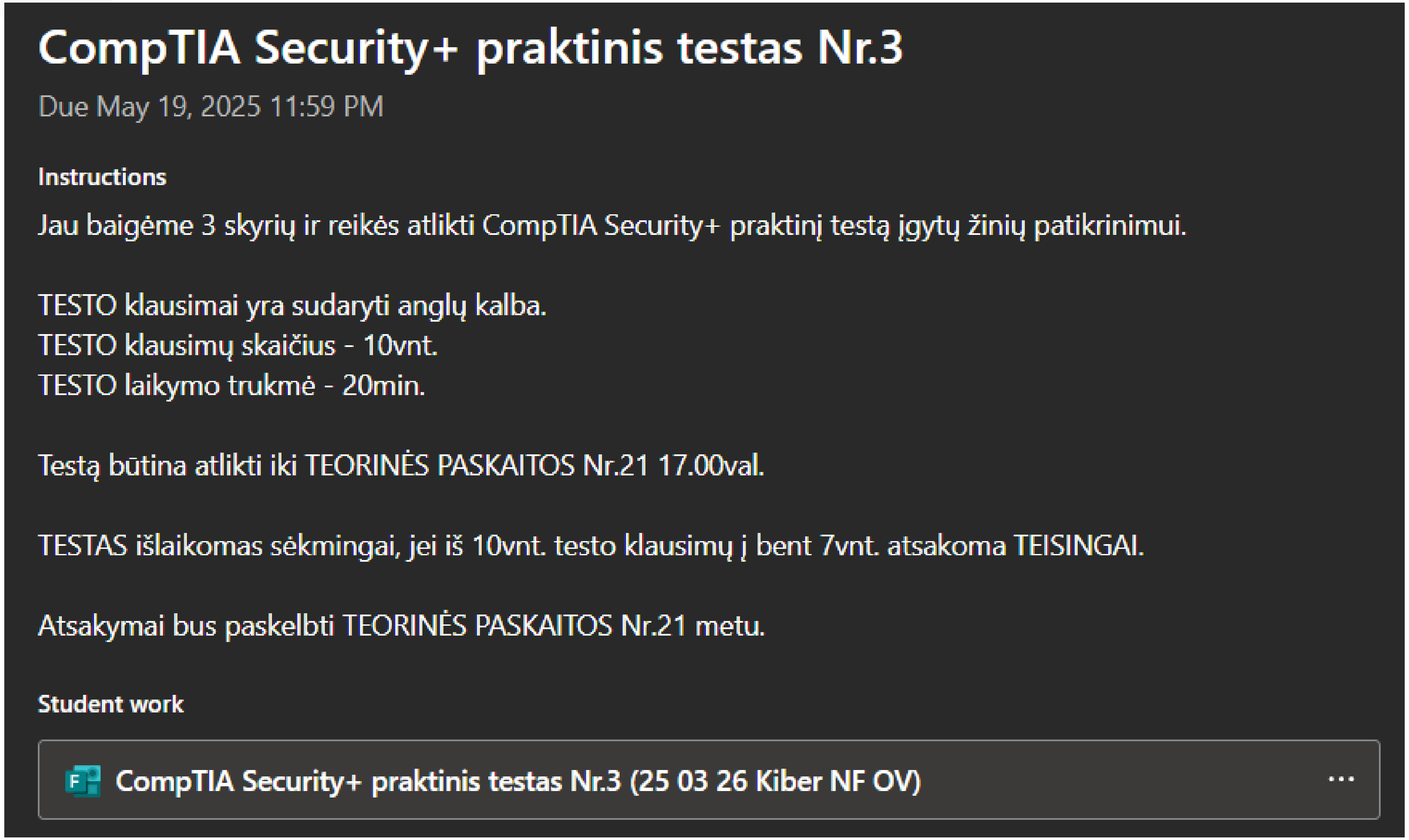
Cyber Security
Lession 21

Labs

Assignments



CompTIA Security+ praktinis testas Nr.3

Due May 19, 2025 11:59 PM

Instructions

Jau baigėme 3 skyrių ir reikės atlikti CompTIA Security+ praktinį testą įgytų žinių patikrinimui.

TESTO klausimai yra sudaryti anglų kalba.
TESTO klausimų skaičius - 10vnt.
TESTO laikymo trukmė - 20min.

Testą būtina atlikti iki TEORINĖS PASKAITOS Nr.21 17.00val.

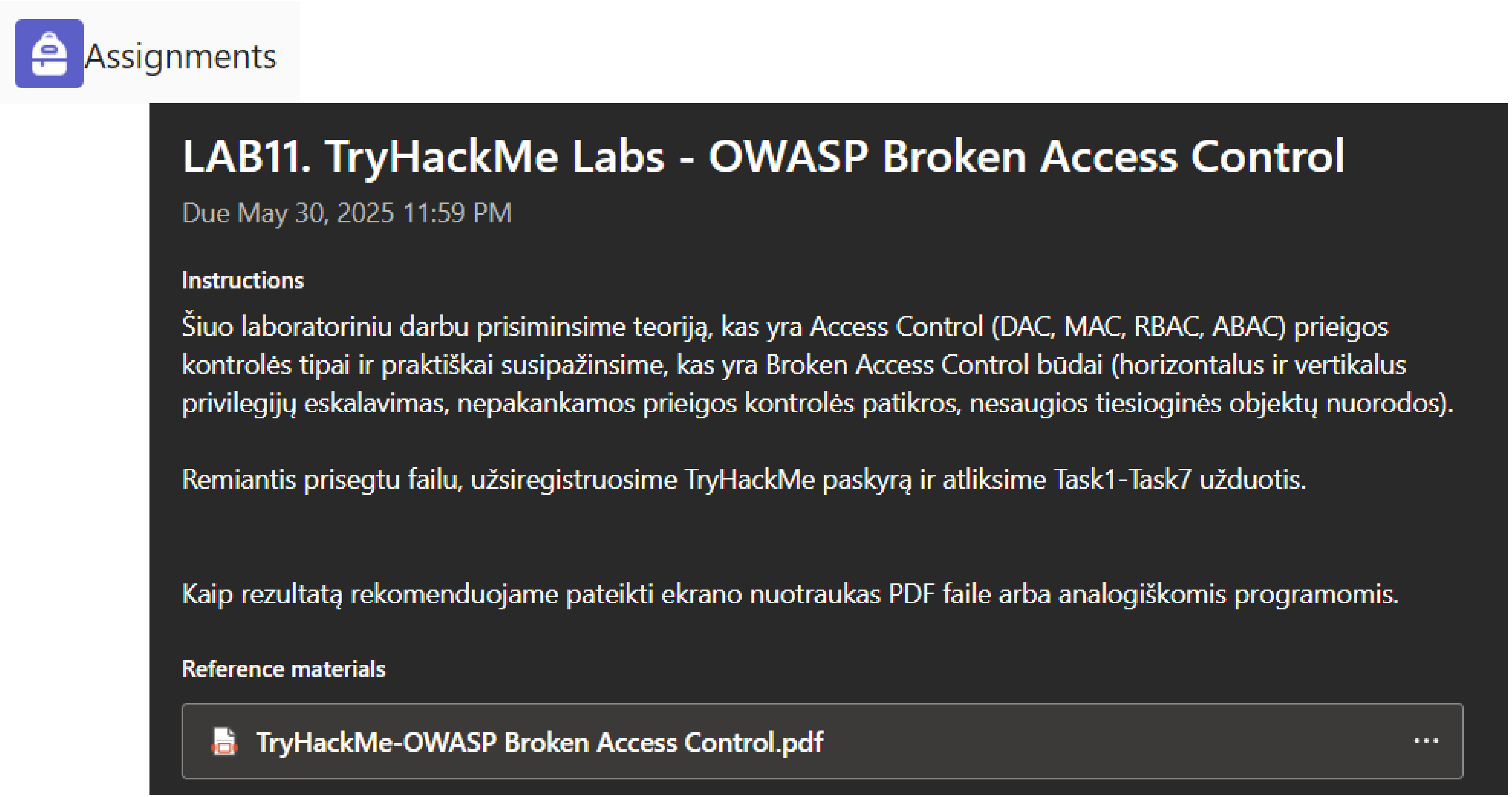
TESTAS išlaikomas sėkmingai, jei iš 10vnt. testo klausimų į bent 7vnt. atsakoma TEISINGAI.

Atsakymai bus paskelbti TEORINĖS PASKAITOS Nr.21 metu.

Student work

CompTIA Security+ praktinis testas Nr.3 (25 03 26 Kiber NF OV) ···

Labs



Assignments

LAB11. TryHackMe Labs - OWASP Broken Access Control

Due May 30, 2025 11:59 PM

Instructions

Šiuo laboratoriniu darbu prisiminsime teoriją, kas yra Access Control (DAC, MAC, RBAC, ABAC) prieigos kontrolės tipai ir praktiškai susipažinsime, kas yra Broken Access Control būdai (horizontalus ir vertikalus privilegijų eskalavimas, nepakankamos prieigos kontrolės patikros, nesaugios tiesioginės objektų nuorodos).

Remiantis prisegtu failu, užsiregistruosime TryHackMe paskyrą ir atliksime Task1-Task7 užduotis.

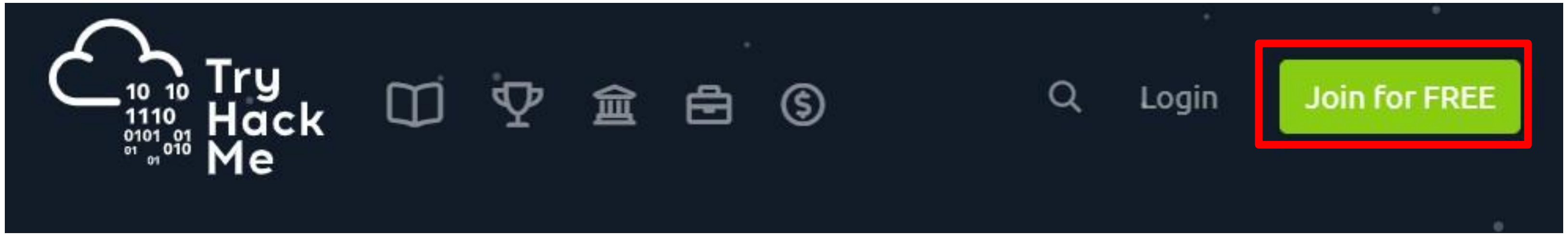
Kaip rezultatą rekomenduojame pateikti ekrano nuotraukas PDF faile arba analogiškomis programomis.

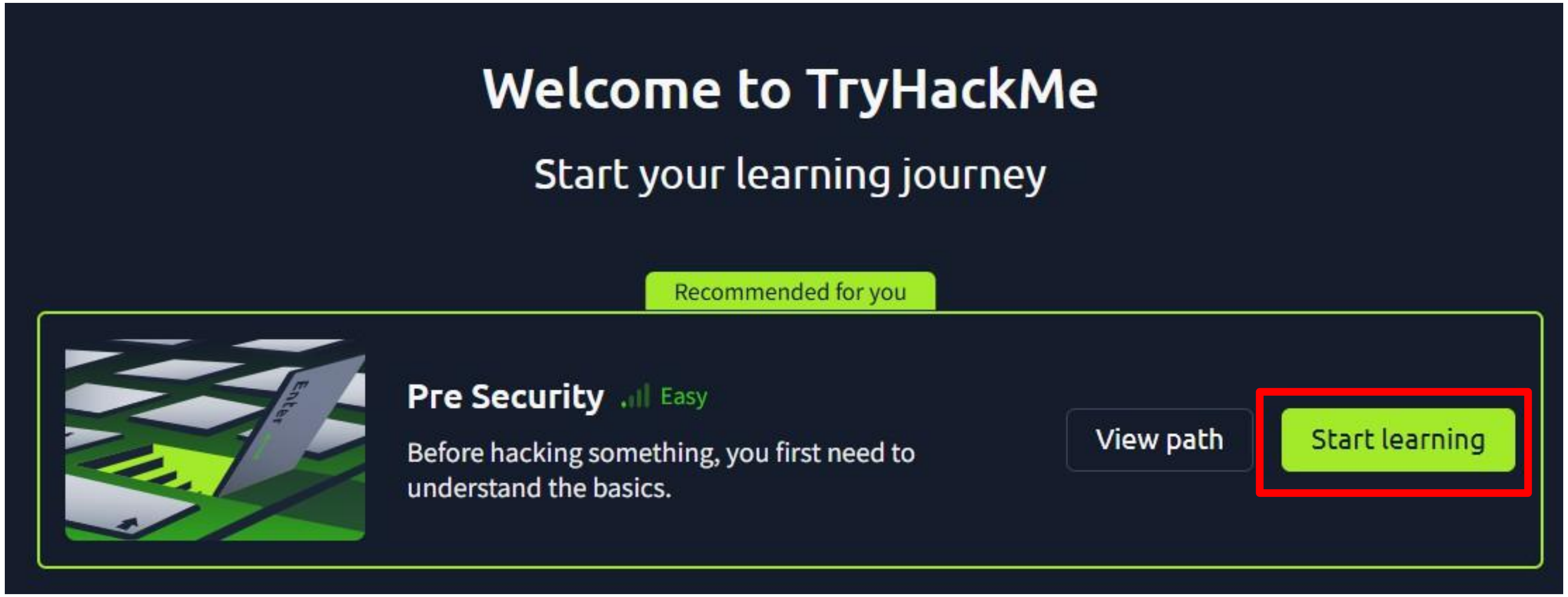
Reference materials

TryHackMe-OWASP Broken Access Control.pdf

Labs

Create the account: https://tryhackme.com





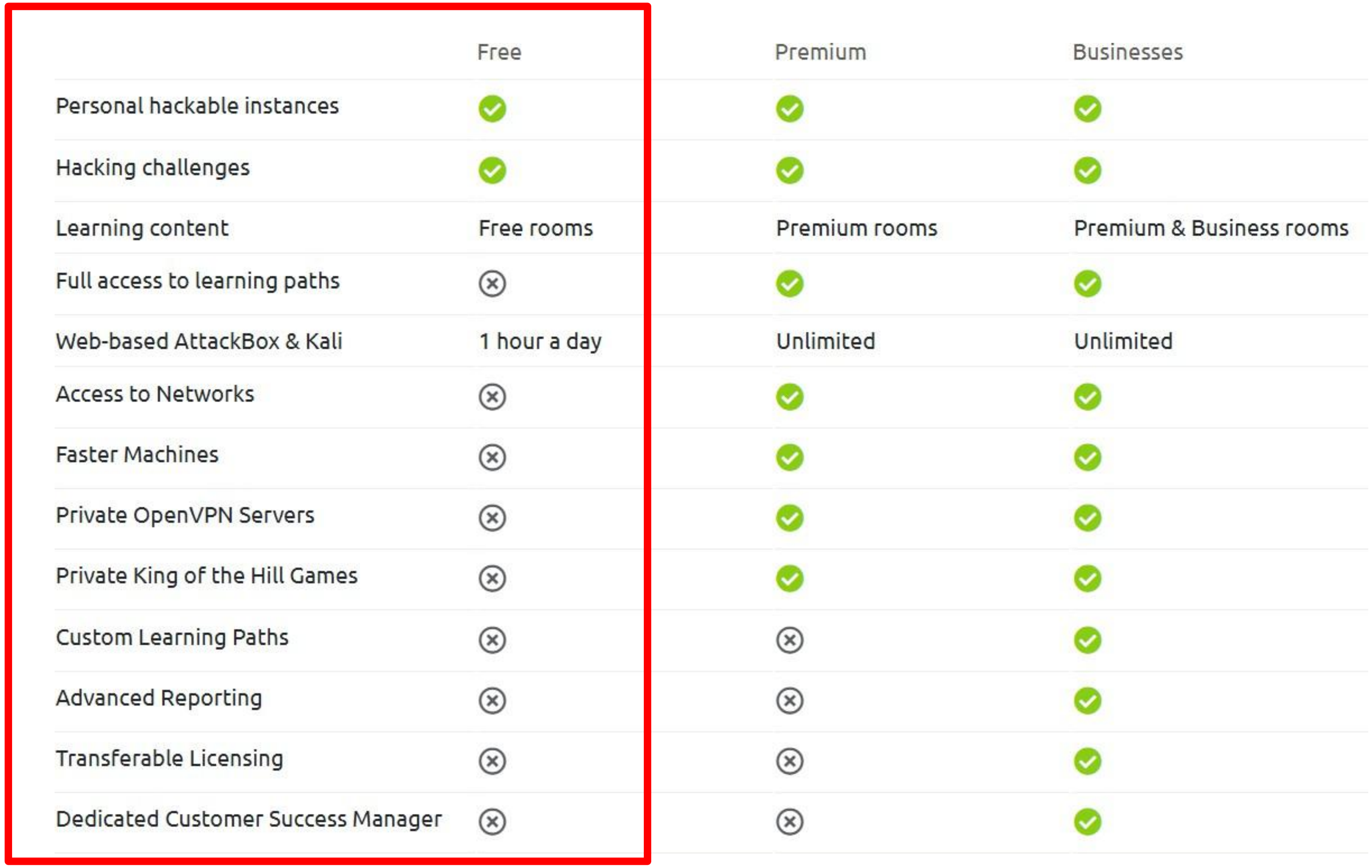
Welcome to TryHackMe

Start your learning journey

Before hacking something, you first need to understand the basics.

Labs

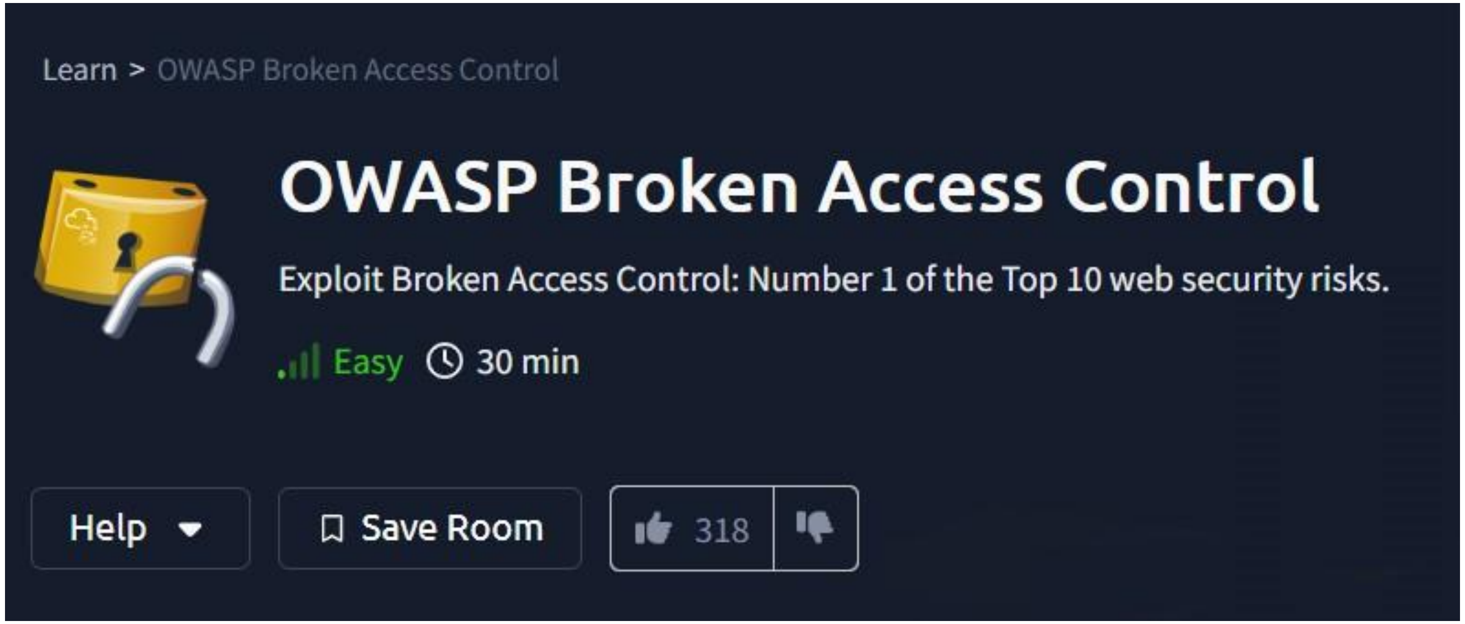
TryHackMe free account limitations:



	Free	Premium	Businesses
Personal hackable instances	✓	✓	✓
Hacking challenges	✓	✓	✓
Learning content	Free rooms	Premium rooms	Premium & Business rooms
Full access to learning paths	⊗	✓	✓
Web-based AttackBox & Kali	1 hour a day	Unlimited	Unlimited
Access to Networks	⊗	✓	✓
Faster Machines	⊗	✓	✓
Private OpenVPN Servers	⊗	✓	✓
Private King of the Hill Games	⊗	✓	✓
Custom Learning Paths	⊗	⊗	✓
Advanced Reporting	⊗	⊗	✓
Transferable Licensing	⊗	⊗	✓
Dedicated Customer Success Manager	⊗	⊗	✓

Labs

Go to the room: https://tryhackme.com/room/owaspbrokenaccesscontrol



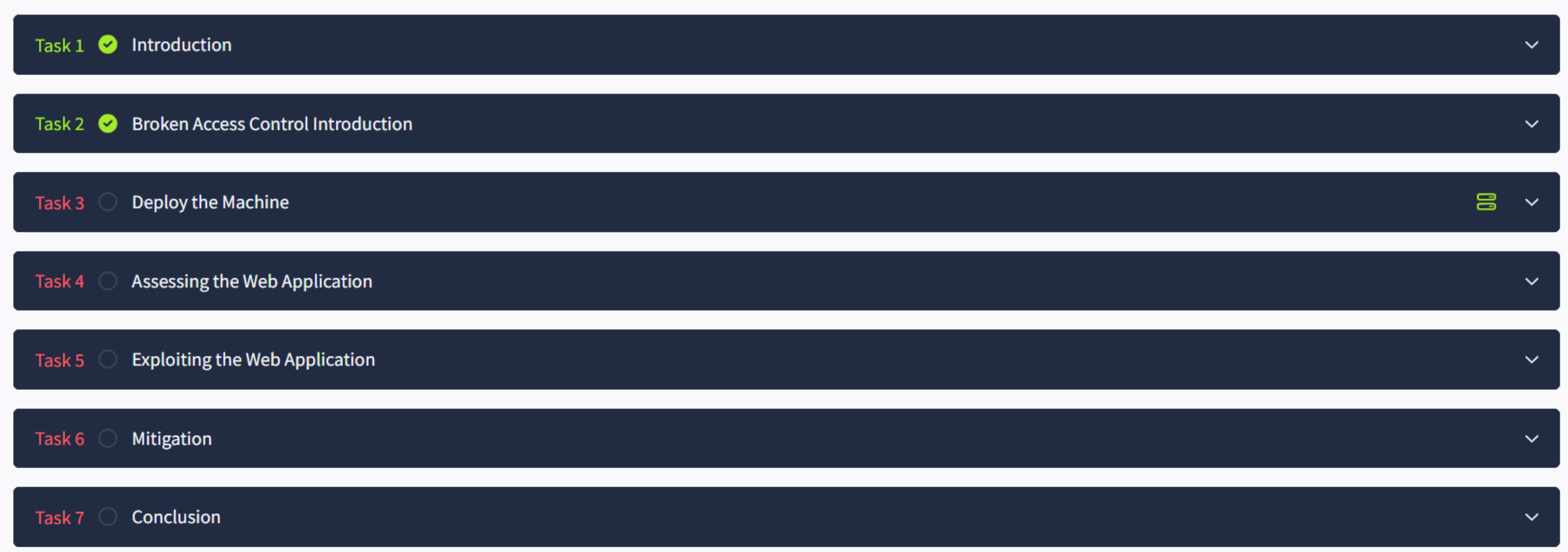
Learn > OWASP Broken Access Control

OWASP Broken Access Control

Exploit Broken Access Control: Number 1 of the Top 10 web security risks.

Labs

Step-by-step complete 7 tasks: https://medium.com/@kamalkannanares/tryhackme-owasp-broken-access-control-7985ecede0d9



Task 1 ✓ Introduction

Task 2 ✓ Broken Access Control Introduction

Task 3 ○ Deploy the Machine

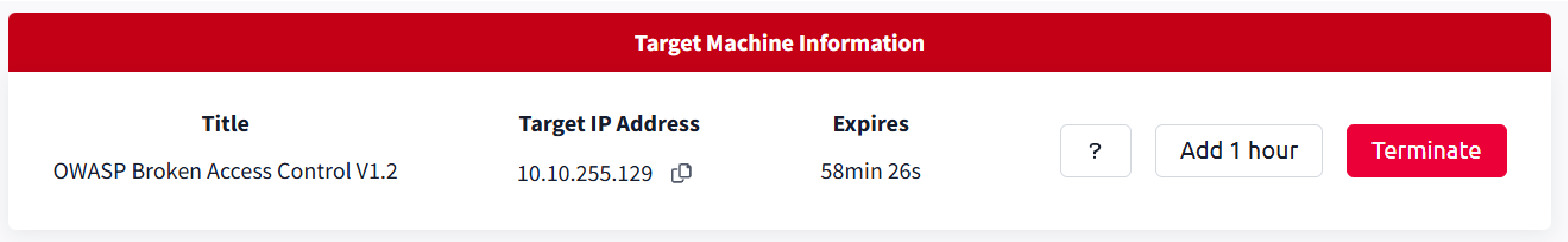
Task 4 ○ Assessing the Web Application

Task 5 ○ Exploiting the Web Application

Task 6 ○ Mitigation

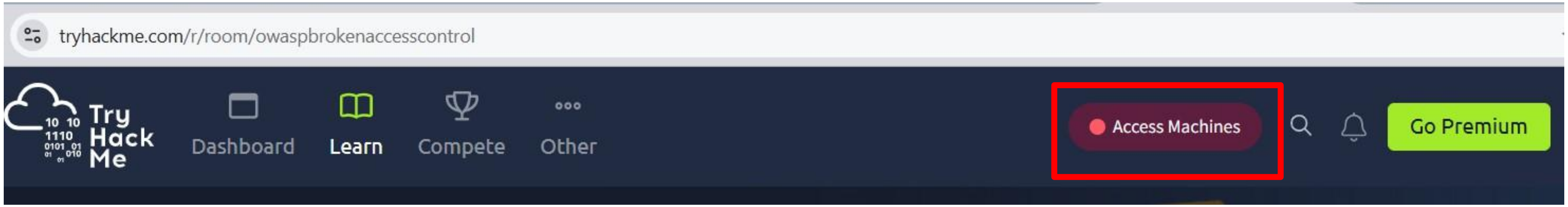
Task 7 ○ Conclusion

After starting the virtual machine:



Target Machine Information

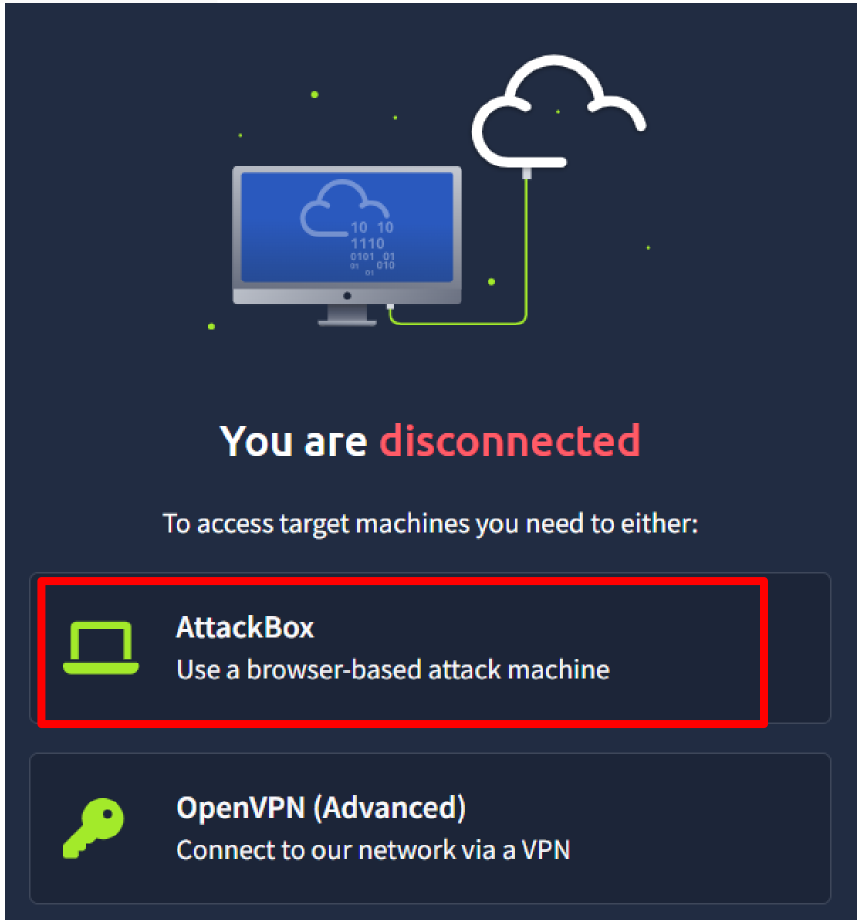
Title	Target IP Address	Expires
OWASP Broken Access Control V1.2	10.10.255.129	58min 26s



tryhackme.com/r/room/owaspbrokenaccesscontrol

Labs

Assignments

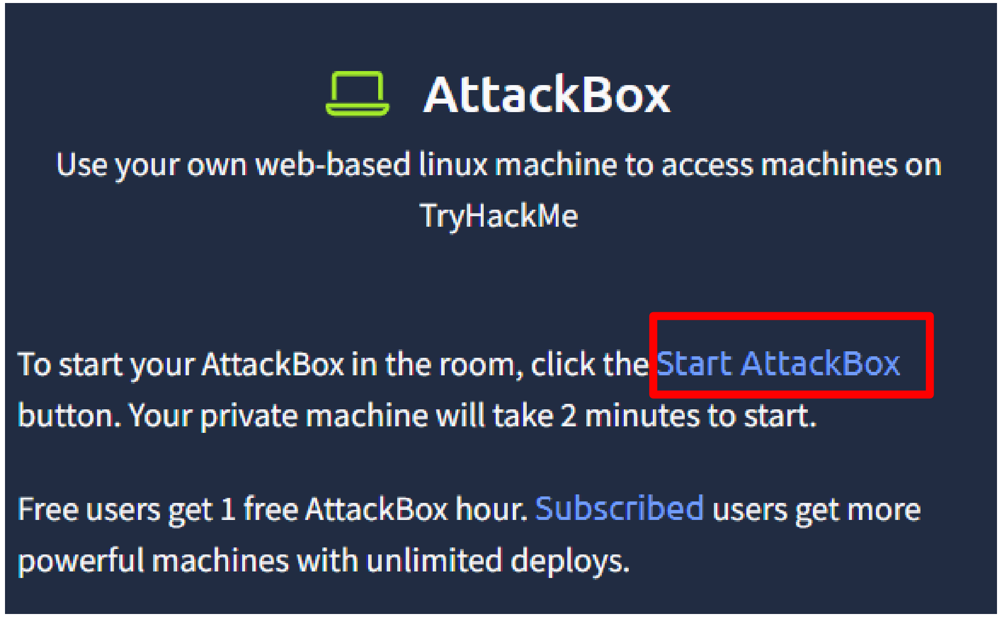


You are disconnected

To access target machines you need to either:

AttackBox
Use a browser-based attack machine

OpenVPN (Advanced)
Connect to our network via a VPN

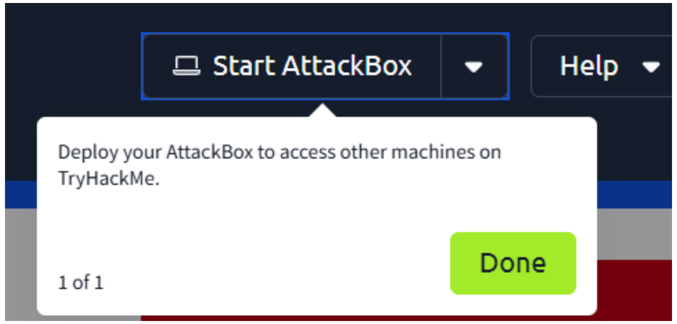


AttackBox

Use your own web-based linux machine to access machines on TryHackMe

To start your AttackBox in the room, click the Start AttackBox button. Your private machine will take 2 minutes to start.

Free users get 1 free AttackBox hour. Subscribed users get more powerful machines with unlimited deploys.

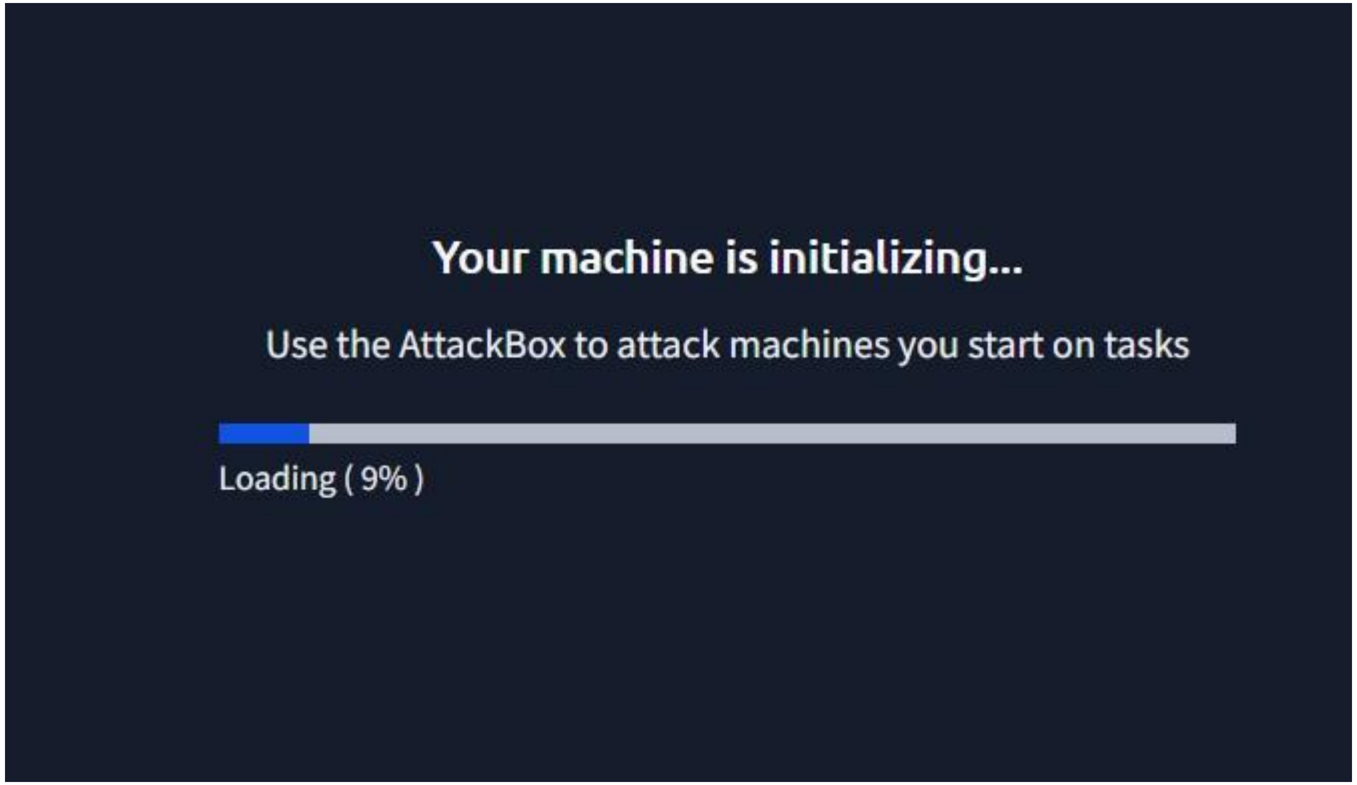


Deploy your AttackBox to access other machines on TryHackMe.

1 of 1

Labs

Assignments



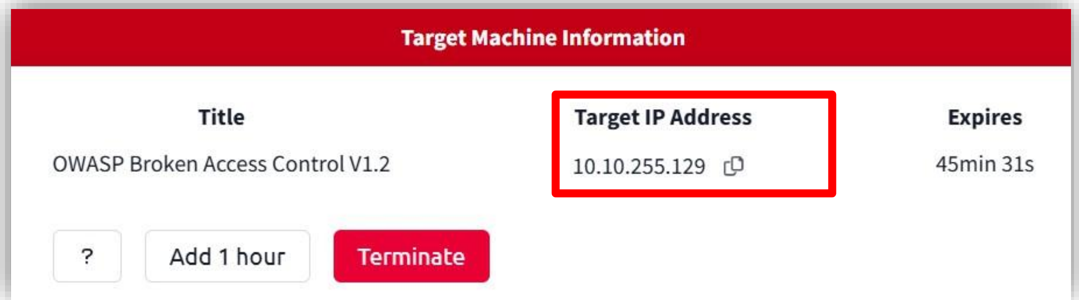
Your machine is initializing...

Use the AttackBox to attack machines you start on tasks

Loading (9%)

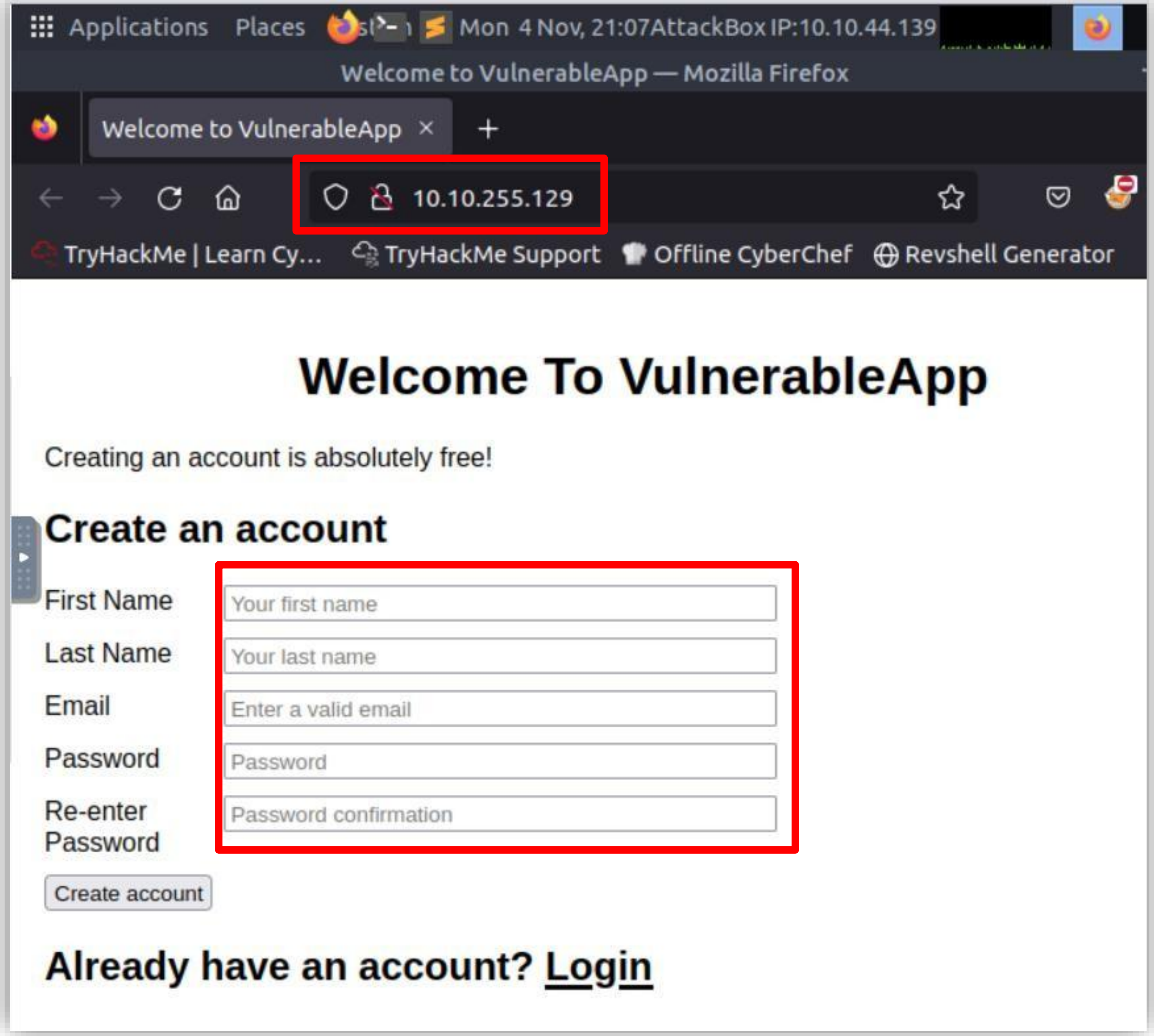
Labs

Assignments



Target Machine Information

Title	Target IP Address	Expires
OWASP Broken Access Control V1.2	10.10.255.129	45min 31s



Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

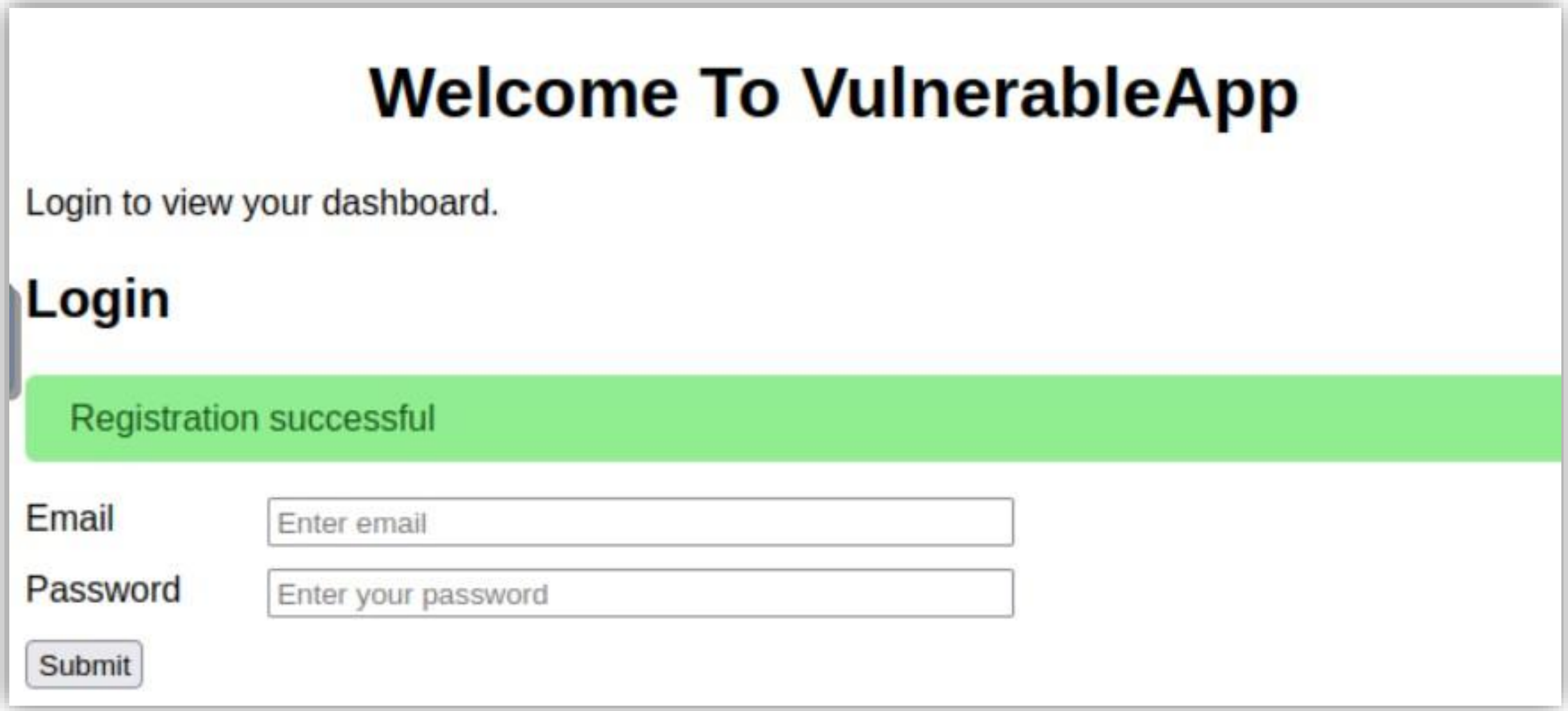
First Name	Your first name
Last Name	Your last name
Email	Enter a valid email
Password	Password
Re-enter Password	Password confirmation

Create account

Already have an account? Login

Labs

Assignments



Welcome To VulnerableApp

Login to view your dashboard.

Login

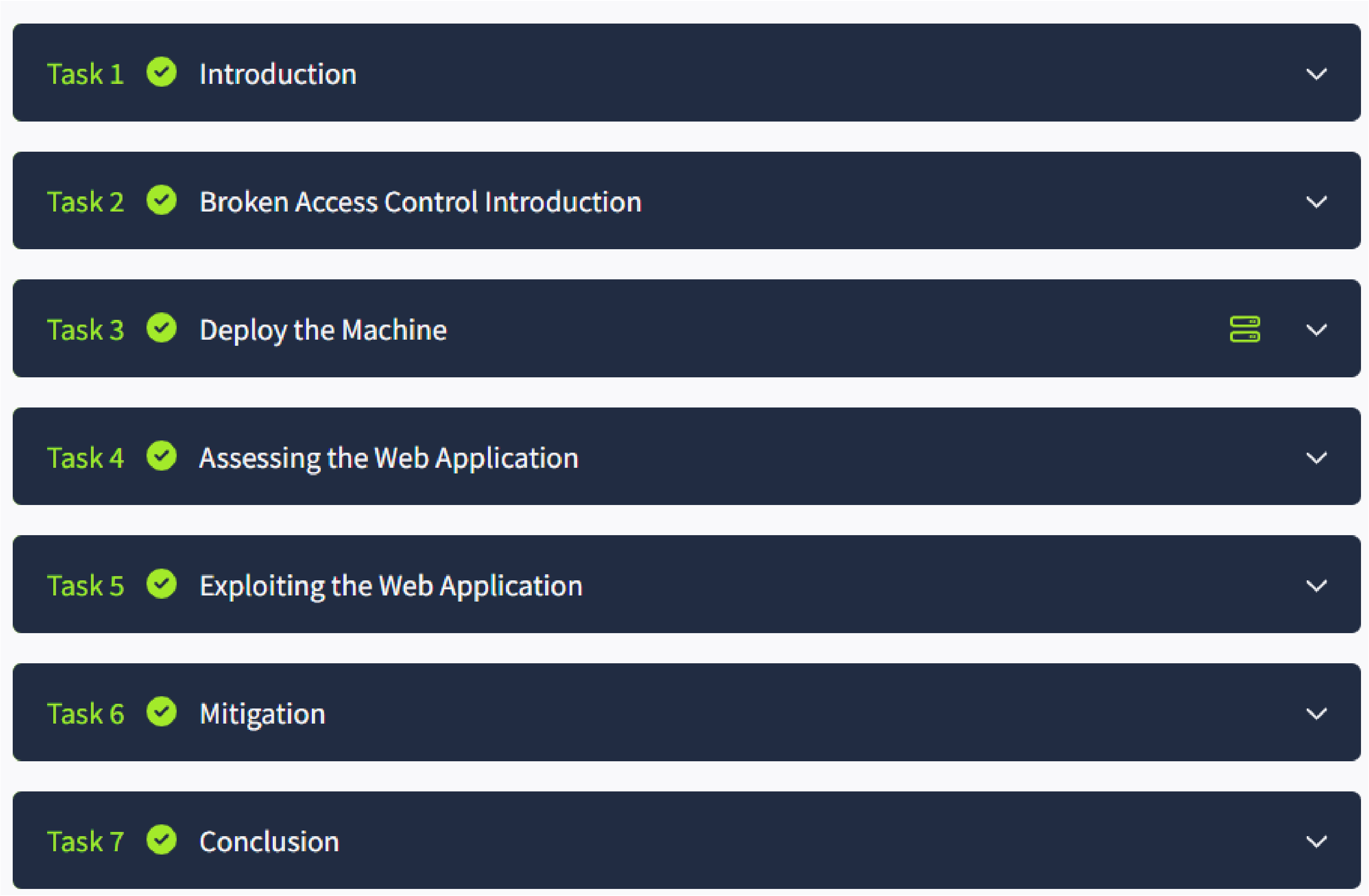
Registration successful

Email Enter email

Password Enter your password

Labs

Completed tasks:



Task 1 ✓ Introduction

Task 2 ✓ Broken Access Control Introduction

Task 3 ✓ Deploy the Machine

Task 4 ✓ Assessing the Web Application

Task 5 ✓ Exploiting the Web Application

Task 6 ✓ Mitigation

Task 7 ✓ Conclusion

In the previous lession…

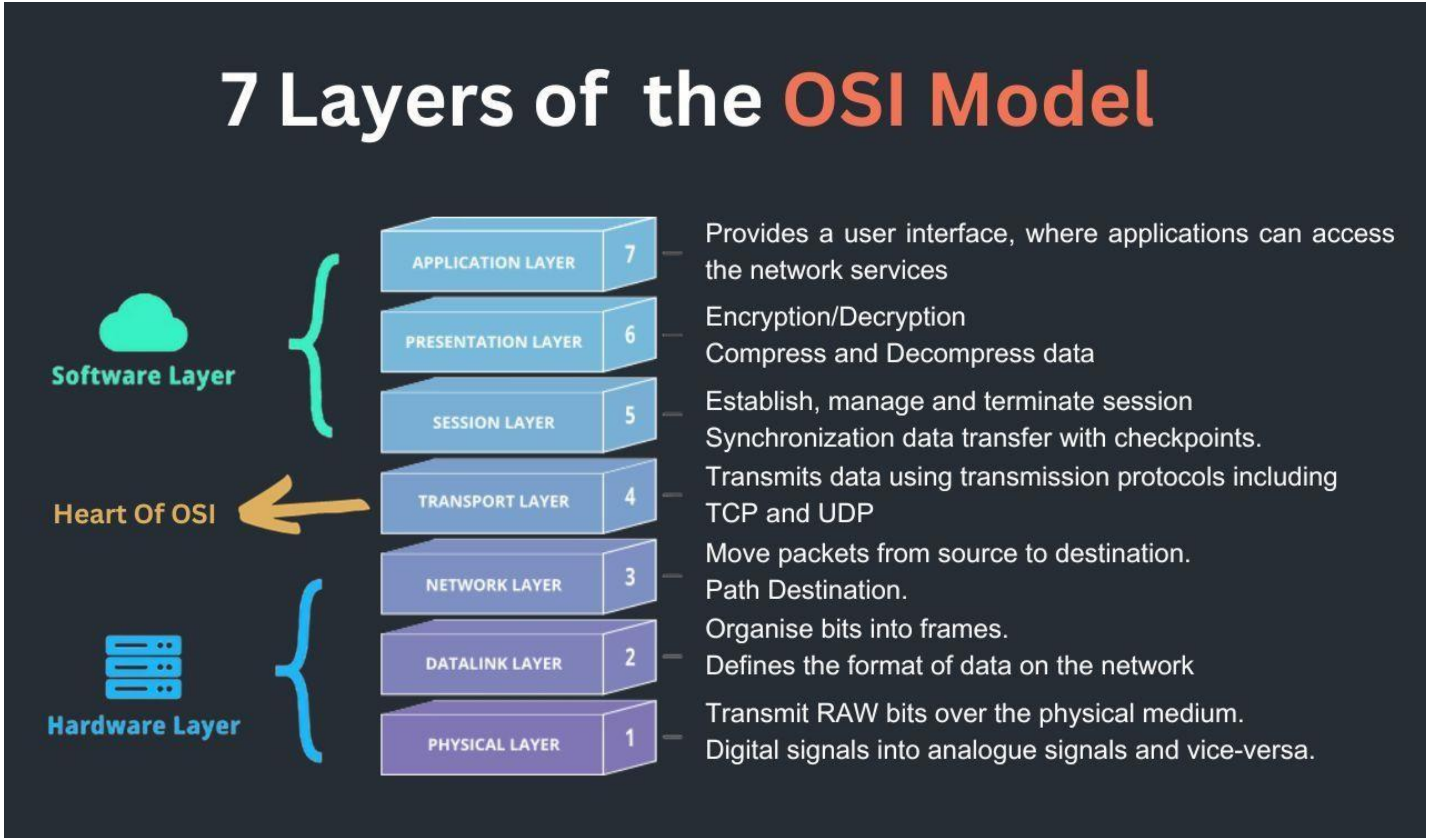
Exploring Network Technologies and Tools

(Chapter 4)

Introduction

- Reviewing Basic Networking Concepts DONE
- Basic Networking Protocols
- Understanding Basic Network Devices
- Implementing Network Designs
- Routing and Switching

Open Systems Interconnection (OSI) model



7 Layers of the OSI Model

APPLICATION LAYER 7 — Provides a user interface, where applications can access the network services

PRESENTATION LAYER 6 — Encryption/Decryption
Compress and Decompress data

SESSION LAYER 5 — Establish, manage and terminate session
Synchronization data transfer with checkpoints.

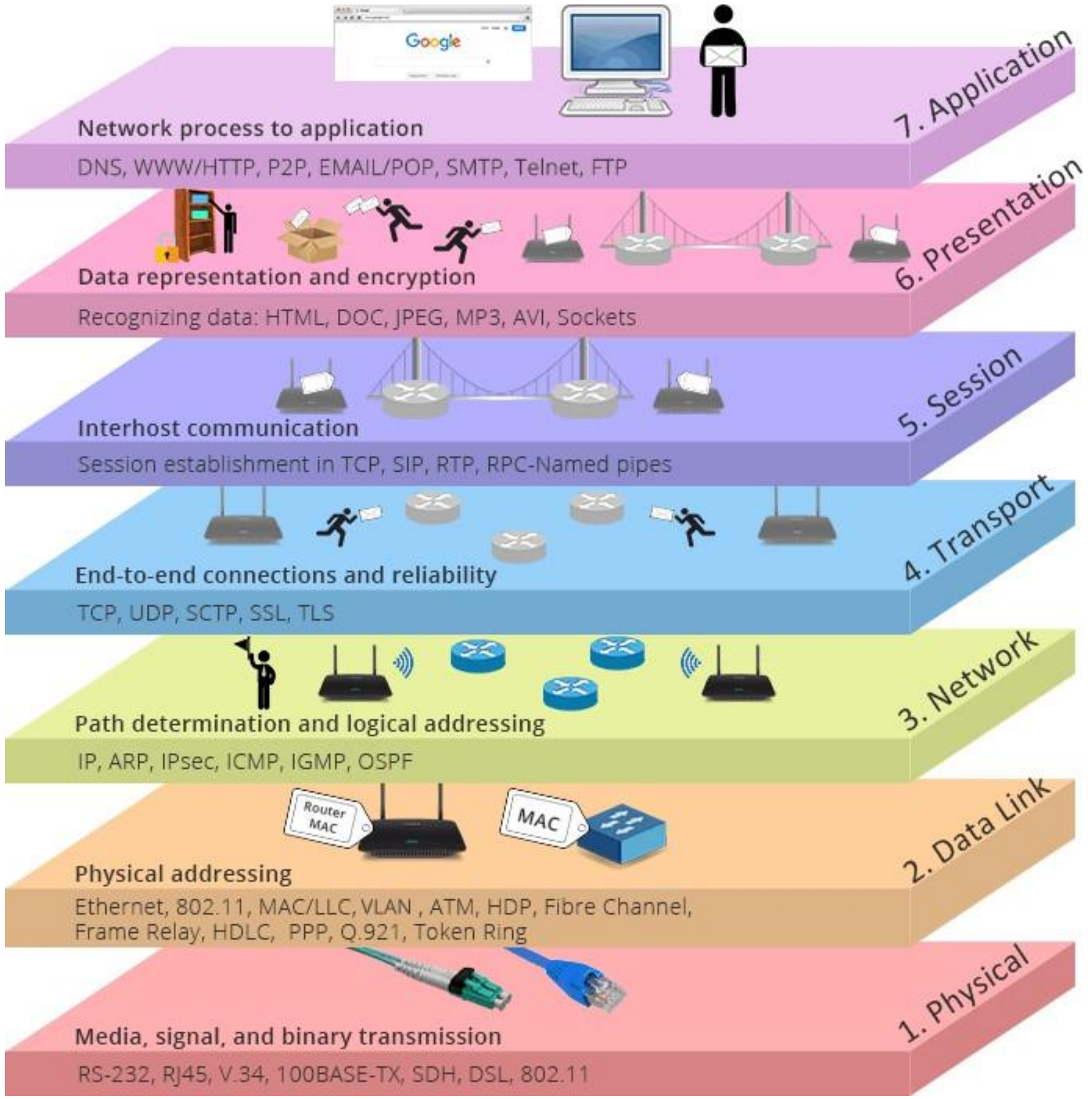
TRANSPORT LAYER 4 — Transmits data using transmission protocols including TCP and UDP

NETWORK LAYER 3 — Move packets from source to destination.
Path Destination.

DATALINK LAYER 2 — Organise bits into frames.
Defines the format of data on the network

PHYSICAL LAYER 1 — Transmit RAW bits over the physical medium.
Digital signals into analogue signals and vice-versa.

Components of OSI models



7. Application

Network process to application

DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP

6. Presentation

Data representation and encryption

Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets

5. Session

Interhost communication

Session establishment in TCP, SIP, RTP, RPC-Named pipes

4. Transport

End-to-end connections and reliability

TCP, UDP, SCTP, SSL, TLS

3. Network

Path determination and logical addressing

IP, ARP, IPsec, ICMP, IGMP, OSPF

2. Data Link

Physical addressing

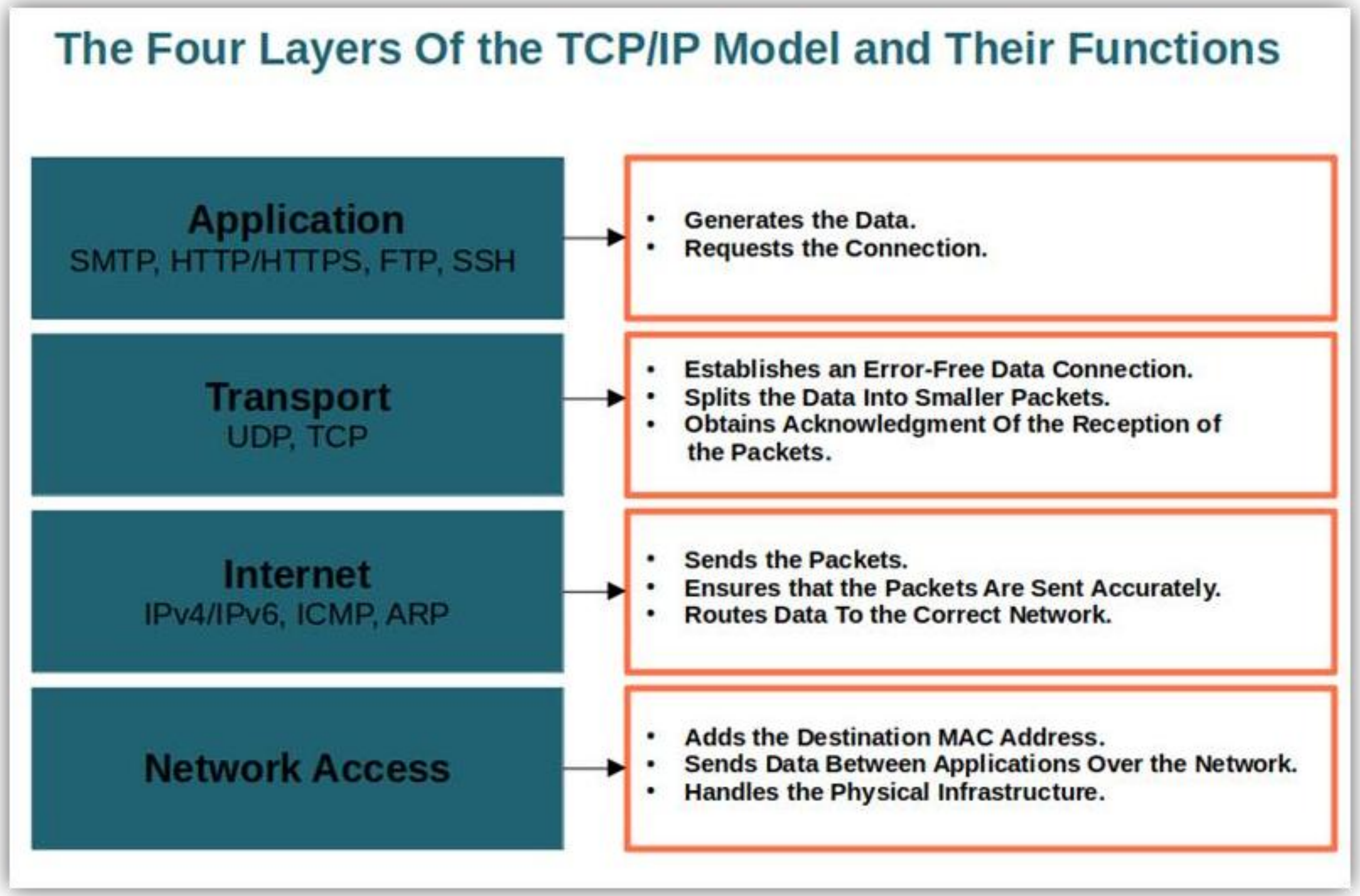
Ethernet, 802.11, MAC/LLC, VLAN , ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring

1. Physical

Media, signal, and binary transmission

RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

TCP/IP model



The Four Layers Of the TCP/IP Model and Their Functions

Application
SMTP, HTTP/HTTPS, FTP, SSH

- Generates the Data.
- Requests the Connection.

Transport
UDP, TCP

- Establishes an Error-Free Data Connection.
- Splits the Data Into Smaller Packets.
- Obtains Acknowledgment Of the Reception of the Packets.

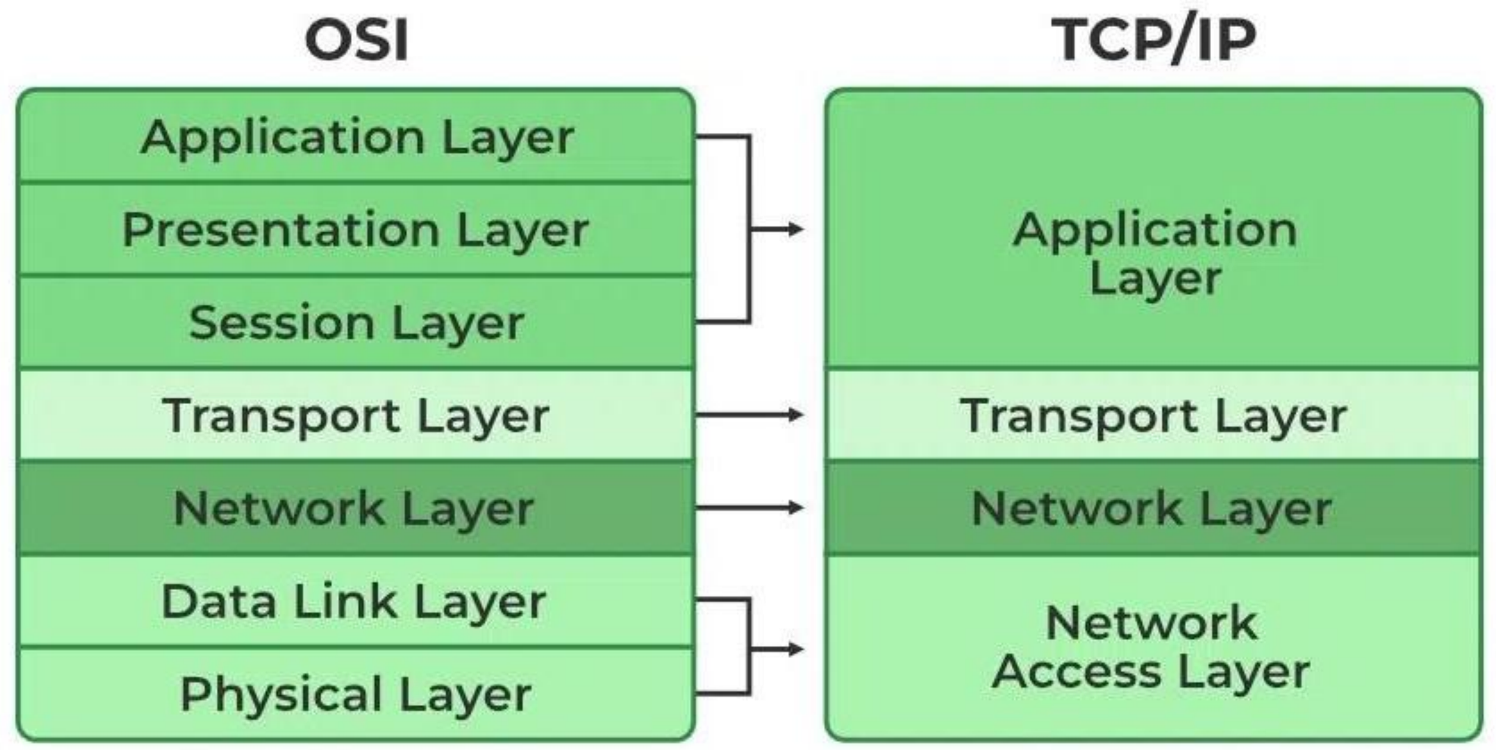
Internet
IPv4/IPv6, ICMP, ARP

- Sends the Packets.
- Ensures that the Packets Are Sent Accurately.
- Routes Data To the Correct Network.

Network Access

- Adds the Destination MAC Address.
- Sends Data Between Applications Over the Network.
- Handles the Physical Infrastructure.

OSI vs TCP/IP



OSI

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

TCP/IP

Application Layer

Transport Layer

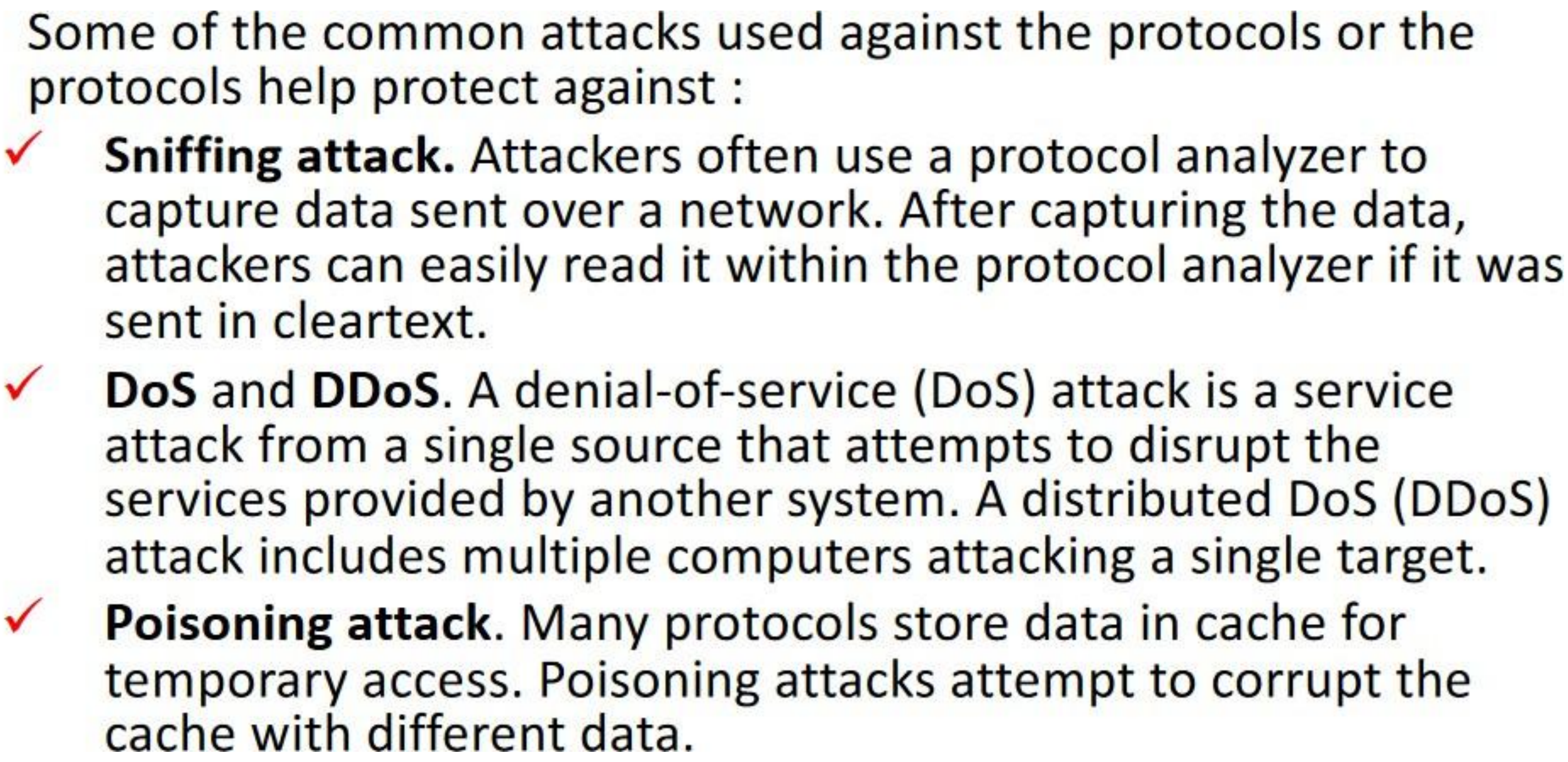
Network Layer

Network Access Layer

Well-known Ports

Networking	DNS UDP/53 TCP/53	DHCP UDP/67 UDP/68	NBT UDP/TCP 137-139	SNMP UDP/161 UDP/162	LDAP TCP/389
Remote access	SSH TCP/22	Telnet TCP/23	RDP TCP/3389		
File transfer	FTP TCP/20 TCP/21	HTTP TCP/80	HTTPS TCP/443	SMB TCP/445	
Email	SMTP TCP/25	POP3 TCP/110	IMAP TCP/143		

Related Attacks



- Some of the common attacks used against the protocols or the protocols help protect against :
  - ✓ **Sniffing attack.** Attackers often use a protocol analyzer to capture data sent over a network. After capturing the data, attackers can easily read it within the protocol analyzer if it was sent in cleartext.
  - ✓ **DoS** and **DDoS**. A denial-of-service (DoS) attack is a service attack from a single source that attempts to disrupt the services provided by another system. A distributed DoS (DDoS) attack includes multiple computers attacking a single target.
  - ✓ **Poisoning attack**. Many protocols store data in cache for temporary access. Poisoning attacks attempt to corrupt the cache with different data.

Exploring Network Technologies and Tools

(Chapter 4)

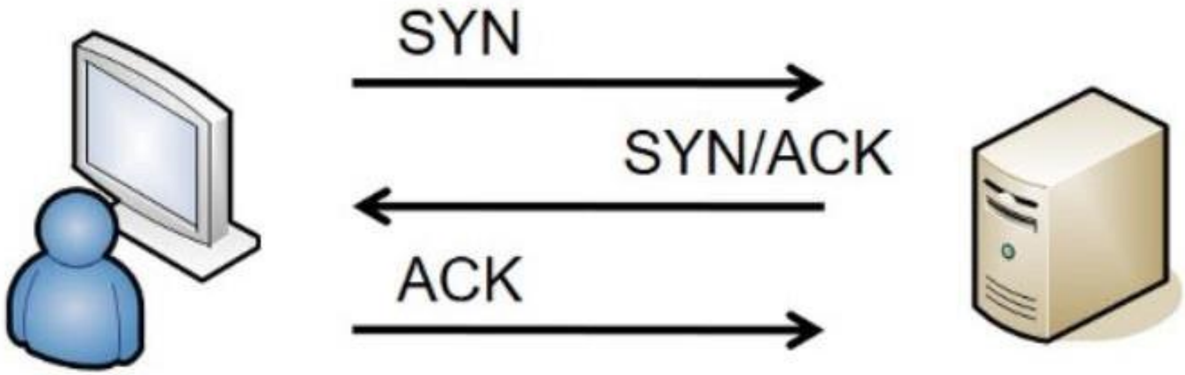
Lession 21

Introduction

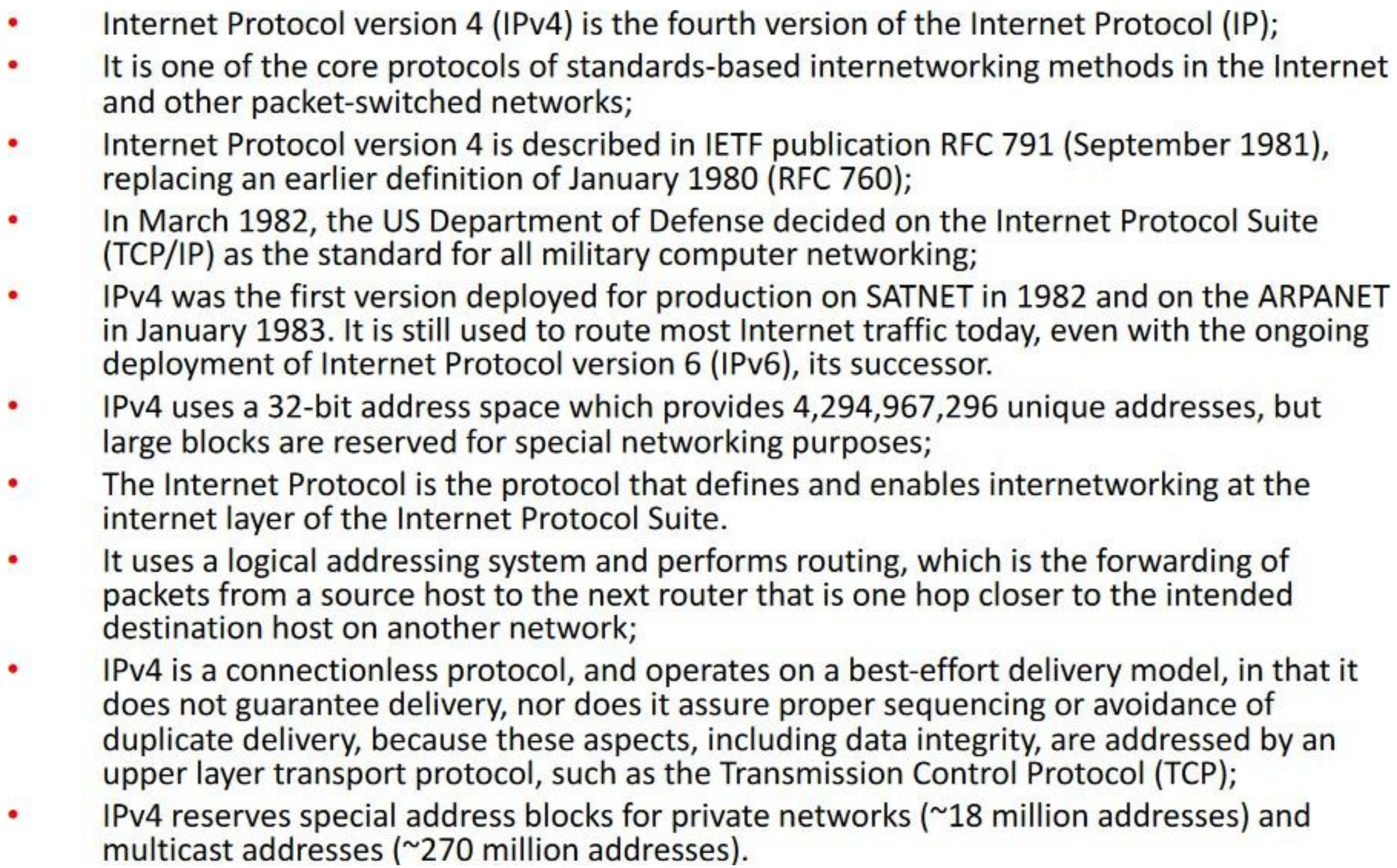
- Reviewing Basic Networking Concepts DONE
- Basic Networking Protocols
- Understanding Basic Network Devices
- Implementing Network Designs
- Routing and Switching

Basic Networking Protocols

- Basic Connectivity Protocols
  - ✓ TCP
    - ➢ Guaranteed delivery;
    - ➢ Three-way handshake;
  - ✓ UDP
    - ➢ Best effort.

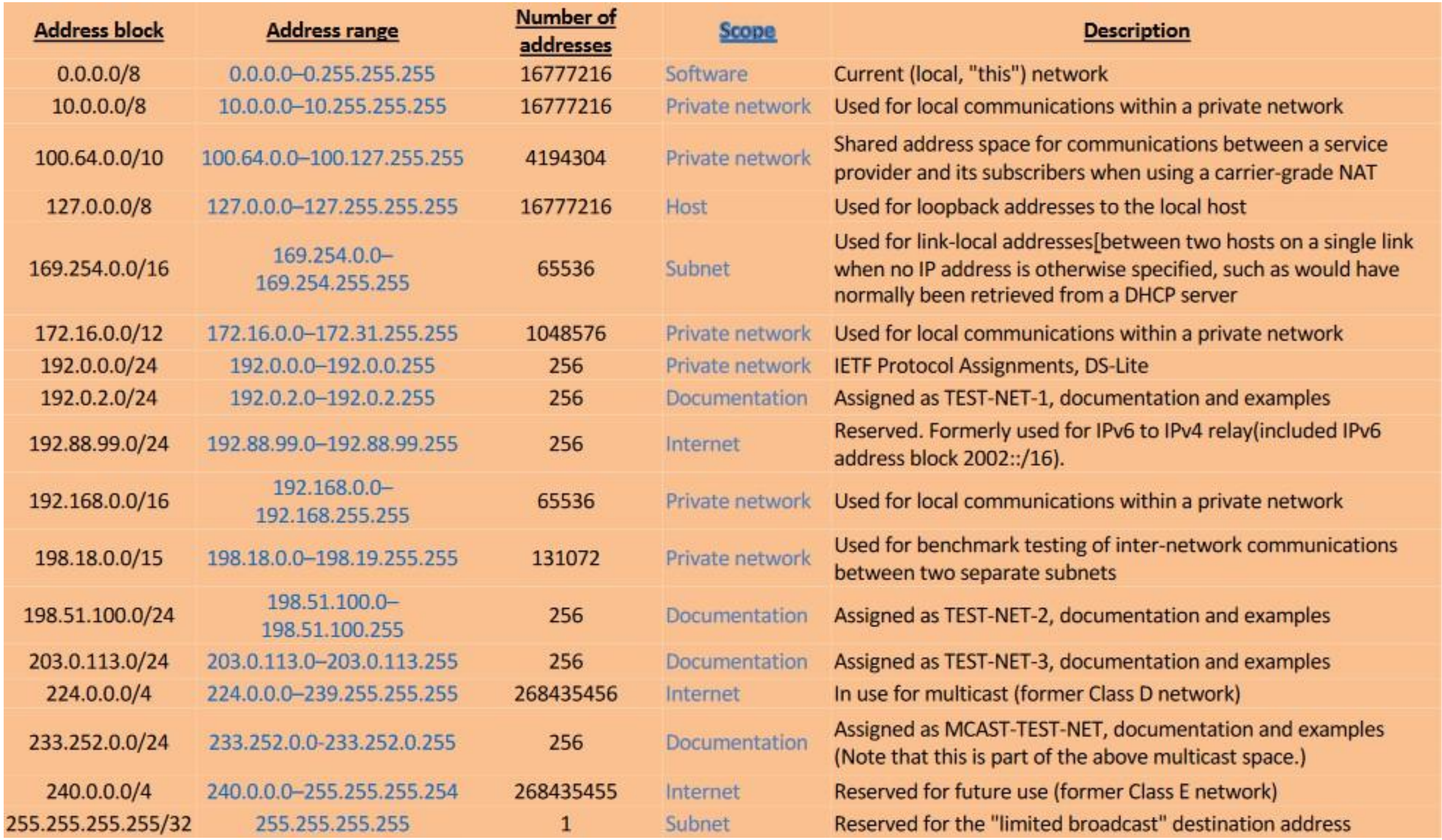


IPv4



- Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP);
- It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks;
- Internet Protocol version 4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition of January 1980 (RFC 760);
- In March 1982, the US Department of Defense decided on the Internet Protocol Suite (TCP/IP) as the standard for all military computer networking;
- IPv4 was the first version deployed for production on SATNET in 1982 and on the ARPANET in January 1983. It is still used to route most Internet traffic today, even with the ongoing deployment of Internet Protocol version 6 (IPv6), its successor.
- IPv4 uses a 32-bit address space which provides 4,294,967,296 unique addresses, but large blocks are reserved for special networking purposes;
- The Internet Protocol is the protocol that defines and enables internetworking at the internet layer of the Internet Protocol Suite.
- It uses a logical addressing system and performs routing, which is the forwarding of packets from a source host to the next router that is one hop closer to the intended destination host on another network;
- IPv4 is a connectionless protocol, and operates on a best-effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery, because these aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP);
- IPv4 reserves special address blocks for private networks (~18 million addresses) and multicast addresses (~270 million addresses).

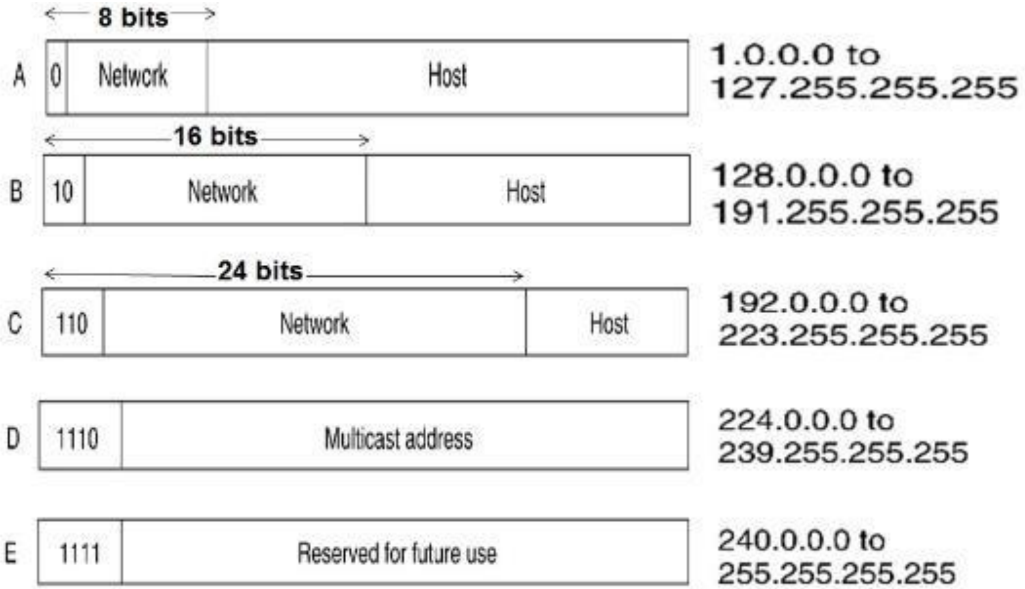
Special-use addresses

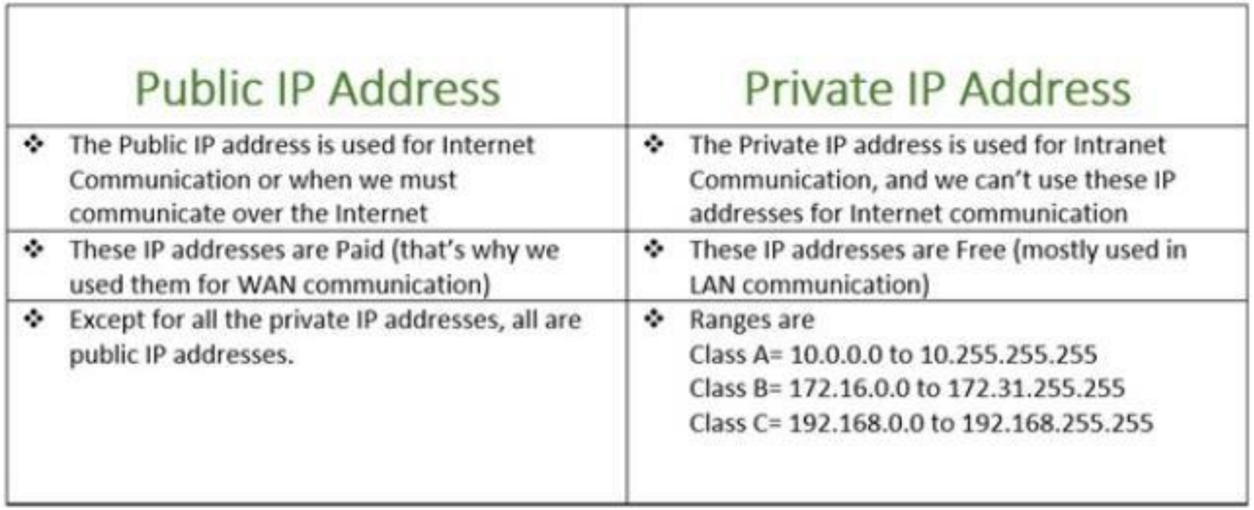


Address block	Address range	Number of addresses	Scope	Description
0.0.0.0/8	0.0.0.0–0.255.255.255	16777216	Software	Current (local, "this") network
10.0.0.0/8	10.0.0.0–10.255.255.255	16777216	Private network	Used for local communications within a private network
100.64.0.0/10	100.64.0.0–100.127.255.255	4194304	Private network	Shared address space for communications between a service provider and its subscribers when using a carrier-grade NAT
127.0.0.0/8	127.0.0.0–127.255.255.255	16777216	Host	Used for loopback addresses to the local host
169.254.0.0/16	169.254.0.0–169.254.255.255	65536	Subnet	Used for link-local addresses[between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a DHCP server
172.16.0.0/12	172.16.0.0–172.31.255.255	1048576	Private network	Used for local communications within a private network
192.0.0.0/24	192.0.0.0–192.0.0.255	256	Private network	IETF Protocol Assignments, DS-Lite
192.0.2.0/24	192.0.2.0–192.0.2.255	256	Documentation	Assigned as TEST-NET-1, documentation and examples
192.88.99.0/24	192.88.99.0–192.88.99.255	256	Internet	Reserved. Formerly used for IPv6 to IPv4 relay(included IPv6 address block 2002::/16).
192.168.0.0/16	192.168.0.0–192.168.255.255	65536	Private network	Used for local communications within a private network
198.18.0.0/15	198.18.0.0–198.19.255.255	131072	Private network	Used for benchmark testing of inter-network communications between two separate subnets
198.51.100.0/24	198.51.100.0–198.51.100.255	256	Documentation	Assigned as TEST-NET-2, documentation and examples
203.0.113.0/24	203.0.113.0–203.0.113.255	256	Documentation	Assigned as TEST-NET-3, documentation and examples
224.0.0.0/4	224.0.0.0–239.255.255.255	268435456	Internet	In use for multicast (former Class D network)
233.252.0.0/24	233.252.0.0-233.252.0.255	256	Documentation	Assigned as MCAST-TEST-NET, documentation and examples (Note that this is part of the above multicast space.)
240.0.0.0/4	240.0.0.0–255.255.255.254	268435455	Internet	Reserved for future use (former Class E network)
255.255.255.255/32	255.255.255.255	1	Subnet	Reserved for the "limited broadcast" destination address

Classes

- Class A (0-127)
- Class B (128-191)
- Class C (192-223)
- Class D (224-239)
- Class E (240-255)





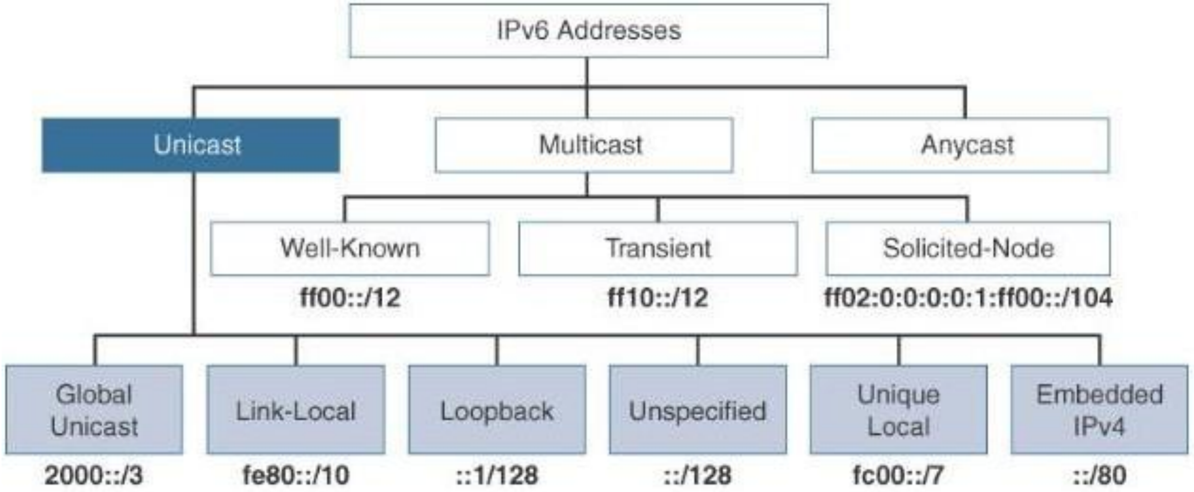
Public IP Address	Private IP Address
❖ The Public IP address is used for Internet Communication or when we must communicate over the Internet	❖ The Private IP address is used for Intranet Communication, and we can't use these IP addresses for Internet communication
❖ These IP addresses are Paid (that's why we used them for WAN communication)	❖ These IP addresses are Free (mostly used in LAN communication)
❖ Except for all the private IP addresses, all are public IP addresses.	❖ Ranges are Class A= 10.0.0.0 to 10.255.255.255 Class B= 172.16.0.0 to 172.31.255.255 Class C= 192.168.0.0 to 192.168.255.255

IPv6

- Devices on the Internet are assigned a unique IP address for identification and location definition, but, with the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect devices than the IPv4 address space had available;
- Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet;
- IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion, and was intended to replace IPv4;
- In December 1998, IPv6 became a Draft Standard for the IETF, which subsequently ratified it as an Internet Standard on 14 July 2017;
- IPv6 uses 128-bit addresses, theoretically allowing 2128, or approximately 3.4×1038 total addresses. The actual number is slightly smaller, as multiple ranges are reserved for special usage or completely excluded from general use. The two protocols are not designed to be interoperable, and thus direct communication between them is impossible, complicating the move to IPv6. However, several transition mechanisms have been devised to rectify this;
- IPv6 provides other technical benefits in addition to a larger addressing space :
  - ✓ In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables;
  - ✓ The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services;
  - ✓ Device mobility, security, and configuration aspects have been considered in the design of the protocol;
- IPv6 addresses are represented as eight groups of four hexadecimal digits each, separated by colons;
- The full representation may be shortened; for example, 2001:0db8:0000:0000:0000:8a2e:0370:7334 becomes 2001:db8::8a2e:370:7334.

IPv6 structure

- By the way, there is no broadcast address in IPv6 world. As you remember, we were using IPv4 broadcast addresses (https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml)
- IPv6 Special Addresses are the addresses which are used for different purposes. We have such IP addresses for IPv4 too;
- IPv6 Unicast Addresses are single node or single interface ip addresses. When we send a traffic to a unicast address, this traffic is sent only to that node or interface. In IPv6 world, we have three different IPv6 Unicast Addresses;
- IPv6 Multicast Addresses are IPv6 addresses which identify a group of interface or nodes. When we send a traffic to a multicast address, this traffic is sent to that group;
- IPv6 Anycast Addresses is the new additional ip address type in IPv6 world. When we send a traffic to an anycast address, this traffic is sent to the nearest interface which is configured with the same anycast ip address.



Basic Networking Protocols

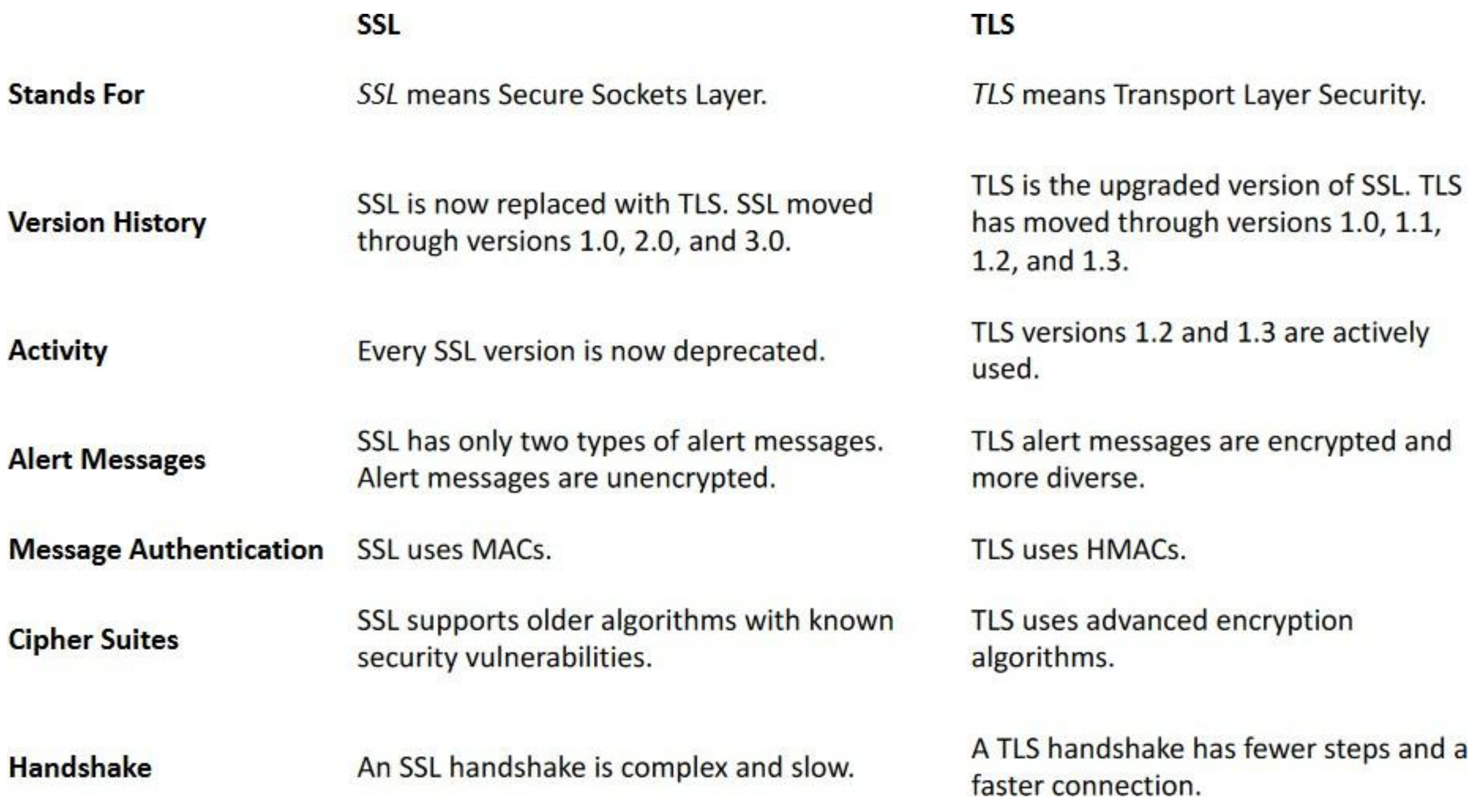
- Reviewing Basic Connectivity Protocols
  - ✓ IPv4 and IPv6;
  - ✓ ICMP
    - ➢ Commonly blocked at firewalls;
    - ➢ If ping fails, ICMP may be blocked;
  - ✓ ARP
    - ➢ Resolves MAC addresses for IPv4.

Protocols and Use Cases

- Transport voice and video over network
  - ✓ RTP & SRTP;

- Transfer files over a network
  - ✓ FTP;
  - ✓ TFTP;
  - ✓ SSH;
  - ✓ SSL;
  - ✓ TLS;
  - ✓ Ipsec;
  - ✓ SFTP;
  - ✓ FTPS.

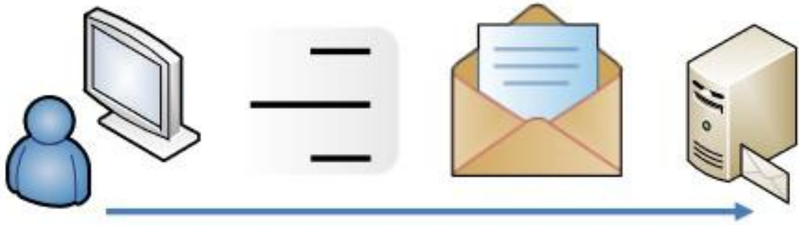
SSL vs TLS

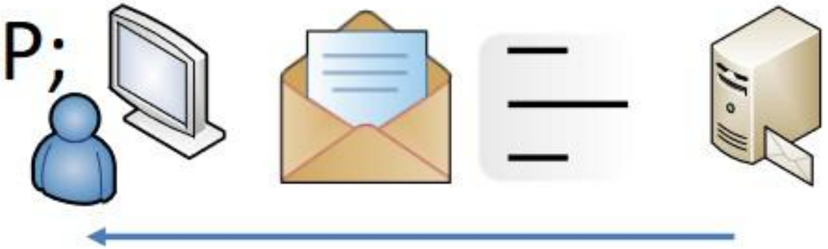


	SSL	**TLS**
Stands For	*SSL* means Secure Sockets Layer.	*TLS* means Transport Layer Security.
Version History	SSL is now replaced with TLS. SSL moved through versions 1.0, 2.0, and 3.0.	TLS is the upgraded version of SSL. TLS has moved through versions 1.0, 1.1, 1.2, and 1.3.
Activity	Every SSL version is now deprecated.	TLS versions 1.2 and 1.3 are actively used.
Alert Messages	SSL has only two types of alert messages. Alert messages are unencrypted.	TLS alert messages are encrypted and more diverse.
Message Authentication	SSL uses MACs.	TLS uses HMACs.
Cipher Suites	SSL supports older algorithms with known security vulnerabilities.	TLS uses advanced encryption algorithms.
Handshake	An SSL handshake is complex and slow.	A TLS handshake has fewer steps and a faster connection.

Protocols and Use Cases

- Email and web usage
  - ✓ SMTP;
  - ✓ POP3 & Secure POP;
  - ✓ IMAP4 and Secure IMAP;
  - ✓ HTTP;
  - ✓ HTTPS.





Protocols and Use Cases

- Directory services
  - ✓ LDAP – 389
    - ➢ Port 636 when encrypted with SSL or TLS;
  - ✓ Kerberos – Port 88.

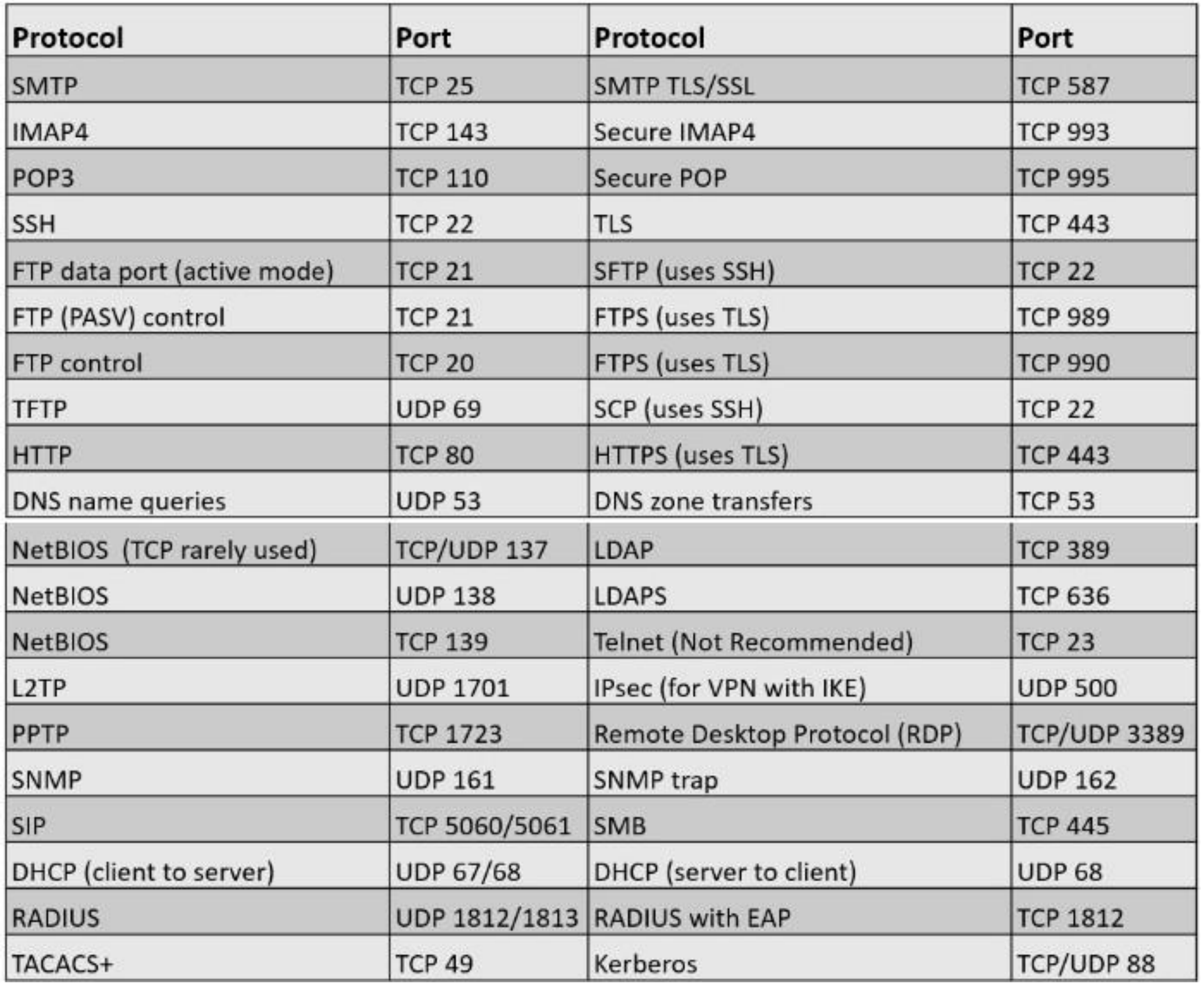
- Remote access
  - ✓ SSH;
  - ✓ Netcat;
  - ✓ RDP.

Protocols and Use Cases

- OpenSSH;

- Time synchronization
  - ✓ NTP;
  - ✓ SNTP.

Important ports



Protocol	Port	Protocol	Port
SMTP	TCP 25	SMTP TLS/SSL	TCP 587
IMAP4	TCP 143	Secure IMAP4	TCP 993
POP3	TCP 110	Secure POP	TCP 995
SSH	TCP 22	TLS	TCP 443
FTP data port (active mode)	TCP 21	SFTP (uses SSH)	TCP 22
FTP (PASV) control	TCP 21	FTPS (uses TLS)	TCP 989
FTP control	TCP 20	FTPS (uses TLS)	TCP 990
TFTP	UDP 69	SCP (uses SSH)	TCP 22
HTTP	TCP 80	HTTPS (uses TLS)	TCP 443
DNS name queries	UDP 53	DNS zone transfers	TCP 53
NetBIOS (TCP rarely used)	TCP/UDP 137	LDAP	TCP 389
NetBIOS	UDP 138	LDAPS	TCP 636
NetBIOS	TCP 139	Telnet (Not Recommended)	TCP 23
L2TP	UDP 1701	IPsec (for VPN with IKE)	UDP 500
PPTP	TCP 1723	Remote Desktop Protocol (RDP)	TCP/UDP 3389
SNMP	UDP 161	SNMP trap	UDP 162
SIP	TCP 5060/5061	SMB	TCP 445
DHCP (client to server)	UDP 67/68	DHCP (server to client)	UDP 68
RADIUS	UDP 1812/1813	RADIUS with EAP	TCP 1812
TACACS+	TCP 49	Kerberos	TCP/UDP 88

Network Address Allocation

- IPv4 – 32 bits (192.168.1.5);

- Private IP Addresses

✓ 10.x.y.z
10.0.0.0 through 10.255.255.255;

✓ 172.16.y.z–172.31.y.z
172.16.0.0 through 172.31.255.255;

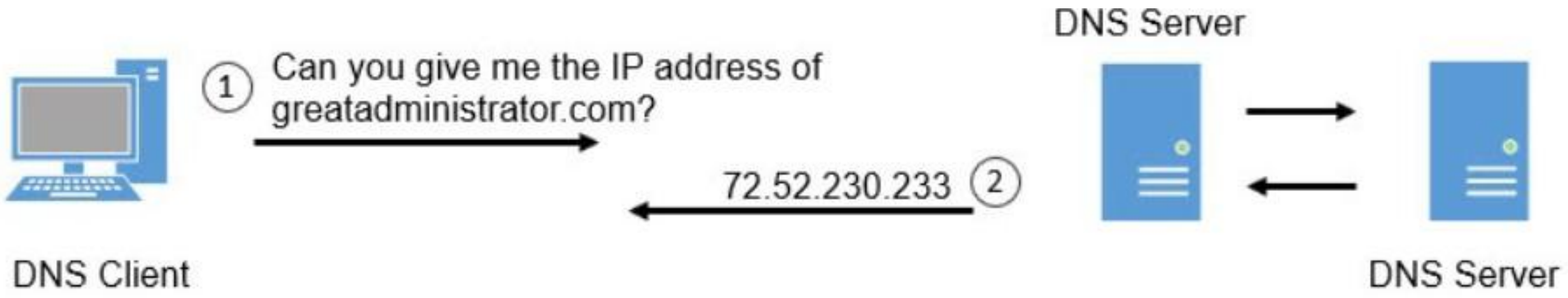
✓ 192.168.y.z
192.168.0.0 through 192.168.255.255.

Network Address Allocation

- IPv6 – 128 bits
  - fe80:0000:0000:0000:02d4:3ff7:003f:de62.

- DHCP Snooping
  - DHCP Discover;
  - DHCP Offer;
  - DHCP Request;
  - DHCP Acknowledge.

Understanding DNS



Records :

- A - IPv4 Host;
- AAAA - IPv6 Host;
- PTR – Pointer;
- MX - Mail server;
- CNAME – Alias;
- SOA – TTL.

Understanding DNS

- Queries to DNS server use UDP port 53;

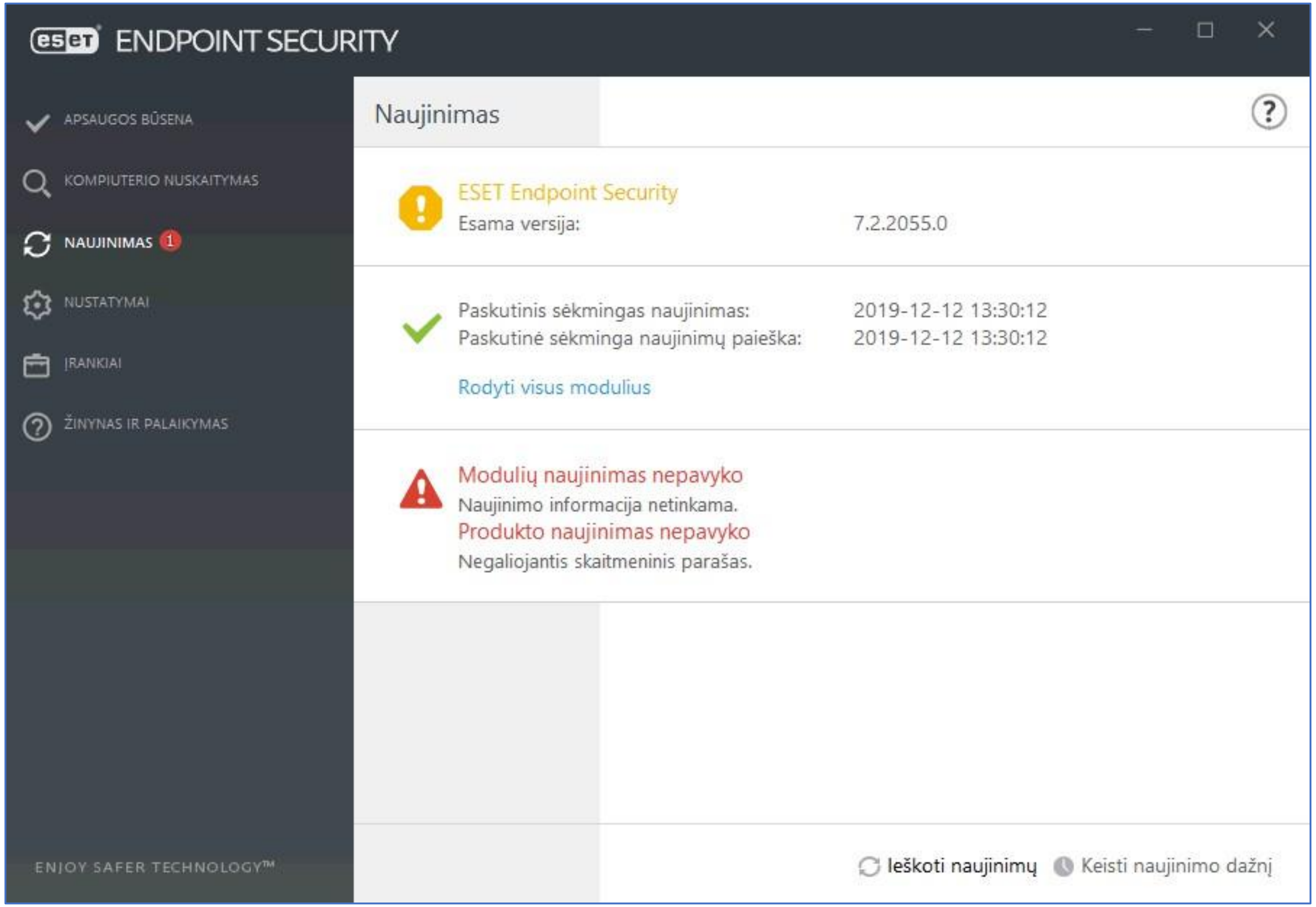
- Zone transfers between servers use TCP port 53;

- DNSSEC
  - ✓ DNS poisoning.

Protocols and Use Cases

- Commands
  - ✓Nslookup;
  - ✓Dig;
- Subscription services;
- Quality of Service.

Troubleshooting Example



Naujinimas

ESET Endpoint Security
Esama versija: 7.2.2055.0

Paskutinis sėkmingas naujinimas: 2019-12-12 13:30:12
Paskutinė sėkminga naujinimų paieška: 2019-12-12 13:30:12

Rodyti visus modulius

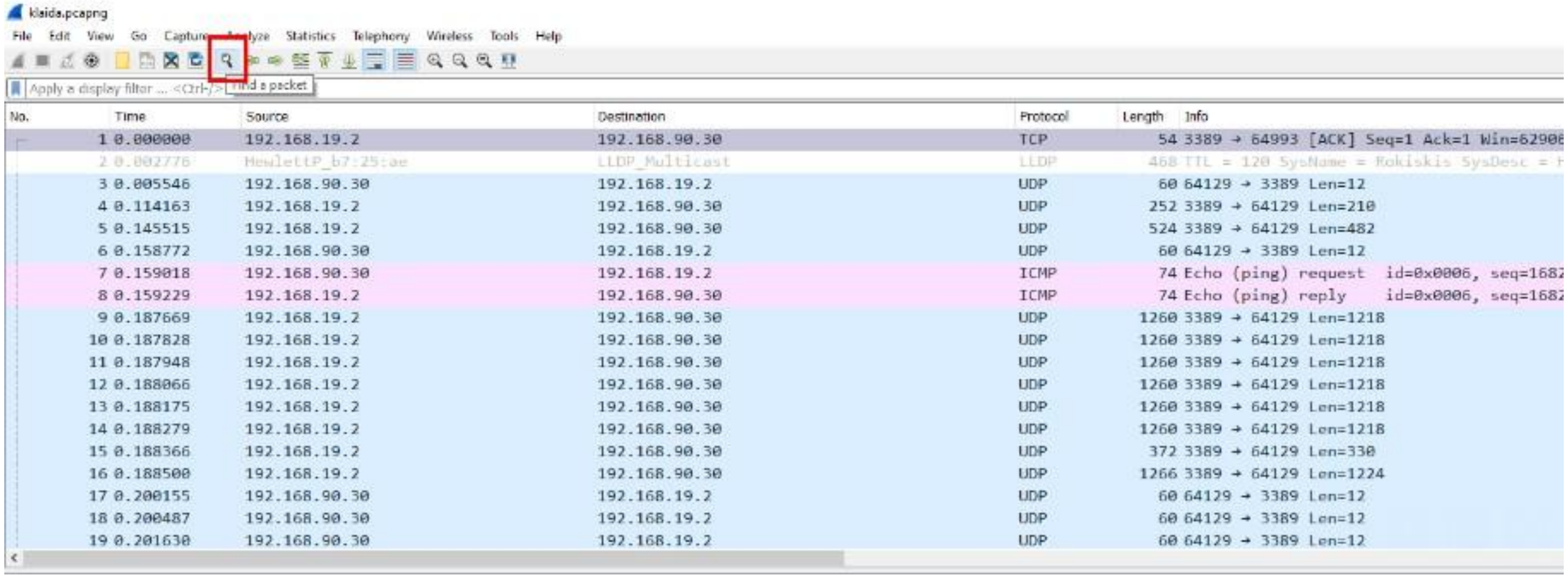
Modulių naujinimas nepavyko
Naujinimo informacija netinkama.
Produkto naujinimas nepavyko
Negaliojantis skaitmeninis parašas.

Troubleshooting Example

Collect logs ***.pcapng** format

Troubleshooting Example

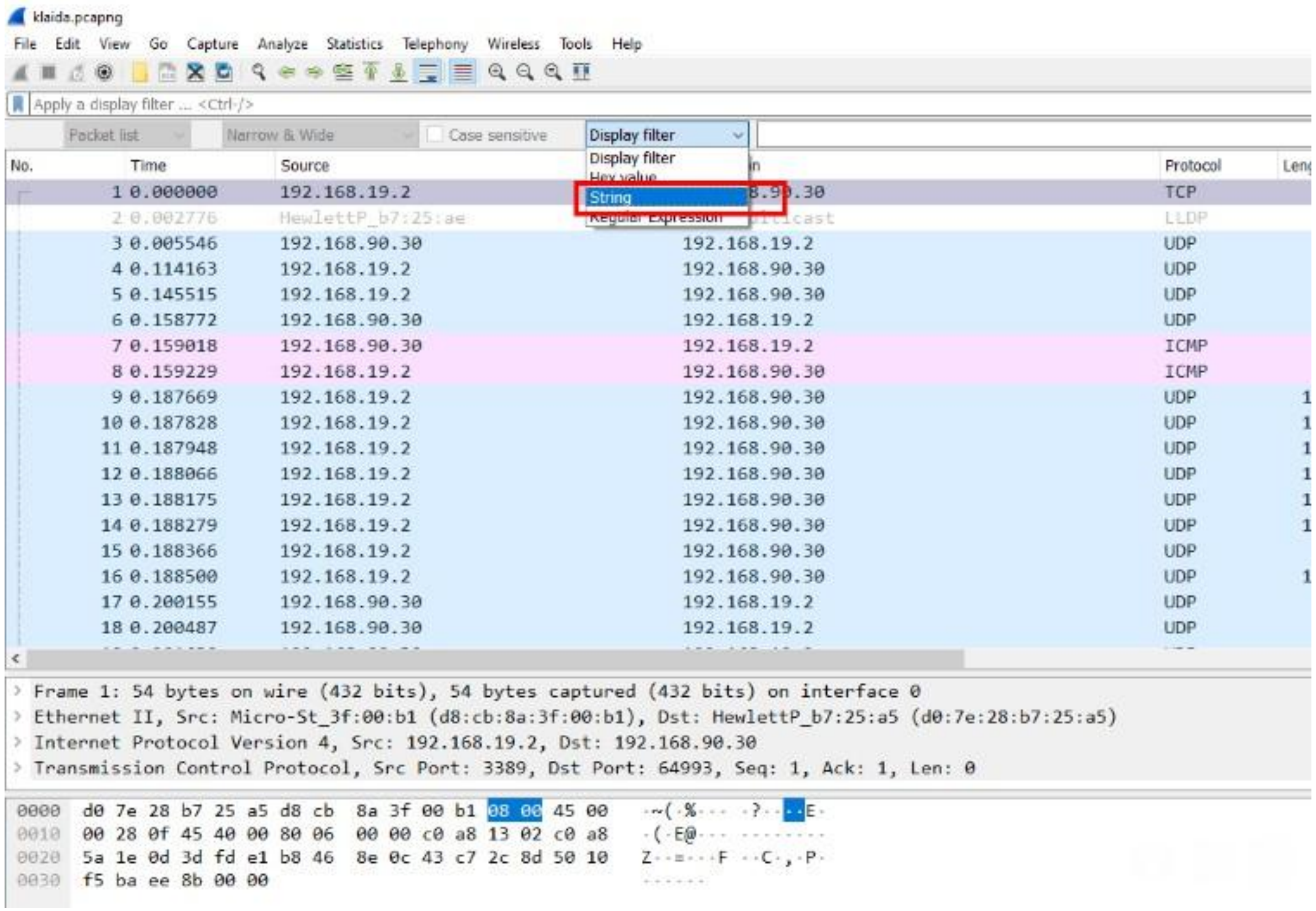
1. Wireshark programoje spaudžiame raudonai apibrauktą mygtuką "Find a packet":



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.19.2	192.168.90.30	TCP	54	3389 → 64993 [ACK] Seq=1 Ack=1 Win=6290
2	0.002776	HewlettP_b7:25:ae	LLDP_Multicast	LLDP	468	TTL = 120 SysName = Rokiskis SysDesc =
3	0.005546	192.168.90.30	192.168.19.2	UDP	60	64129 → 3389 Len=12
4	0.114163	192.168.19.2	192.168.90.30	UDP	252	3389 → 64129 Len=210
5	0.145515	192.168.19.2	192.168.90.30	UDP	524	3389 → 64129 Len=482
6	0.158772	192.168.90.30	192.168.19.2	UDP	60	64129 → 3389 Len=12
7	0.159018	192.168.90.30	192.168.19.2	ICMP	74	Echo (ping) request id=0x0006, seq=1682
8	0.159229	192.168.19.2	192.168.90.30	ICMP	74	Echo (ping) reply id=0x0006, seq=1682
9	0.187669	192.168.19.2	192.168.90.30	UDP	1260	3389 → 64129 Len=1218
10	0.187828	192.168.19.2	192.168.90.30	UDP	1260	3389 → 64129 Len=1218
11	0.187948	192.168.19.2	192.168.90.30	UDP	1260	3389 → 64129 Len=1218
12	0.188066	192.168.19.2	192.168.90.30	UDP	1260	3389 → 64129 Len=1218
13	0.188175	192.168.19.2	192.168.90.30	UDP	1260	3389 → 64129 Len=1218
14	0.188279	192.168.19.2	192.168.90.30	UDP	1260	3389 → 64129 Len=1218
15	0.188366	192.168.19.2	192.168.90.30	UDP	372	3389 → 64129 Len=330
16	0.188500	192.168.19.2	192.168.90.30	UDP	1266	3389 → 64129 Len=1224
17	0.200155	192.168.90.30	192.168.19.2	UDP	60	64129 → 3389 Len=12
18	0.200487	192.168.90.30	192.168.19.2	UDP	60	64129 → 3389 Len=12
19	0.201630	192.168.90.30	192.168.19.2	UDP	60	64129 → 3389 Len=12

Troubleshooting Example

2. Paskui atsidariusioje paieškoje pakeičiame kriterijų į "String":



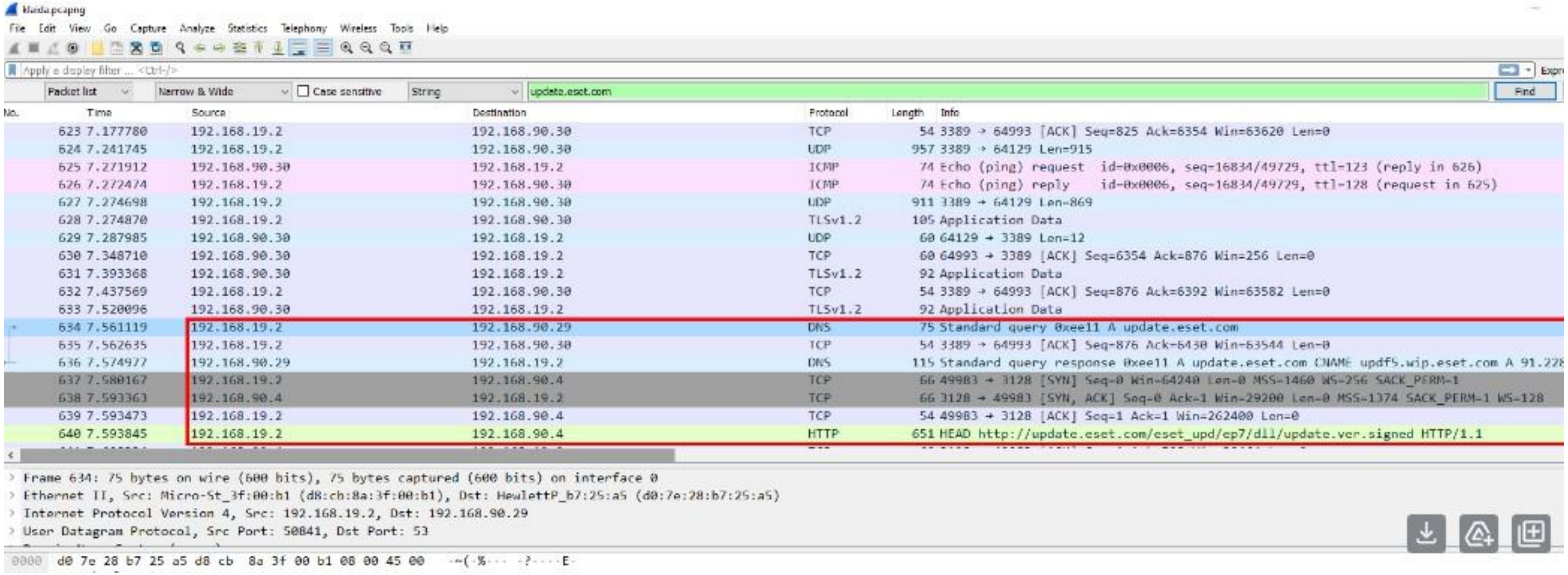
```
No.      Time       Source                          n                 Protocol  Leng
       1 0.000000   192.168.19.2                   8.9 .30            TCP
       2 0.002776   HewlettP_b7:25:ae                  icast          LLDP
       3 0.005546   192.168.90.30               192.168.19.2          UDP
       4 0.114163   192.168.19.2                192.168.90.30         UDP
       5 0.145515   192.168.19.2                192.168.90.30         UDP
       6 0.158772   192.168.90.30               192.168.19.2          UDP
       7 0.159018   192.168.90.30               192.168.19.2          ICMP
       8 0.159229   192.168.19.2                192.168.90.30         ICMP
       9 0.187669   192.168.19.2                192.168.90.30         UDP        1
      10 0.187828   192.168.19.2                192.168.90.30         UDP        1
      11 0.187948   192.168.19.2                192.168.90.30         UDP        1
      12 0.188066   192.168.19.2                192.168.90.30         UDP        1
      13 0.188175   192.168.19.2                192.168.90.30         UDP        1
      14 0.188279   192.168.19.2                192.168.90.30         UDP        1
      15 0.188366   192.168.19.2                192.168.90.30         UDP
      16 0.188500   192.168.19.2                192.168.90.30         UDP        1
      17 0.200155   192.168.90.30               192.168.19.2          UDP
      18 0.200487   192.168.90.30               192.168.19.2          UDP
```

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: Micro-St_3f:00:b1 (d8:cb:8a:3f:00:b1), Dst: HewlettP_b7:25:a5 (d0:7e:28:b7:25:a5)
> Internet Protocol Version 4, Src: 192.168.19.2, Dst: 192.168.90.30
> Transmission Control Protocol, Src Port: 3389, Dst Port: 64993, Seq: 1, Ack: 1, Len: 0
```

```
0000  d0 7e 28 b7 25 a5 d8 cb  8a 3f 00 b1 08 00 45 00   ·~(·%··· ·?····E·
0010  00 28 0f 45 40 00 80 06  00 00 c0 a8 13 02 c0 a8   ·(·E@··· ········
0020  5a 1e 0d 3d fd e1 b8 46  8e 0c 43 c7 2c 8d 50 10   Z··=···F ··C·,·P·
0030  f5 ba ee 8b 00 00                                  ······
```

Troubleshooting Example

3. Įrašome, ko ieškome, mūsų atveju rašome "update.eset.com", nes jums neveikė ESET atnaujinimai, ir surandame ko ieškojome:


klaida.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expr
Packet list
Narrow & Wide
□ Case sensitive
String
update.eset.com
Find

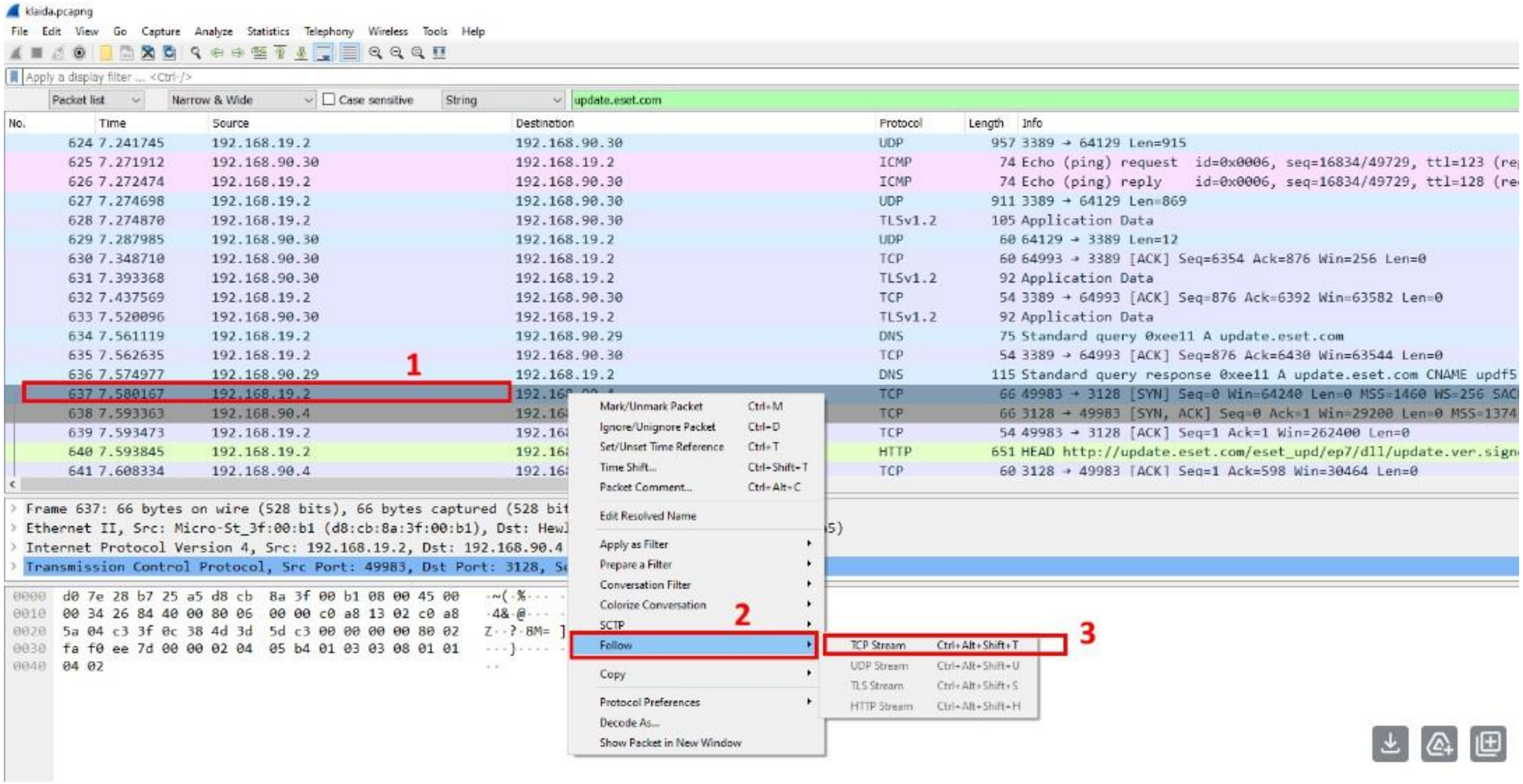
No.	Time	Source	Destination	Protocol	Length	Info
623	7.177780	192.168.19.2	192.168.90.30	TCP	54	3389 → 64993 [ACK] Seq=825 Ack=6354 Win=63620 Len=0
624	7.241745	192.168.19.2	192.168.90.30	UDP	957	3389 → 64129 Len=915
625	7.271912	192.168.90.30	192.168.19.2	ICMP	74	Echo (ping) request id=0x0006, seq=16834/49729, ttl=123 (reply in 626)
626	7.272474	192.168.19.2	192.168.90.30	ICMP	74	Echo (ping) reply id=0x0006, seq=16834/49729, ttl=128 (request in 625)
627	7.274698	192.168.19.2	192.168.90.30	UDP	911	3389 → 64129 Len=869
628	7.274870	192.168.19.2	192.168.90.30	TLSv1.2	105	Application Data
629	7.287985	192.168.90.30	192.168.19.2	UDP	60	64129 → 3389 Len=12
630	7.348710	192.168.90.30	192.168.19.2	TCP	60	64993 → 3389 [ACK] Seq=6354 Ack=876 Win=256 Len=0
631	7.393368	192.168.90.30	192.168.19.2	TLSv1.2	92	Application Data
632	7.437569	192.168.19.2	192.168.90.30	TCP	54	3389 → 64993 [ACK] Seq=876 Ack=6392 Win=63582 Len=0
633	7.520096	192.168.90.30	192.168.19.2	TLSv1.2	92	Application Data
634	7.561119	192.168.19.2	192.168.90.29	DNS	75	Standard query 0xee11 A update.eset.com
635	7.562635	192.168.19.2	192.168.90.30	TCP	54	3389 → 64993 [ACK] Seq=876 Ack=6430 Win=63544 Len=0
636	7.574977	192.168.90.29	192.168.19.2	DNS	115	Standard query response 0xee11 A update.eset.com CNAME updf5.wip.eset.com A 91.228
637	7.580167	192.168.19.2	192.168.90.4	TCP	66	49983 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
638	7.593363	192.168.90.4	192.168.19.2	TCP	66	3128 → 49983 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1374 SACK_PERM=1 WS=128
639	7.593473	192.168.19.2	192.168.90.4	TCP	54	49983 → 3128 [ACK] Seq=1 Ack=1 Win=262400 Len=0
640	7.593845	192.168.19.2	192.168.90.4	HTTP	651	HEAD http://update.eset.com/eset_upd/ep7/dll/update.ver.signed HTTP/1.1

```
> Frame 634: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
> Ethernet II, Src: Micro-St_3f:00:b1 (d8:cb:8a:3f:00:b1), Dst: HewlettP_b7:25:a5 (d0:7e:28:b7:25:a5)
> Internet Protocol Version 4, Src: 192.168.19.2, Dst: 192.168.90.29
> User Datagram Protocol, Src Port: 50841, Dst Port: 53
```

```
0000  d0 7e 28 b7 25 a5 d8 cb  8a 3f 00 b1 08 00 45 00   ·~(·%··· ·?····E·
```

Troubleshooting Example

4. Tuomet spaudžiame dešinįjį klavišą ant pirmo pilko laukelio ir išsirenkame iš atsidariusio meniu "Follow" ir "TCP Stream":



klaida.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packet list
Narrow & Wide
□ Case sensitive
String
update.eset.com
1
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
2
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
3
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

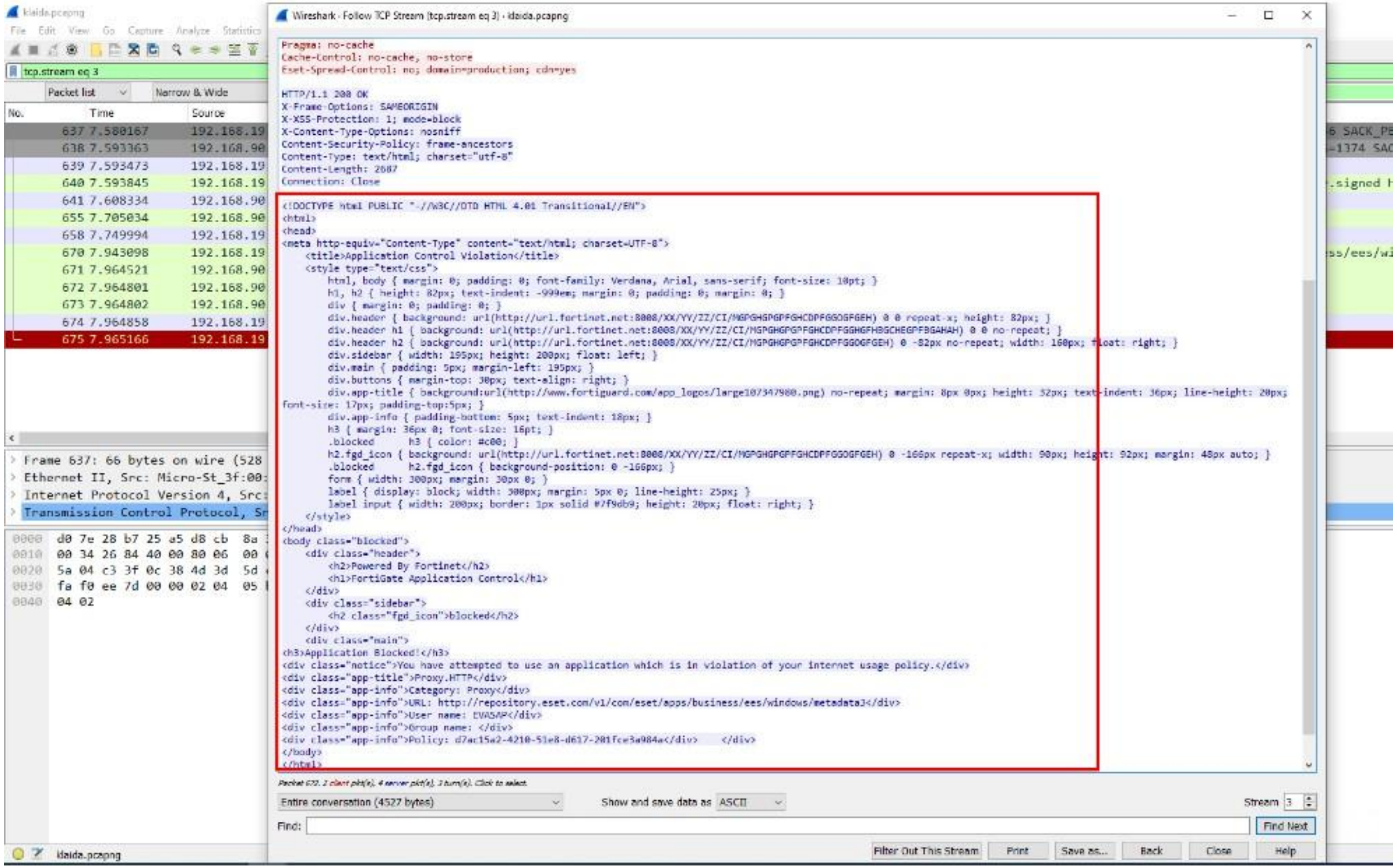
```
No.      Time         Source           Destination      Protocol  Length Info
    624 7.241745     192.168.19.2     192.168.90.30    UDP          957 3389 → 64129 Len=915
    625 7.271912     192.168.90.30    192.168.19.2     ICMP          74 Echo (ping) request  id=0x0006, seq=16834/49729, ttl=123 (re
    626 7.272474     192.168.19.2     192.168.90.30    ICMP          74 Echo (ping) reply    id=0x0006, seq=16834/49729, ttl=128 (re
    627 7.274698     192.168.19.2     192.168.90.30    UDP          911 3389 → 64129 Len=869
    628 7.274870     192.168.19.2     192.168.90.30    TLSv1.2      105 Application Data
    629 7.287985     192.168.90.30    192.168.19.2     UDP           60 64129 → 3389 Len=12
    630 7.348710     192.168.90.30    192.168.19.2     TCP           60 64993 → 3389 [ACK] Seq=6354 Ack=876 Win=256 Len=0
    631 7.393368     192.168.90.30    192.168.19.2     TLSv1.2       92 Application Data
    632 7.437569     192.168.19.2     192.168.90.30    TCP           54 3389 → 64993 [ACK] Seq=876 Ack=6392 Win=63582 Len=0
    633 7.520096     192.168.90.30    192.168.19.2     TLSv1.2       92 Application Data
    634 7.561119     192.168.19.2     192.168.90.29    DNS           75 Standard query 0xee11 A update.eset.com
    635 7.562635     192.168.19.2     192.168.90.30    TCP           54 3389 → 64993 [ACK] Seq=876 Ack=6430 Win=63544 Len=0
    636 7.574977     192.168.90.29    192.168.19.2     DNS          115 Standard query response 0xee11 A update.eset.com CNAME updf5
    637 7.580167     192.168.19.2     192.168          TCP           66 49983 → 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC
    638 7.593363     192.168.90.4     192.16           TCP           66 3128 → 49983 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1374
    639 7.593473     192.168.19.2     192.16           TCP           54 49983 → 3128 [ACK] Seq=1 Ack=1 Win=262400 Len=0
    640 7.593845     192.168.19.2     192.16           HTTP         651 HEAD http://update.eset.com/eset_upd/ep7/dll/update.ver.sign
    641 7.608334     192.168.90.4     192.16           TCP           60 3128 → 49983 [ACK] Seq=1 Ack=598 Win=30464 Len=0
```

```
> Frame 637: 66 bytes on wire (528 bits), 66 bytes captured (528 bit
> Ethernet II, Src: Micro-St_3f:00:b1 (d8:cb:8a:3f:00:b1), Dst: Hewl                          5)
> Internet Protocol Version 4, Src: 192.168.19.2, Dst: 192.168.90.4
> Transmission Control Protocol, Src Port: 49983, Dst Port: 3128, S
```

```
0000  d0 7e 28 b7 25 a5 d8 cb  8a 3f 00 b1 08 00 45 00   ·~(·%···
0010  00 34 26 84 40 00 80 06  00 00 c0 a8 13 02 c0 a8   ·4&·@···
0020  5a 04 c3 3f 0c 38 4d 3d  5d c3 00 00 00 00 80 02   Z··?·8M= ]
0030  fa f0 ee 7d 00 00 02 04  05 b4 01 03 03 08 01 01   ···}····
0040  04 02                                              ··
```

Troubleshooting Example

5. Taip ir gauname Fortigate įrašą apie blokavimą:



```
No.     Time        Source
    637 7.580167    192.168.19
    638 7.593363    192.168.90
    639 7.593473    192.168.19
    640 7.593845    192.168.19
    641 7.608334    192.168.90
    655 7.705034    192.168.90
    658 7.749994    192.168.19
    670 7.943098    192.168.19
    671 7.964521    192.168.90
    672 7.964801    192.168.90
    673 7.964802    192.168.90
    674 7.964858    192.168.19
    675 7.965166    192.168.19

> Frame 637: 66 bytes on wire (528
> Ethernet II, Src: Micro-St_3f:00:
> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr

0000  d0 7e 28 b7 25 a5 d8 cb  8a
0010  00 34 26 84 40 00 80 06  00
0020  5a 04 c3 3f 0c 38 4d 3d  5d
0030  fa f0 ee 7d 00 00 02 04  05
0040  04 02
```

klaida.pcapng
Wireshark · Follow TCP Stream (tcp.stream eq 3) · klaida.pcapng

```
Pragma: no-cache
Cache-Control: no-cache, no-store
Eset-Spread-Control: no; domain=production; cdn=yes

HTTP/1.1 200 OK
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: frame-ancestors
Content-Type: text/html; charset="utf-8"
Content-Length: 2687
Connection: Close

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <title>Application Control Violation</title>
    <style type="text/css">
        html, body { margin: 0; padding: 0; font-family: Verdana, Arial, sans-serif; font-size: 10pt; }
        h1, h2 { height: 82px; text-indent: -999em; margin: 0; padding: 0; margin: 0; }
        div { margin: 0; padding: 0; }
        div.header { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGOGFGEH) 0 0 repeat-x; height: 82px; }
        div.header h1 { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGHGFHBGCHEGPFBGAHAH) 0 0 no-repeat; }
        div.header h2 { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGOGFGEH) 0 -82px no-repeat; width: 160px; float: right; }
        div.sidebar { width: 195px; height: 200px; float: left; }
        div.main { padding: 5px; margin-left: 195px; }
        div.buttons { margin-top: 30px; text-align: right; }
        div.app-title { background:url(http://www.fortiguard.com/app_logos/large107347980.png) no-repeat; margin: 8px 0px; height: 32px; text-indent: 36px; line-height: 20px;
font-size: 17px; padding-top:5px; }
        div.app-info { padding-bottom: 5px; text-indent: 18px; }
        h3 { margin: 36px 0; font-size: 16pt; }
        .blocked      h3 { color: #c00; }
        h2.fgd_icon { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGOGFGEH) 0 -166px repeat-x; width: 90px; height: 92px; margin: 48px auto; }
        .blocked      h2.fgd_icon { background-position: 0 -166px; }
        form { width: 300px; margin: 30px 0; }
        label { display: block; width: 300px; margin: 5px 0; line-height: 25px; }
        label input { width: 200px; border: 1px solid #7f9db9; height: 20px; float: right; }
    </style>
</head>
<body class="blocked">
    <div class="header">
        <h2>Powered By Fortinet</h2>
        <h1>FortiGate Application Control</h1>
    </div>
    <div class="sidebar">
        <h2 class="fgd_icon">blocked</h2>
    </div>
    <div class="main">
<h3>Application Blocked!</h3>
<div class="notice">You have attempted to use an application which is in violation of your internet usage policy.</div>
<div class="app-title">Proxy.HTTP</div>
<div class="app-info">Category: Proxy</div>
<div class="app-info">URL: http://repository.eset.com/v1/com/eset/apps/business/ees/windows/metadata3</div>
<div class="app-info">User name: EVASAP</div>
<div class="app-info">Group name: </div>
<div class="app-info">Policy: d7ac15a2-4210-51e8-d617-201fce3a984a</div>    </div>
</body>
</html>
```

Packet 672. 2 client pkt(s), 4 server pkt(s), 3 turn(s). Click to select.

Entire conversation (4527 bytes)

Show and save data as: ASCII

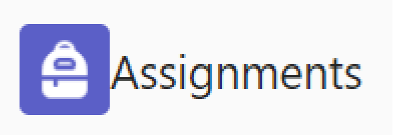
Stream: 3

Find:

Troubleshooting Example

```
<html>
<head>
<meta http-equiv="Content-Type"  content="text/html; charset=UTF-8">
<title>Application Control Violation</title>
<style type="text/css">
html, body { margin: 0; padding: 0; font-family: Verdana, Arial, sans-serif; font-size: 10pt; }
h1, h2 { height: 82px; text-indent: -999em; margin: 0; padding: 0; margin: 0; }
div { margin: 0; padding: 0; }
div.header { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGOGFGEH) 0 0 repeat-x; height: 82px; }
div.header h1 { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGHGFHBGCHEGPFBGAHAH) 0 0 no-repeat; }
div.header h2 { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGOGFGEH) 0 -82px no-repeat; width: 160px; float: right; }
div.sidebar { width: 195px; height: 200px; float: left; }
div.main { padding: 5px; margin-left: 195px; }
div.buttons { margin-top: 30px; text-align: right; }
div.app-title { background:url(http://www.fortiguard.com/app_logos/large107347980.png) no-repeat; margin: 8px 0px; height: 32px; text-indent: 36px; line-height: 20px; font-size: 17px; padding-top:5px; }
div.app-info { padding-bottom: 5px; text-indent: 18px; }
h3 { margin: 36px 0; font-size: 16pt; }
.blocked h3 { color: #c00; }
h2.fgd_icon { background: url(http://url.fortinet.net:8008/XX/YY/ZZ/CI/MGPGHGPGPFGHCDPFGGOGFGEH) 0 -166px repeat-x; width: 90px; height: 92px; margin: 48px auto; }
.blocked h2.fgd_icon { background-position: 0 -166px; }
form { width: 300px; margin: 30px 0; }
label { display: block; width: 300px; margin: 5px 0; line-height: 25px; }
label input { width: 200px; border: 1px solid #7f9db9; height: 20px; float: right; }
</style>
</head>
<body class="blocked">
<div class="header">
<h2>Powered By Fortinet</h2>
<h1>FortiGate Application Control</h1>
</div>
<div class="sidebar">
<h2 class="fgd_icon">blocked</h2>
</div>
<div class="main">
<h3>Application Blocked!</h3>
<div class="notice">You have attempted to use an application which is in violation of your internet usage policy.</div>
```

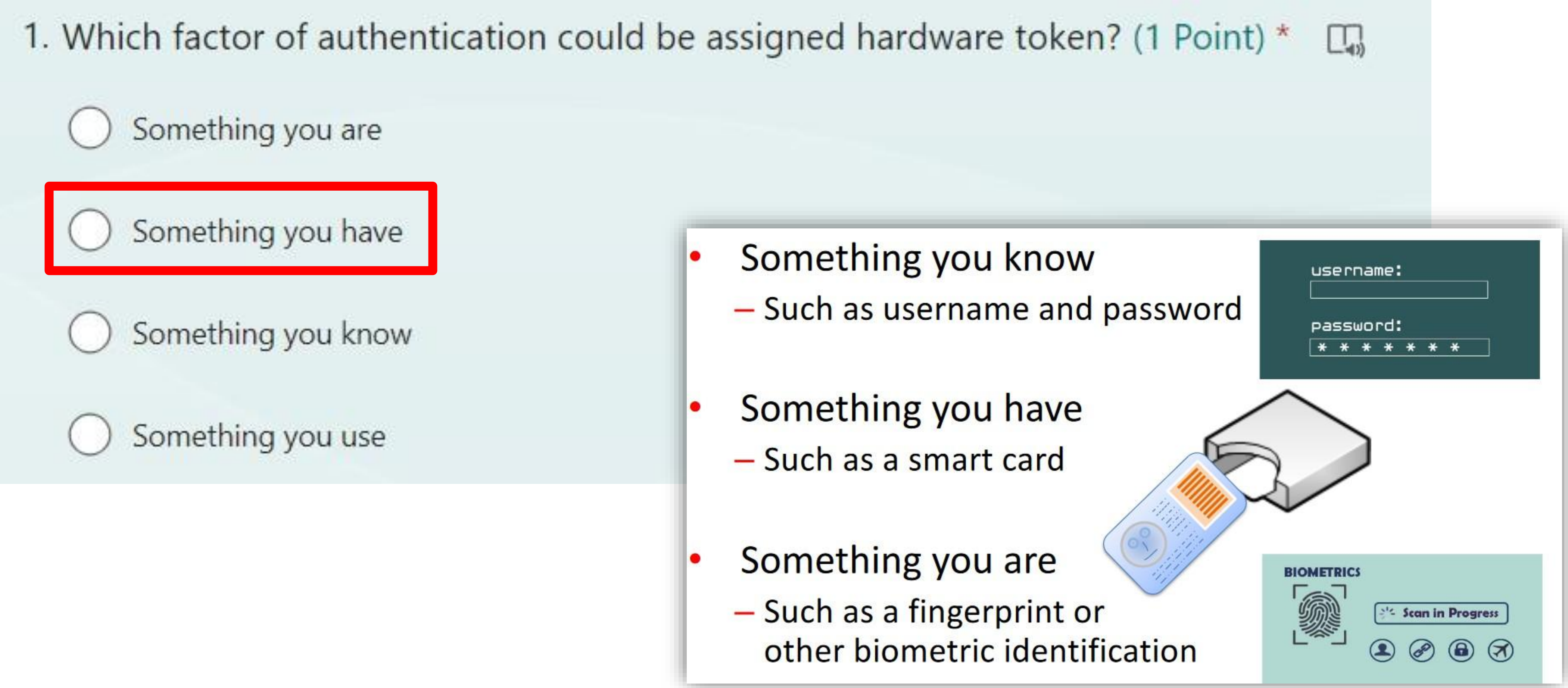
Quiz


Assignments

10 Questions
20 minutes

5+ correct – passed
<5 correct – not passed

Labs



1. Which factor of authentication could be assigned hardware token? (1 Point) *

○ Something you are

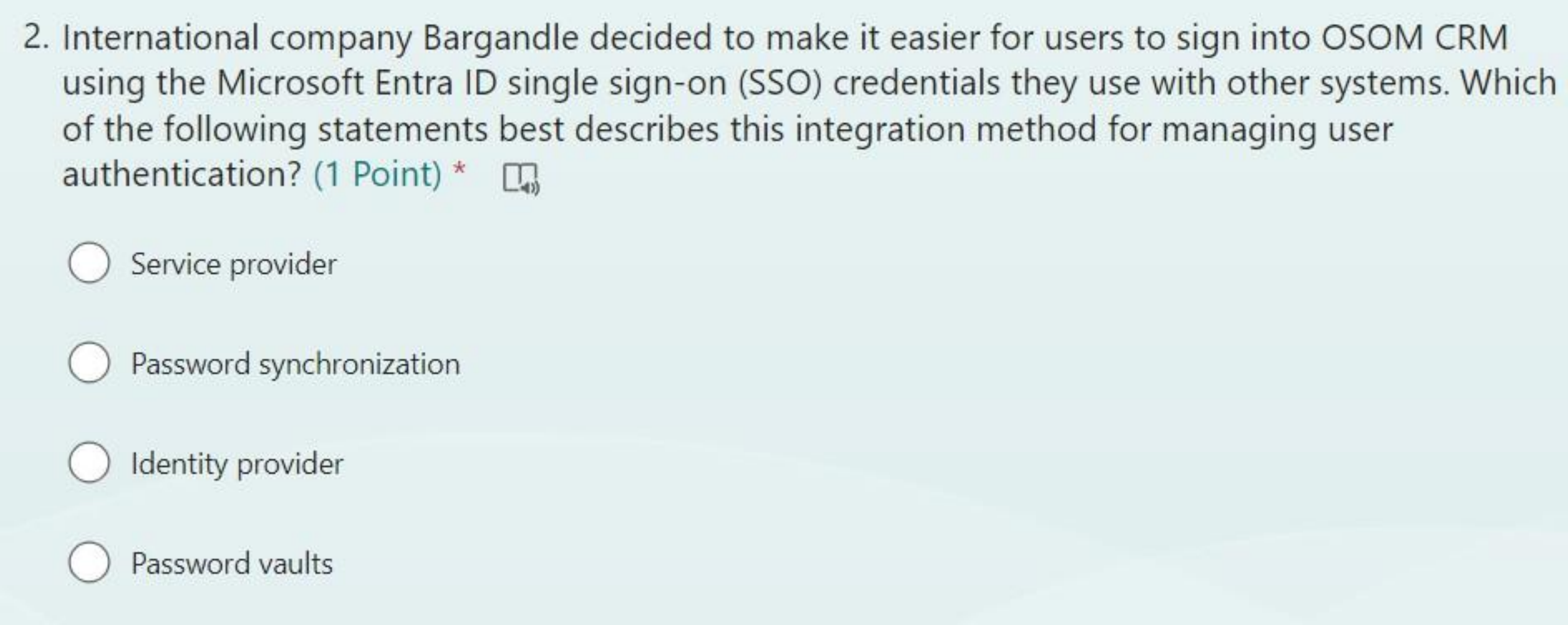
[✓ ○ Something you have]

○ Something you know

○ Something you use

- Something you know
  - Such as username and password
- Something you have
  - Such as a smart card
- Something you are
  - Such as a fingerprint or other biometric identification

Labs



2. International company Bargandle decided to make it easier for users to sign into OSOM CRM using the Microsoft Entra ID single sign-on (SSO) credentials they use with other systems. Which of the following statements best describes this integration method for managing user authentication? (1 Point) *

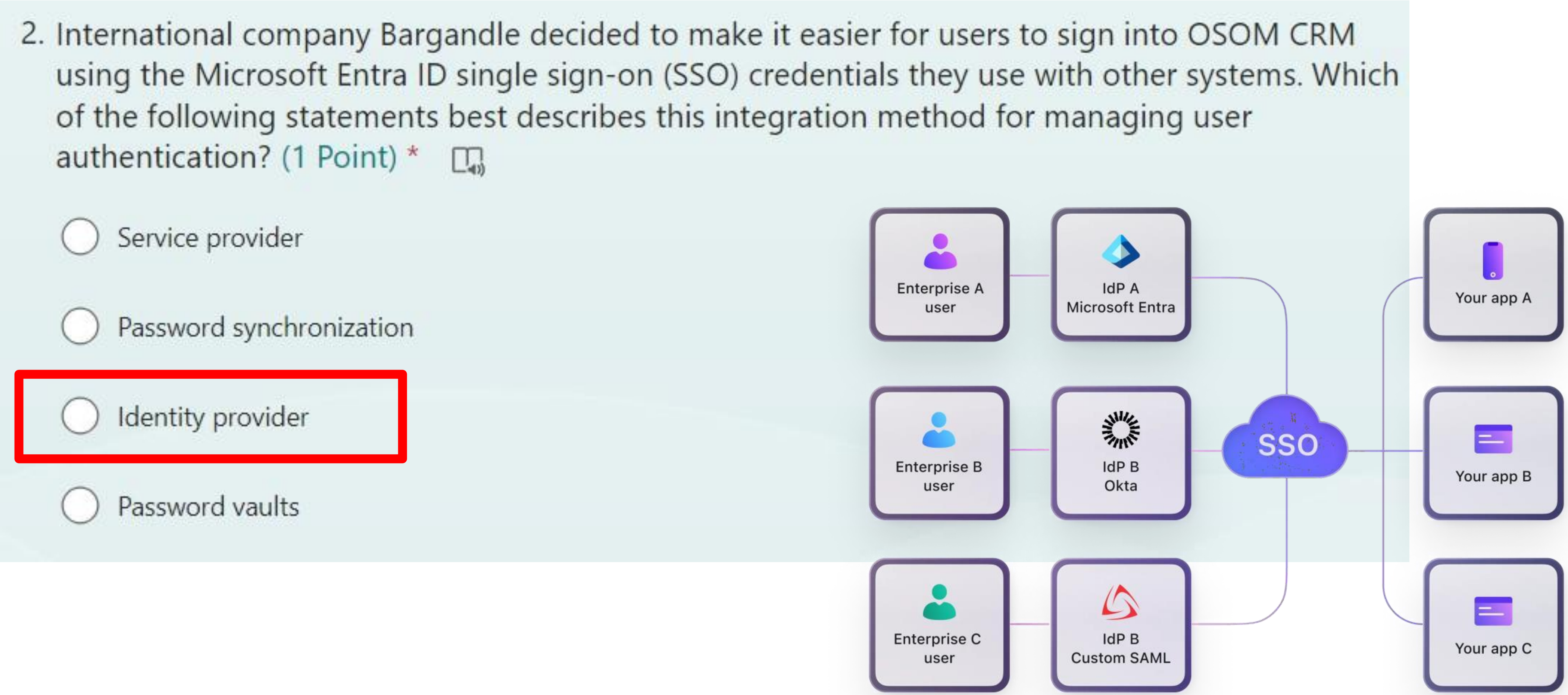
○ Service provider

○ Password synchronization

○ Identity provider

○ Password vaults

Labs



2. International company Bargandle decided to make it easier for users to sign into OSOM CRM using the Microsoft Entra ID single sign-on (SSO) credentials they use with other systems. Which of the following statements best describes this integration method for managing user authentication? (1 Point) *

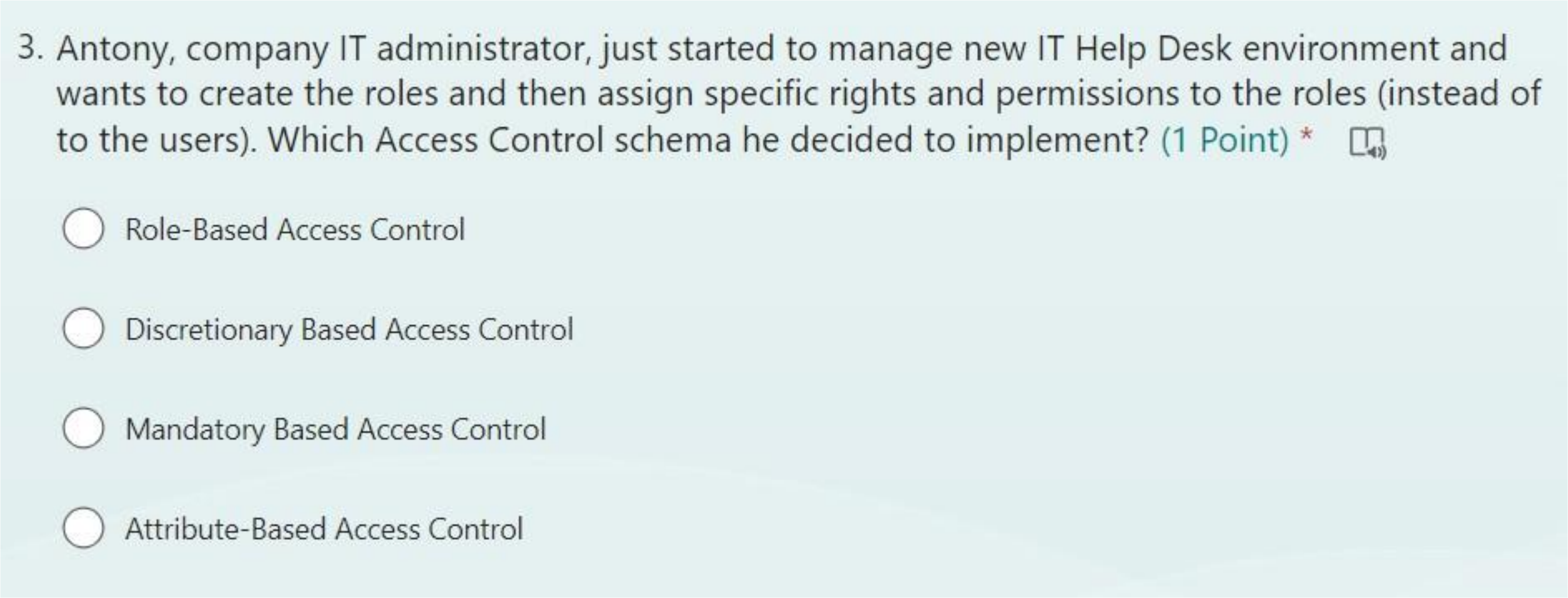
○ Service provider

○ Password synchronization

○ [✓ Identity provider]

○ Password vaults

Labs



3. Antony, company IT administrator, just started to manage new IT Help Desk environment and wants to create the roles and then assign specific rights and permissions to the roles (instead of to the users). Which Access Control schema he decided to implement? (1 Point) *

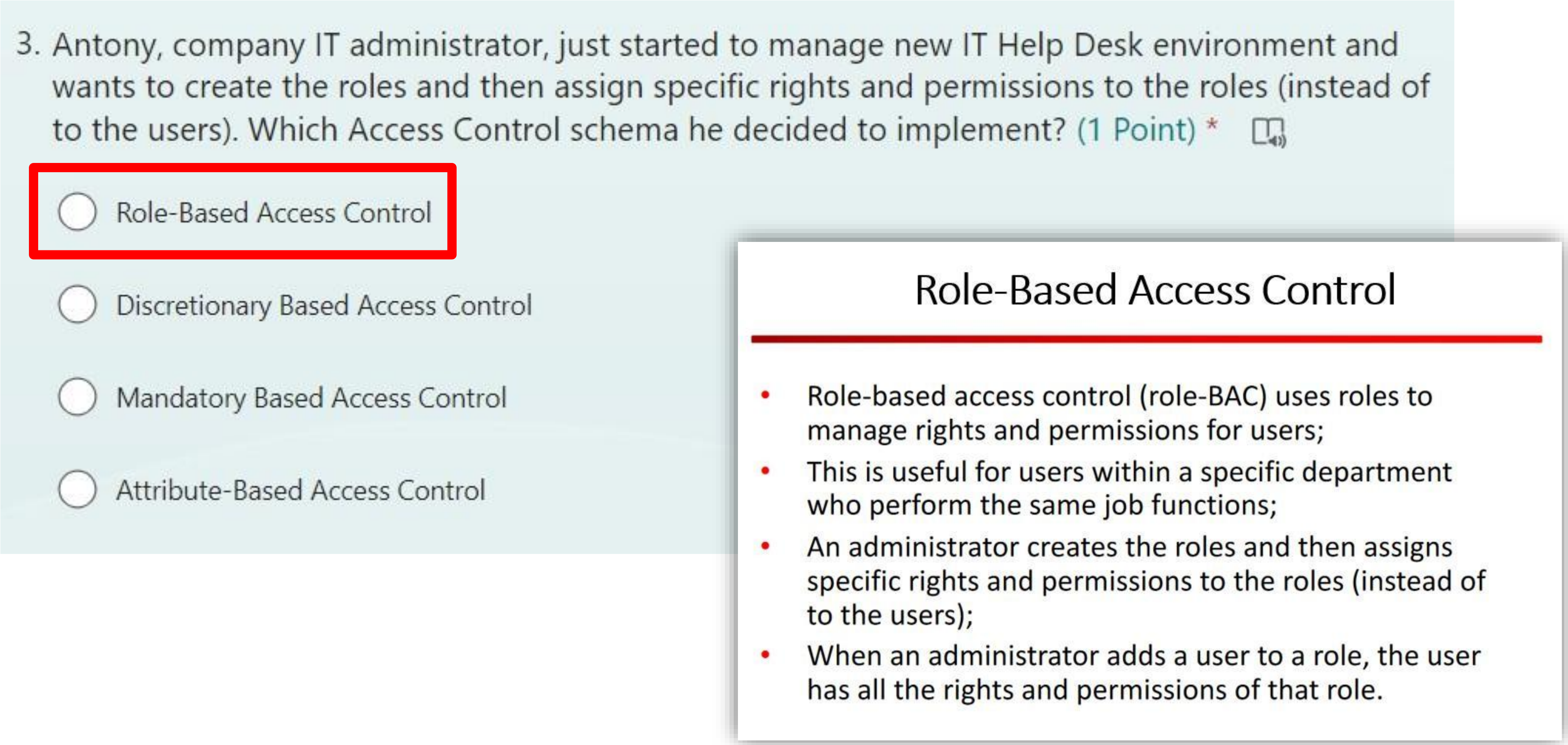
○ Role-Based Access Control

○ Discretionary Based Access Control

○ Mandatory Based Access Control

○ Attribute-Based Access Control

Labs



3. Antony, company IT administrator, just started to manage new IT Help Desk environment and wants to create the roles and then assign specific rights and permissions to the roles (instead of to the users). Which Access Control schema he decided to implement? (1 Point) *

[✓ ○ Role-Based Access Control]

○ Discretionary Based Access Control

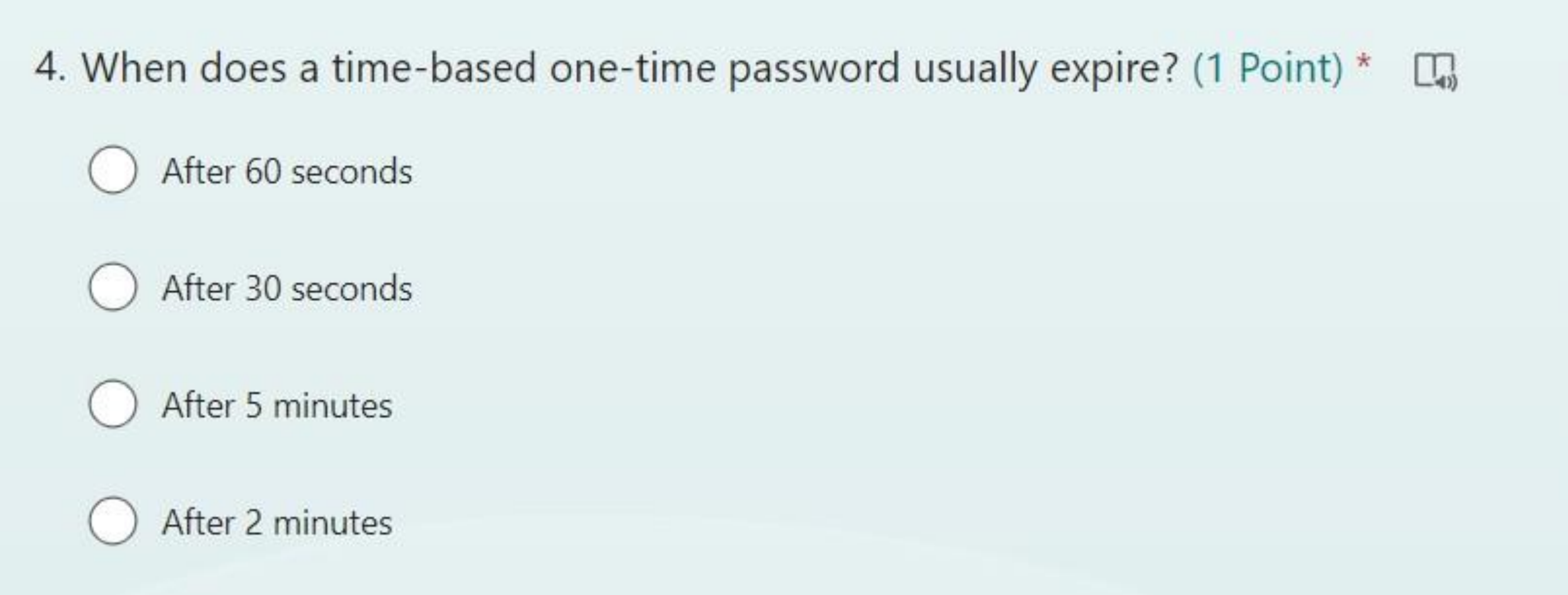
○ Mandatory Based Access Control

○ Attribute-Based Access Control

Role-Based Access Control

- Role-based access control (role-BAC) uses roles to manage rights and permissions for users;
- This is useful for users within a specific department who perform the same job functions;
- An administrator creates the roles and then assigns specific rights and permissions to the roles (instead of to the users);
- When an administrator adds a user to a role, the user has all the rights and permissions of that role.

Labs



4. When does a time-based one-time password usually expire? (1 Point) *

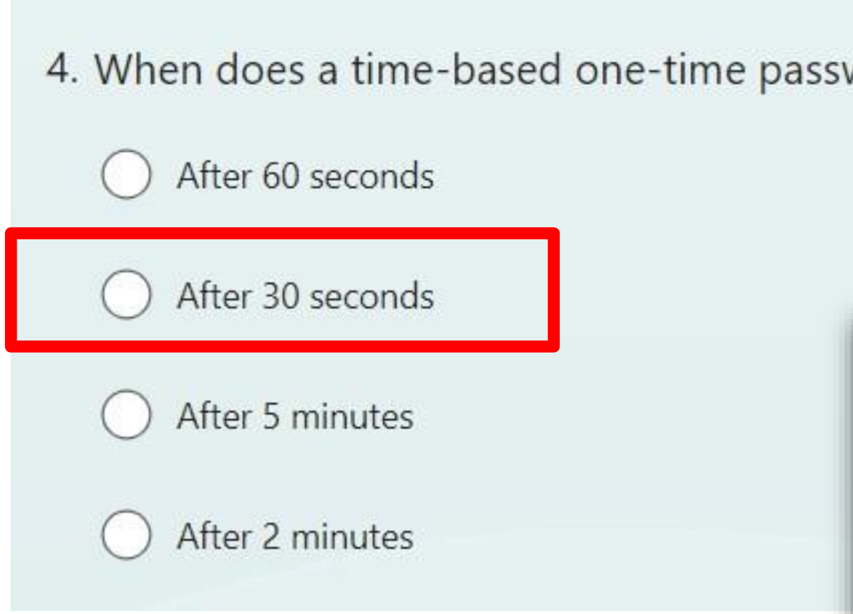
○ After 60 seconds

○ After 30 seconds

○ After 5 minutes

○ After 2 minutes

Labs



4. When does a time-based one-time password usually expire? (1 Point) *

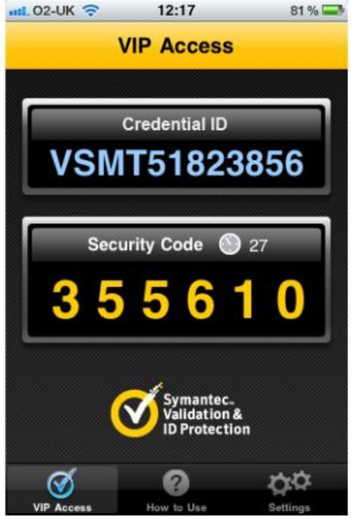
○ After 60 seconds

[✓ ○ After 30 seconds]

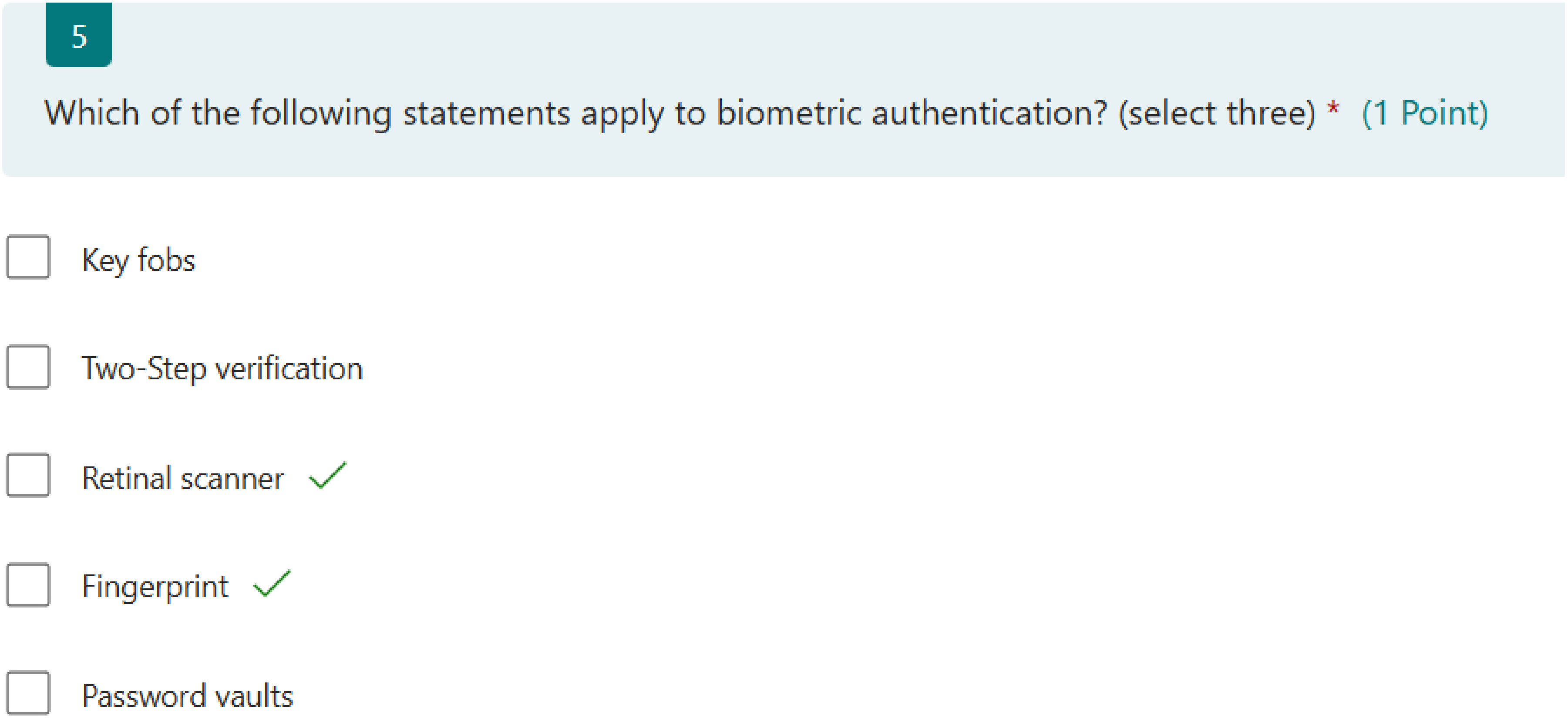
○ After 5 minutes

○ After 2 minutes

- HOTP and TOTP used in hardware tokens
- HOTP
  - HMAC-based One-Time Password
- TOTP
  - Time-based One-Time Password
  - Expire after 30 seconds



Labs



5

Which of the following statements apply to biometric authentication? (select three) * (1 Point)

□ Key fobs

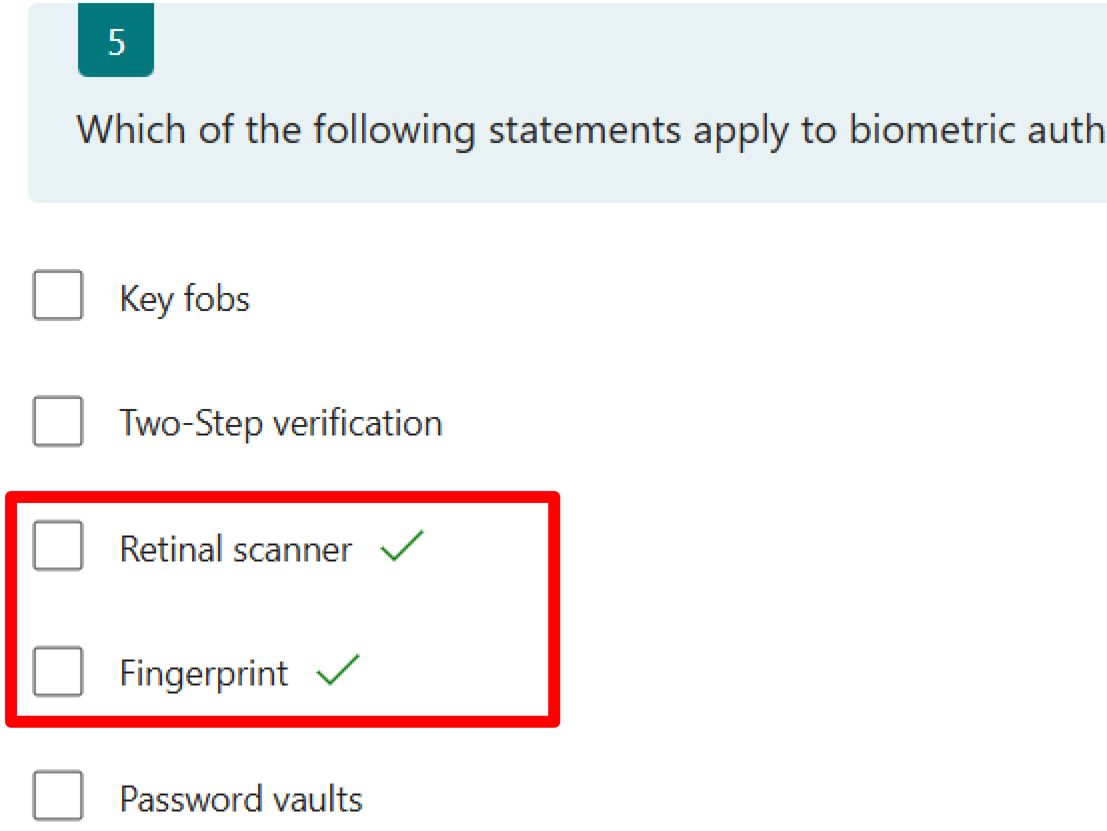
□ Two-Step verification

□ Retinal scanner ✓

□ Fingerprint ✓

□ Password vaults

Labs



5

Which of the following statements apply to biometric authentication? (select three) * (1 Point)

□ Key fobs

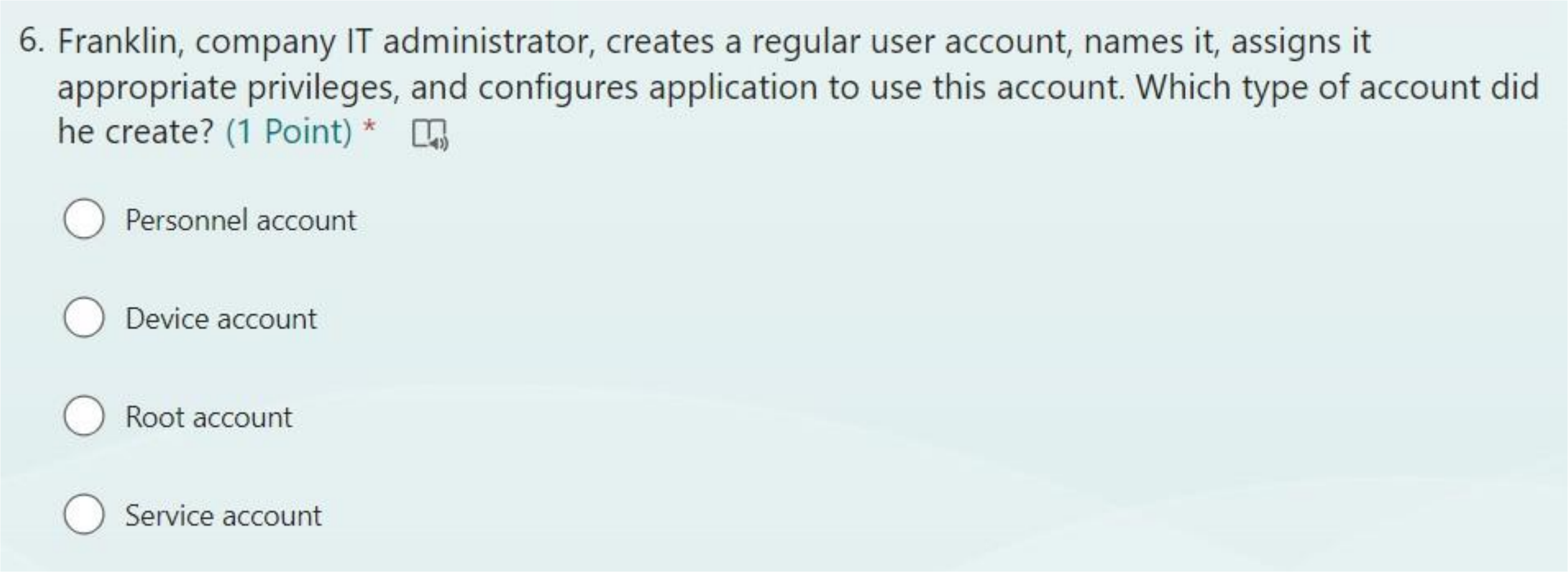
□ Two-Step verification

□ Retinal scanner ✓

□ Fingerprint ✓

□ Password vaults

Labs



6. Franklin, company IT administrator, creates a regular user account, names it, assigns it appropriate privileges, and configures application to use this account. Which type of account did he create? (1 Point) *

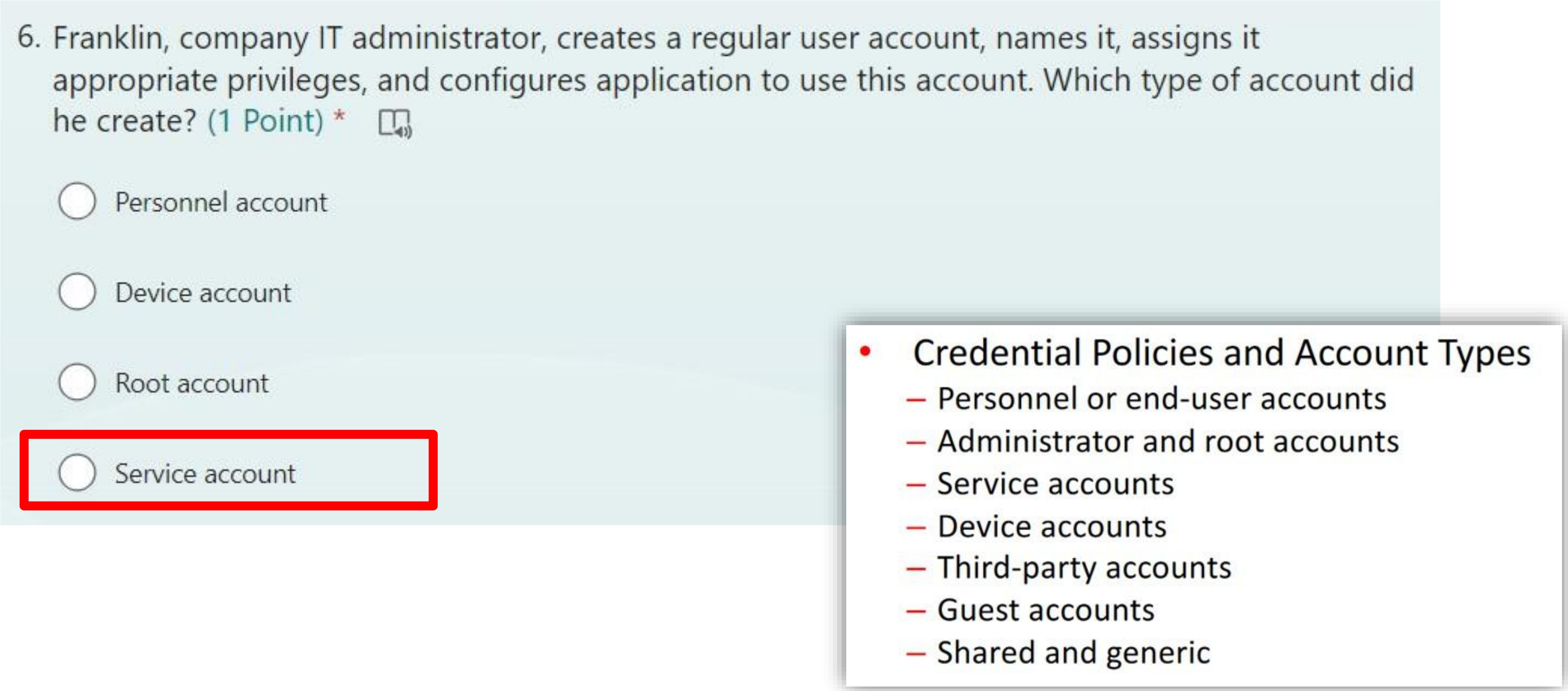
○ Personnel account

○ Device account

○ Root account

○ Service account

Labs



6. Franklin, company IT administrator, creates a regular user account, names it, assigns it appropriate privileges, and configures application to use this account. Which type of account did he create? (1 Point) *

○ Personnel account

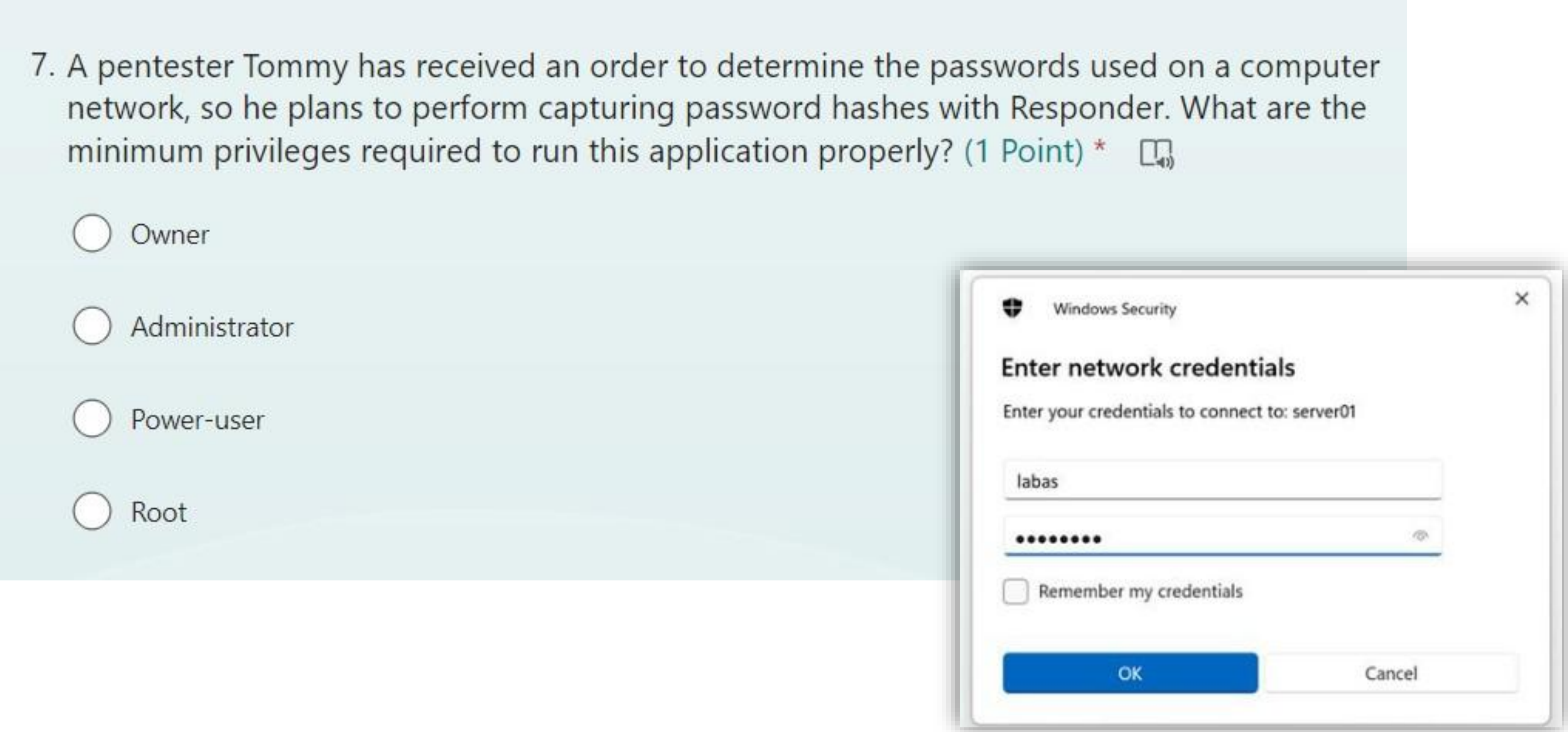
○ Device account

○ Root account

○ [✓ Service account]

- Credential Policies and Account Types
  - Personnel or end-user accounts
  - Administrator and root accounts
  - Service accounts
  - Device accounts
  - Third-party accounts
  - Guest accounts
  - Shared and generic

Labs



7. A pentester Tommy has received an order to determine the passwords used on a computer network, so he plans to perform capturing password hashes with Responder. What are the minimum privileges required to run this application properly? (1 Point) *

○ Owner

○ Administrator

○ Power-user

○ Root

Windows Security

Enter network credentials

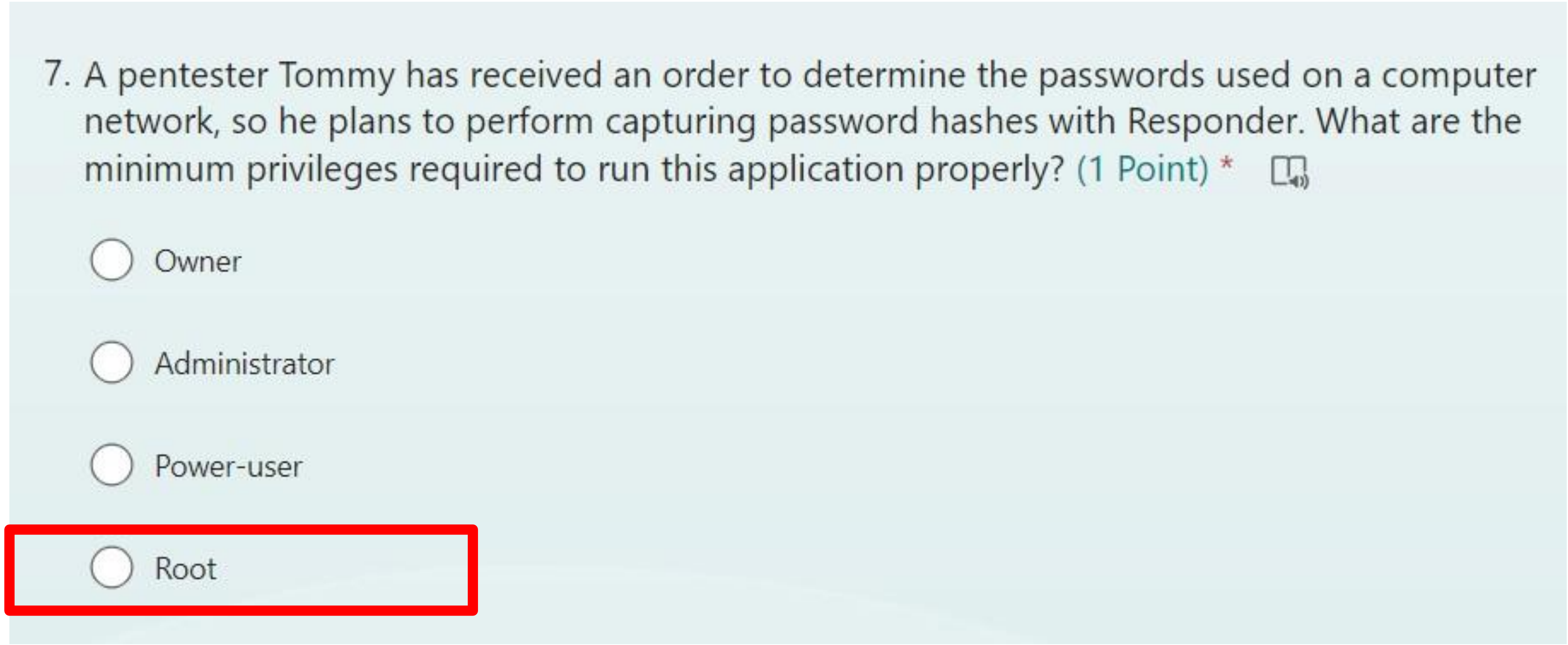
Enter your credentials to connect to: server01

labas

••••••••

□ Remember my credentials

Labs



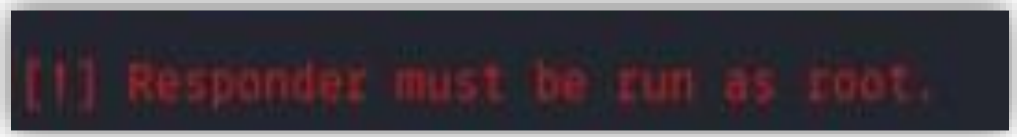
7. A pentester Tommy has received an order to determine the passwords used on a computer network, so he plans to perform capturing password hashes with Responder. What are the minimum privileges required to run this application properly? (1 Point) *

○ Owner

○ Administrator

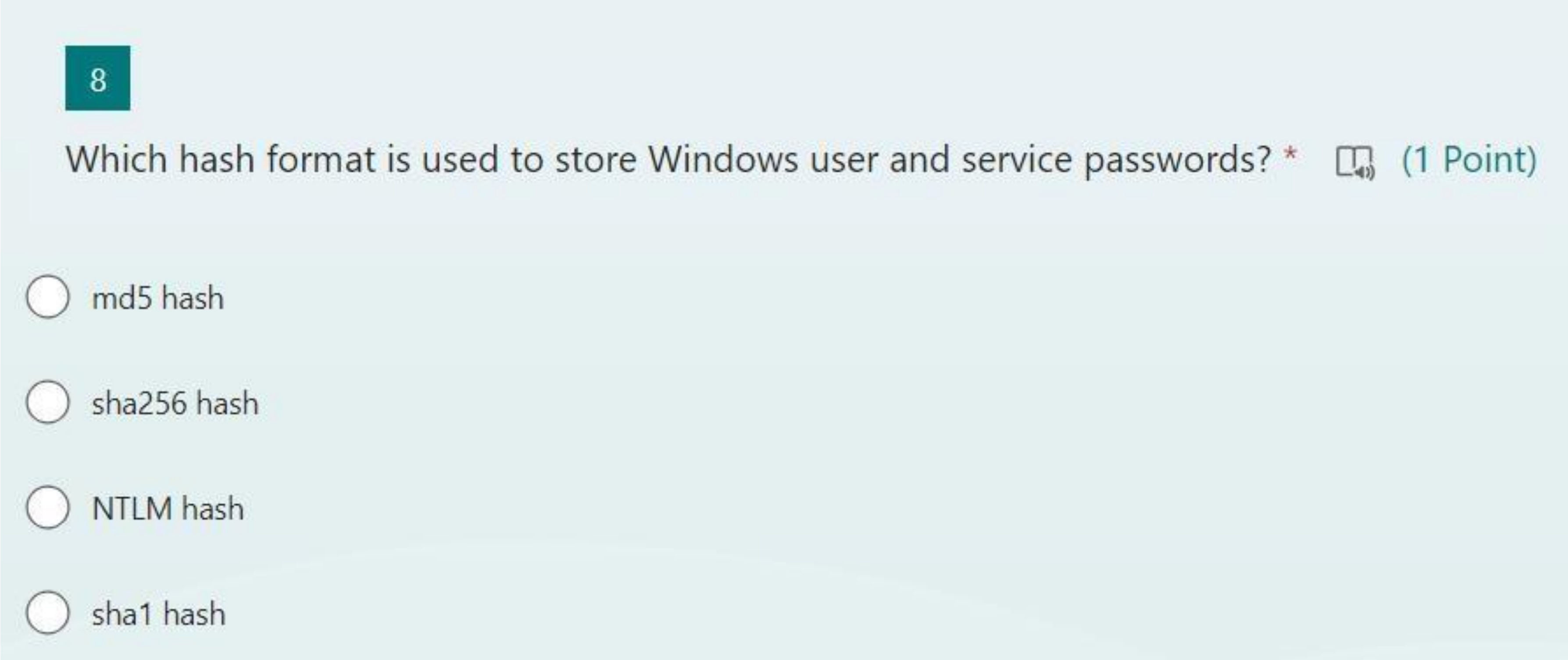
○ Power-user

[✓ ○ Root]



```
[!] Responder must be run as root.
```

Labs



8

Which hash format is used to store Windows user and service passwords? * (1 Point)

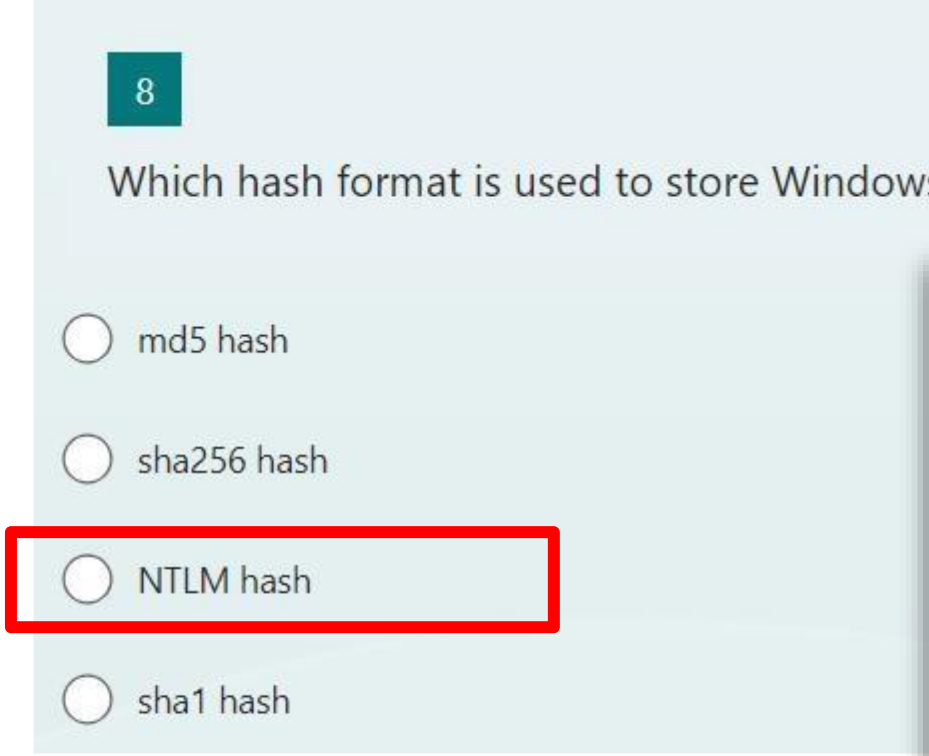
○ md5 hash

○ sha256 hash

○ NTLM hash

○ sha1 hash

Labs



8

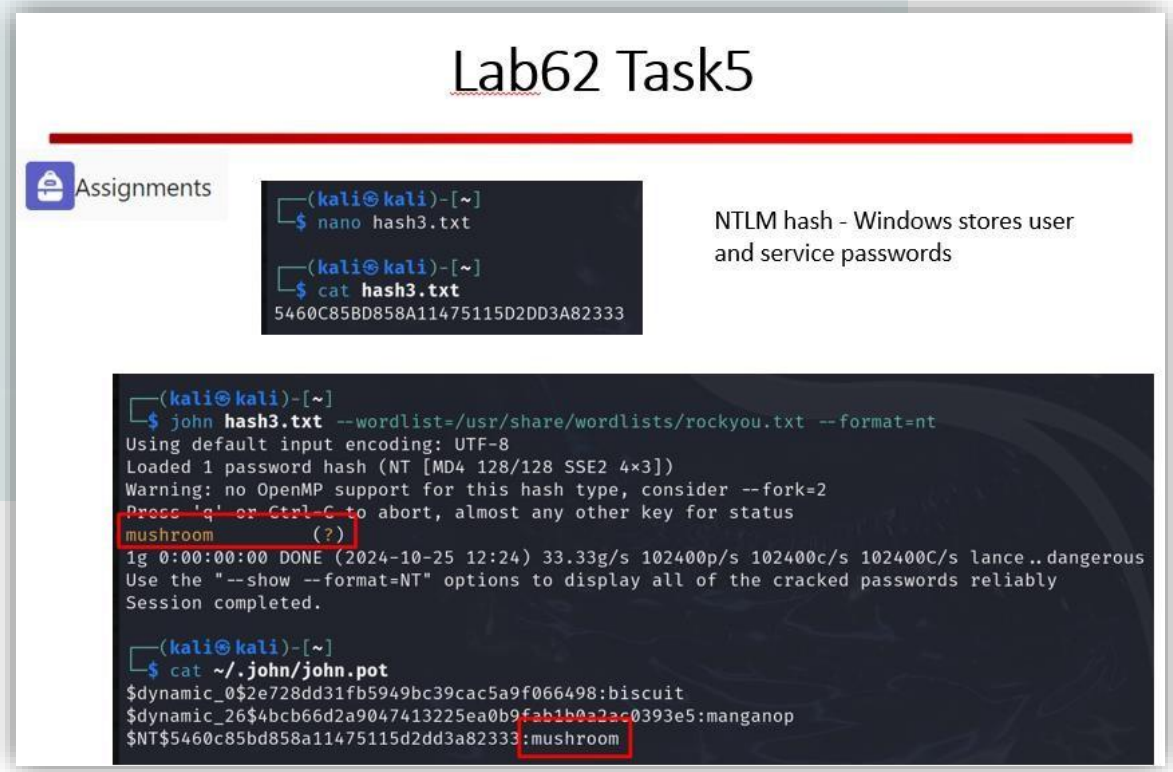
Which hash format is used to store Windows user and service passwords? * (1 Point)

○ md5 hash

○ sha256 hash

○ NTLM hash

○ sha1 hash



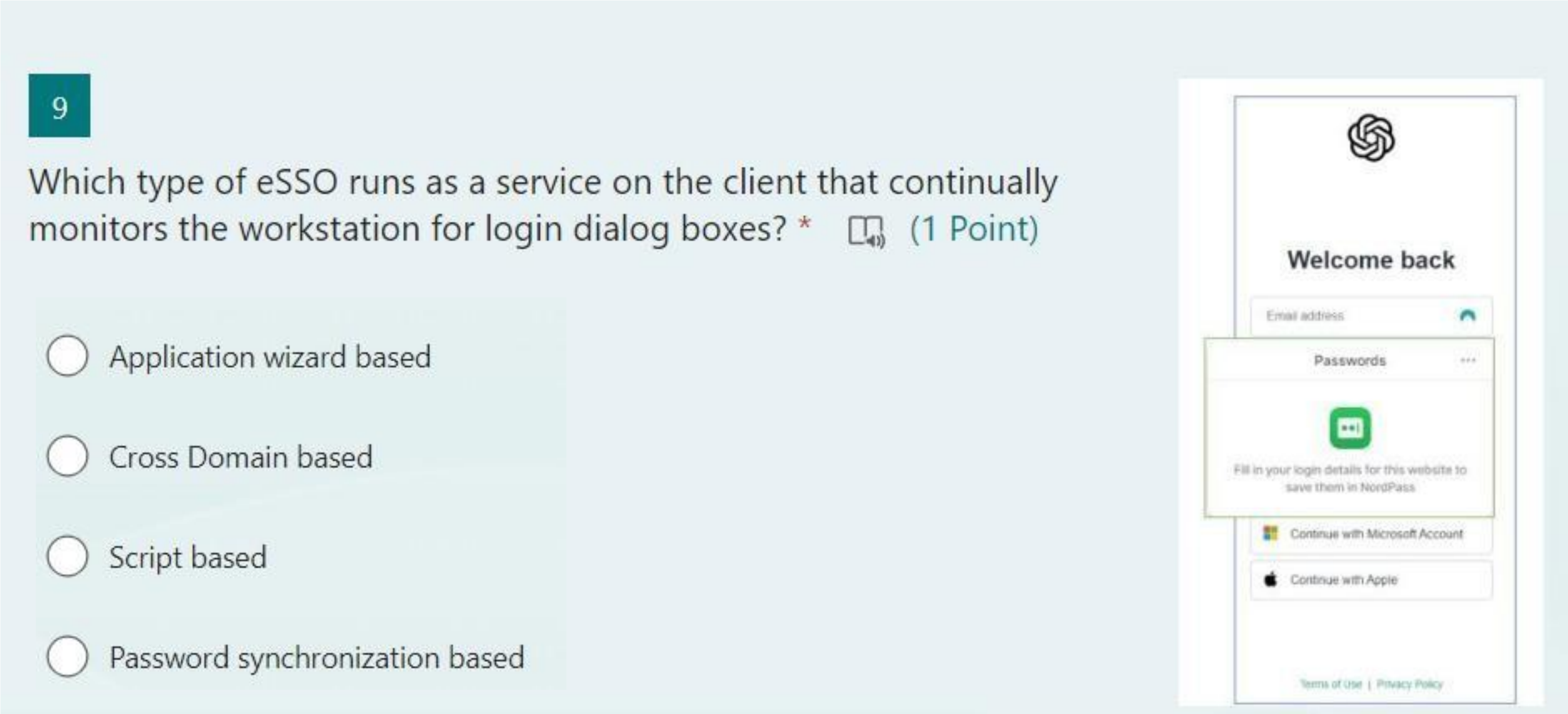
Lab62 Task5

```
┌──(kali㉿kali)-[~]
└─$ nano hash3.txt

┌──(kali㉿kali)-[~]
└─$ cat hash3.txt
5460C85BD858A11475115D2DD3A82333
```

NTLM hash - Windows stores user and service passwords

```
┌──(kali㉿kali)-[~]
└─$ john hash3.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=nt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
mushroom         (?)
1g 0:00:00:00 DONE (2024-10-25 12:24) 33.33g/s 102400p/s 102400c/s 102400C/s lance..dangerous
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ cat ~/.john/john.pot
$dynamic_0$2e728dd31fb5949bc39cac5a9f066498:biscuit
$dynamic_26$4bcb66d2a9047413225ea0b9fab1b0a2ac0393e5:manganop
$NT$5460c85bd858a11475115d2dd3a82333:mushroom
```

Labs



9

Which type of eSSO runs as a service on the client that continually monitors the workstation for login dialog boxes? * (1 Point)

○ Application wizard based

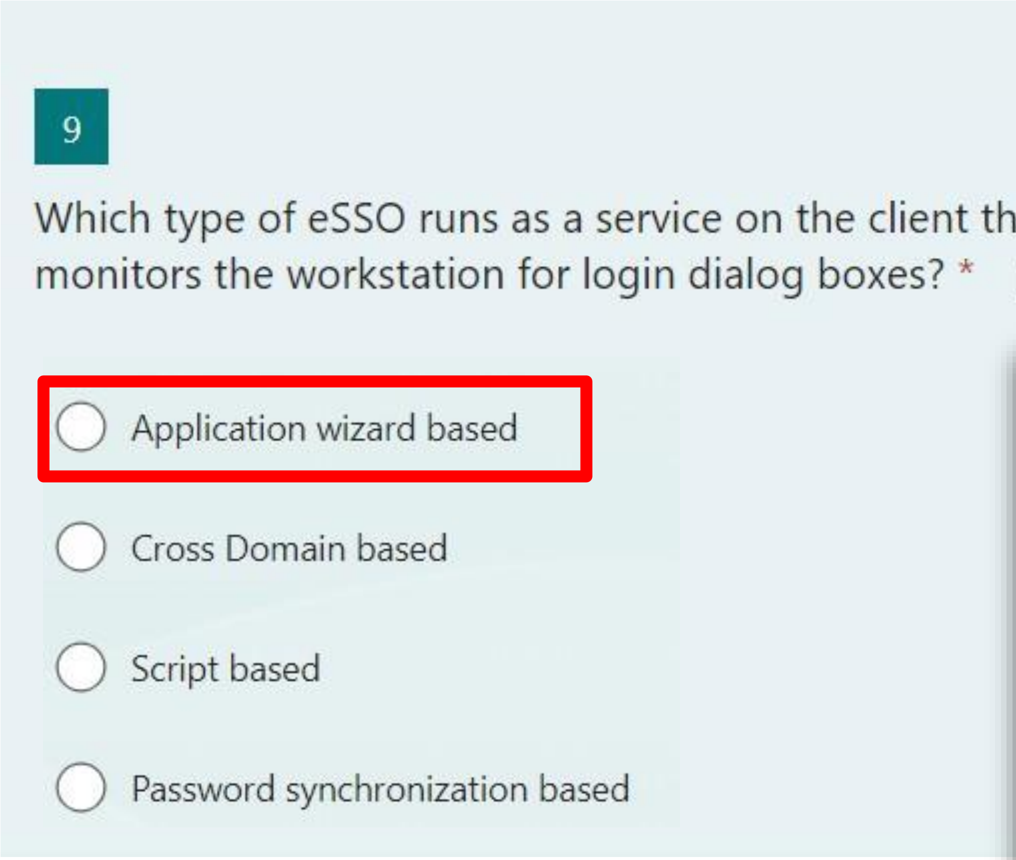
○ Cross Domain based

○ Script based

○ Password synchronization based

Welcome back
Email address
Passwords
Fill in your login details for this website to save them in NordPass
Continue with Microsoft Account
Continue with Apple
Terms of Use | Privacy Policy

Labs



9

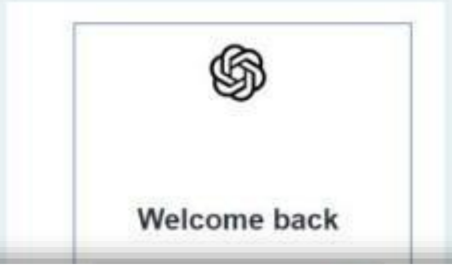
Which type of eSSO runs as a service on the client that continually monitors the workstation for login dialog boxes? * (1 Point)

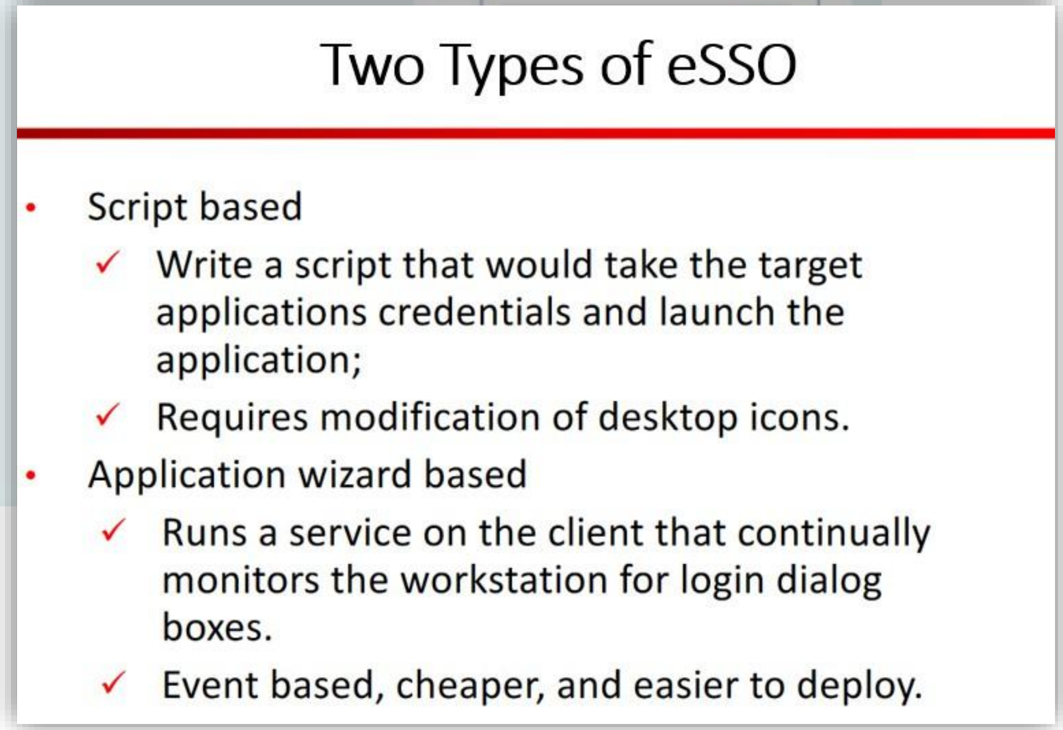
[✓ ○ Application wizard based]

○ Cross Domain based

○ Script based

○ Password synchronization based

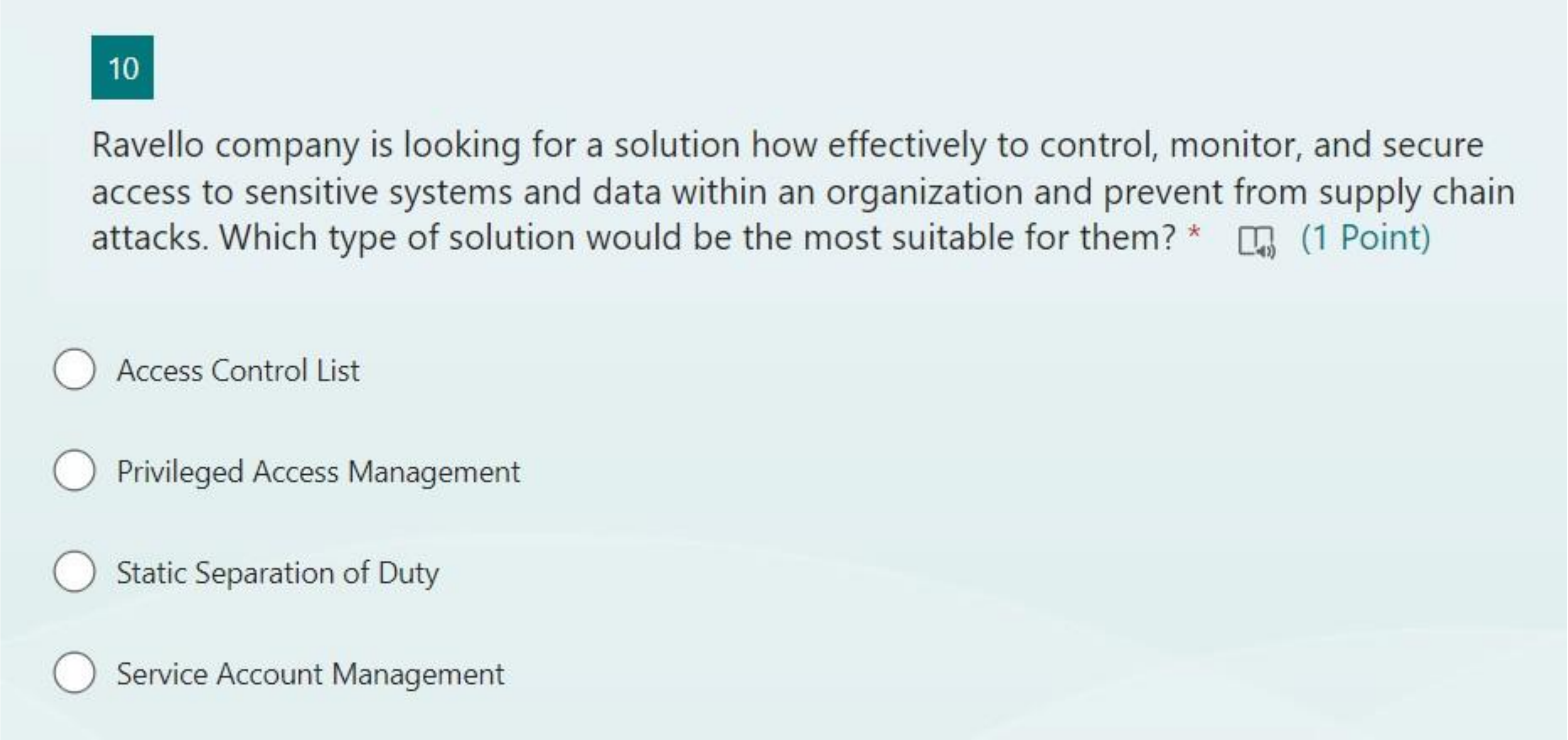




Two Types of eSSO

- Script based
  - ✓ Write a script that would take the target applications credentials and launch the application;
  - ✓ Requires modification of desktop icons.
- Application wizard based
  - ✓ Runs a service on the client that continually monitors the workstation for login dialog boxes.
  - ✓ Event based, cheaper, and easier to deploy.

Labs



10

Ravello company is looking for a solution how effectively to control, monitor, and secure access to sensitive systems and data within an organization and prevent from supply chain attacks. Which type of solution would be the most suitable for them? * (1 Point)

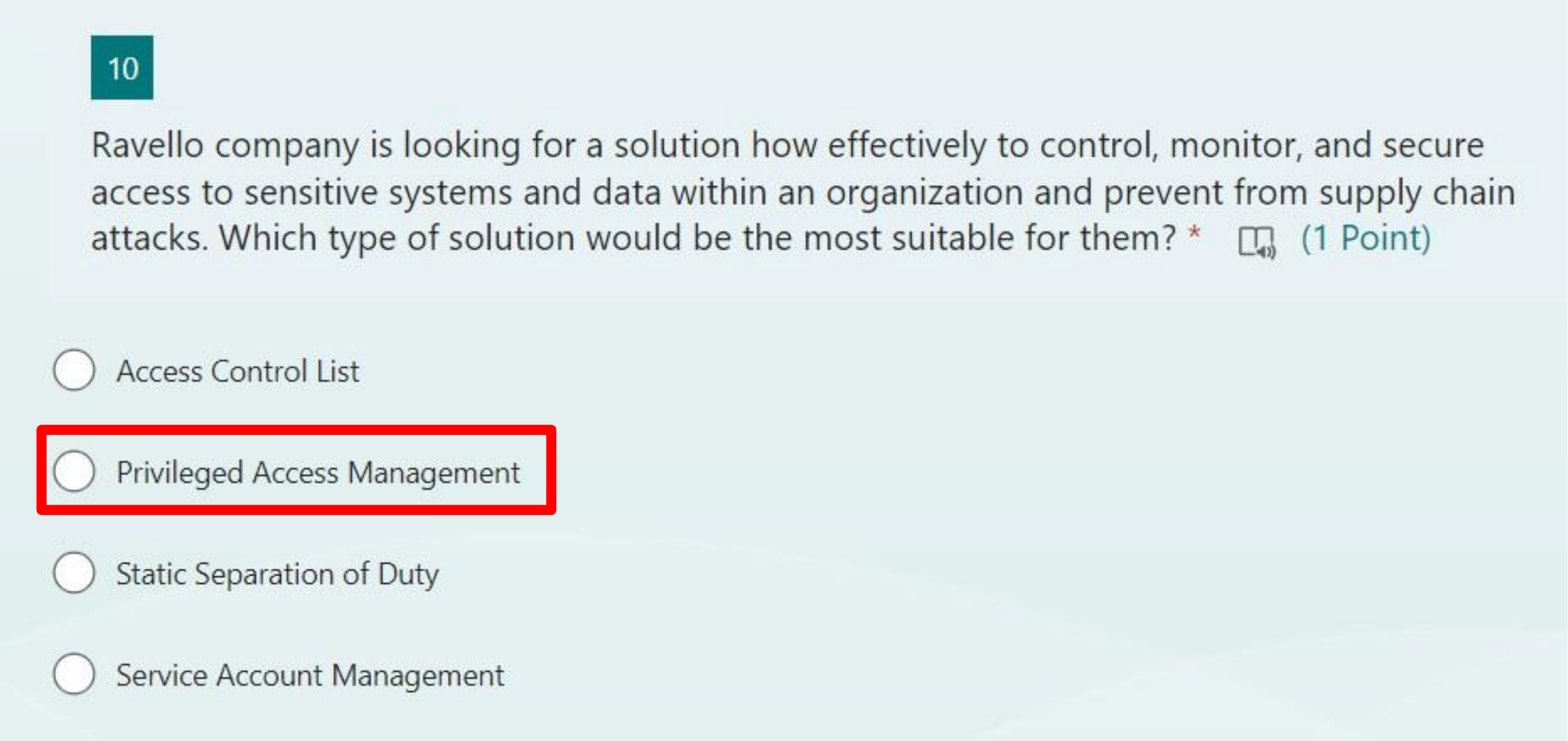
○ Access Control List

○ Privileged Access Management

○ Static Separation of Duty

○ Service Account Management

Labs



10

Ravello company is looking for a solution how effectively to control, monitor, and secure access to sensitive systems and data within an organization and prevent from supply chain attacks. Which type of solution would be the most suitable for them? * (1 Point)

○ Access Control List

[✓ ○ Privileged Access Management]

○ Static Separation of Duty

○ Service Account Management