broadcastبوده و بجز کامپیوتر مقصد تمامی دستگاه های موجود در شبکه این بسته را رؤیت کرده و کامپیوتری که مهاجم به آن دسترسی دارد یک کپی از بسته را برای سازماندهی عملیات هکر در خود نگهداری مینماید.

موارد استفاده از Packet Sniffer ها را میتوان به لیست زیر تقسیم کرد:

- تحلیل مشکلات شبکه ای
- تشخیص حمله های نفوذی
- استفاده غیر معمول از شبکه توسط کاربران داخلی و خارجی
- بدست آوردن اطلاعات مربوط به یک شبکه برای نفوذ به آن
- مانیتورینگ پهنای باند شبکه هایWAN
- مانیتورینگ استفاده های کاربران خارجی و داخلی شبکه
- مانیتورینگ داده های موجود در جریان داده یک شبکه
- مانیتورینگ وضعیت های امنیتی شبکهWAN

- جمع آوری و گزارش آمارهای مربوط به شبکه
- فیلتر سازی اطلاعات مشکوک از ترافیک شبکه
- جاسوسی بر روی شبکه های دیگر برای جمع آوری اطلاعات حساس مانند رمزهای عبور
- اشکال زدایی مربوط به ارتباط Client/Server بر روی شبکه
- اشکال زدایی طراحی پروتکل های شبکه

انواع حملات Packet Sniffing

1. حالت غیر فعال یا Passive: مهاجم بر روی کلیه کامپیوترهای یک شبکه LAN نرم افزار شنود را راه اندازی مینماید ، البته باتوجه به افزایش اهمیت امنیت شبکه های کابلی امروزه این روش کمتر رخ میدهد ولی در شبکه های وایرلسی مهاجم با دسترسی به کارت شبکه وایرلس سیستم موجود در مجموعه امکان شنود و Capture اطلاعات را دارد. درگذشته باتوجه به مکانیزم فعالیتی که HUB ها داشتند، داده ها در کلیه پورت ها ارسال و نرم افزار Sniffer امکان شنود کلی و یکجا اطلاعات تبادلی در شبکه را داشتند. در اصطلاح به این نوع حملات Passive Sniffing گفته میشود چون هکر نیازی به انجام هیچ کاری برای دریافت اطلاعات از شبکه ندارد و عملاً کسی متوجه حضور مهاجم نمی شود.

2. حالت فعال یا Active: در این حالت تعداد فراوانی MAC Address جعلی به سمت سوییچ از طرف نرم افزار شنود ارسال میگردد و جدول آدرس MAC یا MAC Table سرریز شده که باعث تغییر وضعیت سوییچ به یک HUB خواهد شد، سوییچی که با هاب تبدیل گردیده است ترافیک را بر روی تمامی پورت های خود

ارسال می کند و فرآیند شنود راه اندازی میگردد. شنود در این روش برای شبکه های وایرلس نیز ممکن است به اینصورت که در Passive Wireless Sniff ، مهاجم به محض ارسال بسته Access Point به سیستم مورد نظر همزمان درخواست های زیادی را به Access Point ارسال مینماید و این دستگاه مجبور به پاسخگویی شده و در نتیجه امکان شنود آن فراهم خواهد شد. تکنیک های Sniffing فعال عبارتند از MAC Flooding ، DHCP Attacks، DNS Poisoning، Spoofing Attacks و ARP Poisoning.

پروتکل های آسیب پذیر در مقابل حملات Packet Sniffing

•با بهره گیری از این سرویس امکان دسترسی امن با رایانه کاری به سرور پست الکترونیکی یا پرونده ها محیا میشود.

•پروتکل HTTP که برای ارسال متن کارایی دارد.

•پروتکل SMTP که اساساً در انتقال ایمیل ها مورد استفاده قرار می گیرد.

•پروتکل NNTP که برای تمامی ارتباطات استفاده می شود و داده ها را بصورت متن واضح یا clear text بر روی شبکه ارسال مبادله مینماید.

•پروتکل POP که دریافت ایمیل از سرور را فراهم میسازد.

•پروتکل FTP که ارسال و دریافت فایل بصورت متن ساده را ممکن مینماید.

•پروتکل IMAP که همچون SMTP در عملیات ایمیل مورد استفاده قرار میگیرد.

•پروتکل Telnet که همه اطلاعات مانند نامهای کاربری و رمزهای عبور را بر روی شبکه به عنوان clear text ارسال می کند.

در حملات sniffing بطور معمول اطلاعات حساس زیر شنود میگردند:

1. Email traffic
2. FTP passwords
3. Web traffics
4. Telnet passwords
5. پیکربندی روتر یا Router configuration
6. جلسات گفتگو یا Chat sessions
7. DNS traffic

ابزارهای پرکاربرد Sniffer یا Packet Analyzers

با پیشرفت در علوم کامپیوتری ابزارهای متعددی برای sniff شبکه با ویژگی های خاص تولیده شده اند تا تجزیه و تحلیل ترافیک و اطلاعات بر اساس سلیقه افراد امکان پذیر باشد، برخی از این ابزار به شرح زیر میباشند:

- ابزار قدرتمند BetterCAP که انعطاف پذیر و قابل حمل بوده و برای انجام انواع حملات MITM علیه شبکه، دستکاری و HTTP HTTPS همچنین ترافیک TCP به صورت لایو به کار میرود.
- ابزار Ettercap که مجموعه جامع برای حملات میانی میباشد و قابلیت شنود ارتباطات زنده و فیلتر کردن محتوا از جمله ویژگی های آن است.
- ابزار Wireshark که معروف ترین sniffer به شمار میرود و دارای ویژگی کمک به تجزیه و تحلیل ترافیک و اطلاعات میباشد.
- ابزار Tcpdump که تجزیه و تحلیل ترافیک در خط فرمان را عهده دار است و توانایی پیگیری و مشاهده TCP / IP و دیگر بسته ها را در هنگام انتقال در شبکه

فراهم میسازد.

- ابزار WinDump که ابزار خط فرمانی برای نمایش اطلاعات هدر رفته در شبکه میباشد.
- ابزار Dsniff که مجموعه ای از ابزارهای شنود با پروتکل های مختلف با هدف سرقت پسوردها در شبکه برای سیستم عامل های یونیکس و لینوکس را در اختیاز مهاجمان قرار میدهد.
- ابزار EtherApe که برای لینوکس یا یونیکس میباشد و نمایش گرافیکی اتصالات ورودی و خروجی سیستم را طراحی مینماید.
- ابزار NetWitness و NextGen که مبتنی بر سخت افزار به همراه ویژگی های زیادی میباشند و برای نظارت و تجزیه و تحلیل تمام ترافیک در شبکه طراحی شده اند.
- ابزار Microsoft Network Monitor
- ابزار Kismet
- ابزار Fiddler
- ابزار ngrep Network Grep
- ابزار Packet Capture
- ابزار PRTG Network Monitor
- ابزار Steel Central Packet Analyzer
- ابزار SolarWinds Packet Analysis Bundle
- ابزار Wireshark

Available libraries for packet sniffing & packet analyzing in C language on linux:

کتابخانه های موجود جهت انجام packet sniffing & packet analyzing :

1- **Libpcap** :

- Open source library.
- The oldest packet capturing library.
- High level interface to the network packet capture systems.
- Platform independent API.
- C/C++.
- Other languages like all java libraries provides this library by using wrappers.
- Windows version called Winpcap or Win10pcap. These libraries has not been updated for the last 5 years.

Libpcap is a packet capture library for linux which can be used to sniff packets or network traffic over a network interface.
Pcap Documentation gives a description of the methods and data structures available in the libpcap library.
To install libpcap on your linux distro you can either download the source from the website and compile it and install.
Or if you are on a distro like ubuntu then it can be installed from synaptic package manager. In the list of packages in Synaptic

Package Manager look for 2 packages named as libpcap0.8 and libpcap0.8-dev. Install both of them.

2- winpcap :

It’s the same tool for windows and we just wanna use linux for this project thus we won’t go about it.

3- Libtins :

The packet crafting and sniffing library
libtins is a high-level, multiplatform C++ network packet sniffing and crafting library.
Its main purpose is to provide the C++ developer an easy, efficient, platform and endianness-independent way to create tools which need to send, receive and manipulate network packets.
It uses a BSD-2 license and it's hosted at `github`.

4- Libcrafter

Libcrafter is a high level library for C++ designed to create and decode network
packets. It is able to craft or decode packets of most common networks protocols,
send them on the wire, capture them and match requests and replies.
It enables the creation of networking tools in a few lines with a interface
very similar to Scapy.

A packet is described as layers that you stack one upon the other. Fields of
each layer have useful default values that you can overload.

منابع تحقیق :

https://www.garlandtechnology.com/blog/what-is-a-packet-analyzer
https://www.paessler.com/it-explained/packet-sniffing
https://www.parsdata.com/articles/what-is-packet-sniffing
https://searchnetworking.techtarget.com/answer/Whats-the-difference-between-packet-sniffers-and-protocol-analyzers