Ofenzivna sigurnost

Penetracijsko testiranje temeljeno na obavještajnom radu (ILPT)

Martin Bugarin, 15.12.2025.

Pregled predavanja

- Motivacija
- Pitanja za ispite
- Uvod u ILPT
- Nužnost ILPT-a
- Globalni okviri
  - TIBER-EU, CBEST
- Općenita metodologija
- Zaključak

Motivacija

- Velike organizacije trpe napade svaku minutu
  - Napadači se uz to i stalno unaprjeđuju
- Obični pentestovi su dobri, no imaju svoja ograničenja
- Pentestovi temeljeni na obavještajnom radu daju detaljniji uvid u mane sustava

Pitanja za ispite

- Koja je razlika između red teaminga i penetracijskog testiranja temeljenog na obavještajnom radu?
- Nabroji 3 okvira za provođenje ILPT-a
- Koje su 3 glavne faze TIBER-EU okvira i opiši jednu?
- Kada je DORA regulativa stupila na snagu te koji je njezin zahtjev?
- Navedi izazove u implementaciji ILTP-a

Pentest temeljen na obavještajnom radu

- eng. *Intelligence-Led Penetration Testing (ILPT)*
- Napredni oblik sigurnosnog testiranja koji koristi stvarne obavještajne podatke o prijetnjama (Threat Intelligence - TI) za simulaciju stvarnih napada
- Imitiranje taktika, tehnika i procedura stvarnih prijetnji

- Za razliku od običnog penetracijskog testiranja, djeluje u cjelovitom scenariju u više dimenzija
  - Cilj testirati cjelokupnu sposobnost ljudi, procesa i tehnologije
- Prilagođene taktike temeljene na stvarnim prijetnjama
- Standardni testovi često ne otkrivaju kako bi se organizacija branila od *prave* prijetnje
- *Kontrolirana simulacija napada*

Usporedba običnog pentesta i ILPT-a

- Klasični pentest
  - Fokus na pronalasku maksimalnog broja ranjivosti
  - Ograničeno vrijeme i opseg izvedbe
- Pentest temeljen na obavještajnom radu
  - Fokus na simulaciju specifičnih prijetnji(npr APT grupe ili kriminalne skupine)
  - Testira detekciju i odgovor obrane
  - Scenariji se temelje na stvarnim podacima o tome tko napada specifično područje

Razlike između Red teaminga i ILPT-a

- Red teaming i ILPT se razlikuju tako što se u Red teamingu odgovor branitelja ispituje koristeći proizvoljne metode dok se u ILPT-u koriste točne metode koje koristi nekakav postojeći napadač kojeg operacija imitira

Nužnost ILPT-a

- Evolucija napadača
  - Napadači su sve sofisticiraniji i potrebnije su naprednije metode obrane
- Stvarnost
  - Organizacije dobivaju dojam o tome kako se mogu odviti stvarni napadi

Globalni okviri (frameworks)

- Postoje razni standardizirani okviri kojima se osigurava kvaliteta i sigurnost testiranja
  - TIBER-EU - Europska Unija
  - CBEST - Velika Britanija, financijski sektor
  - GBEST - Velika Britanija, vladin sektor
  - CORIE - Australija

TIBER-EU

- eng. *Threat Intelligence-based Ethical Red Teaming*
- Okvir Europske Unije čiji je cilj poboljšati zaštitu, otkrivanje napada i uzvraćanje
- Razvijen primarno za testiranje financijskih institucija u EU

TIBER-EU

- Struktura
  - White team (organizacija i nadzor)
  - Obavještajci
  - Provoditelji pentesta

TIBER-EU faze

- 1. faza pripreme
- 2. faza testiranja
- 3. završna faza

Faza pripreme

- Formiraju se timovi odgovorni za nadgledanje testa
- Test se odobrava od strane nadležnih tijela

Faza testiranja

- Prikupljanje obavještajnih podataka
- Pružatelj usluge obavještajnog rada (TI provider) priprema *Izvješće o ciljanim obavještajnim podacima o prijetnjama(Targeted Threat Intelligence Report – TTI Report)*
  - njime postavlja scenarij za test i daje korisne informacije o meti

Faza testiranja

- TTI izvješće se koristi dalje za razvoj napada
  - Suradnja između TI i provoditelja pentesta
- Započinje se provođenje pentesta

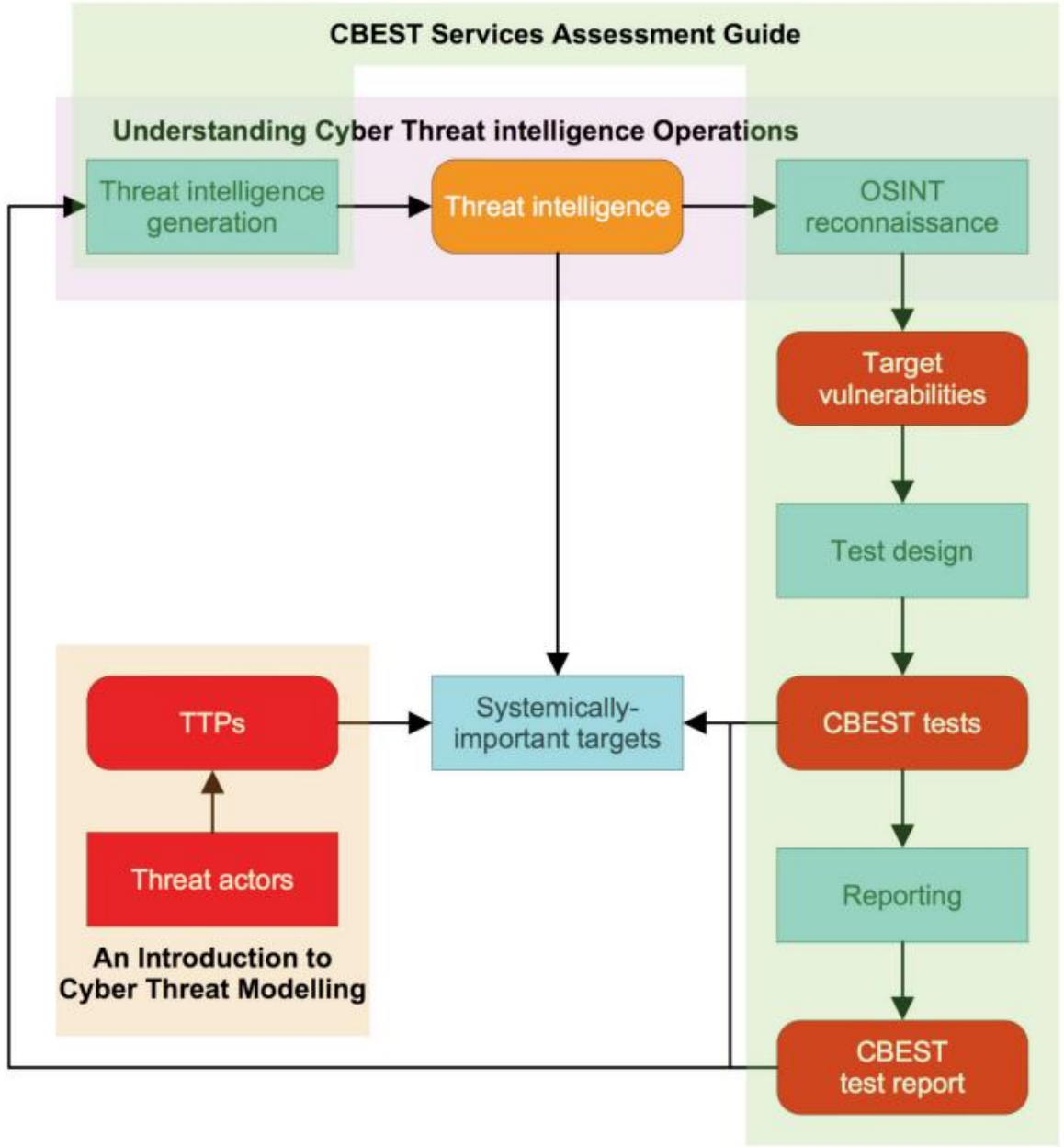
Faza zatvaranja

- Provoditelji pentesta izrađuju izvješće
  - Opis detalja i pristupa u pentestu
  - Savjeti za napredak
- Izrada *Plana sanacije*
  - Upute za saniranje grešaka
- Podjela rezultata s ostalim nadležnim tijelima

CBEST

- Prvi formalni okvir ove vrste (2014. godina)
- Zaštita financijskih institucija u Ujedinjenom Kraljevstvu
- Nadziran od strane regulatora
  - PRA – brinu se da banke imaju dovoljno novca
  - FCA – brinu se da banke ne varaju klijente

CBEST


CBEST Services Assessment Guide
Understanding Cyber Threat intelligence Operations
Threat intelligence generation
Threat intelligence
OSINT reconnaissance
Target vulnerabilities
Test design
TTPs
Systemically-important targets
CBEST tests
Threat actors
Reporting
An Introduction to Cyber Threat Modelling
CBEST test report

Općenita metodologija

- 1. faza – priprema
  - Formiranje white teama (nadzor) i ostalih timova
  - Identifikacija ključnih funkcija
- 2. faza – obavještajni rad
  - Izvještaj o meti
  - Opći trendovi
  - Pronalaženje primjera specifičnog napadača

Općenita metodologija

- 3. faza – Planiranje napada
  - Konkretan plan napada
  - Definiranje ciljeva
  - Odobrenje koraka plana
- 4. faza – Izvršenje napada
  - Inicijalni upad, lateralno kretanje i ostale metode
  - 10 – 12 tjedana
- 5. faza - Purple teaming/zatvaranje
  - Plavi i crveni timovi zajedno analiziraju

Zakonska regulativa

- DORA
  - Zahtijeva napredno testiranje svake 3 godine
  - Sankcije za neusklađenost do 2% ukupnog prihoda
  - Stupila na snagu 17. siječnja 2025.

Izazovi implementacije ILTP-a

- Visoka cijena zbog angažmana vrhunskih stručnjaka
- Organizacija mora imati zrele procese
- Mogućnost nenamjernog prekida rada sustava tijekom testa

Zaključak

- ILPT daje pravu sliku rizika koju ne može dati niti jedan drugi test
- Cilj nije neprobojna obrana, već brzo otkrivanje i oporavak
- Razni standardizirani okviri za provedbu
- Skup, ali isplativ za dugoročnu i odličnu zaštitu

Literatura

- TIBER-EU Framework, European Central Bank https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework_2025~b32eff9a10.en.pdf

- TIBER-EU Services Procurement Guidelines, European Central Bank https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf

- CBEST Threat Intelligence-Led Assessments, Bank of England https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide

- TIBER-EU White Team Guidance, European Central Bank https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf

- FS-ISAC
  https://www.fsisac.com/
- Fundamental Elements of Threat-Led Penetration Testing, European Central Bank
  https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2018-G7-fundamental-elements-for-threat-led-penetration-testing.en.pdf
- TIBER-NL guide, DeNederlandischeBank
  https://www.dnb.nl/media/1mdf3lmq/75069-dnb-ia_tiber-guide_web.pdf
- DORA regulativa, EUR-Lex
  https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Hvala!