Ofenzivna sigurnost

Oblici ofenzivne sigurnosti

izv. prof. dr. sc. Stjepan Groš

Pregled prezentacije

- Motivacija
- Modeli ponašanja napadača
- Taktike, tehnike, pod-tehnike, procedure
- Operacije i strategije
- CTF-ovi, pentestovi, crveni timovi, napadači
- Kibernetički prostor i kibernetičko ratovanje

Pojmovi koji se vežu uz ofenzivnu sigurnost

- Jako je puno pojmova koji se koriste kada je ofenzivna sigurnost u pitanju
  - Penetracijsko testiranje, crveni tipovi, AD CTF-ovi, CTF-ovi, cyber kill chain, …
- Ti pojmovi (značajan dio) nemaju strogu i općeprihvaćenu definiciju
  - Pokušat ćemo ih malo pojasniti i „posložiti”
  - Budite sigurni da će se uvijek naći netko tko vidi sve na drugi način

Model ponašanja napadača

- Napadači su razlog zašto sve ovo radimo i zato krećemo od njih i njihovog ponašanja
- Cilj je strukturirati ponašanje napadača
  - Olakšava obranu jer ograničava što je moguće, a što nije
  - Olakšava i učenje ofenzivne sigurnosti
- Najpoznatiji (i prvi) model ponašanja napadača je *Cyber Kill Chain*
  - Postoji još mnoštvo drugih modela
  - Unified kill chain, Diamond model, Mandiant cyber kill chain

Cyber kill-chain

- Definiran 2011. godine
- Sastoji se od 7 slijednih **taktičkih koraka**
  - Izviđanje (engl. reconnaissance)
  - Naoružavanje (engl. weaponization)
  - Isporuka (engl. delivery)
  - Iskorištavanje (engl. exploitation)
  - Instalacija (engl. installation)
  - Upravljanje (engl. command & control)
  - Postizanje ciljeva (engl. actions on objectives)

Taktike

- Pojmovi koji su preuzeti iz vojnih znanosti
  - Nisu u potpunosti preuzeta i značenja!
- Taktika
  - Odgovara na pitanje ŠTO se želi postići
  - Taktike prema MITRE ATT&CK su: Inicijalni ulaz, Izvršavanje, Perzistencija, Podizanje privilegija, Izbjegavanje obrane, Pristup vjerodajnicama, Otkrivanje, Lateralno kretanje, Prikupljanje, C&C, Eksfiltracija, Udar

Tehnike

- Tehnike odgovaraju na pitanje KAKO postići određen taktički korak
  - Za pristup određenim mrežnim resursima treba „dumpati” vjerodajnice iz radne memorije računala
- U određenim slučajevima tehnike su ŠTO napadač dobije s nekom akcijom
  - Ovo je bitno kod taktike otkrivanja
- Pod-tehnike dodatno definiraju pojedine tehnike
  - Skeniranje LSASS procesa kako bi se „dumpale” vjerodajnice
  - Pristup datotekama /etc/shadow i /etc/passwd

Procedure

- Specifične implementacije tehnika i pod-tehnika
  - Primjerice, korištenje PowerShell-a kako bi se „dumpala” memorija procesa lsass.exe
- Procedure u MITRE ATT&CK okviru mogu uključivati više tehnika i pod-tehnika
  - Primjerice, procedura za „dumpanje” vjerodajnica uključuje
    - PowerShell (pod-tehnika „Command and Scripting Interpreter” tehnike)
    - „Process Injection” (tehnika)
    - LSASS Memory (pod-tehnika „OS Credential Dumping” tehnike)

Strategija i operacije

- Strategija
  - Definira što želimo postići i definira strateške ciljeve
  - U vojnom kontekstu strategija definira zadaću vojnog djelovanja, to je politički cilj
- Operacija
  - Niz taktičkih koraka kojim se postiže određeni strateški cilj
  - U vojnom kontekstu operacija je cijeli proces planiranja, provođenja, nadziranja niza taktičkih koraka koji dovode do željenog krajnjeg stanja

Oblici ofenzivne sigurnosti

- Capture the Flag (CTF) natjecanja
- Penetracijska ispitivanja
- Crveni timovi
- Napadači
- Kibernetičko ratovanje

Capture the Flag natjecanja

- Prvo CTF natjecanje organizirano na DEFCON-u 1996. godine
  - Od tada do danas je postalo jako rašireno
  - Dobra stranica koja prati razna CTF natjecanja je ctftime.org
- Zadatak pronaći ili dohvatiti zastavicu (flag)
  - Zastavice su obično tekstni nizovi
- Mogu se rješavati (igrati) u timovima ili individualno
- Ima više varijanti CTF-ova koji su donekle različiti
  - Jeopardy, attack-defence, king-of-the-hill

Jeopardy CTF

- Skup zadataka po kategorijama
  - Naziv dobio po *Jeopardy* kvizu
  - Kategorije: web, forenzika, kriptografija, steganografija, …
- Postoje značajne razlike u odnosu na djelovanje napadača
  - Isključivo su to razni tehnički zadaci
    - Uvježbavanje jednog tehničkog koraka
  - Određene tehnike česte u ovim natjecanjima napadači ne koriste
    - Loša kriptografija, steganografija, …

Attack-Defense CTF (1)

- Prvi oblik CTF-a (DEFCON)
- Sudjeluju gotovo isključivo timovi
- Svaki tim ima mrežu ili računalo koje brani te istovremeno napada druge timove
  - Nužno je osigurati dostupnost svojih usluga i spriječiti krađu zastavica
  - Potpuno povezana mreža
- Najzahtjevniji oblik CTF-a
  - Stres, potreba za obranom, traženje ranjivosti

Attack-Defense CTF (2)

- Organizacija tima
  - Raspodjela po odgovornostima (praćenje mrežnog prometa/logova, traženje ranjivosti, pisanje exploita), definiranje voditelja/koordinatora, tko šalje zastavice
- Prilagodba infrastrukture
  - Instalacija SSH ključeva, promjena lozinki, povećanje razine logiranja, postavljanje zaštita (IDS/IPS, WAF, HIDS)
- Traženje ranjivosti
  - Korištenje alata za traženje ranjivosti, praćenje drugih timova radi otkrivanja ranjivosti, analiza servisa i koda

Attack-Defense CTF (3)

- U odnosu na Jeopardy CTF
  - Veći naglasak na traženju i iskorištavanju ranjivosti
  - Postojanje određenih taktika koje nisu prisutne u JCTF
  - Potreba za znanjem DevOpsa i općenito obrambene strane
- U odnosu na napadača
  - Postojanje obrambene strane, napadači se ne brane
  - Napadači nisu ograničeni po pitanju onoga što mogu napasti
  - Napadači nemaju identičnu konfiguraciju kao i branitelji

King-of-the-Hill (KotH) CTF

- Cilj je kompromitirati neki poslužitelj
  - Nakon kompromitiranja treba postaviti zastavicu i zaštititi ga od drugih timova!
- Specifičnosti
  - Potreba za lateralnim kretanjem – složenija mrežna topologija
  - Postavljanje implantata – zakrpe i stražnja vrata
  - Priprema – kroz skeniranje mreže i pisanje implantata

Pwn2Own

- Oblik natjecanja u kojemu je potrebno kompromitirati potpuno zakrpan sustav
  - Održava se pod pokroviteljstvo Zero Day Initiative
  - Podjela nagrada u iznosu od $1M+
- Karakteristike
  - Pokriva prva četiri koraka Cyber Kill Chaina
  - Preklapa se s aktivnošću traženja ranjivosti (engl. vulnarability research)

Penetracijsko testiranje (1)

- Penetracijsko testiranje (engl. penetration testing, pentest) je metodologija testiranja u kojoj procjenitelji, koji obično rade pod određenim ograničenjima, pokušavaju zaobići ili poništiti sigurnosne značajke sustava.

Penetracijsko testiranje (2)

- Jasno definirana ograničenja tijekom provođenja pentesta
  - Vrijeme u kojemu se provodi nije dugo
  - Cilj napada je jasno definiran
  - Niz pravnih, poslovnih i etičkih ograničenja
- Ograničenja u odnosu na napadače
  - Rijetko korištenje/pronalaženje ranjivosti nultog dana
  - Nema lateralnog kretanja
  - Ograničen opseg
  - Etička ograničenja

Crveni timovi (engl. red teams)

- Sve popularniji pojam
  - Nastao u vojsci tijekom hladnog rata – označavao Sovjetski savez
  - Uz njih se veže pojam *plavi tim* (engl. blue team) – označava branitelje
- Crveni timovi
  - Kontinuirano treniranje branitelja – dugoročni proces
  - Korištenje u treninzima na kibernetičkim poligonima (engl. cyber ranges)
  - Neke tvrtke imaju dedicirane crvene timove – Facebook (Red Team X) Microsoft, Google

Crveni timovi vs. pentesteri

- Jako se miješaju ta dva pojma
- Razlika je u svrsi i ponašanju – ne u ljudima koji čine te grupe
- Pentest
  - pronalaženje i validacija ranjivosti radi njihova uklanjanja
  - Vremenski ograničen
- Za oboje vrijede ista ograničenja
  - Poslovna, pravna i etička ograničenja

Kibernetički poligoni

- Virtualizirana okruženja koja se koriste za
  - Uvježbavanje ofenzivnih i defenzivnih timova
  - Emulaciju i simulaciju različitih situacija
- Mnoštvo različitih proizvoda na tržištu
  - Cijene mogu biti i reda veličine $1M+
- U HR samo jedan kibernetički poligon u vlasništvu OS RH (SimSpace)
  - SPAN je nekada imao CyberGym

Napredne ustrajne prijetnje

- Mogu napadati dobavljače i sve povezane s ciljanom organizacijom
- Sadrže niz operacija za podršku djelovanju
- Napadi traju kroz dulje vrijeme
- Motivacija ovisi o vlasniku
  - I nije treniranje plavih timova

Rat i ratovanje (1)

- Pojam **ratovanje** (engl. warfare) je više tehnički nego pravni izraz i odnosi se na aktivnosti vođenja rata, uključujući oružje i metode koje se koriste.
  - Drugim riječima, radi se prvenstveno o taktikama i tehnikama
- Kibernetičko ratovanje (engl. cyber warfare) obuhvaća
  - TTP-ove opisane u MITRE ATT&CK matrici
  - Aktivnosti za upotrebu TTP-ova, koji se obično vežu uz vojno djelovanje (planiranje, priprema, vođenje, analiza)

Rat i ratovanje (2)

- **Rat (engl. war)** – u kontekstu međunarodnog prava – je pravno stanje, stanje oružanog sukoba između različitih država ili nacija unutar jedne države.
  - Da li je neka država u ratu – pravno gledano – ovisi o statusu protivnika, npr. jesu li oni države, nacije, narodi, zaraćene strane ili pobunjenici.
  - Ne stvara svaki čin neprijateljstva ili uporabe oružane sile nužno rat u smislu međunarodnog prava
  - Ako se stvori stanje rata, to ima pravne posljedice za strane u sukobu i za cijelu međunarodnu zajednicu.
  - Pravne posljedice su primarno određene Poveljom Ujedinjenih naroda.
- Kibernetički rat (cyberwar) se ne može desiti!

A što je s kibernetičkim ratom?

Understandably, ***Western nations have been historically hesitant to group asymmetric forms of power—such as economic or political coercion—as an act of force or aggression****. Accordingly, when the* ***United Nations Charter was designed, it was too proscriptive as to the definition of force****; conversely, the North Atlantic Treaty Organization's charter was too broad.* ***The hazy demarcation of what is and is not war provided clarity only to international-level politics with respect to classical forms of conflict****. This construct* ***has benefited Western nations as it provided the ability to leverage their size, position, and economic power against smaller states or ostracized nations****.**

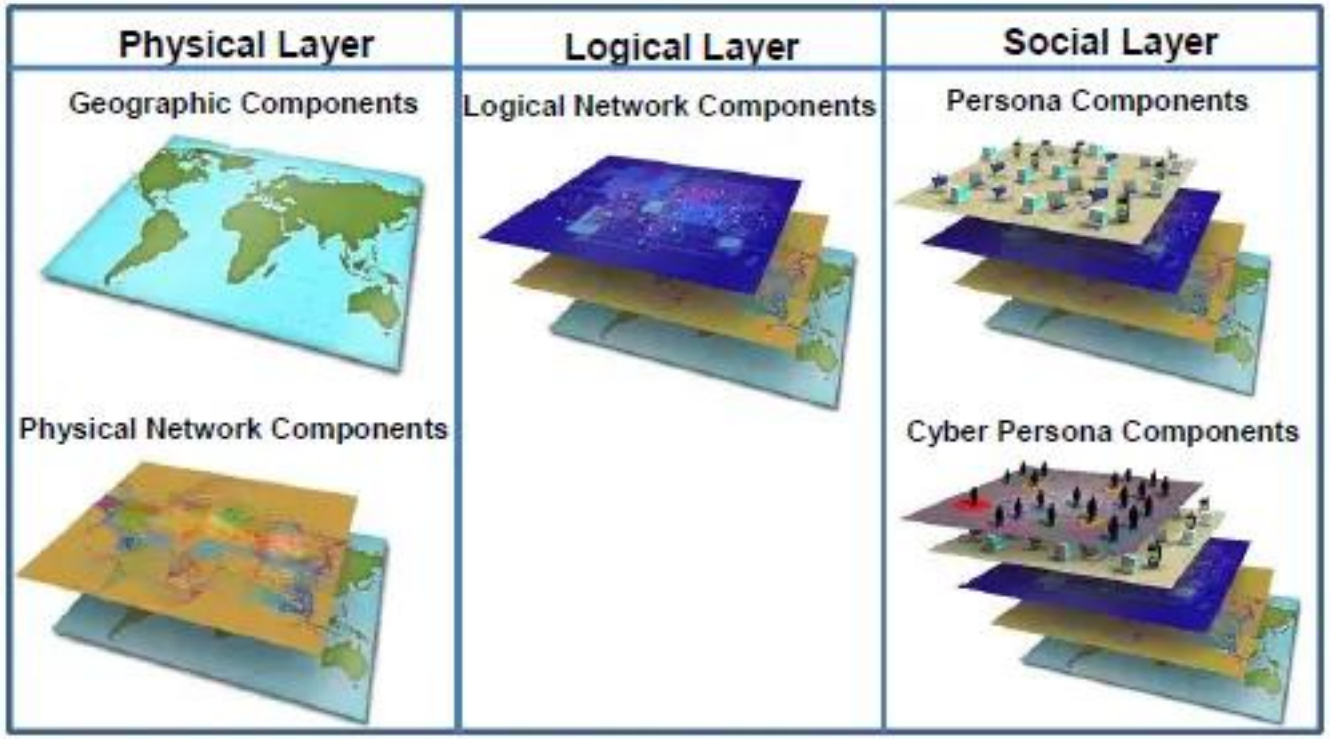
* Arthur, John E. "Russian Cyber Campaigns in Support of Military Operations." American Intelligence Journal 37.1 (2020): 49-53.

Kibernetički prostor – 5 domena ratovanja

- Tradicionalno se rat temelji na **kinetičkom djelovanju** u četiri domene
  - Zemlja, more, zrak, svemir
- S razvojem Interneta i njegovom primjenom nastala je i **peta domena** - kibernetički prostor
- Kibernetičko ratovanje (engl. cyberwar) je proširenje ratovanja u kibernetički prostor
- Vojske i vojni savezi to uzimaju u obzir osnivanjem zapovjedništava za kibernetički prostor
  - USCYBERCOM, Zapovjedništvo za kibernetički prostor (HRV)

Struktura kibernetičkog prostora

- Kibernetički prostor se sastoji od tri sloja
  - Fizički sloj
  - Logički sloj
  - Sloj osoba



Karakteristike kibernetičkog ratovanja

- Kibernetičko ratovanje djeluje na duge vremenske periode
  - Ne daje brze rezultate kao i kinetičko ratovanje
- Radi se o asimetričnom djelovanju

Hvala!