

→ User interaction like browser, team viewer...
هذا من الواقع يعني دخول المتصفح او البرامج التي يدخلها المستخدم

تحويل البيانات إلى Binary + عملية المخطط + التشفير وفك التشفير
Hello → 01011101

عمل واغلاق حماقة + الكشف عن انواع هدف صلاحيه
تصفح المتصفح + تنظيم الكاميرا

هي تساعد على تحديد الموجه وتنقلها خط الاتصال
الموجه / بحث الموجهات
ويتأكد من ادراكه
رسائل عن IP راجع عن IP

رسائل عن MAC ونحوها مثل الكواكب

هي مسؤولة عن الواسطط مثل الكواكب

الواع المهمات على المعنونة

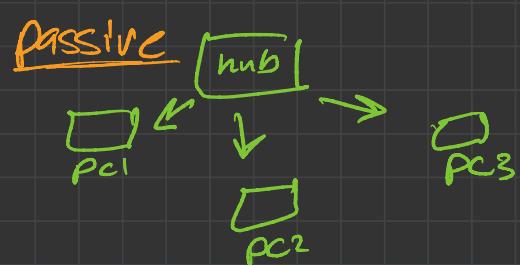
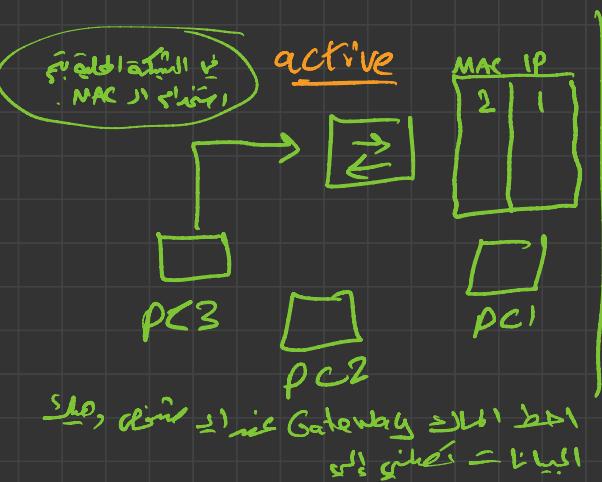
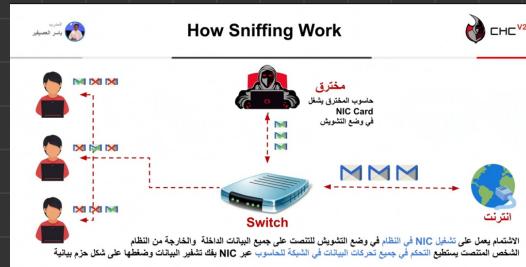
Network Sniffing

الاشتمام وهي عملية متابعة ومراقبة جميع البيانات الحزم العابرة عبر الشبكات باستخدام أي أداة للاشتتمام، الكثير من الشركات للأختراق منفذ اتصال الانترنت لديها مفتوحة وغير آمنة، اي مستخدم في نفس المكان يستطيع استخدام الانترنت باستخدام

:Sniffing

البيانات الحساسة التي تتسرب بواسطة عملية الـ **Ethernet Cable**

إعدادات الراوتر	Syslog Traffic	Telnet مرور	DNS Traffic	Email Traffic	Web Traffic	جلسات المحادثات	كلمات مرور FTP
-----------------	----------------	-------------	-------------	---------------	-------------	-----------------	----------------



يعمل على معاشرة كل المنشآت

- المختنق يجعل كلها ورثة

ا ببساطة

المخترق يحصل في الكمبيوتر الخاص به في منفذ موزع الاتصال Switch		1
يتشغيل أداة استكشاف وبحث للتعرف على البنية التحتية للشبكة		2
يستطع المخترق التعرف على جهاز الضحية ليتمكن من الهجوم		3
يستطع المخترق تسميم أو توثيق جهاز الضحية باستخدام ARP spoofing techniques		4
الإذدام الحركي Traffic hijacking في الشبكة وجهاز الضحية يتم تحويله بشكل أوتوماتيكي للبيانات للمخترق		5
يسنقر المخترق كلمات المرور والبيانات الحساسة من طريقة تحويل التلقائية للبيانات للمخترق		6

لثغرات البروتوكولات : Sniffing

HTTP بيانات مرسلة على شكل نصوص		IMAP كلمات المرور والبيانات المرسلة بشكل نصوص
Telnet and Rlogin ضربات مفاتيح لوحة المفاتيح بالإضافة إلى اسم المستخدم و كلمات المرور		SMTP and NNTP كلمات المرور والبيانات المرسلة بشكل نصوص
POP كلمات المرور والبيانات المرسلة على شكل نصوص		FTP كلمات المرور والبيانات المرسلة بشكل نصوص

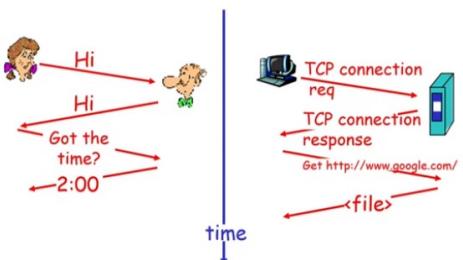
كيفية الدفاع ضد عملية Sniffing

Retrieve MAC Address Spoofing مباشرة من NIC بدلاً من نظام التشغيل هذه الطريقة سوف تمنع عمليات		WPA and WPA2 شفر اتصال اللاسلكي الوايبرس والبيانات بشفر قوي مثل		استخدام SFTP بدلاً من FTP لنقل الملفات بشكل آمن		HTTPS بدلاً من HTTP لحماية أسماء المستخدمين و كلمات المرور
Switch استخدام hub بدلاً من السويفيش ووصل البيانات للمستلم فقط		PGP and S/MIME, VPN, IPSec, SSL/TLS, Secure shell (SSH) . بالإضافة إلى استخدام One-time (passwords) (OTP		Switch استخدام hub بدلاً من السويفيش ووصل البيانات للمستلم فقط		Switch استخدام hub بدلاً من السويفيش ووصل البيانات للمستلم فقط



ما معنى بروتوكول Protocol ؟

هو لغة التواصل بين أجهزة الكمبيوتر المتصلة عبر الشبكة، بهدف تبادل المعلومات.



مصطلحات:

Protocol Suite 🔍
مجموعة من البروتوكولات

Protocol Stack 🔍
مجموعة بروتوكولات ترسل وتستقبل البيانات

TCP

؟ TCP 🔍

TCP : Transmission Communication Protocol

هو بروتوكول نقل الاتصال او ان مهمة هذا البروتوكول هي نقل البيانات عبر الشبكة. بروتوكول TCP يتحقق من وصول الارسال بين الحواسيب كما يتأكد من ان جميع الرزم التي ارسلاه تم استلامها من المهد الآخر . وفي حالة لم يصل هذه الرزم يقوم TCP بترسلها مرة ثانية . واما تم الاستلام يأخذ شهادة صدقته ويقوم بارسال الملفة الناقلة .



VS.

UDP

؟ UDP 🔍

UDP : User Datagram Protocol

وتعني بروتوكول بباقات بيانات.

كيف يعمل بروتوكول UDP ? 🔍

يقدم الرسالة الى اجزاء ويرسل هذه الاجزاء الى المستقبل مع وضع عنوان المستقبل في كل اجزاء رسائله وهذه الاجزاء لا تلتقي في الطريق في النهاية لذلك لا يوجد اي معاين لوصول الرسالة صحيفة ١٠٠٪ لأن هدف هذا البروتوكول هو إيصال الرسالة بسريع وقت ولين وصولها صحيفه.

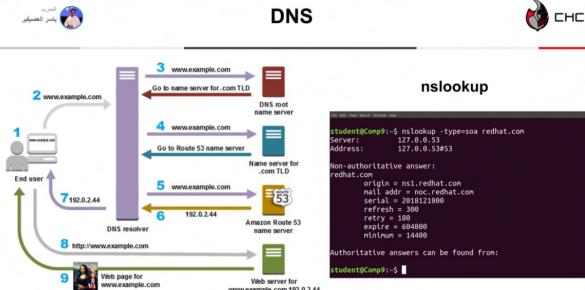
البروتوكولات

Port	Protocol	Service/Transport
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
143/1434	MSSQL	TCP

البروتوكولات

- Hypertext Transfer Protocol (HTTP)
- ARP (Address resolution protocol)
- Secure Hypertext Transfer Protocol (S-HTTP or HTTPS)
- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Simple Mail Transport Protocol (SMTP)
- Post Office Protocol 3 (POP3)
- Internet Mail Access Protocol 4 (IMAP4)
- Network Time Protocol (NTP)
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Simple Network Management Protocol (SNMP)
- Telnet & SSH
- ICMP

DNS



nslookup

```
student@Comp91:~$ nslookup -type=soa redhat.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
redhat.com.
origin = ns1.redhat.com
mail addr = noc.redhat.com
serial = 2011030500
refresh = 3600
retry = 600
expire = 684000
minimum = 14400

Authoritative answers can be found from:
```

Bastion Host

هو عبارة عن نظام حاسوب مصمم ومحظى لحماية مصادر الشبكة من أي عمليات هجوم، اي ببيانات تتصل الدخالة والخارجية من الشبكة يجب ان تمرر هذا الجدار الناري بمراحلتين:



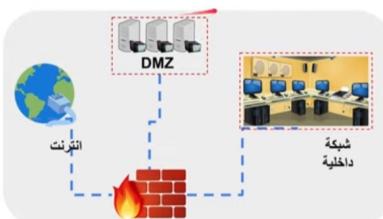
شبكة داخلية

Bastion Host

Firewall Architecture**Screened Subnet**

:The screened subnet or DMZ

عبارة عن مساحة إضافية تحتوي على استضافات توفر خدمات عامة



:The DMZ zone

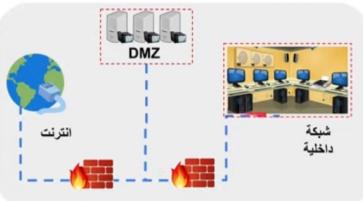
- تفاعل مع الطلبات العامة ولا تحتوى على استضافات للدخول إلى الشبكات الخاصة الداخلية

:Private zone

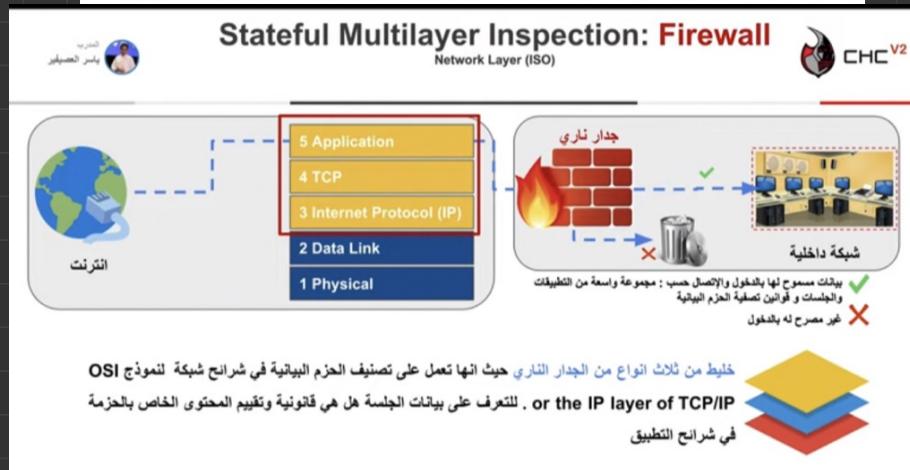
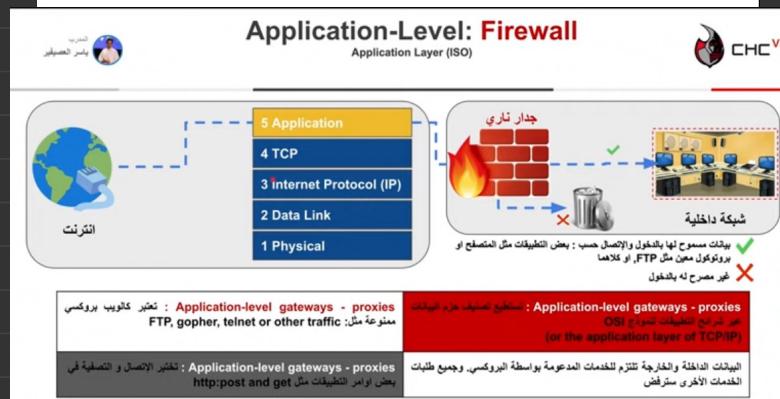
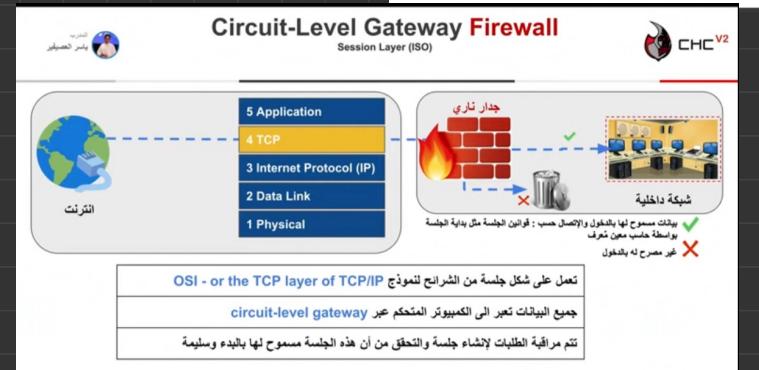
- لا يمكن الدخول عليها بواسطة مستخدمين الانترنت

Firewall Architecture**Multi-homed Firewall**

هو عبارة عن جدار ناري مع اثنين او اكثر من الوجهات المعروضة Interfaces لسماع بدخول اقسام فرعية من الشبكات على حسب بعض المتطلبات الحماية في الشركة.

**أنواع Firewall****Circuit Level Gateways****Packet Filters****Stateful Multilayer Inspection Firewalls****Application Level Gateways**

فيه كاملاً



Firewall Identification: Firewalking



هي تقنية تستخدم قيمة TTL للنقرف على المخرج ACL filtering ورسم مخطط الشبكات بواسطة ردود فعل حزم بيانات IP

1

يرسل المخترق حزم TCP and UDP لجدار الناري المستهدف مع TTL set to one hop اكبر من الجدار الناري

2

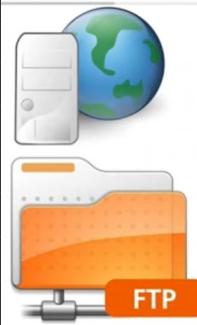
لو الحزم البيانية تحطت المخرج gateway سوف ترسل الى المركز الذي يحتوي على TTL and ICMP

3

هذه الطريقة تساعد في ثبيت الجدار الناري و خدمات إضافية مثل البصمة والتعرف على الثغرات

4

Firewall Identification: Banner Grabbing



:Banner
خدمة تتيهات متوفرة بواسطة خدمات الاستجابة لطلبات الاتصال واحتياها تحمل نسخة بيانات الباين.
وهي طريقة بسيطة للبصمة تساعد في التعرف على الجدار الناري للباين ونسمة الجدار الناري.

مثال على : SMTP banner grabbing :

Telnet mail targetcompnay.org 25

FTP •

Telnet •

Web servers •

Honeybot ↴

- المصيدة Honeypot



هي منفذ لمحاولة دخول او
لتلقيه المخترق و ضربات
الكمبيوتر الخاصة بالمخترق.



لا تحتوي على تصاريح
للمشاطها ولا تحتوي على حماية
او اي اتصال بها يكون عبارة عن
هوم



نظم مصادر معلوماتية
متخصصة لإصطدام وطلب
المخترين الذين يحاولون
اقتحام شبكة الشركة



Type of Honeypot



هذا النوع يحاكي كمية محددة من الخدمات والتطبيقات للنظام المستهدف او الشبكة

هذا النوع يحصل على جميع البيانات بشكل متماثل عن الصنفية مثل الشبكة ونشاطات البرمجيات

الخبيثة مثل: Specter, Honeyd, KFsensor



Low-interface Honeypots

هذا النوع يحاكي جميع نوع الخدمات والتطبيقات

يمكن تسويفه بشكل كامل بواسطة المخترق الحصول على خمول كامل للنظام

تبع وقطع كل البيانات عن عملية الهجوم مثل طريقة الهجوم، الأدوات، والتوابع للآخر في Symantec Decoy server and Honeynets:

مثل:蜜罐网关和蜜罐服务器



High-interface Honeypots

IDS

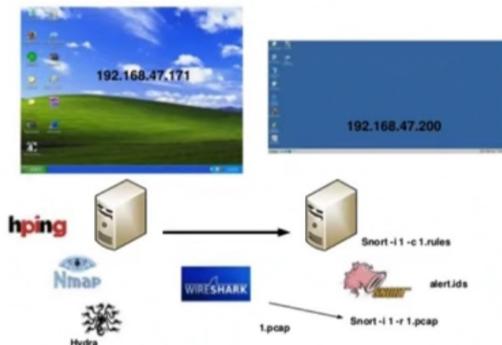


IDS



ما هو IDS؟

Intrusion Detection System



نظام حماية يشبه مضاد الفيروسات الموجود على أجهزتنا يقوم بتحليل كل Traffic عبر الشبكة. الهدف من IDS هو تحليل Traffic وتحذيرنا في حالة كان هناك خطر محتمل أو هجنة محتملة تستهدف جهازنا أو شبكتنا.

أهمية في عالم الانترنت؟

كشف الثغرات الموجودة في أنظمة الحماية

أرسفة كل أنواع التهديدات التي تحدث للشبكة

تحديد الأخطاء التي وقع فيها مسؤولين الحماية وتصحيحها



Intrusion Detection Tool: Snort

```
Administrator: Símbolo del sistema
C:\>Snort>snort
--> Snort! <-
      Version 2.8.5.3-ODBC-MySQL-FlexRESP-WIN32 GRE <Build 124>
      By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
      can
      Copyright (C) 1998-2009 Sourcefire, Inc., et al.
      Using PCRE version: 7.4 2007-09-21
      USRGTE: snort -c <options>
      snort -S<SERVICE> /INSTALL <c-options> <filter options>
      snort -S<SERVICE> /UNINSTALL
      snort -S<SERVICE> /SHOW
      Options:
      -q      Set alert node: fast, full, console, test or none <alert fil
      e alerts only>
      -b      Log packets in tcpdump format <much faster!>
      -B <mask> Obfuscate IP addresses in alerts and packet dumps using CIDR
      mask
      -c <rules> Use Rules File <rules>
      -C      Print out payloads with character data only <no hex>
      -d      Dissect the Application Layer
      -D      Dump raw bytes to file <header info>
      -E      Log alert messages to NT Eventlog. <Win32 only>
      -f      Turn off fflush() calls after binary log writes
      -F <file> Read BPF filters from file <file>
      -G <file> Read configuration file uniquely id events for multiple snorts
      -H <file> Read configuration file
      -I <file> Read interface configuration file
      -L <file> Listen on interface <file>
      -M <mode> Choose mode: <all>,<snmp>,<ntcp>,<ndnp>,<noicnp>,<none>
      -N <mode> Logging mode: <pcapdefault>,<ascii>,<none>
      -l <file> Log to directory <file>
      -L <file> Log to this tcpdump file
      malavida.com
```

- نظام مفتوح المصدر للتعرف على الشبكات المصابة أو المخترقة وتحليل بيانات الاتصال وحزم البيانات في الشبكة بشكل مباشر وهي

- إمكانية تحليل البروتوكولات ومحظى البحث والتطبيق وستستخدم أيضاً للتعرف على الهجمات مثل: overflows, stealth port scan, CGI attacks

- مرنة في الاستخدام وسهولة في شرح كيفية جمع الإتصالات او غيره والتعرف على الآلة والبيئة

- :Snort يستخدم

- اشتام حزم لبيانات مثل packet logger
- tcpdump

- نظام لمنع الشبكات من الاختراق او التلاعب

Snort Rules



هي عبارة عن قواعد لتلبية احتياجات الشبكة. يساعد للتفرق بين الشفاطات الطبيعية للانترنت والنشاطات الخبيثة.

:Snort Rules

هي عبارة عن قواعد لتلبية احتياجات الشبكة. يساعد للتفرق بين الشفاطات الطبيعية للانترنت والنشاطات الخبيثة.

يوجد جزئين منطقين:

.alerts, log, pass, activate, dynamic, .rule header

يوجد جزئين منطقين:

.rule options



Snort Rules: Rule Actions and IP Protocols

IP Protocols	Rule Actions
TCP UDP	 :The rule header يحدد ثلاثة أنواع من البروتوكولات التي تدعى لها

:The rule header يحدد ثلاثة أنواع من البروتوكولات التي تدعى لها

الأفضل التي تطبقه

الأخيرة وجد حزمة بيانات متغيرة مع معايير

القواعد

:Snort يحدد نوع من القواعد للأ

Alert-1

Log-2

Pass-3

الـ Session Hijacking

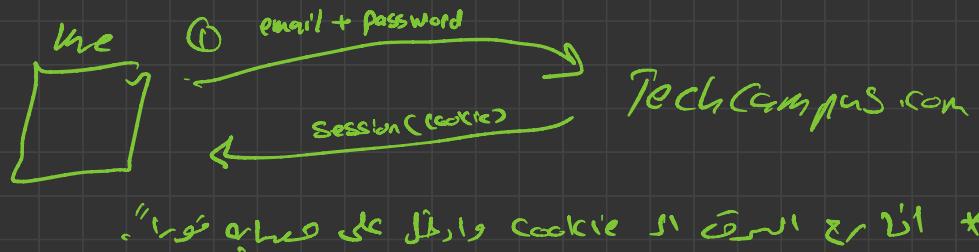
Session Hijack

1- Session Hijacking هو عبارة عن هجوم يحدث عندما يستلم المخترق التحكم باتصال فعال لجسسة ياستخدام منفذ TCP.

2- وبما أن أغلب جلسات الـ TCP تبدأ بطريقة فقط بالتحقق يسمح للمخترق من الدخول على الجهاز.

3- المخترق يعمل على sniffing اشتمام البيانات والاتصالات من بدء الجلسة TCP و التعرف على كيفية السرقة و بيانات السارق وغيرها.

4- المخترق يسرق رمز لجسسة فعالة و يستخدمه للتحقق بنفسه من الخادم



Why Session Hijacking is Successful ?

	رموز الجلسات الفير
	مضاد مفاصد
	أغلب البروتوكلات لا تبدأ بالعمل بعد استخدام التشفير
	الحواسيب تُغافل
	تُستخدم TCP/IP
	لاحدود ولا حظر على رموز الجلسة الفير
	فتقد
	Weak session ID generation algorithm or small session IDs
	التعريف على وقت انتهاء الجلسة

Session Hijacking Process		
Brute Forcing 	التخمين 	السرقة

المخترق يحاول تخمين رمز الجلسة بواسطة
رموز الجلسة ID . هذه بعضطرق المستخدمة لسرقة رمز الجلسة:

- Sniffing network traffic
- Use HTTP referer header
- Send Trojan on client machine
- Using Cross-site-scripting attacks

Session Hijacking Process

طريقة سرقة رمز جلسة ID

1- باستخدام Referrer attack يمكن للمخترق تحويل المخادعه باطريقه المستخدم للنضج على رابط موقع خبيث مثل موقع : www.hacksite.com

عند ضغط المستخدم على هذا الرابط سوف يتم تحويله تلقائياً بالمتصلع الى موقع اخر ملغم بذوق عمه هذا الرابط يرسل رمز الجلسة اليه الى موقع المخترق في هذه الحالة يستطيع المخترق على رمز الجلسة للمستخدم

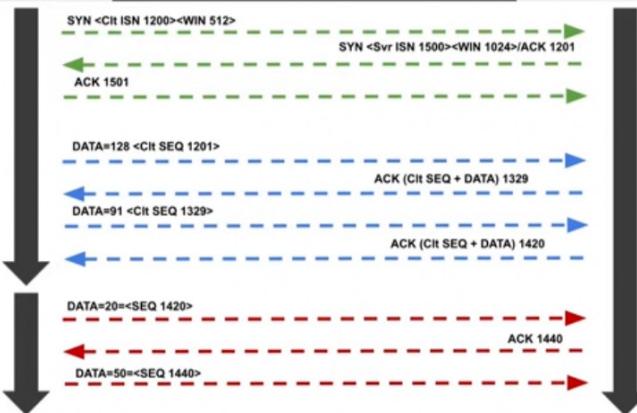
2-



ضحية



مخترق



خادم

قبل ما يرسل الضحية حزمة بيانات يقوم المخترق بتغيير الرقم التسلسلي التالي وارسال البيانات الى الخادم. هذه الطريقة قد تنشأ اتصال بين المخترق والخادم.

Spoofing vs. Hijacking

Spoofing



المخترق يمثل انه مستخدم آخر او جهاز ضحية للدخول على النظام
المخترق لا يستولى على الجلسات الفعالة ولكن يتم إنشاء جلسة جديدة باستخدام معلومات الدخول للضحية

Hijacking



اخطاف الجلسة هي خطوات للتحكم في اي اتصال حالياً فعال
المخترق يعتمد على مستخدم موثوق لعمل الاتصال والتحقق

Types of session Hijacking



مخترق



ضحية

Passive

المخترق يختطف الجلسة ولكن لا يتحكم بها فقط يقوم بتجسس ومراقبة جميع الاتصالات المرسلة

Active

عليها

Session Hijacking in OSI Model

هي عبارة عن إيقاف الحزم البيانات خلال الانتقال بين العميل والخادم في جبنة TCP and UDP

Network Level Hijacking



الحصول على التحكم على جلسات المستخدمين HTTP's بواسطة الحصول على رمز الجلسة

Application Level Hijacking



Wireshark - Filters

Frame Relay		ICMPv6	
Voice-Wireshark_Display_Filters.pdf	fr.ds	icmpv6.all_cop	icmpv6.option.name.type.tqde
fr.chdlctype	fr.dcli	icmpv6.checksum	icmpv6.option.name.x501
fr.control	fr.dstore_control	icmpv6.checksum.bad	icmpv6.option.rss.key.hash
fr.dscontrol_r	fr.dscontrol_r	icmpv6.dscontrol	icmpv6.option.rss.lifetime
fr.control_type	fr.foce	icmpv6.dscontrol	icmpv6.rss.cur_hop_limit
fr.control_n_r	fr.lower_dcli	icmpv6.hdr_hw_addr	icmpv6.rs.reachable_time
fr.control_n_s	fr.rapid	icmpv6.identifier	icmpv6.rs.retrans_timer
fr.control_p	fr.second_dcli	icmpv6.option	icmpv6.rs.router_lifetime
fr.second_dcli_type	fr.secnd_dcli	icmpv6.option.cgi	icmpv6.resursive_dns_serv
fr.control_n_modifier_cnf	fr.snp	icmpv6.option.length	icmpv6.type
fr.control_n_modifier_resp	fr.sntype	icmpv6.option.name_type	
fr_cr	fr.third_dcli		RIP
fr_dc	fr.upper_dcli	rip.auth.passwd	rip.route_map
PPP		rip.auth.type	rip.metric
ppp.address	ppp.direction	rip.command	rip.routing_domain
ppp.control	ppp.protocol	rip.family	rip.netmask
MPLS		BGP	
mpls.buttons	mpls.oam_detect_location	bgp_aggregator_as	bgp_ip_neigh_nrib.ipv6_prefix
mpls_oam_control	mpls_oam_detect_type	bgp_aggregator_origin	bgp_ip_neigh_nrib.ipv6_prefix
mpls_oam_f	mpls_oam_freeness	bgp_ip_neigh_nrib_path	bgp_ip_neigh_nrib_disc
mpls_exp	mpls_oam_function_type	bgp_ip_neigh_nrib_identifier	bgp_neigh_hop
mpls_label	mpls_oam_ttl	bgp_ip_neigh_nrib_list	bgp_ip_neigh_prefix
mpls_oam_bip16	mpls_tt	bgp_community	bgp_originator_id
ICMP		bgp_community_value	bgp_originator_id
icmp.ident	icmp.seq	bgp_local_pref	bgp_type
icmp.checksum_bad	icmp.stu	bgp_ip_nrib_tnh_id	bgp_withdrawn_prefix
icmp.code	icmp.redirect_gw		
DTP		HTTP	
dtp.neighbor	dtp_tv_type	http.accept	http.proxy_authorisation
dtp_tv_tv	dtp.version	http.accept_encoding	http.proxy_connect_host
		http.accept_language	http.proxy_connect_port
		http.authbasic	http.referrer

Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.dst.hw_mac
eth.dst	eth.lg	arp.dst.proto_ip4
eth.ig	eth.multicast	arp.hw.size
	eth.type	arp.src.hw_mac
		arp.src.proto_ip4
		arp.type
		arp.opcode
		TCP
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	
ip.dsfield.dsfp	ip.version	
Ethernet	Ethernet	ARP
eth.addr	eth.len	arp.proto.size
eth.dst	eth.lg	arp.proto.type
eth.ig	eth.multicast	
	eth.type	
IEEE 802.1Q	IPv4	
vlan.cfi	vlan.id	vlan.priority
vlan.etype	vlan.len	vlan.trailer
IPv4		
ip.addr	ip.fragment.overlap.conflict	
ip.checksum	ip.fragment.toolongfragment	
ip.checksum_bad	ip.fragments	
ip.checksum_good	ip.hdr_len	
ip.dsfield	ip.host	
ip.dsfield.ce	ip.id	
ip.dsfield.dsdp	ip.len	
ip.dsfield.ect	ip.proto	
ip.dsfield.dsfp	ip.reassembled_in	
ip.dsfield.dsfp	ip.src	
ip.dsfield.dsfp	ip.src_host	
ip.dsfield.dsfp	ip.tos	
ip.dsfield.dsfp	ip.tos.cost	
ip.dsfield.dsfp	ip.tos.delay	
ip.dsfield.dsfp	ip.tos.precedence	
ip.dsfield.dsfp	ip.tos.reliability	
ip.dsfield.dsfp	ip.tos.throughput	
ip.dsfield.dsfp	ip.ttl	

