SurfaceScan Academy

Resmi Tedris Beledcisi ve Imtahan Proqrami

Ixtisas Kodu: CDESA

DNS ve E-poct Tehlukesizliyi Arxitektoru

Imtahan Telebleri: 30 Sual | 35 Deqiqe | Kecid Heddi: 80%

1. IXTISAS HAQQINDA VE IMTAHANIN EHATE DAIRESI

DNSSEC kriptoqrafik etibar zenciri, CAA qaydalari, SPF optimizasiyasi, DKIM acarlari, DMARC saxtakarliq bloklamasi ve BIMI

2. EHATE OLUNAN ESAS MOVZULAR

* DNSSEC kok etibar zenciri, RRSIG, DNSKEY ve DS qeydleri
* CAA qeydleri: issue, issuewild ve iodef xeberdarliqlari
* SPF sintaksisi, dovreleri ve 10 DNS axtaris limiti
* DKIM aciq acar sifrelemesi, selektorlar ve kanoniklesdirme
* DMARC siyasetleri (p=none, quarantine, reject) ve rua/ruf hesabatlari
* MTA-STS, TLS-RPT ve BIMI brend loqo standarti

Imtahan Qaydalari ve Kocurmeye Qarsi Tehlukesizlik Sistemi:

* Duzgun cavablar yalniz server terefinde saxlanilir ve brauzere gonderilmir.
* Suallar ve variantlar her namized ucun tesadufi ardicilliqla qarisdirilir.
* Imtahan zamani vaxt nezareti aparilir ve pencere deyismesi qeyde alinir.

CHAPTER 1: DNSSEC: Domen Adlari Sisteminin Qorunmasi

DNS qeydlerinin kriptoqrafik tesdiqi ve kes zeherlenmesinin qarsisinin alinmasi.

Standart DNS sorgulari sifrelenmemis UDP paketleridir ve asanliqla saxtalasdirila biler (DNS cache poisoning). DNSSEC butun DNS qeydlerini asimmetrik kriptoqrafiya ile imzalayir:

- RRSIG: Muvafiq qeydler (A ve ya MX) ucun reqemsal imza.
- DNSKEY: RRSIG imzalarini yoxlamaq ucun istifade olunan aciq acar.
- DS (Delegation Signer): Ana zonada (.com, TLD) yerlesdirilen hash-dir ve ICANN kok zonasina qeder qirilmaz etibar zenciri yaradir.

```
# Querying DNSSEC validated records
dig +dnssec example.com A
# Verifying DS record presence in parent zone
dig example.com DS +trace
```

CHAPTER 2: Sertifikat Merkezi Selahiyyetlendirilmesi (CAA)

Hansi CA-larin sertifikat vere bileceyini mehdudlasdirmaq ve xeberdarliq teyin etmek.

CAA (RFC 8659) icazesiz sertifikat merkezlerinin domen adiniz ucun sertifikat buraxmasinin qarsisini alir:

- issue: Xususi CA-lara (mes: letsencrypt.org, digicert.com) standart hostlar ucun icaze verir.
- issuewild: Wildcard (*.domain.com) sertifikatlarin buraxilmasini ayrica mehdudlasdirir.
- iodef: Qayda pozuntusu cehdlerinin gonderileceyi email ve ya veb unvan.

```
example.com. IN CAA 0 issue "letsencrypt.org"
example.com. IN CAA 0 issuewild ";"
example.com. IN CAA 0 iodef "mailto:security@example.com"
```

CHAPTER 3: SPF ve Ciddi 10 DNS Axtaris Limiti

SPF sintaksisi ve axtaris limitinin asilmasindan yaranan xetalarin qarsisinin alinmasi.

RFC 7208 standartina gore SPF qeydinin yoxlanilmasi en cox 10 DNS axtarisi (include, a, mx, redirect) teleb ede biler. Eger 11 ve ya daha cox axtaris olarsa:

Poct serverleri SPF-i PermError (Xeta) kimi qebul edir ve sizin qanuni mektublarinizi spama atir ve ya redd edir.

Tovsiye: Lazimsiz ucuncu teref xidmetleri temizlenmeli ve qeyd -all (qeti redd) ve ya ~all ile bitmelidir, hec vaxt +all yazilmamalidir.

```
v=spf1 include:_spf.google.com include:mailgun.org ~all
```

© 2026 SurfaceScan · CDESA Certification Curriculum

CHAPTER 4: DKIM ve DMARC Siyaseti Muhafizesi

Emaillerin reqemsal imzalanmasi ve saxtakarligin p=reject ile qarsisinin alinmasi.

DKIM cixan emailleri gizli acarla imzalayir ve alici server DNS-deki aciq acarla mektubun yolda deyisdirilmediyini yoxlayir.

DMARC ise SPF ve DKIM-i birlesdirir:

- p=none: Yalniz musahide aparir, saxta mektublari bloklamir.
- p=quarantine: Subheli mektublari Spam qovluguna gonderir.
- p=reject: Domen adinizdan gonderilen saxta mektublari derhal serverde bloklayir ve musterilerinizi fisinqden qoruyur.

SurfaceScan-da A+ almaq ucun DMARC mutleq p=reject ve aktiv rua unvani ile sazlanmalidir.

```
_dmarc.example.com. IN TXT "v=DMARC1; p=reject; sp=reject; pct=100; rua=mailto:dmarc-reports@example.com"
```