Tietoturvan työkalut ja niiden käyttö kentällä

Tervetuloa esitykseeni tietoturvavälineistä ja -teknologioista. Tänään käymme läpi erilaisia työkaluja ja tekniikoita, joita käytetään tietoturvan alalla.

Sisällysluettelo

Radio-tekniikan vaarat tietoturvatutkijoille

- Mikä on riskinä?

Vaikka radio-tekniikka on voimallinen työkalu tietoturvatutkimuksessa, se voi myös aiheuttaa vakavia riskejä, erityisesti jos sen käyttöön ei ole tarvittavaa asiantuntemusta.

- Vaaralliset käyttötapaukset

1. Laittomat tai eettisesti kyseenalaiset lähetykset: Tietämättömyys tai huolimattomuus voi johtaa lähetyksiin, jotka rikkovat lakia tai aiheuttavat eettisiä dilemmoja.

2. Järjestelmien häirintä: Tutkimuksissa voidaan vahingossa tai tarkoituksellisesti häiritä kriittisiä järjestelmiä, kuten sairaalalaitteita tai liikenteenohjausjärjestelmiä.

3. Anonyymiuden menetys: Virheellisesti suoritetut radiolähetykset voivat paljastaa tutkijan henkilöllisyyden tai sijainnin.

4. Säteilyaltistus: Erityisesti voimakkaat lähetykset voivat aiheuttaa terveysriskejä säteilyn muodossa, mikä on huomioitava tutkimuksessa.

OMG Cable Elite

- Mikä se on?

”OMG Cable Elite on älykäs USB-kaapeli, joka on suunniteltu näyttämään ja toimimaan kuin tavallinen USB-latauskaapeli. Ero on siinä, että kaapeliin on sisäänrakennettu pieni tietokone ja langaton yhteys, joka mahdollistaa kaapelin etäkäytön ja -hallinnan. Tämä tekee siitä erittäin tehokkaan työkalun tietoturvatutkimukselle ja penetraatiotesteille.”

- Mihin sitä käytetään?

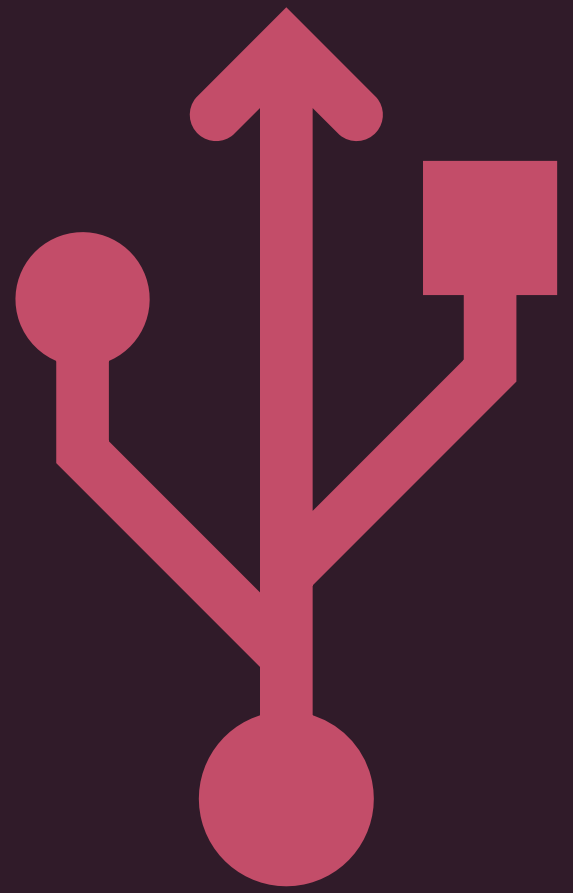
1. Penetraatiotestaus: Testaaminen, kuinka helposti järjestelmä tai verkko voi olla altis hyökkäyksille.

2. Tietoturvakoulutus: Demonstroimaan, kuinka helppoa on joutua uhriksi näennäisesti vaarattomille laitteille.

3. Tietojen kerääminen: Mahdollisuus kerätä tietoja kohteesta, esimerkiksi näppäimistön syötteet tai verkkoliikenne.

- Esimerkkejä käytöstä?

1. Data Harvesting: Kaapelin avulla voidaan salaa kerätä tietoja käyttäjän toiminnasta.
2. Man-in-the-Middle hyökkäykset: Kaapelin avulla voidaan reitittää ja manipuloida verkkoliikennettä.
3. Fyysiset hyökkäykset: Jos kaapeli on kytketty esimerkiksi lukon avausmekanismiin, sitä voidaan etäohjata avamaan lukko.



OMG Cable Elite tehtävät

1. SELVITÄ, KUINKA OMG CABLE ELITE EROAA TAVALLISISTA USB-KAAPELEISTA.
2. TUTKI, MITEN KAAPELI VOIDAAN KONFIGUROIDA JA HALLITA.
3. MIETI MITEN JA MIKSI OMG CABLE ELITE ON VAARALLINEN.
4. MIETI MYÖS MITEN LÄHTISIT ESTÄMÄÄN OMG KAAPELIA.

Proxmark

- Mikä se on?

Proxmark on avoimen lähdekoodin laite, joka on suunniteltu RFID-tunnisteiden lukemiseen ja kirjoittamiseen.

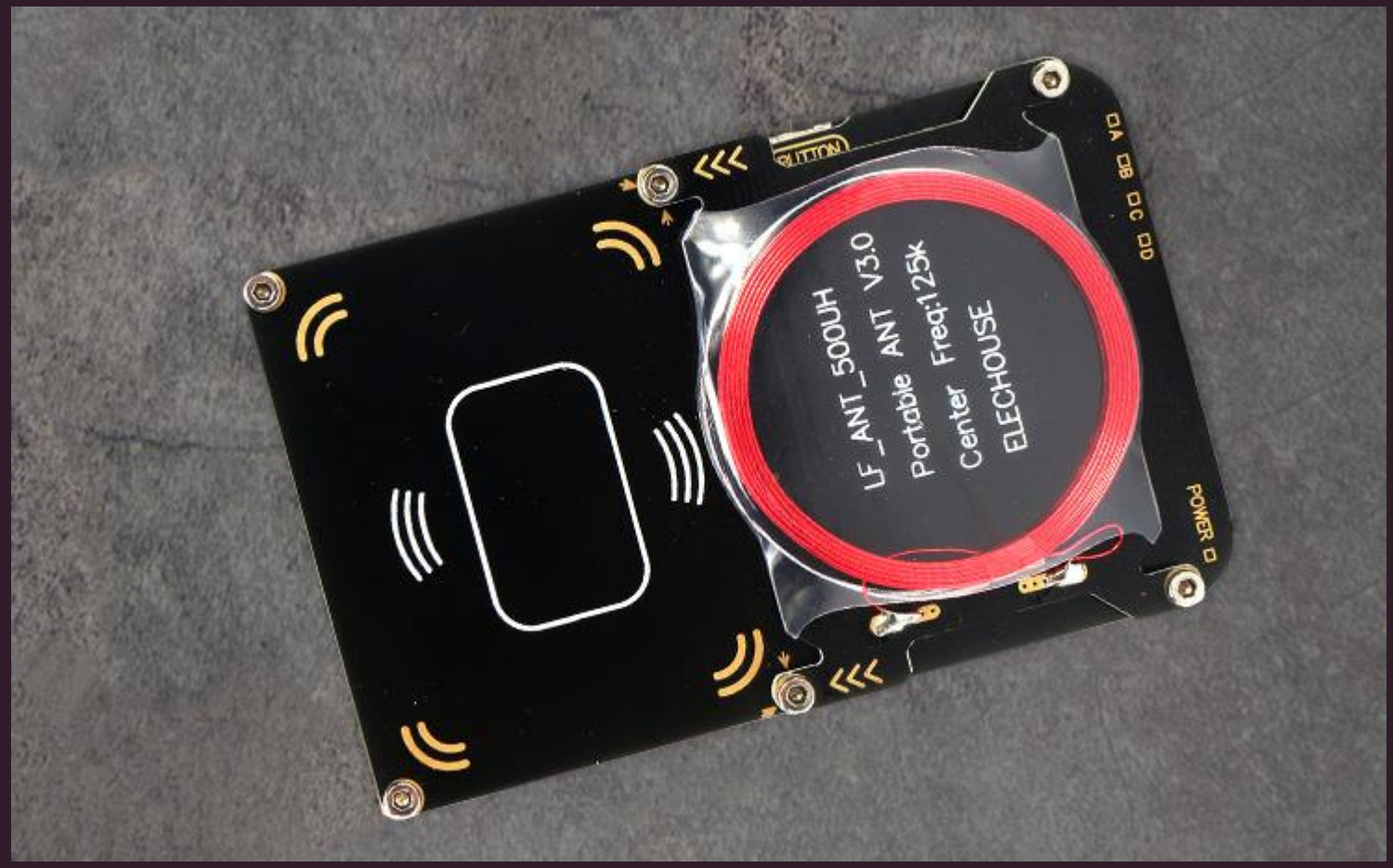
- Mihin sitä käytetään?

Käytetään pääasiassa tietoturvatestauksessa ja RFID-järjestelmien tutkimuksessa.

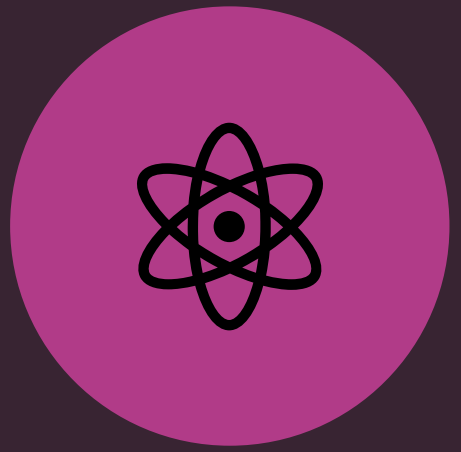
- Esimerkkejä käytöstä

RFID-tagien kloonaus

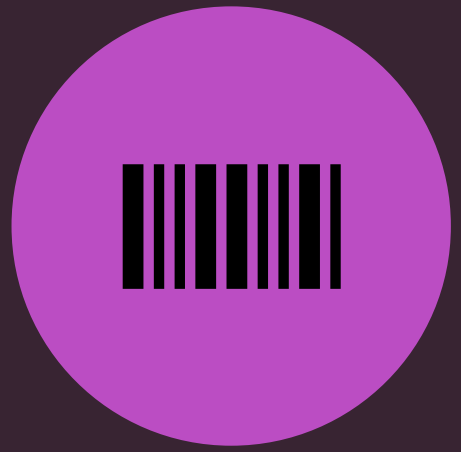
Tietoturva-analyysi



Proxmark tehtävät



TEE PIENI DEMONSTRAATIO PROXMARKIN KÄYTÖSTÄ.



KOKEILE KLOONATA RFID-TAG

WiFi Pineapple

- Mikä se on?

WiFi Pineapple on laite, joka on suunniteltu testaamaan ja hyödyntämään Wi-Fi-verkkojen tietoturvaa.

- Mihin sitä käytetään?

Käytetään Wi-Fi-verkkojen tietoturvan testaamiseen ja opetukseen.

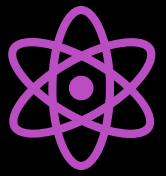
- Esimerkkejä käytöstä

Man-in-the-Middle -hyökkäykset

Verkkoliikenteen kaappaus

Wifi Pineapple tehtävät

Selvitä, kuinka WiFi Pineapple pystyy tekemään Man-in-the-Middle -hyökkäyksen.



Tee laboratoriotesti turvallisessa ympäristössä.

Flipper Zero

- Mikä se on?

Flipper Zero on monitoimityökalu tietoturvaharrastajille ja -asiantuntijoille.

- Mihin sitä käytetään?

Käytetään erilaisten laitteiden ja järjestelmien testaamiseen ja hallintaan.

- Esimerkkejä käytöstä

Automaatio

Signaalien lähettäminen

Flipper Zero tehtävät

IR-KOMENNON KLOONAUS JA LÄHETYS: OPETTELE KLOONAAMAAN KAUKOSÄÄTIMEN INFRAPUNAKOMENTO (ESIM. TV:N KAUKOSÄÄDIN) JA LÄHETÄ SE FLIPPER ZERON AVULLA.

RFID/NFC-SKANNAUS JA KLOONAUS: KÄYTÄ FLIPPER ZEROA SKANNAAMAAN JA KLOONAAMAAN RFID-TAI NFC-TAG. TARKASTELE, MITÄ TIETOJA VOIT SAADA JA MITEN SITÄ VOIDAAN HYÖDYNTÄÄ.

SDR tekniikan ymmärtäminen

- Perusperiaatteet

Digitaalinen Signaalinkäsittely: SDR käyttää digitaalista signaalinkäsittelyä (DSP) vastaanottamiseen ja lähettämiseen.

Taajuusalue: SDR-laitteet voivat operoida eri taajuusalueilla, jolloin samalla laitteella voidaan käsitellä useita eri signaalityyppejä.

Ohjelmoitavuus: Toiminnallisuus määritellään ohjelmistolla, jolloin laite on erittäin joustava.

SDR komponentit

- Toiminnalliset Komponentit

1. Vastaanotin (Rx): Kaappaa radiotaajuisen signaalin ilmasta.
2. Lähetin (Tx): Lähettää moduloidun signaalin.
3. Dekooderi: Kääntää vastaanotetun signaalin ymmärrettävään muotoon.

Kuinka se Toimii?

1. Signaalin Vastaanotto: Antenni kaappaa radiotaajuisen signaalin.
2. ADC (Analog-to-Digital Converter): Muuttaa analogisen signaalin digitaaliseksi.
3. Digitaalinen Signaalinkäsittely: Ohjelmisto suorittaa tarvittavat laskutoimitukset signaalin dekoodaamiseksi ja analysoimiseksi.

ADS-B Pakettien Kaappaus

- Mikä on ADS-B?

Automatic Dependent Surveillance–Broadcast (ADS–B) on ilmailuliikenteen seurantatekniikka, joka mahdollistaa lentokoneiden sijaintitiedon lähettämisen reaaliajassa. Laivoilla on samanlainen järjestelmä joka on AISKuinka SDR liittyy

- ADS-B:hen?

SDR-laitteet, kuten RTL-SDR tai HackRF, voivat vastaanottaa ADS-B-signaaleja ja näin seurata lähialueen ilmailuliikennettä…

ADS-B Pakettien kaappauksen toimintaperiaate

- Vastaanotto: SDR-laitteen avulla voidaan kaapata ADS-B-signaaleja taivaalta.
- Dekoodaus: Ohjelmisto kuten Dump1090 dekoodaa signaalin ja esittää sen selkeässä muodossa.
- Visualisointi: Käyttäen karttaohjelmistoja, kuten Virtual Radar Server, voit nähdä lentokoneiden sijainnit reaaliajassa.

HackRF PortaPack H2

- Mikä se on?

HackRF PortaPack H2 on SDR (Software Defined Radio) -laite.

- Mihin sitä käytetään?

Käytetään radiotaajuuksien analysointiin ja testaukseen.

- Esimerkkejä käytöstä

FM-radiotaajuuden kuuntelu

Spektrianalyysi

HackRF PortaPack H2 tehtävät

KUUNTELE FM-RADIOTA KANAVAA HACKRF PORTAPACK H2:LLA.

TUTKI, KUINKA LAITE VOIDAAN ASETTAA SPEKTRIANALYSAATTORIKSI.

BladeRF

- Mikä se on?

BladeRF on toinen SDR-laite, joka on suunniteltu ammattikäyttöön.

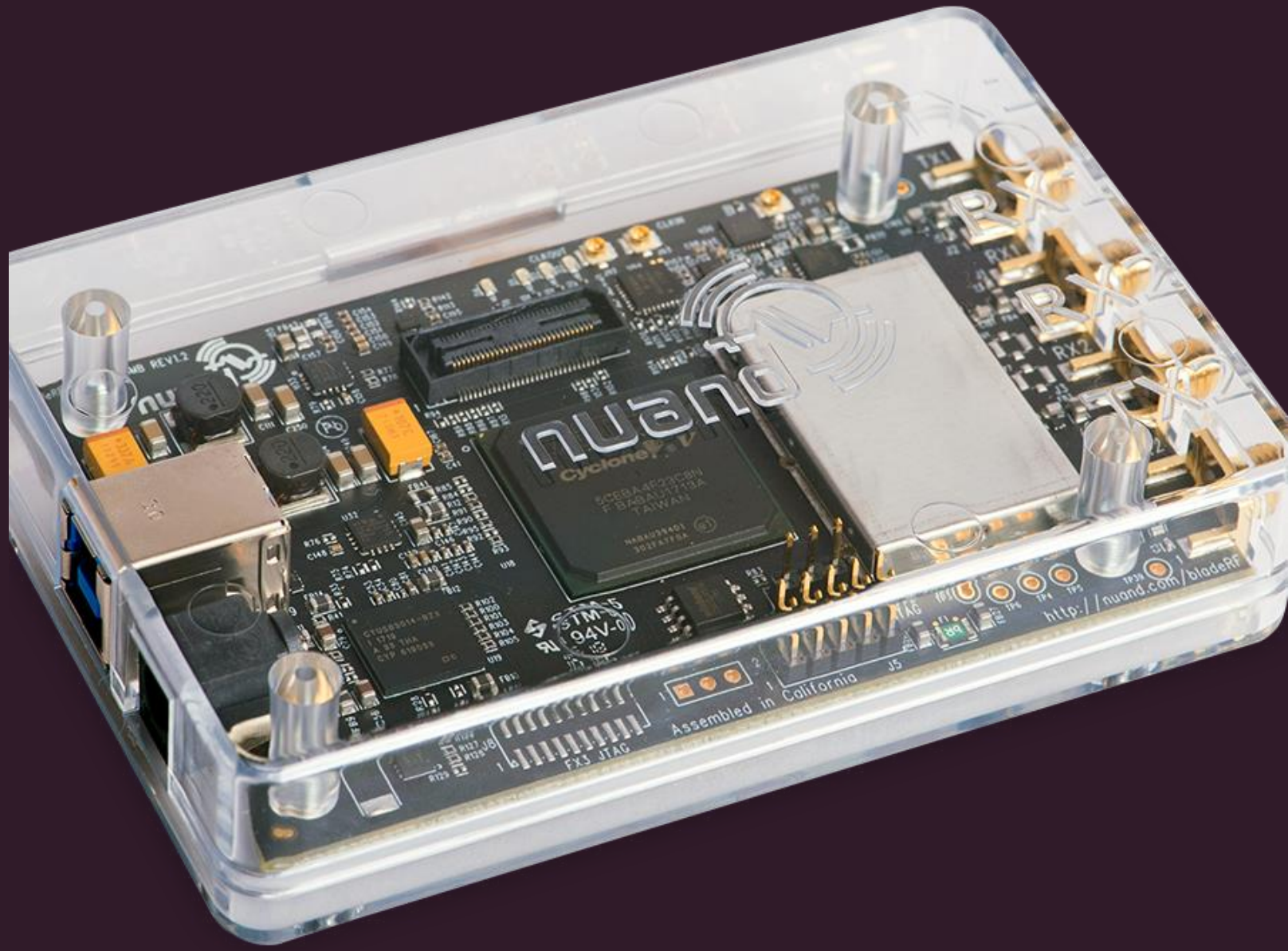
- Mihin sitä käytetään?

Käytetään monimutkaisempiin radiotaajuusprojekteihin ja tutkimukseen.

- Esimerkkejä käytöstä

Radiotaajuuden kaappaus

Tiedonsiirto



Tiirikointi ja Lainsäädäntö Suomessa

- Mikä on tilanne?

Tiirikointi on Suomessa säädelty toiminta, ja sen laillisuus vaihtelee tilanteen ja tarkoituksen mukaan. Tässä diassa keskitymme erityisesti tietoturvatutkijoiden näkökulmaan.

- Keskeiset lait ja pykälät

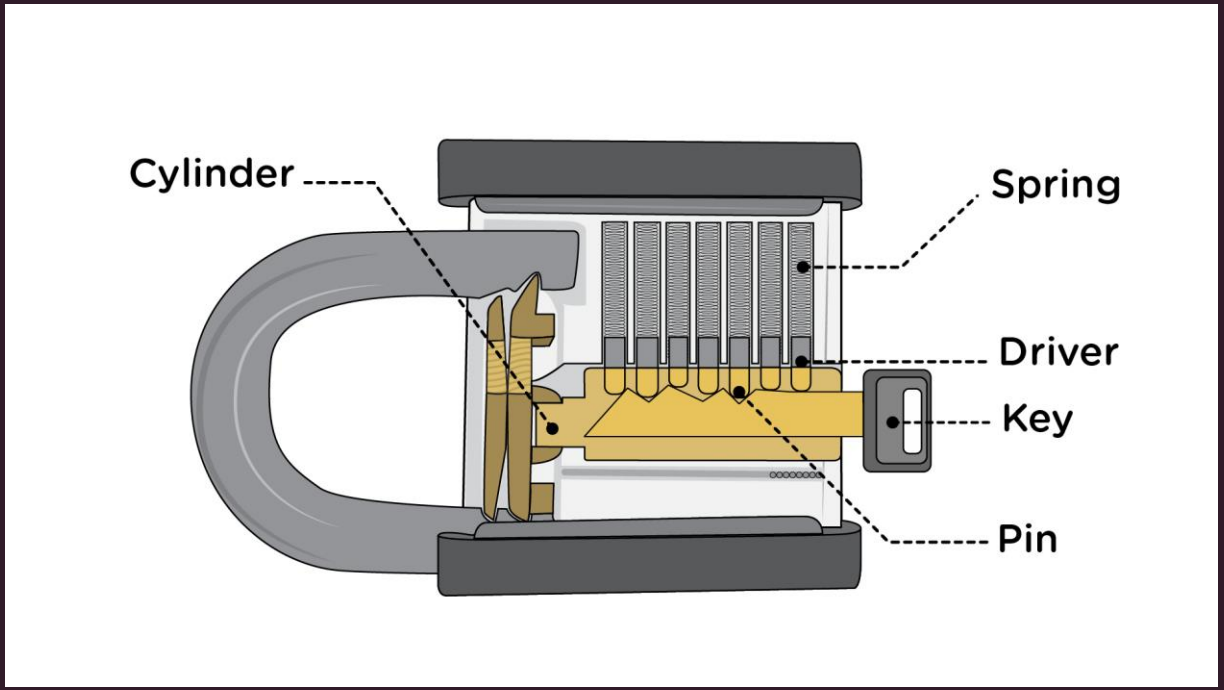
1. Luvaton Avaintehtailu (Rikoslaki 28 luku 8§): Luvaton avaintehtailu on rangaistavaa, jos se tehdään rikoksen tekemistä varten.

2. Luvaton Käyttö (Rikoslaki 28 luku 7§): Lukon avaaminen ilman lupaa on laitonta.

3. Varkaus ja Törkeä Varkaus (Rikoslaki 28 luku 1-2§): Tiirikoinnin avulla tehty omaisuuden anastus luokitellaan varkauksiksi.

4. Luvanvarainen Liiketoiminta: Tiirikointivälineiden myynti ja lukkoseppätoiminta voivat olla luvanvaraista.

Lukon Tiirikointi



- Mikä se on?

Lukon tiirikointi on tekniikka, jolla avataan mekaanisia lukkoja ilman avainta.

- Mihin sitä käytetään?

Käytetään yleensä turvallisuustestauksessa, lukkojen arvioinnissa sekä hätätilanteissa avainten puuttuessa.

- Esimerkkejä käytöstä

Koulutus ja opetus

Penetraatiotestaus

Tiirikointi työkalut

- Yleisimmät Tiirikointityökalut

Jännitystyökalu (Tension Wrench): Käytetään lukon sylinterin kääntämiseen ja jännittämiseen, jotta nastat voidaan asettaa oikein.

- Eri kokoiset ja muotoiset tiirikat:

1. Kärkitiirikka: Yleisin, yksinkertainen ja monikäyttöinen.
2. Rake-tiirikka: Käytetään 'raking'-tekniikassa.
3. Pallotiirikka: Käytetään erityisesti levytelkolukoissa.

Perustekniikat

- Tiirikoinnin Perustekniikat

1. Yksittäisen Nastan Asettaminen (Single Pin Picking): Käytetään jännitystyökalua ja kärkitiirikkaa asettamaan yksittäiset nastat yksi kerrallaan.
2. Raking-menetelmä: Käytetään rake-tiirikkaa ja jännitystyökalua nopeaan avaukseen. Ei yhtä tarkka kuin yksittäisen nastan asettaminen.
3. Bumping: Käyttää erityistä "bump key" -avainta ja jännitystyökalua. Tekniikka perustuu äkilliseen iskuun, joka saa nastat hyppäämään paikoiltaan.

Yleiset Lukkotyypit

- Lukkotyypit

1. Sylinterilukot: Yleisimpiä lukkoja, joissa on pyöreä sylinteri ja sarja nastoja.
2. Levytelkolukot: Käytetään usein polkupyörälukoissa ja arkistoissa. Levyjen sijaan nastoja.
3. Abloy-lukot (Suomessa yleisiä): Perustuvat kiekkoihin eikä nastoihin, ja vaativat erityisen tiirikkasetin.

Lukon Tiirikointi tehtävät

- Mieti mitä tapahtuu kun yrität tiirikoida lukkoa.
- Kokeille harjoitus lukkoa.

Loppu Tiivistelmä

- Mitä Olemme Oppineet?

Tänään olemme sukeltaneet syvälle tietoturvan ihmeelliseen maailmaan, aina älykkäistä USB-kaapeleista radio-tekniikan saloihin ja lukkojen tiirikoinnista lainsäädäntöön. Toivottavasti olette nyt varustettu uusilla taidoilla ja tiedolla - ja ehkä myös uudella kunnioituksella näitä työkaluja ja tekniikoita kohtaan!

Hauska Fakta Loppuun!

Tiesittekö, että salasana "123456" on yksi yleisimmistä salasanoista maailmassa? Jos se on salasanasi, nyt olisi hyvä hetki päivittää se!

By: Eetu Heino date:9.11.2023