Pitanja za ispite

- Navedi i opiši jedan virus iz rane faze zlućudnog koda
- Navedi i opiši jedan virus iz rane Windows faze zlućudnog koda
- Navedi i opiši jednog mrežnog crva
- Navedi i opiši jedan rootkit ili ucjenjivačkog zlućudnog koda
- Navedi i opiši jedan primjer virtualne špijunaže i sabotaže

Pitanja za ispite

- 1) Što je social engineering?
- 2) Što je scamming?
- 3) Koji su najpopularniji oblici scamminga?
- 4) Kako prepoznati prevarantske komentare?
- 5) Što je malvertising?

Pitanja za ispite

- Koje su ključne karakteristike industrijske špijunaže?
- Kako se razlikuju industrijska špijunaža i konkurentski obavještajni rad?
- Navedi barem pet najčešćih metoda industrijske špijunaže?
- Koje su moguće posljedice industrijske špijunaže za tvrtke?
- Kako se tvrtke mogu zaštititi od industrijske špijunaže?

Pitanja za ispite

- Što je Tor i kako je najčešće implementiran?
- Što je Onion Routing i o čemu ovisi koliko slojeva enkripcija postoji?
- Kako se može otkriti identitet korisnika na Tor-u?
- Što je skrivena usluga?
- Što je ECID u FBI-ovom NIT i kako on nastaje?

Pitanja za ispite

- Što je operacijska sigurnost?
- Kako je Harvard uhvatio studenta koji je slao terorističke prijetnje?
- Što je korelacijski napad u kontekstu Tor mreže?
- Kako je deanonimiziran Dread Pirate Roberts?
- Kako je deanonimiziran Pharoah, owner Incognito Marketa?

Pitanja za ispite

- Koja je razlika između *first-party* i *third-party* web *trackera*?
- Navedi 3 vrste web *trackera* po ulozi i ukratko objasni što su.
- Zašto ima malo informacija o povijesti *web trackera*?
- Zašto je *Google Analytics* bio toliko dominantan među ostalim *web trackerima*?
- Zašto *web trackerima* raste međusobna povezanost kroz godine?

Pitanja za ispite

- Objasni što je ucjenjivački softver i kako funkcionira
- Navedi dionike u procesu plaćanja otkupnine
- Navedi korake šifriranja podataka WannaCry ucjenjivačkog softvera
- Ukratko opiši kako funkcionira EternalBlue eksploit
- Kako funkcionira “killswitch” za WannaCry

Pitanja za ispit

- Navedi svojstva infrastrukture
- Zašto nastaje infrastruktura kibernetičkog kriminala
- Koji su tipovi infrastrukture korišteni u kibernetičkom kriminalu
- Što je zajedničko administratorima legitimnih i udomljenih nezakonitih foruma
- Koji su rizici kod infrastrukture za nezakonitu aktivnost

2

1. Ugrađenost, Transparentnost, Širok doseg, Učenje članstvom, Povezanost za konvencije, Ovisnost o standardima, Građeno na postojećoj osnovi, Postoji vidljiva u kvaru, Popravlja se u dijelovima

2. Zbog mogućnosti prodaje otkrivenih ranjivosti u obliku lako upotrebljivih alata, te potrebom za tržišnom infrastrukturom

3. Legitimna infrastruktura korištena u svrhe kriminalne aktivnosti i Infrastruktura izgrađena za kibernetički kriminal

4. Žele zaustaviti razgovore tema koje su otvoreno nezakonite, kako forum ne bi bio zatvoren

5. Poslužitelji koji ih neće blokirati,
   Pristupačnost infrastrukture za izgradnju velike zajednice,
   Izbjegavanje DDoS napada,
   Blokiranje automatiziranih čitaća stranica

Pitanja za ispite

- Navedite slojeve weba i ukratko objasnite svaki od njih.
- Što su skrivene web usluge?
- Navedite i ukratko objasnite dva spomenuta načina pretraživanja dark weba.
- Opišite način korištenja Tor2Web usluge.
- Navedite neke aktivnosti kibernetičkog kriminala koje se provode na dark webu.

Pitanja za ispite

- Nabroji 3 najčešća oblika scamminga na društvenim mrežama.
- Koje oblike plaćanja prevaranti najčešće koriste i zašto?
- Što su "comment scams" i kako funkcioniraju?
- Što je "pig butchering" i kako funkcionira?
- Kako prevaranti zaobilaze mehanizme za detekciju?

Pitanja za ispite

- Koje su prednosti korištenja Bitcoina a koje Monera?
- Zašto autori *ransomwarea* i dalje u velikoj količini prihvaćaju Bitcoin?
- Koja je valuta (od dvije spomenute) bolja za pranje novca i zašto?
- Koje se tehnike otkrivanja koriste u svrhu deanonimizacije Bitcoin transakcija?
- Zašto tehnika *clusteringa* ne funkcionira na Moneru?
- Nabroji barem 3 načina deanonimizacije transakcija na *blockchainu*

1. Popularnost, dostupnost. Anonimnost, nedostupnost transakcija.
2. Zbog popularnosti i jednostavnog korištenja
3. Monero. Jer ne ostavlja gotovo nikakav trag
4. Grupiranje (clustering) adresa koje pripadaju istom korisniku/entitetu, praćenja toka novca, praćenje IP adresa, analiza coin mixera, analiza izlaznih točaka…
5. Monero skriva pošiljatelja, primatelja i iznos tako da clustering koji se na tome temelji ne funkcionira.
6. Clustering, analiza ponašanja, off-chain podatci…

Pitanja za ispite

- Navedite prednost digitalnog oglašavanja u odnosu na tradicionalno oglašavanje.
- Navedite korake procesa digitalnog oglašavanja.
- Navedite vrste napade u digitalnom oglašavanju.
- Ukratko objasnite jedan od napada u digitalnom oglašavanju.
- Navedite barem dvije mjere zaštite u digitalnom oglašavanju i koje napade sprječavaju.

Pitanja za ispite

- Što je to Threat Hunting te što mu je cilj?
- Objasnite razliku između reaktivnog i proaktivnog pristupa kibernetičkoj sigurnosti.
- Ukratko opišite proces Threat Hunting-a.
- Navedite važnost baze znanja MITRE ATT&CK.
- Što su to taktike, a što tehnike opisane bazom znanja MITRE ATT&CK. Navodite po jedan primjer za svaku.

Pitanja za ispite

- Što su crime scripts?
- Koji su neki od izvora podataka koji se koriste za izradu crime scripti?
- Koja je svrha crime scripti?
- Koje su prednosti korištenja crime scripti u odnosu na druge metode analize kriminala?
- Koje su scene u općenitom crime scriptu?

- Što su crime scripts?
Crime scripte su detaljni planovi koji opisuju korake koje počinitelji poduzimaju prije, tijekom i nakon počinjenja kaznenog djela.

- Koji su neki od izvora podataka koji se koriste za izradu crime scripti?
koriste se primarni i sekundarni izvori podataka, uključujući policijska izvješća, sudske podatke, intervjue sa žrtvama i stručnjacima, policijsku statistiku, snimke nadzornih kamera i otvorene izvore podataka (OSINT)

- Koja je svrha crime scripti?
Svrha: Crime scripte se koriste kako bi se stekao uvid u kriminalni proces, identificirali čimbenici i mehanizmi koji dovode do kaznenog djela te osmislili učinkovitije metode prevencije. Također, pomažu u razumijevanju odluka koje donose počinitelji.

- Koje su prednosti korištenja crime scripti u odnosu na druge metode analize kriminala?
crime scripte pružaju detaljan, korak-po-korak prikaz procesa počinjenja kaznenog djela, što omogućuje precizniju identifikaciju točaka intervencije i

Pitanja za ispite

- Nabrojite barem tri stadija životnog ciklusa mreže kompromitiranih računala
- Nabrojite barem tri izvora novčane dobiti koje pruža mreža kompromitiranih računala
- Nabrojite barem tri motivacije za izradu mreže kompromitiranih uređaja
- Na koji način se radi marketing mreže kompromitiranih računala?
- Koja je najpopularnija metoda širenja mreže kompromitiranih računala?