NOOR MEISTER 2026

Küberkaitse kutsemeistrivõistlus

TEINE VÕISTLUSPÄEV

1. ÜLDINFO

1.1. Formaat

Teise päeva võistlus koosneb kahest osast:
1) Praktiline IT-taristu turvamine ning turvaintsidendi analüüs
2) Teoreetiline valikvastustega test

Võistlustööks on aega 6 tundi.

1.2. Punktiarvestus

Teisel võistluspäeval on võimalik teenida kuni 75 punkti (s.o 75% kogupunktidest):
1) Praktilises osas tuleb 28 ülesannet, millede punktiväärtus on kokku 65
2) Teoreetilises osas tuleb 20 küsimust punktiväärtusega 0.5 / tk

NB! Võistluspäeva lõppedes peab virtuaalmasinad jätma tööle. Hindamine viiakse läbi sellises seisus masinates, nagu nad on tööle jäetud. Taaskäivitusi või sisselülitamisi ei tehta.

1.3. Tehniline tugi

Võistluse ajal osutatakse võistlejatele tehnilist tuge (nt olukordadeks kus võistleja virtuaalmasin või võistlusega seotud infrastuktuur on maas/tõrgub, vms).

Tehnilise toe pöördumiste esitamise ja menetlemise kord on järgnev:
1. Võistkond kirjutab probleemi kirjelduse paberile ja tõstab käe.
2. Kohtunik tuleb kohale ja võtab pöördumise (paberi) vastu.
3. Kohtunikud tegelevad probleemiga ja koostavad vastuse/lahenduse.
4. Kohtunik tuleb kohale ja edastab võistkonnale vastuse/lahenduse suuliselt **või** edastakse teade kõigile võistkonadele (kas iga laua juures eraldi või üle saali hõigates)

Kui probleem põhjustab ühele või mitmele võistkonnale ebaausa seisu (nt kaotati võistlusaega), siis kohtunikud hindavad mõju ja püüavad leida võimalikult õiglase lahenduse.

2. VÕISTLUSREEGLID

Teise võistluspäeva reeglid:

1. Keelatud on interneti (sh tehisintellekti) kasutamine.
2. Keelatud on igasugune koostöö, lahenduste ja vastuste jagamine, või ülesannete arutamine võõrastega (sh teiste võistkondadega või sõpradega internetis).
3. Lubatud on kasutada ainult teie võistkonnale kuuluvaid virtuaalmasinaid.
4. Keelatud on DoS, hävitavad tegevused, *brute-force* ründed, võistkonna ulatusest väljapoole jäävate masinate skannimine ja/või masinate halvendav tegevus.

Reeglite rikkumisel on kohtunikel õigus:

- Esimesel rikkumisel teha võistkonnale hoiatus või trahv kuni 15 punkti
- Korduval rikkumisel teha võistkonnale trahv kuni 75 punkti

3. VÕISTLUSKESKKOND JA LIGIPÄÄS

Võistlus leiab aset virtuaalkeskkonnas Proxmox VE, kus igale võistkonnale on eraldatud võistlustööks vajalik ressurss ja on ette valmistatud võistlusülesandega seotud IT-infrastruktuur, sealhulgas arvutivõrgud, server- ja tööarvutid, rakendused ja nende seaded.

Virtuaalkeskkond asub aadressil: https://prox.edu.voco.ee

Virtuaalkeskkonna kasutajatunnused jagatakse võistluspäeva hommikul.

Virtuaalmasinates on administratiivne konto:

- **Kasutajanimi:** meister
- **Parool:** Passw0rd!

4. VÕISTLUSÜLESANNE (PRAKTILINE OSA)

4.1. Üldine

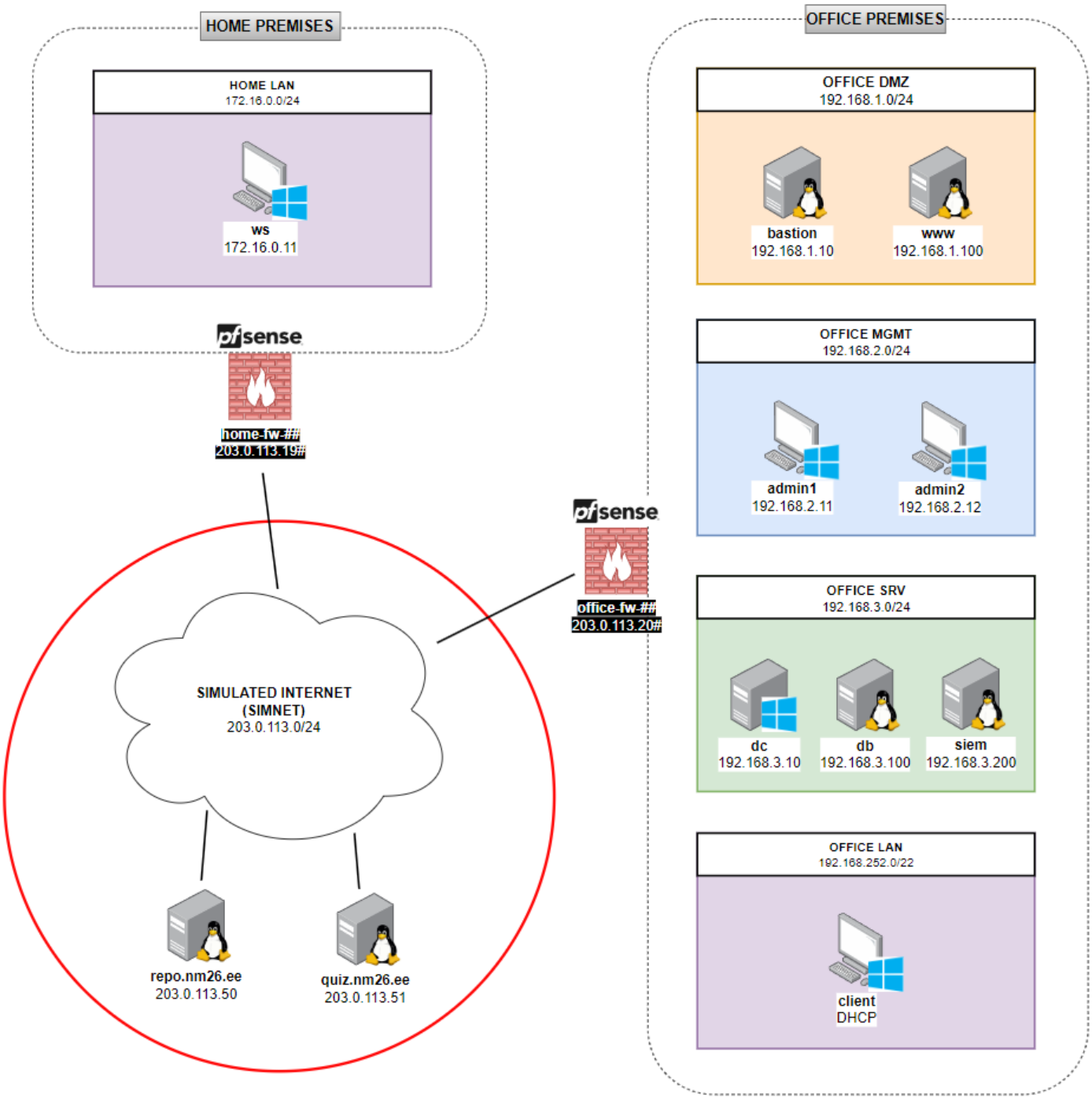
Teid kahte on palgatud tööle IT- ja tubeinseneridena reklaamiettevõttesse „Nova Media 26“. Juba esimesel tööpäeval saate te aru, et ettevõtte IT-s on täielik korralagedus ja häkkerid on suutnud ettevõtte süsteemidesse sisse häkkida ja kodulehe maha võtta. Teie ülesanne on taastada kord, viia ellu võimalikult palju turvaparendusi, ning analüüsida turvaintsidenti.

Võistlustööd sooritades peab läbivalt järgima järgnevaid nõudeid:

- Osades virtuaalmasinates on kasutajakontod nimega **kohtunik** ja/või **scorer**. Nende kasutajakontode seisundi või parameetrite muutmine on keelatud.

- Kui pole öeldud teisiti, siis kasutada parooli: **Passw0rd!**
- Masinate nimedes ja domeeninimedes ning IP-aadressites märgitud **#** tähistab unikaalset võistkonna numbrit, mis loositakse võistluspäeval kohapeal.

4.2. Võrgujoonis



NB! Võistkond töötab ainult masinatega, mis jäävad punasest ringist väljapoole

4.3. Konfiguratsioon

RUUTERID

Asukoht	Nimi	Liides	IP-aadress	Võrk
Office	**office-fw** (pfSense 2.8.1)	Port 1	203.0.113.20#	SIMNET
		Port 2	192.168.1.1	Office DMZ
		Port 3	192.168.2.1	Office MGMT
		Port 4	192.168.3.1	Office SRV
		Port 5	192.168.252.1	Office LAN
Home	**home-fw** (pfSense 2.8.1)	Port 1	203.0.113.19#	SIMNET
		Port 2	172.16.0.1	Home LAN

SERVERID/TÖÖJAAMAD

Asukoht	Nimi	OS	Võrk	Teenused
Office	**dmz-bastion**	Ubuntu 24.04	Office DMZ	OpenSSH server (kodukontori IT-administraatori ligipääsupunkt ettevõtte sisevõrku)
	dmz-www	Ubuntu 24.04	Office DMZ	Apache2 veebiserver, custom PHP veebirakendus
	mgmt-admin1	Windows 11	Office MGMT	Võistkonna tööjaam 1
	mgmt-admin2	Windows 11	Office MGMT	Võistkonna tööjaam 2
	srv-dc	Windows Server 2025	Office SRV	AD, DNS, DHCP
	srv-db	Ubuntu 24.04	Office SRV	MariaDB (custom PHP veebirakenduse andmebaas)
	srv-siem	Ubuntu 24.04	Office SRV	Wazuh SIEM/XDR
	lan-client	Windows 11	Office LAN	Ettevõtte töötaja 1
Home	**home-ws**	Windows 11	Home LAN	Kodukontori IT-administraator

KESKSED TEENUSED

Asukoht	Nimi	IP-aadress	Teenused
SIMNET	**repo.nm26.ee**	203.0.113.50	APT repositoorium, tarkvarahoidla
SIMNET	**quiz.nm26.ee**	203.0.113.51	Teooriatest

4.4. Ülesanne

Ülesanne 2.1.1 (5p) Asukoht: srv-siem (Wazuh)

Ettevõtte **dmz-bastion** serverisse on sisse tungitud ning sellele järgnenud pahatahtlik tegevus. Õnneks on Wazuhis talletatud antud intsidendiga seotud logid. Teie ülesanne on logida sisse Wazuhi ning otsida välja ja uurida antud logisid. Nende põhjal tuleb koostada kirjalik raport, mis vastab küsimustele:

1. Mis oli intsidendi ajavahemik?
2. Mis oli ründaja IP-aadress (või IP-aadressid)?
3. Millise teenuse kaudu saadi ligipääs ning millist kasutajakontot kasutati?
4. Milliseid pahatahtlikke tegevusi tehti pärast ligipääsu saamist?
5. Mida ründaja nende tegevustega saavutada või ette valmistada üritas?
6. Mida tuleb teha, et taastada süsteemi turvalisus pärast antud intsidenti?

Raport tuleb jätta **mgmt-admin1** töölauale nimega „Incident Report – Bastion“.

NB! Raport võib olla kirjutatud nii eesti kui inglise keeles.

Ülesanne 2.1.2 (0.5p) Asukoht: srv-siem (Wazuh)

Ettevõtte **dmz-bastion** serveri vastu on toime pandud rünnak ning Wazuhis on olemas antud intsidendiga seotud logid (vt ülesanne 2.1.1). Teie ülesanne on luua Wazuh keskkonnas nende logide põhjal tulpdiagramm (bar chart), mis näitab SSH autentimiskatsete arvu ajas.

Valmis visualiseering tuleb salvestada nimega „Bastion SSH Auths”.

Ülesanne 2.1.3 (3p) Asukoht: srv-siem (Wazuh) + office-fw

Seadista **office-fw** logide edastamine **srv-siem** serverisse rsyslogd abil, ning sealt Wazuhi.

Tulemus loetakse korrektseks, kui Wazuhis on loodud eraldi vaade (Discovery → Save) nimega „Office FW Logs“, ja selles vaates on näha reaalseid **office-fw** logisid.

Ülesanne 2.2.1 (2p) Asukoht: dmz-www + srv-db

Ettevõtte koduleht on häkitud ja seal vandaalitsetud. Õnneks on teie töölaual veebirakenduse ja andmebaasi varukoopia. Teie ülesanne on taastada ettevõtte koduleht, taastades veebirakenduse failid serverisse **dmz-www**, ning andmebaas serverisse **srv-db**.

Tulemus loetakse korrektseks, kui koduleht on kättesaadav ja sinna saab sisse logida.

Ülesanne 2.2.2 (5p) Asukoht: dmz-www

Analüüsi ettevõtte kodulehe (PHP rakenduse) lähtekoodi, tuvasta seal ründega seotud turvanõrkus, ning paranda see. Koosta kirjalik raport, mis sisaldab vähemalt järgnevat:

1. Faili nimi ja koodilõik/funktsioon, kus turvanõrkus esineb?
2. Mis viga on ja kuidas seda saab ära kasutada (lühidalt)?
3. Kuidas viga parandada (kirjeldus + parandatud kood)?
4. Kuidas veendusite, et rakendus pärast parandust töötab?

Raport tuleb jätta **mgmt-admin1** töölauale nimega „Security Report – Web App“.

NB! Raport võib olla nii eesti kui inglise keeles.

NB! Veenduge, et te ei tee kodulehte katki!

Ülesanne 2.2.3 (3p) Asukoht: dmz-www

Paigalda serverisse Apache2 ModSecurity ning seadista see blokeerima HTTP päringud, mis sisaldavad stringi „..“ (ilma jututmärkideta) ehk potentsiaalset *path traversal* rünnakut.

Ülesanne 2.2.4 (1p) Asukoht: dmz-www

Genereeri TLS privaatvõti (ilma paroolita) ja TLS sertifikaat etteantud parameetrite alusel:

Privaatvõtme tüüp: EC
Privaatvõtme asukoht: /etc/apache2/ssl/www**#**.nm26.ee.key

Sertifikaadi CN: www#.nm26.ee
Sertifikaadi kehtivus: 90 päeva
Sertifikaadi asukoht: /etc/apache2/ssl/www**#**.nm26.ee.crt

= võistkonna number

Ülesanne 2.2.5 (0.5p) Asukoht: dmz-www

Muuda eelnevalt loodud privaatvõtme faili õigused turvaliseks:
Omanik (User): root
Õigused: ainult omanikul lugemine + kirjutamine

Ülesanne 2.2.6 (2p) Asukoht: dmz-www

Loo ja aktiveeri Apache2-s eraldi VirtualHost, mis võtab vastu TLS (HTTPS) ühendusi ning kasutab eelnevalt loodud privaatvõtit ja sertifikaati.

ServerName väärtus peab olema: www**#**.nm26.ee **#** = võistkonna number

Ülesanne 2.2.7 (2p) Asukoht: dmz-www

Paigalda serverisse **auditd** tarkvara ning seadista see logima ettevõtte kodulehe failide kataloogis (/var/www/intranet/*) tehtud kirjutamisi (w) ja atribuutide muutusi (a).

Auditd-reegel peab kasutama järgnevat võtit (key): **php-modification**

Ülesanne 2.2.8 (1p) Asukoht: dmz-www

Paigalda **unattended-upgrades** ning seadista see teostama automaatsed turvauuendused.

Ülesanne 2.3.1 (0.5p) Asukoht: srv-db

Korrasta MariaDB turvaseaded kasutades default skripti, mis määrab **root** kasutaja parooli, keelab **root** kasutaja kaugsisselogimise, eemaldab test-kontod ja test-andmebaasi.

Ülesanne 2.3.2 (1p) Asukoht: srv-db

Piira MariaDB kasutaja **www** õigused nii, et tal oleks ligipääs ja õigused ainult PHP veebirakenduse andmebaasile (nova_media), ning et tal puuduks GRANT-õigus.

Ülesanne 2.3.3 (1p) Asukoht: srv-db

Loo MariaDB kasutaja **admin** ning anna kõikidele andmebaasidele kõik õigused, sh GRANT.

Ülesanne 2.4.1 (1p) Asukoht: srv-dc

Loo AD grupid **IT Support** ja **DNS Admins**.
Loo AD kasutajakonto **helpdesk**.
Tee kasutajakonto **helpdesk** grupi **IT Support** liikmeks.
Tee grupp **IT Support** grupi **DNS Admins** liikmeks.

Ülesanne 2.4.2 (3p) Asukoht: srv-dc

Loo Group Policy Object (GPO), mis kehtestab järgmised turvaseaded:

- Tulemüür on sisse lülitatud (kõik profiilid)
- Tugev paroolipoliitika
    - Minimum password length: 12
    - Password must meet complexity requirements: Enabled
    - Maximum password age: 90 days
    - Minimum password age: 1 day
    - Enforce password history: 10
- Kontolukustus (Lockout Policy)
    - Account lockout threshold: 5 attempts
    - Account lockout duration: 15 min
    - Reset account lockout counter after: 15 min

GPO peab rakenduma vähemalt järgmistele objektidele:

- OU=Nova Media,OU=Users
- OU=Nova Media,OU=Computers

Tulemus loetakse korrektseks, kui GPO on rakendunud ning kontrollitav masinas **client**

Ülesanne 2.5.1 (1p) Asukoht: dmz-bastion

Paigalda **fail2ban** ja seadista see blokeerima ebaõnnestunud SSH sisselogimisi järgnevalt: ühelt IP-lt 5 ebaõnnestunud SSH katset 5 minuti jooksul blokeerib IP-aadressi 5 minutiks.

Ülesanne 2.5.2 (3p) Asukoht: dmz-bastion

Asenda SSH serveris paroolipõhine-autentimine võtmepõhise-autentimisega. Genereeri **home-ws** masinas uus SSH võtmepaar, ning lisa see kasutaja **meister** *authorized keys* hulka.

NB! Tulemust testitakse masinast **home-ws** ja kasutajaga **meister**.

Ülesanne 2.5.3 (3p) Asukoht: dmz-bastion

Paigalda **google-authenticator** ning seadista SSH autentimisel teiseks faktoriks TOTP.
TOTP *seed-value* on ette antud ja see asub **home-ws** töölaual. Masina **home-ws** töölaual on ka rakendus Ente Auth, mille abil saab vaadata jooksvat TOTP koodi.

NB! Tulemust testitakse masinast **home-ws** ja kasutajaga **meister**.

Ülesanne 2.5.4 (2p) Asukoht: dmz-bastion

Loo eraldi konto **haldur** ning anna sudo-õigused. Eemalda kasutaja **meister** sudo-õigused.

Ülesanne 2.5.5 (2p) Asukoht: dmz-bastion

Paigalda **SELinux** ning seadista see **Enforcing** režiimi. Veendu, et SSH teenus töötab SELinuxi all ning serverisse on võimalik endiselt luua SSH ühendus **home-ws** masinast.

Ülesanne 2.5.6 (3p) Asukoht: dmz-bastion

Seadista PAM-is tugev paroolipoliitika:

- Minimum password length: 12
- Must include at least:
  - 1 lowercase letter
  - 1 uppercase letter
  - 1 digit
  - 1 special character

Ülesanne 2.5.7 (3p) Asukoht: dmz-bastion

Seadista PAM-is kontolukustus ebaõnnestunud sisselogimiste korral järgnevalt:
konto lukustub pärast 5 ebaõnnestunud katset ja lukustus kestab 5 minutit.

Ülesanne 2.6.1 (0.5p) Asukoht: office-fw + home-fw

Muuda pfSense default administraatori parool.

Ülesanne 2.6.2 (1p) Asukoht: office-fw

Piira tulemüüri reeglit „NAT SSH from WAN to DMZ-BASTION“ nii, et SSH ligipääs **dmz-bastion** masinale oleks lubatud ainult teie **home-fw** WAN-võrguliidese IP-aadressilt.

Ülesanne 2.6.3 (5p) Asukoht: office-fw

Võrkudevahelised tulemüüri reeglid on liiga avatud. Koosta ja rakenda tulemüüri reeglid nii, et lubatud oleks ainult teenustele vajaminev liiklus, ning kõik ülejäänud oleks keelatud.

Kirjelda kehtestatud tulemüüri reeglid ka järgnevas kolmes tabelis:

Table 1: From INTERNET to INTERNAL NETWORK(S)

Source	Destination	Protocol	Port(s)	Why / Purpose

Table 2: From INTERNAL NETWORK(S) to INTERNET

Source	Destination	Protocol	Port(s)	Why / Purpose

Table 3: From INTERNAL NETWORK(S) to INTERNAL NETWORK(S)

Source	Destination	Protocol	Port(s)	Why / Purpose

Ülesanne 2.6.4 (5p) Asukoht: office-fw

Seadista OpenVPN-baasil remote-access VPN, et koduvõrgust (**home-ws** masinast) saaks luua VPN-ühenduse ettevõtte sisevõrku. OpenVPN nõuded ja seaded:

- **Autentimine:**
  - Tüüp: kasutajanimi + parool (ei ole TLS klient-sertifikaadi põhine)
  - Loo eraldi kasutajakonto nimega **meister**
- **Protokoll ja port:** UDP/1194
- **VPN tunnelvõrk:** 10.8.0.0/24
- **Push route:** ainult võrku 192.168.3.0/24 (Office SRV)

Lisaks OpenVPN serveri seadistamisele peab looma ka tulemüüri reeglid, mis lubavad:

- WAN-ist ühenduda tulemüüri pihta pordile UDP/1194
- VPN tunnelvõrgust ühenduda võrku 192.168.3.0/24

Ekspordi **.ovpn** konfiguratsioon ja jäta see **home-ws** töölauale nimega **office-vpn.ovpn**

NB! Tulemus on korrektne kui **home-ws** brauseris avaneb Wazuh (https://192.168.3.200)

Ülesanne 2.7.1 (5p)

Varundage kõik olulised andmed ja konfiguratsioonid (vaadake ja hinnake ise, mis on oluline). Pakkige see kokku **mgmt-admin1** töölauale nimega „Backup.zip“. Kirjeldage järgnevas tabelis mida te varundasite, miks te seda tegite, ja kuidas seda taastada saab:

Table 1: Backup Components

Name	Contents	Source	Why / Purpose	How to Restore

5. VÕISTLUSÜLESANNE (TEOREETILINE OSA)

5.1. Ülesanne

Võistkonnal tuleb võistluspäeva jooksul sooritada teoreetiline valikvastustega test (inglise keeles), mis koosneb 20-st küsimusest, ja katavad vähemalt järgnevaid teemasid:

- **Information Security Concepts** (CIA triad, risk/threat/vulnerability security controls)
- **Authentication & Authorization** (identity vs access, MFA, sessions/tokens, RBAC/ABAC)
- **Crypto Fundamentals** (symmetric vs asymmetric, encryption vs signing, key exchange)
- **Firewalls & Filtering** (stateful vs stateless, allowlisting vs blocklisting, ingress/egress)
- **Web Security Basics** (HTTP protocol, OWASP Top 10)
- **Incident Response Plans** (detect → contain → eradicate → recover)
- **Secure Development** (dependency/supply-chain risk, code review, SAST/DAST)

Test-keskkond asub veebilehel: https://quiz.nm26.ee

NB! Vastuseid saab esitada vaid ühe korra. Mõelge valikud hoolikalt läbi.