CyberTAPA 2019
Kurz praktickej kybernetickej obrany

Ako uvažujú hackeri? Kde útočia? Naučte sa ako myslieť ako špičkový hacker, aby ste sa mohli brániť! Dvojdňový kurz praktickej kybernetickej obrany. Zaregistrujte sa na **kurz praktickej kybernetickej obrany** určený pre expertov kybernetickej bezpečnosti. Kurz organizujeme v spolupráci s SK-CERT.

Účastníci kurzu získajú certifikát účasti. Súčasťou ceny je občerstvenie.

Ako nájsť vypátrať útok v počítačovej sieti? Ako navrhnúť bezpečnú sieť? Naučte sa rýchlo analyzovať aktivitu v sieti a nájsť útočníka!

12.11.2019

1. Table-Top cvičenie „Podozrivý mail je len začiatok“

Termín: 12. 11. 2019 Hotel Crowne Plaza 8:30 – 11:30 h (3 hodiny)
Lektor: Matej Šalmík, Národné centrum kybernetickej bezpečnosti SK-CERT

Table-top cvičenia sú druhom netechnických cvičení, ktoré sa zameriavajú na trénovanie rozhodovania, ako aj na precvičenie, otestovanie vlastných postupov a procesov, trénovanie úloh a zodpovedností jednotlivých rolí, a to všetko v súvislosti s riešením vzorových kybernetických bezpečnostných incidentov. Scenár cvičenia prenesie účastníkov do fiktívneho prostredia s hypotetickými udalosťami, na ktoré musia reagovať tak, ako by sa stali naozaj.

Účastníci po absolvovaní budú mať znalosť ako sa rýchlo a efektívne rozhodovať pri rôznych typoch bezpečnostných incidentov.

Cvičenie je vhodné najmä pre non-IT vyšších manažérov z organizácií - ideálne obchod, financie, rozvoj, prevádzka, marketing, právne či PR.

2. Best security - THINK LIKE HACKER!

Termín: 12. 11. 2019 Hotel Crowne Plaza 11:30 – 12:30 h (1 hodina)
Lektor: Tomáš Vobruba, Checkpoint

Staňte sa na chvíľu hackermi a cracknite naše systémy. Kto bude najlepší, vyhráva.
Spolu s naším inžinierom sa ponoríme do temných vôd hackerov, prejdeme na druhú stranu barikády a pokúsime sa myslieť ako oni. Stačí, ak si donesiete svoj notebook.

3. The Hacker's Fingerprints

Termín: 12. 11. 2019 Hotel Crowne Plaza 13:30 – 14:30 h (1 hodina)
Lektor: Roman Čupka – produktová časť
Michal Krátky - ethica hacking, Flowmon

V priebehu workshopu zistíme, aké techniky používajú hackeri a aké digitálne stopy zanechávajú v prevádzke na sieti. Preskúmame niekoľko scenárov hackerstva a dozvieme sa niečo o spoofingu DHCP a DNS, o tom, k čomu slúži scanovanie portov alebo ako možno nahradiť dôveryhodný šifrovací certifikát tým falošným v reálnom prostredí spolu s ukážkami na ich detekciu a forénznu analýzu.

4. Úvod do malware analýzy

Termín: 12. 11. 2019 Hotel Crowne Plaza 14:30 – 17:30 h (3 hodiny)
Lektor: Ján Kotrady, Národná agentúra pre sieťové a elektronické služby (NASES)

Ako začať s analýzou škodlivého kódu, takzvaného malware? A čo je vlastne analýza škodlivého kódu a na čo by sme nemali zabudnúť? Úvodný prehľad základných postupov, teoretický úvod, ale aj praktické príklady, na ktorých účastníci získajú základný prehľad o spôsobov analýzy škodlivého kódu, statická a dynamická analýza, prehľad nástrojov, techník a princípov analýzy škodlivého kódu.

Účastníci po absolvovaní budú mať základné znalosti v oblasti analýzy škodlivého kódu a budú schopní plánovať a riadiť proces analýzy, ako aj vykonávať základné aktivity pri analýze škodlivého kódu.

Požiadavky na účastníkov: vlastný laptop s WiFi, Virtualbox alebo VMware. Základné znalosti sietí a programovania.

13.11.2019

5. Ochrana kritického klienta pod útokom

Termín: 13.11.2019 Hotel Crowne Plaza 8:30 – 9:30 (1 hodina)
Lektor: Pavol Draxler, Binary Confidence

Väčšina spoločností sa pripravuje a buduje obranu proti generickým útokom prostredníctvom zneužitia známych zraniteľností. Tieto prieniky páchajú útočníci, ktorý necielia na konkrétnu spoločnosť. Ich cieľom je byť úspešný a preniknúť kamkoľvek.
Stačia tieto opatrenia aj v prípade, kedy chce útočník cielene preniknúť do konkrétnej spoločnosti? Aké sú motivácie útočníkov? Kto sú a ako sa s nimi vysporiadavame?
Na konkrétnych prípadoch útokov proti exponovaným klientom uvedieme možnosti obrany, kde sa prepája digitálny svet s tým fyzickým, kde končí anonymita útočníkov, ktoré inštitúcie vedia pomôcť a ako sú efektívne.

Management zraniteľnosti - čo to žerie a ako mi to pomôže?
V posledných rokoch sa roztrhlo vrece s odhalenými zraniteľnosťami. Mnohé z nich sú zneužívané nielen malwarom, ale aj pri útokoch.
Ukážeme si príklady zraniteľností, ich možné zneužitie, odhaľovanie rôznymi nástrojmi, či technikami. Na konkrétnom príklade si uvedieme systém ich hodnotenia s prioritizáciou a viacerými možnosťami nápravy.

5. Zlepšite svoju viditeľnosť s open source IDS/IPS riešeniami (praktické nasadenie v podmienkach bežnej firmy do malware analýzy)

Termín: 13. 11. 2019 Hotel Crowne Plaza 9:30 – 12:30 h (3 hodiny)
Lektor: Ján Skalný, Národné centrum kybernetickej bezpečnosti SK-CERT

Od jednoduchého hľadania vzoriek, po generovanie NetFlow záznamov obohatených o informácie z aplikačných protokolov. Na tomto štvorhodinovom workshope preskúmame možnosti a obmedzenia Surikaty - moderného systému detekcie narušenia. (IDS)

Budeme sa rozprávať:
- o vnútornostiach a funkcionalite Surikaty,
- ako čítať a písať detekčné pravidlá,
- informácie, čo nám surikata môže poskytnúť,
- nástroje a techniky, ako ukladať a pracovať s výstupmi zo Surikaty,
- špecifiká a možnosti optimalizácie pre spracovávanie väčších dátových tokov,
- automatizácia nasadzovania a údržby surikaty.

Cieľová skupina: linux admini, sieťari a technicky orientovaný bezpečáci

Požiadavky na účastníkov: vlastný laptop s WiFi, SSH klient, základné znalosti networkingu, TCP/IP a Linuxu.

6. Zraniteľnosti v softvéri - útok a obrana

Termín: 13. 11. 2019 Hotel Crowne 13:30 – 17:00 h (3,5 hodiny)
Lektor: Milan Pikula, Národné centrum kybernetickej bezpečnosti SK-CERT

Praktický workshop o tom, ako fungujú bezpečnostné zraniteľnosti v softvéri a ako ich útočníci zneužívajú. Začínajúci penetrační testeri sa naučia, ako tieto zraniteľnosti odhaľovať a programátori sa naučia, ako sa im vyhnúť už počas vývoja softvéru.

Účastníci po absolvovaní budú vedieť ako uvažujú hackeri a ako predísť ich útokom

Požiadavky na účastníkov: vlastný laptop s WiFi, na ňom nainštalovaný virtuálny server s aktuálnou verziou Kali Linux optimálne 32 bit. Základné znalosti sietí a programovania.