



程序代写代做 CS编程辅导

Network Security & Attacks – Part II

WeChat: cstutorcs

Assignment Project Exam Help

COMP90073
Email: tutorcs@163.com
Security Analytics

QQ: 749389476
Dr. Yi Han, CIS

<https://tutorcs.com>
Semester 2, 2021

Outline

程序代写代做 CS编程辅导

- More Network Attacks



- Network Security System

- Case Study – Network Attack Traffic Analysis

WeChat: cstutorcs
Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

- Spoofing Attacks & BGP Hijacking Attack



- Password Attacks

- Wireless Attacks

WeChat: cstutorcs

- Key Patterns for Well-Known Attacks

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- **Spoofing attack:** an attacker impersonates another device to execute an attack
 - **IP address spoofing attack:** The attacker sends IP packets from a fake source address in order to make the network believe the packet came from itself. DDoS attacks typically use IP spoofing to make the source of the attack appear to be from legitimate source IP addresses
 - **ARP spoofing attack:** The attacker sends spoofed ARP packets across the Layer 2 network in order to link the attacker's MAC address with the IP address of a legitimate host
 - **DNS server spoofing attack:** The attacker modifies the DNS server in order to reroute a specific domain name to a different IP address. DNS server spoofing attacks are typically used to spread malware
- **BGP hijacking attack:** a common router manipulation attack, can be launched by an attacker by configuring or compromising an edge router to announce prefixes that have not been assigned to his or her organization, to reroute victim's traffic to the attacker

程序代写代做 CS 编程辅导



WeChat: cstutorcs

Assignment Project Exam Help

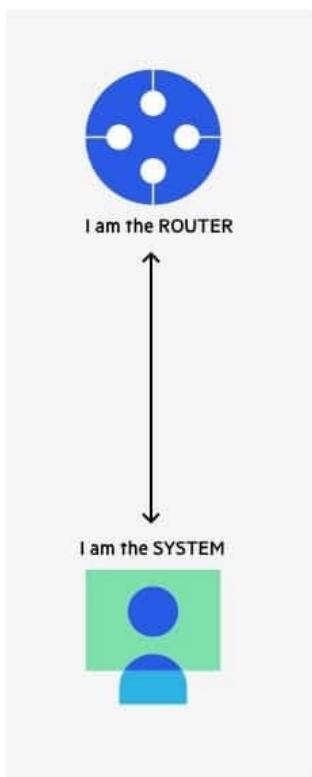
Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

ARP spoofing



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

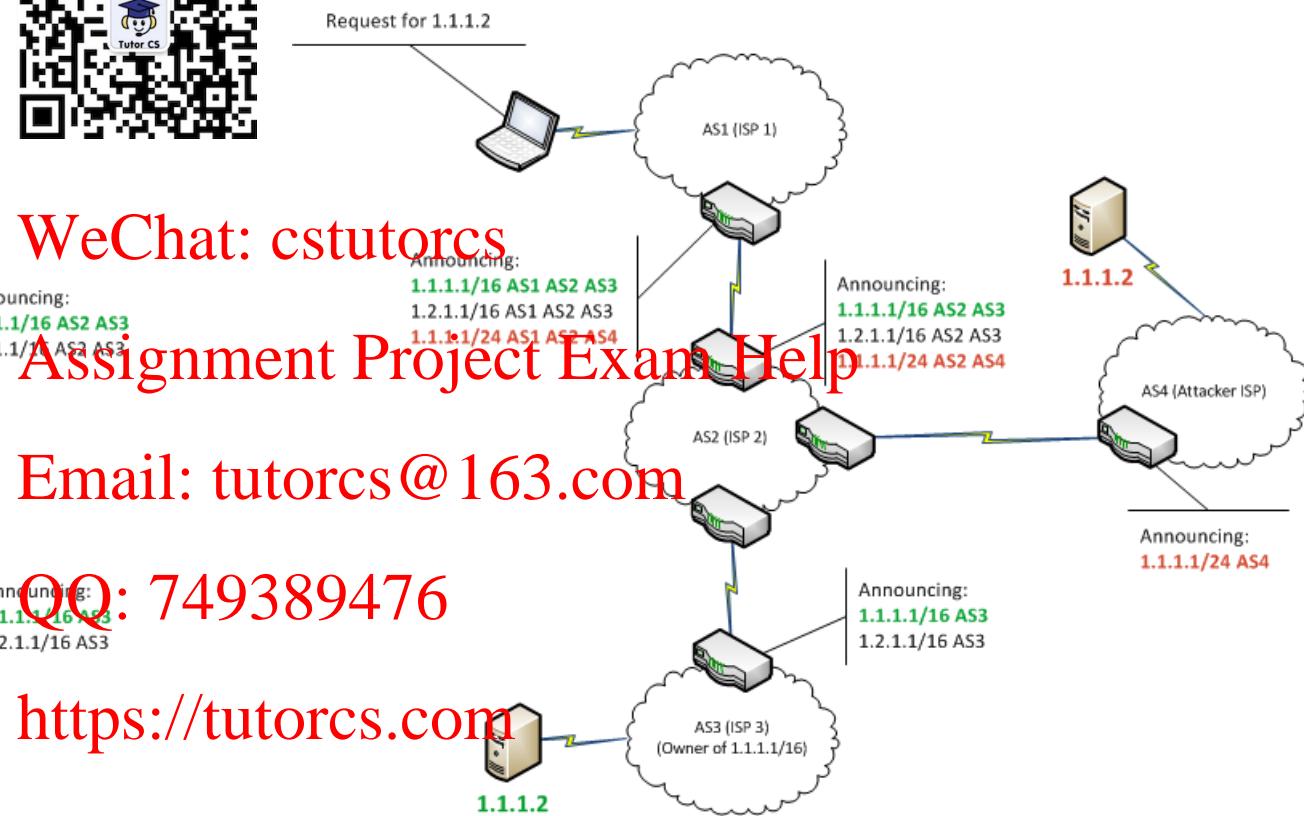
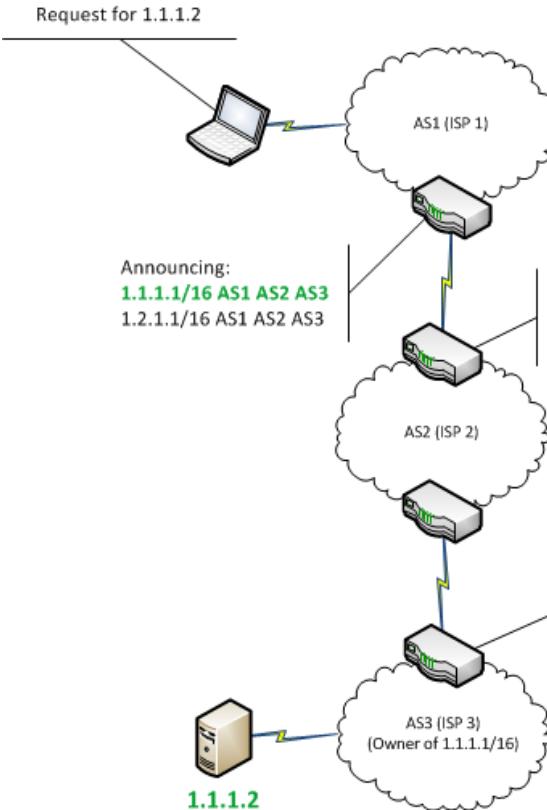
QQ: 749389476



https://www.imperva.com/learn/wp-content/uploads/sites/13/2020/03/thumbnail_he-ARP-spoofing-attacker-pretends-to-be-both-sides-of-a-network-communication-channel.jpg.webp

- BGP Hijacking

程序代写代做 CS编程辅导



<https://labs.bishopfox.com/tech-blog/2015/08/an-overview-of-bgp-hijacking>

程序代写代做 CS编程辅导

- **Password-guessing attack:** This is the most common type of password attack, but sometimes these techniques may be very inefficient. Threat actors can guess passwords locally or remotely using either a manual or automated attack.
- **Password-resetting attack:** In many cases, it is easier to reset passwords than to use tools to guess them. Several cracking tools just attempt to reset passwords. In most cases, the attacker boots from a USB or CD-ROM to bypass typical Windows protections

QQ: 749389476

<https://tutorcs.com>



程序代写代做 CS编程辅导

- **Password cracking:** These attacks work by taking a password hash and converting it to its ciphertext. In this case, the attacker needs tools such as extractors, guessing, rainbow tables for looking up plaintext passwords, and word sniffers to extract authentication information



WeChat: cstutorcs

- **Password sniffing:** The threat actor just sniffs authentication packets between a client and server and extracts password hashes or enough authentication information to begin the cracking process

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

- **Password capturing:** This is typically done by using key loggers or Trojan horses

<https://tutorcs.com>

程序代写代做 CS编程辅导

- **Installing a rogue access point:** The attacker basically installs an access point and can create a backdoor and obtain access to the network and its systems.
 - **Jamming wireless signals and causing interference:** The purpose of this attack is to cause a ~~WeChat~~ ~~tutors~~ full or partial denial-of-service condition in the wireless network
 - **Evil twin attack:** This is done when the attacker is trying to create rogue access points so as to gain access to the network or steal information, e.g.,
 - the attacker purchases ~~https://tutors.com~~ wireless access point, plugs it into the network, and configures it exactly the same as the existing network



Assignment Project Exam Help

程序代写代做 CS 编程辅导

- **War driving:** This is a methodology used by attackers to find wireless access points wherever they may be. The term war driving is used because the attacker can just drive around and gather a huge amount of information over a very short period of time



- **Bluejacking:** The attacker sends unsolicited messages to another device via Bluetooth

WeChat: cstutorcs

- **IV attack:** The attacker can cause some modification on the Initialization Vector (IV) of a wireless packet that is encrypted during transmission. The goal of the attacker is to obtain a lot of information about the plaintext of a single packet and generate another encryption key that then can be used to decrypt other packets using the same IV

Assignment Project Exam Help

Email: tutorcs@163.com

- **WEP/WPA attack:** WEP and several versions of WPA are susceptible to different vulnerabilities and are considered weak

QQ: 749389476
<https://tutorcs.com>

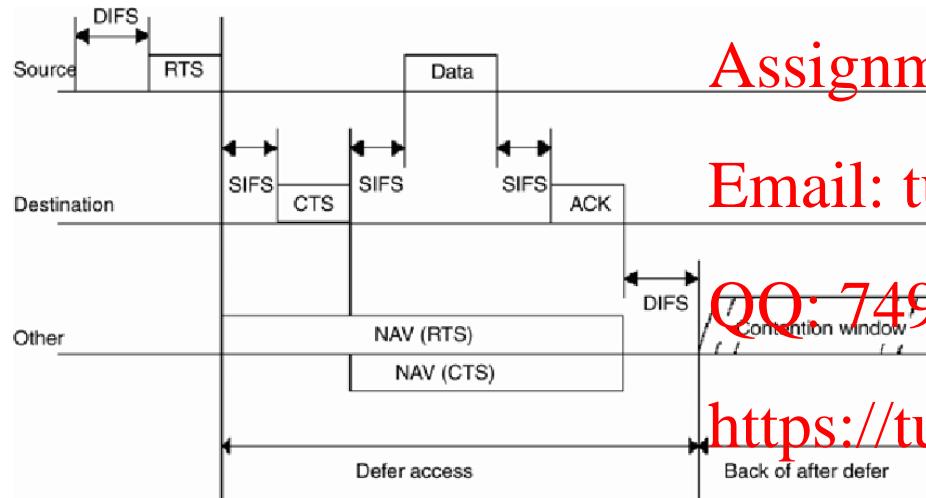
- **WPS attack:** This attack is carried out with WPS password-guessing tools to obtain the WPS passwords and use them to gain access to the network and its data

程序代写代做 CS编程辅导

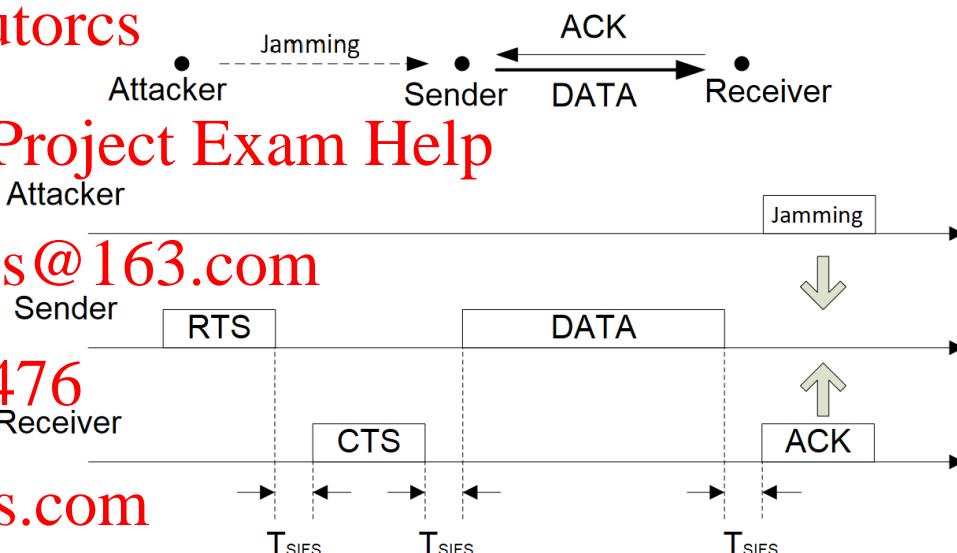
- RTS/CTS
- Jamming attacks [3]:
 - Constant jamming
 - Reactive jamming
 - Random and periodic jamming



WeChat: cstutorcs



RTS/CTS



Reactive jamming

程序代写代做 CS编程辅导

Index Patterns (alert signatures) Attack types

1	srcIP		scans
2	srcIP + srcPrt		crowds response (Jung et al., 2002)
3	srcIP + dstPrt		DDoS launched by Trinoo (CERT Coordination Center, 1999)
4	srcIP + protocol		WeChat: cstutorcs Most worms
5	srcIP + srcPrt + dstPrt		Distributed reflector DoS (Gibson, 2002)
6	srcIP + srcPrt + protocol		SYN flood response (CERT Coordination Center, 1996)
7	srcIP + dstPrt + protocol		Assignment Project Exam Help Email: tutorcs@163.com QQ: 7049389476 W32/Blast worm (CERT Coordination Center,
8	srcIP + srcPrt + dstPrt + protocol		SQL-Slammer worm (CERT Coordination Center, https://tutorcs.com)

Patterns and their corresponding attack activities (Source: [2])

程序代写代做 CS 编程辅导

- **Pattern 1** consists of a single feature - source IP address (srcIP). In most large scale scan scenarios, a common source IP address can be observed across different network domains. Hackers try to map the whole network at once



- **Pattern 2** consists of the combination of source IP address and source port (srcIP + srcPrt). For example, during a flashcrowd (a huge number of hosts create excessive connections to unintentionally overwhelm a server) on a webserver, there are a large number of responses from this webserver that will be sent out in reply to the flashcrowd requests. Consequently, it can be observed that there are many HTTP (srcPrt = 80) traffic flows from this web server(srcIP)

WeChat: cstutorcs
Assignment Project Exam Help
Email: tutorcs@163.com

QQ: 749389476

- **Pattern 3** consists of the combination of source IP address and destination port (srcIP + dstPrt). For example, this pattern can be observed when a master controller instructs its daemons or slave hosts (on destination port 27444) to launch a denial of service attack against a target system

程序代写代做 CS编程辅导

- **Pattern 4** consists of the combination of source IP address and protocol (srcIP + protocol). In most worm  when an infected system tries to spread itself to others, this pattern can be observed across different subnetworks
- **Pattern 5** consists of the combination of source IP address, source port, and destination port (srcIP + srcPrt + dstPrt). For example, this pattern can be observed during a distributed reflector DoS attack

WeChat: cstutorcs
Assignment Project Exam Help

- **Pattern 6** consists of the combination of source IP address, source port and protocol (srcIP + srcPrt + protocol). For example, if a target is undergoing a large-scale SYN flood attack, there will be a large number of SYN-ACK packets sent by the target in reply to the attack sources. From the perspective of the subnetworks that contain the attack sources, they will see many SYN-ACK packets (protocol = TCP) arriving where there is no ongoing transaction, sent by a target system on a certain port (srcIP)

程序代写代做 CS编程辅导

- **Pattern 7** consists of the combination of source IP address, destination port and protocol (srcIP + dstPrt + protocol). For example, this pattern was observed during the ~~WannaCry~~ Master worm outbreak



- **Pattern 8** consists of the combination of source IP address, source port, destination port and protocol (srcIP + srcPrt + dstPrt + protocol). For example, this pattern can be observed across different network domains when an infected system tries to spread itself to others during SQL-Slammer worm outbreak

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导



- Traditional and next-generation firewalls

WeChat: cstutorcs

Assignment Project Exam Help

- Intrusion detection systems (IDSs) & intrusion prevention systems (IPSS)

Email: tutorcs@163.com
QQ: 749389476

<https://tutorcs.com>

Traditional & Next-Generation Firewalls

- Firewalls: devices placed between a trusted and an untrusted network



- Network-based firewalls

QQ: 749389476

- Provide key features used for perimeter security
<https://tutorcs.com>
- Primary task is to deny or permit traffic that attempts to enter or leave the network based on explicit preconfigured policies and rules

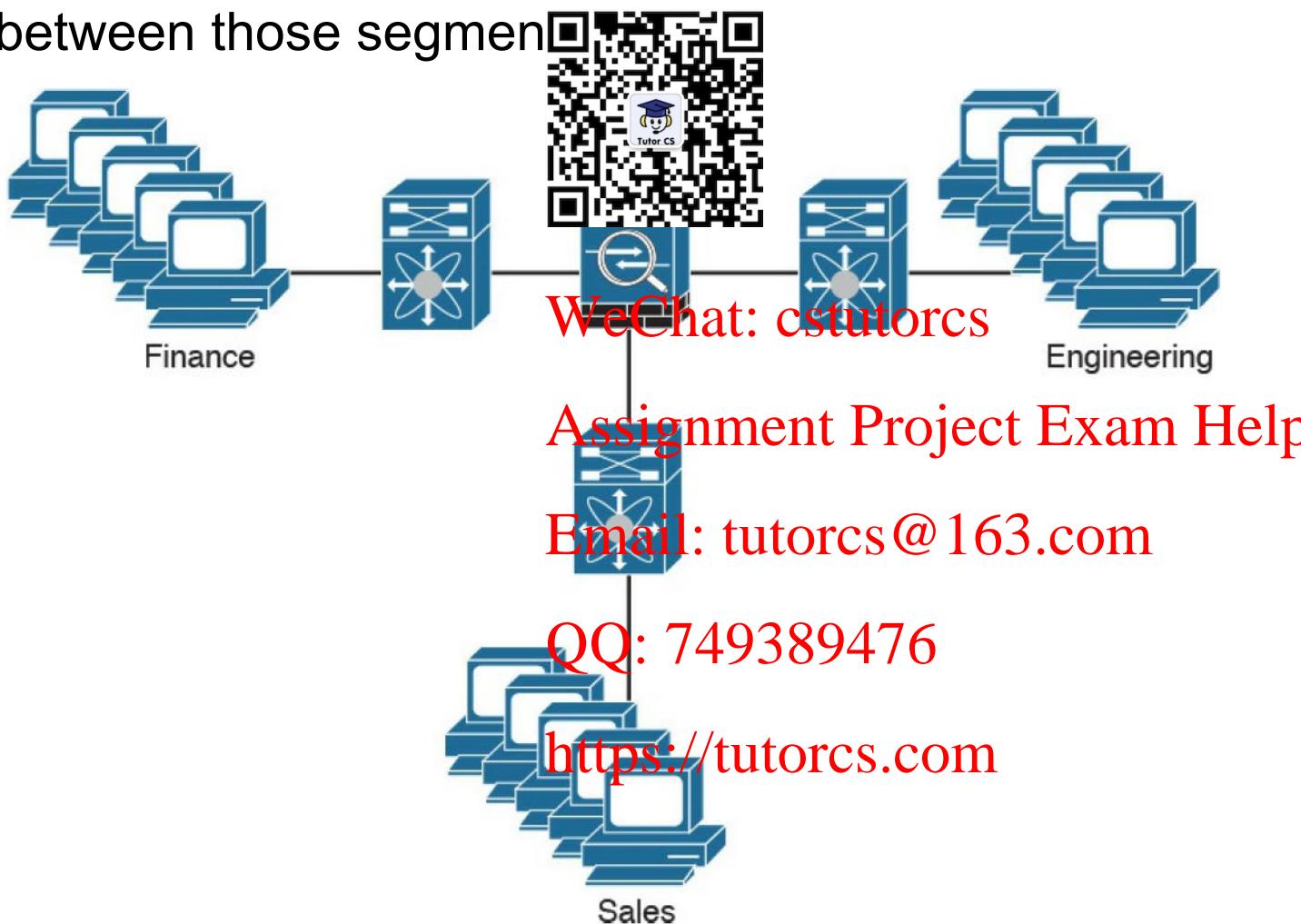
程序代写代做 CS编程辅导

- Demilitarized zones (DMZ): provide security to the systems that reside within them with different security levels and policies between them, e.g.,



Traditional & Next-Generation Firewalls

- Firewall provides **network segmentations** while enforcing policy between those segments



程序代写代做 CS编程辅导

- How do firewalls allow or block traffic:

- Packet-filtering tech



- Application proxies

WeChat: cstutorcs

- Network address translation (NAT)

Email: tutorcs@163.com

- Stateful inspection firewalls

QQ: 749389476

- Next-generation context-aware firewalls

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Purpose: to control access to specific network segments by defining which traffic can pass through them



- ACL (Access Control List): a set of predetermined rules
 - Configured in firewalls, routers, switches, wireless access controllers, and etc.
 - ACE (Access Control Entry): each entry of an ACL, it inspects OSI Layer 2 – 4 headers
 - Layer 2 protocol information such as EtherTypes
 - Layer 3 protocol information such as ICMP, TCP, or UDP
 - Layer 3 header information such as source and destination IP addresses
 - Layer 4 header information such as source and destination TCP or UDP ports

程序代写代做 CS编程辅导

— ACL common practices

- When a new ACE is added to an existing ACL, it is appended to the end of the ACL



- When a packet enters the firewall, the ACEs are evaluated in sequential order. Hence, the order of an ACE is critical

WeChat: cstutorcs

- Implicit deny at the end of all ACEs

Email: tutorcs@163.com

- Return traffic for TCP/UDP is automatically allowed since the connections are considered established and bidirectional
- Return traffic for other protocols such as ICMP is automatically denied since the connections are considered unidirectional

<https://tutorcs.com>

程序代写代做 CS编程辅导

— ACL configuration example on Cisco ASA

- First two ACEs allow traffic destined for 10.10.202.131 and 209.165.202.131 from both client machines
- Last two ACEs allow access to 10.10.20.112 from both machines

WeChat: cstutorcs

```
ASA# configure terminal
ASA(config)# access-list outside_access_in remark ACL to block inbound traffic except
HTTP and SMTP
ASA(config)# access-list outside_access_in extended permit tcp host 10.10.10.1 host
10.10.202.131 eq http
ASA(config)# access-list outside_access_in extended permit tcp host 10.10.10.2 host
209.165.202.131 eq http
ASA(config)# access-list outside_access_in extended permit tcp host 10.10.10.1 host
10.10.20.112 eq smtp
ASA(config)# access-list outside_access_in extended permit tcp host 10.10.10.2 host
10.10.20.112 eq smtp
```

Assignment Project Exam Help
Email: tutorcs@163.com
QQ: 749389476
<https://tutorcs.com>

程序代写代做 CS 编程辅导

- Operate as intermediary agents on behalf of clients that are on a private or protected network



- Clients on the protected network send connection requests to the application proxy to transfer data to the unprotected network or the Internet

WeChat: cstutorcs

- Application proxy (or web proxy) sends the request on behalf of the internal client

Email: tutorcs@163.com

- Work at OSI Layer 7

QQ: 749389476

<https://tutorcs.com>

- Most proxy firewalls can cache information to accelerate their transactions

程序代写代做 CS 编程辅导

- NAT: translate the internal host's private (or real) IP addresses to a publicly routable (or real) address, e.g.,

Host A Private (Physical) Address
10.10.10.123



(Inside)



Firewall

Translated Address
209.165.200.227

(Outside)



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

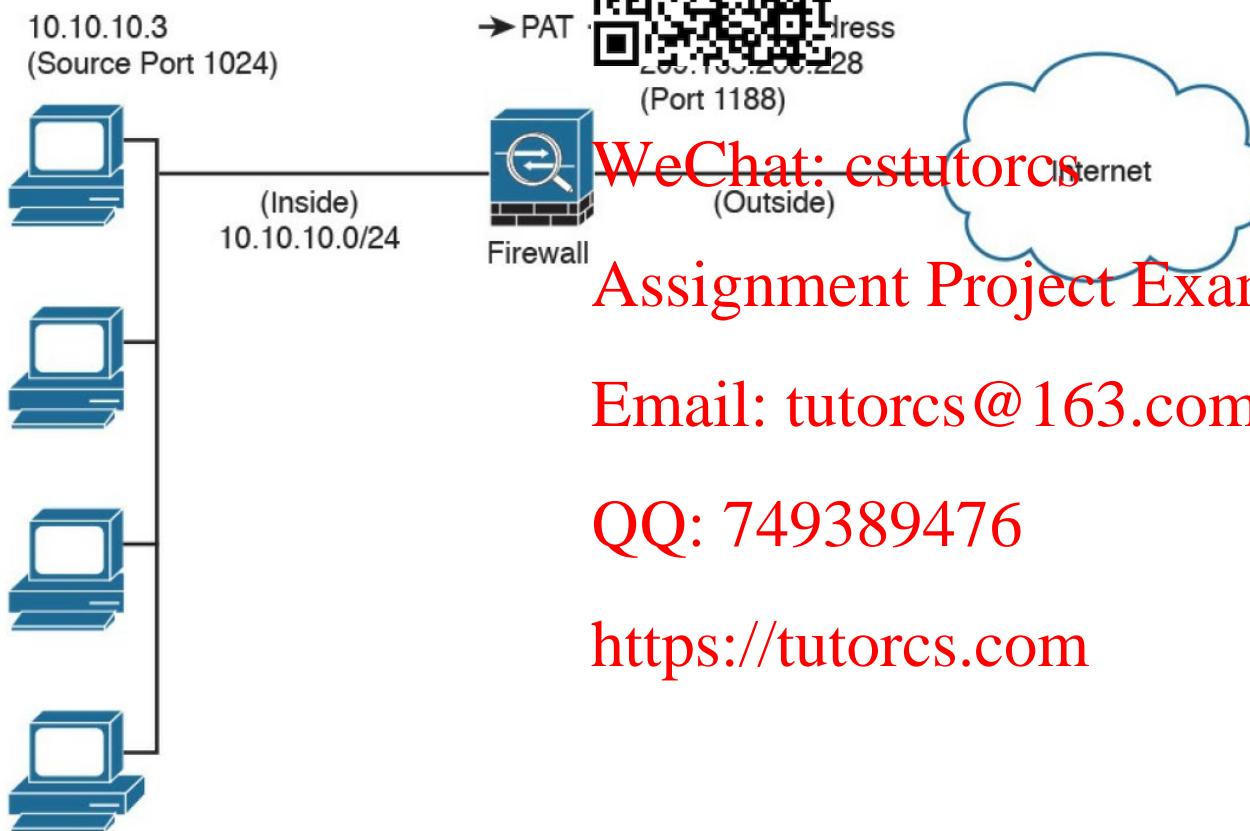
<https://tutorcs.com>

Class	IP Address Range	Networks	Number of Hosts
Class A	10.0.0.0 to 10.255.255.255	1	16,777,214
Class B	172.16.0.0 to 172.31.255.255	16	65,534
Class C	192.168.0.0 to 192.168.255.255	256	254

RFC 1918 Private Address Ranges (Source: [1])

程序代写代做 CS编程辅导

- Port Address Translation (PAT): a subset of NAT, it allows many devices on the internal network to share one IP address by inspecting the Layer 4 port information on the packet, e.g.,



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Track every packet passing through their interfaces by ensuring that they are valid, especially connections.



- Examine not only the header contents but also the application layer information within the payload

WeChat: cstutorcs

- Different rules can be created on the firewall to permit or deny traffic based on specific payload patterns

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

- State table: database of the state of the connection detailing whether such a connection has been established, closed, reset, or is being negotiated

<https://tutorcs.com>

程序代写代做 CS编程辅导



- Context-aware firewalls are aware of not only the applications and users accessing the internet but also the device in use, the location of the user, and the time of day

WeChat: cstutorcs

Assignment Project Exam Help

- Provide granular control of applications, comprehensive user identification, and location-based control

Email: tutors@163.com
QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导



- Traditional and next-generation firewalls

WeChat: cstutorcs

Assignment Project Exam Help

- Intrusion detection systems (IDSs) & intrusion prevention systems (IPSS)

Email: tutorcs@163.com
QQ: 749389476

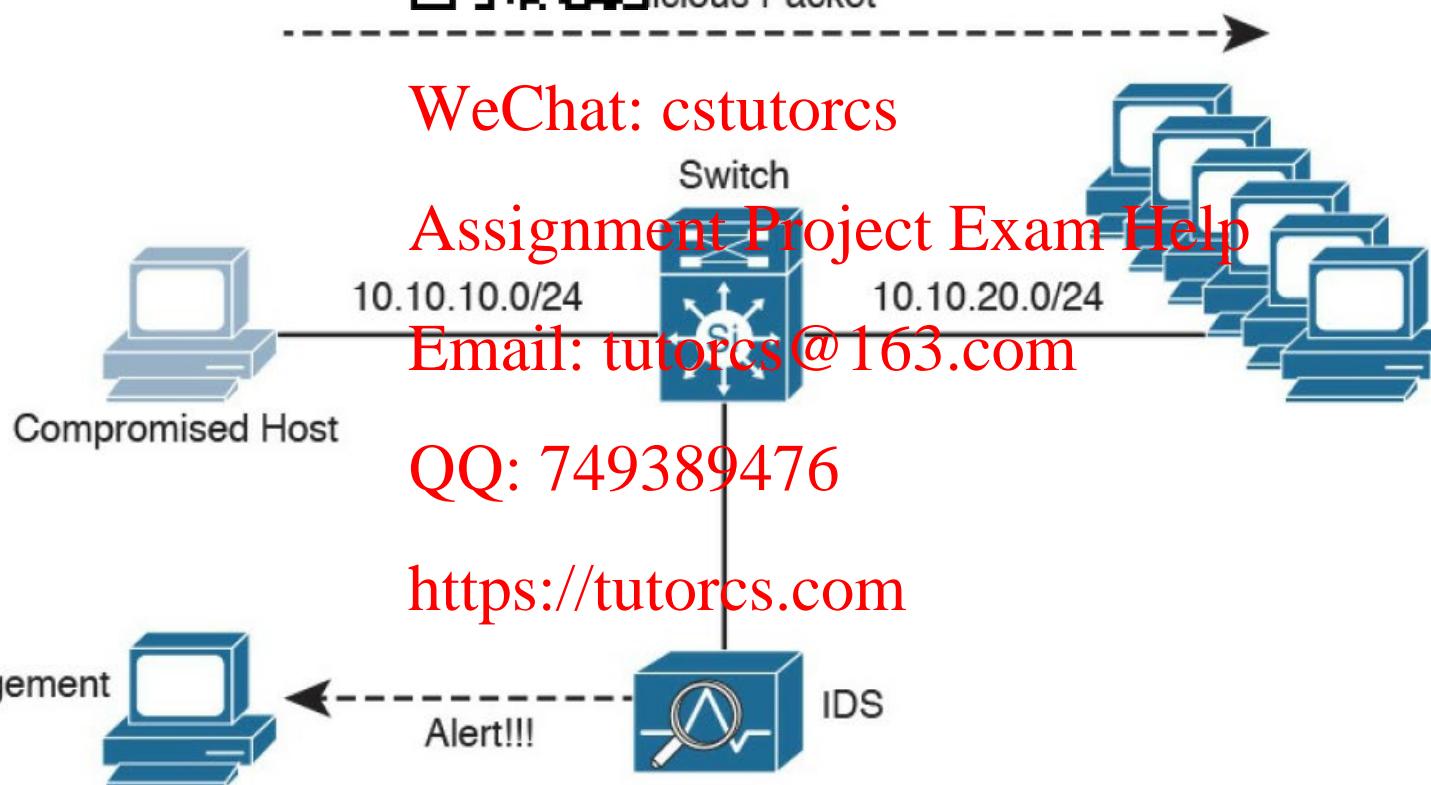
<https://tutorcs.com>

程序代写代做 CS编程辅导

- IDSs: Devices that detect attempts from an attacker to gain unauthorized access to a network or a host, to create performance degradation, to steal information, e.g.,

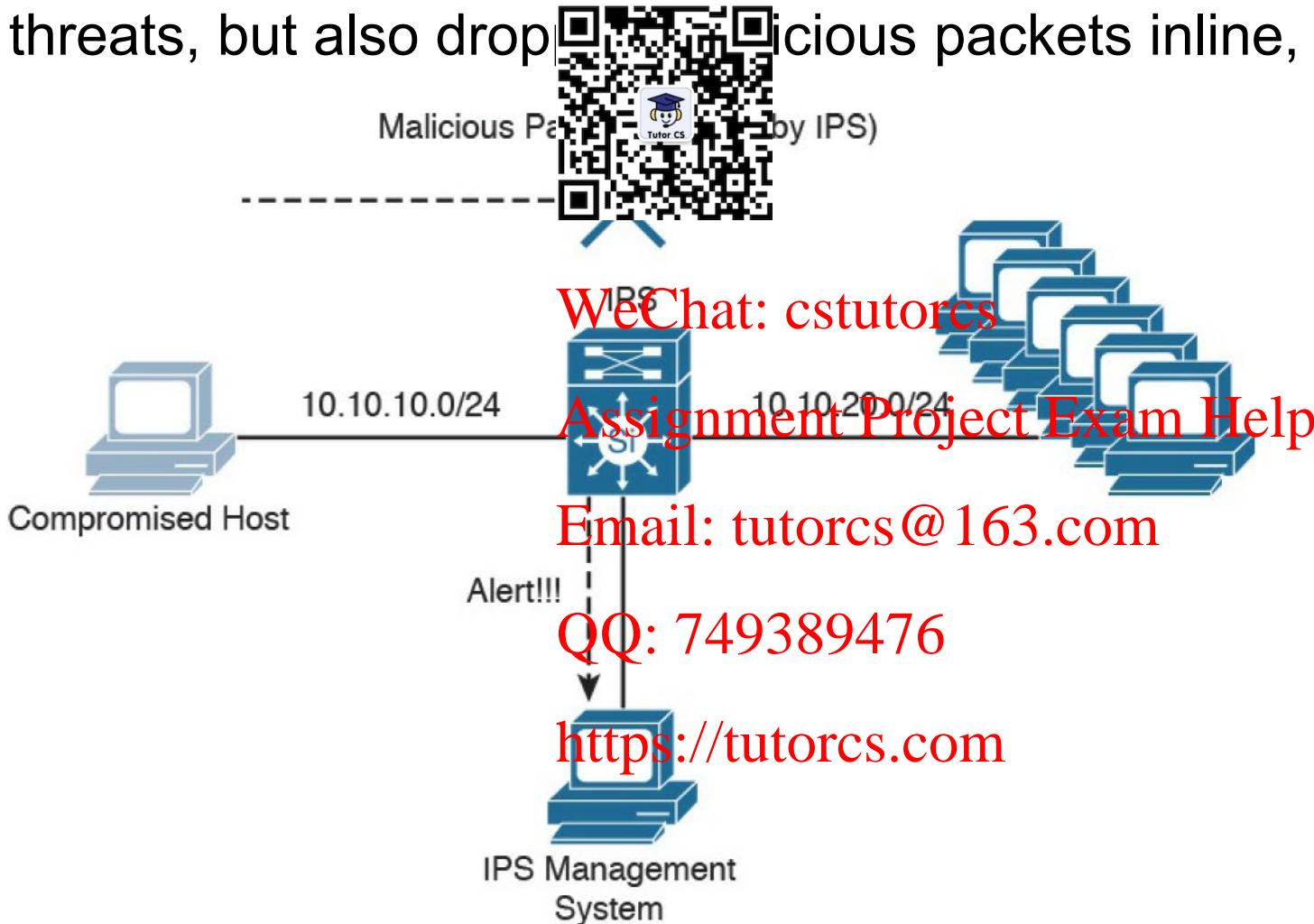


icious Packet



程序代写代做 CS编程辅导

- IPSs: Devices that are capable of not only detecting all security threats, but also drop malicious packets inline, e.g.,



程序代写代做 CS编程辅导

- Detection methodologies



- Pattern matching 

- Protocol analysis 

Assignment Project Exam Help

- Anomaly-based analysis

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS 编程辅导

- Search for a fixed sequence of bytes within the packets traversing the network
- Uses the concept of signatures – a set of conditions that point out some type of intrusion occurrence, e.g.,
 - “TCP packet has a destination port of 1234 and its payload contains the string ff11ff22”

WeChat: cstutorcs

- Pros:
 - Direct correlation of an exploit
 - Trigger alerts on the pattern specified
 - Can be applied across different services and protocols

Assignment Project Exam Help
Email: tutorcs@163.com
QQ: 749389476

- Cons:
 - High false positives
 - High false negatives if attack pattern alters

<https://tutorcs.com>

程序代写代做 CS 编程辅导

- Dictate that systems performing this type of signature analysis must consider the chronological order of packets in a TCP stream, i.e., judge and maintain a careful inspection of such packets and flows
- 

WeChat: cstutorcs
Assignment Project Exam Help
Email: tutorcs@163.com
QQ: 749389476
<https://tutorcs.com>
- Pros:
 - The capability to directly correlate a specific exploit within a given pattern
 - Supports all non-encrypted IP protocols
 - Cons:
 - Uncertain rate of false positives
 - Possibility of some false negatives
 - Resource intensive (Memory & CPU)

程序代写代做 CS 编程辅导

- Decode all protocol or client-server conversations, and identify the elements of the protocol and analyse them while looking for an infringement
- Look at explicit protocol fields in the inspected packets, or more sophisticated techniques such as examination of the length of a field within the protocol or the number of arguments, e.g.,
 - Examine specific commands and fields in SMTP protocol such as HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT

WeChat: tutorcs
Assignment Project Exam Help

- Pros:
 - Low false positives if the protocol being analysed is properly defined and enforced
- Cons:
 - High false positives if the protocol definition is ambiguous or tolerates flexibility in its implementation

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

程序代写代做 CS编程辅导

- Keep track of network traffic that diverges from “normal” behavioural patterns



- Limitation: what is considered to be normal must be defined

WeChat: cstutorcs

- Challenges: to classify a specific behaviour as normal or abnormal based on different factors below:

– Negotiated protocols and ports Email: tutors@163.com

– Specific application changes QQ: [749589476](https://tutorcs.com)

– Changes in the architecture of the network

<https://tutorcs.com>

程序代写代做 CS编程辅导

- LAN segment data:
 - LAN segment range: 172.16.4.0/24
 - Domain: **mind-han**
 - Domain controller: 172.16.4.4 (Mind-Hammer-DC)
 - LAN segment gateway: 172.16.4.1
 - LAN segment broadcast address: 172.16.4.255
- IDS alerts triggered: **Assignment Project Exam Help**

CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
1	2019-07-19...	166.62.111.64	80	172.16.4.205	49190	6	ETPRO CURRENT_EVENTS SocEng/Gholish JS Web Inject Inbound
3	2019-07-19...	81.4.122.101	443	172.16.4.205	49220	6	ET POLICY Lets Encrypt Free SSL Cert Observed
3	2019-07-19...	81.4.122.101	443	172.16.4.205	49220	6	ETPRO TROJAN Observed Malicious SSL Cert (SocGholish Redirect)
6	2019-07-19...	93.95.100.178	443	172.16.4.205	49236	6	ET POLICY Lets Encrypt Free SSL Cert Observed
6	2019-07-19...	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST to an image file (gif)
7	2019-07-19...	172.16.4.205	49249	185.243.115.84	80	6	ETPRO TROJAN POST to a gif file
20	2019-07-19...	172.16.4.205	49249	185.243.115.84	80	6	ETPRO CURRENT_EVENTS JS.SocGholish POST Request
1	2019-07-19...	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP Request on Unusual Port Possibly Hostile
6442	2019-07-19...	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP POST on unusual Port Possibly Hostile
6442	2019-07-19...	172.16.4.205	49255	31.7.62.214	443	6	ETPRO POLICY NetSupport Remote Admin Checkin
3	2019-07-19...	31.7.62.214	443	172.16.4.205	49255	6	ETPRO POLICY NetSupport Remote Admin Response

程序代写代做 CS编程辅导

- Q: What is the IP address, MAC address, and host name of the infected Windows host?
- A: **172.16.4.205, 00:59:b0:63:a4, ROTTERDAM-PC**



No.	Time	Source	Dest	Protocol	Length	Info
141	2.993351	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform – Transaction ID 0...
204...	290.812181	172.16.4.4	172.16.4.205	DHCP	342	DHCP ACK – Transaction ID 0...
204...	291.489122	172.16.4.205	255.255.255.255	DHCP	342	DHCP Inform – Transaction ID 0...

Transaction ID: 0x45714260

Seconds elapsed: 0

▼ Bootp flags: 0x0000 (Unicast)

0.... = Broadcast flag: Unicast

.000 0000 0000 0000 = Reserved flags: 0x0000

Client IP address: 172.16.4.205

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: Lenovoem_b0:63:a4 (00:59:07:b0:63:a4)

Client hardware address padding: 000000000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

▼ Option: (53) DHCP Message Type (Inform)

Length: 1

DHCP: Inform (8)

▼ Option: (61) Client identifier

Length: 7

Hardware type: Ethernet (0x01)

Client MAC address: Lenovoem_b0:63:a4 (00:59:07:b0:63:a4)

▼ Option: (12) Host Name

Length: 12

Host Name: Rotterdam-PC

WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

Case Study – Network Attack Traffic Analysis

程序代写代做 CS编程辅导

- Q: Based on the alerts what is the name of the campaign that delivered the malware?
- A: **SocGholish** also known as **TakeUpdates**



Src IP	SPort	Dst IP	Recent Message				
				PRO CURRENT_EVENTS SocEng/Gholish JS Web Inject Inbound			
No.	Time	Source	Destination	Host	Protocol	Len	Info
2807	29.870141	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	408	GET /wp-content
1144	28.463844	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	406	GET /wp-content
839	28.060880	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	405	GET /wp-content
804	27.981264	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	405	GET /wp-content
662	27.730907	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	405	GET /wp-content
612	27.681192	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	405	GET /wp-content
518	27.483343	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	405	GET /wp-content
908	28.119789	172.16.4.205	166.62.111.64	mysocalledchaos.com	HTTP	404	GET /wp-content

WeChat: cstutorcs
Assignment Project Exam Help
Email: tutorcs@163.com

```

Frame 2807: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits)
Ethernet II, Src: Lenovoem_b0:63:a4 (00:55:07:b0:63:a4) Dst: Cisco_0e:c4:77 (00:15:c6:e6:c4:77)
Internet Protocol Version 4, Src: 172.16.4.205, Dst: 166.62.111.64
Transmission Control Protocol, Src Port: 49199, Dst Port: 80, Seq: 2535, Ack: 178079, Len: 354
Hypertext Transfer Protocol
  GET /wp-content/uploads/2019/04/MomLifeStickers-Feat-400x600.png HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wp-content/uploads/2019/04/MomLifeStickers-Feat-400x600.png HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wp-content/uploads/2019/04/MomLifeStickers-Feat-400x600.png
    Request Version: HTTP/1.1
Host: mysocalledchaos.com\r\n

```

QQ: 749389476
<https://tutorcs.com>

程序代写代做 CS编程辅导

Update Firefox

X



i mysocalledch...
Tutor CS



Search



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

You are using an older version of Firefox

Update now to keep your Firefox browser running smoothly and securely.

QQ: 749389476

Your download will begin automatically. If not, click here:

<https://tutorcs.com>

Update Firefox

Case Study – Network Attack Traffic Analysis

程序代写代做 CS编程辅导

- Q: Based on the alerts, what is the final malware that infected the Windows host?
- A: **NetSupport Manager** The alerts say "NetSupport Remote Admin Checkin" and "NetSupport Remote Admin Response"



ip.src == 31.7.62.214							Expression...
No.	Time	Source	Destination	Protocol	Length	Info	
205...	291.768768	31.7.62.214	172.16.4.205	TCP	66	443 → 49255 [SYN, ACK] Seq=0 Ack...	
205...	292.029983	31.7.62.214	172.16.4.205	HTTP	268	HTTP/1.1 200 OK (application/x-...)	
206...	292.290708	31.7.62.214	172.16.4.205	HTTP	359	HTTP/1.1 200 OK (application/x-...)	
206...	292.697036	31.7.62.214	172.16.4.205	TCP	54	443 → 49255 [ACK] Seq=520 Ack=91...	

Frame 20570: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits)
 ▶ Ethernet II, Src: Cisco_e6:c4:77 (00:15:c6:e6:c4:77), Dst: Lenovo_b0:b3:a1 (00:59:07:b0:b3:a1)
 ▶ Internet Protocol Version 4, Src: 31.7.62.214, Dst: 172.16.4.205
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 49255, Seq: 1, Ack: 215, Len: 214

▼ Hypertext Transfer Protocol

 ▼ [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
 [Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
 [Severity level: Warning]
 [Group: Security]

 ▼ HTTP/1.1 200 OK\n

 ▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\n]
 [HTTP/1.1 200 OK]\n [Severity level: Chat]\n [Group: Sequence]
 Response Version: HTTP/1.1
 Status Code: 200
 [Status Code Description: OK]
 Response Phrase: OK

Server: NetSupport Gateway/1.6 (Windows NT)\n

WeChat: ostutorcs

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

- More Network Attacks

- Compare different types of attacks
- Understand how network work
- Describe examples of different attacks
- Select key patterns to detect attacks



- Network Security Systems

- Traditional and next-generation firewalls
 - Explain DMZ and network segmentation
 - Describe ACL and its common practices
 - Explain NAT & PAT process
 - Understand stateful inspection firewalls
- IDSs & IPSs
 - Compare the difference between IDS and IPS
 - Understand different detection methodologies

- Case Study

- Understand the network attack traffic analysis process
- Apply the analysis process to other network attacks

QQ: 749389476

WeChat: cstutorcs

Assignment Project Exam Help

Email: tutors@163.com

<https://tutorcs.com>

程序代写代做 CS编程辅导

- [1] Omar Santos, et al., 2017, CCNA Cyber Ops SECFND #210-250 Official Cert Guide (Certification Guide), Cisco Press
- [2] C.V.Zhou, et al., 2009, *Centralized multi-dimensional alert correlation for collaborative intrusion detection*, Journal of Network and Computer Applications
- [3] Hossein Pirayesh, Huacheng Zeng, *Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey*. Available from: <https://arxiv.org/pdf/2101.00292.pdf>

Email: tutorcs@163.com

QQ: 749389476

<https://tutorcs.com>

