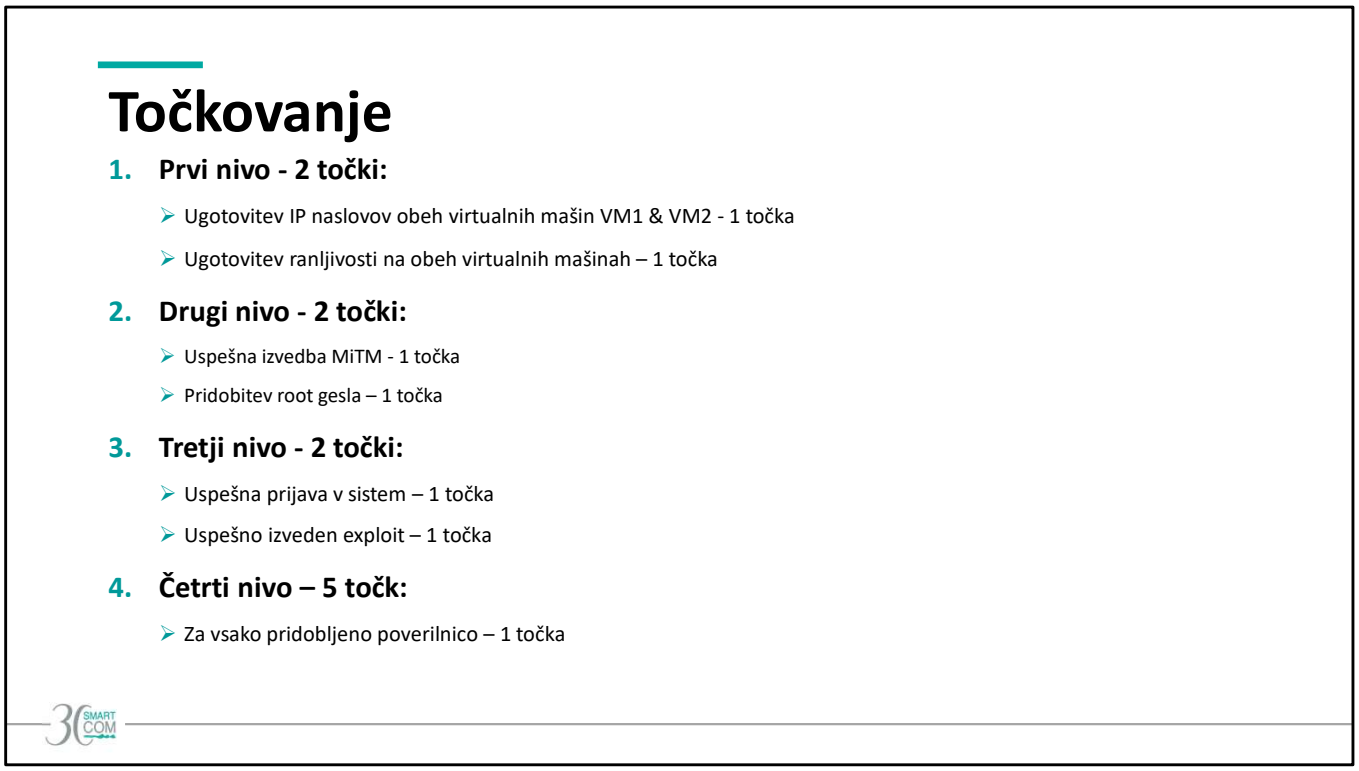

SMART COM
prihekaj si
nagrado
Raspberry Pi 400


SMART
COM
UDEJANJAMO VAŠE VIZIJE

Posameznike iz najboljše skupine NAGRADIMO!

Današnji izziv

- IZZIV = pridobitev privilegiranih gesel virtualnih strežnikov VM 1 in VM 2
- Sestavljen iz 5 nivojev
- Zmagovalna je tista skupina, ki prva odda poročilo in predstavitev (šteje se poslana dokumentacija na naslov **hekaton@smart-com.si**), ter zbere največ točk. V primeru, da nihče ne pride do konca zmaga skupina, ki zbere največ točk.
- Pri reševanju izziva lahko uporabite Jokerja, ki vam odbije 1 točko.
- **„Factory password reset / ponastavitev root gesla“ ni opcija za uspešno opravljen izziv in se šteje, da izziv ni opravljen.**



Izziv je končan, ko pridobite privilegirano root gesla za obe virtualni mašini (VM1 & VM2). Maksimalno število točk dosežete, če pridete do cilja najhitreje, postopek ustrezno dokumentirate, ugotovitve uspešno zagovarjate in ne izkoristite nobenega Jokerja. Vsa potrebna orodja s katerimi izvajate raziskovanje, preverjate ranljivosti, brišete sledi, … so naložena v virtualni mašini KALI. Vsako aktivnost, ki jo uspešno opravite na poti do cilja predstavlja določen nivo. Možnih poti do cilja je več, ključno pa je, da pri izzivu uporabite sledeče tehnike, ki predstavljajo tudi posamezne nivoje:

1. nivo: Priprava virtualnega okolja naj bo v Bridge načinu. Za namestitev dodatnih orodij v Kaliju, če jih potrebujete, je potrebno začasno nastaviti NAT način, s katerim pridobite dostop do interneta. Ugotovitev IP naslovov obeh virtualnih mašin VM1 & VM2 prinaša 1 točko. Ko izveste IP naslove nadaljujete s poizvedovanjem in raziskovanjem komunikacij obeh virtualnih mašin (VM1 & VM2). Virtualno omrežje je potrebno nastaviti tako, da boste imeli vse virtualne mašine v istem subneet-u (ista L2 domena). Nato poiščete in dokumentirate ranljivosti posameznih servisov, ki bi jih bilo možno izrabiti za napad na obeh virtualnih mašinah. To storite s pomočjo virtualne mašine z imenom KALI. Za dokumentiran seznam ranljivosti dobite še drugo točko. Za prvi nivo lahko skupaj zberete 2 točki.

2. nivo: Izvesti je potrebno mrežni penetracijski test na obe virtualni mašini VM1 & VM2 in odkriti tudi ostala uporabniška imena in gesla. V nadaljevanju izziva predlagamo, da

izvedete »man in the middle« napad med obema virtualnima mašinama VM1 & VM2. S pomočjo tega napada boste pridobili vsaj enega od obeh privilegiranih (root) gesel (HINT: root ni nujno root). Uspešna izvedba MiTM vam prinaša 1 točko, drugo točko pridobite s pridobitvijo root gesla na enem izmed strežnikov in dokumentiranjem postopka.

3. nivo: Ko pridobite privilegirano geslo na eni virtualni mašini se osredotočite na drugi strežnik. PAZI NAMIG!!! - Nekatere poverilnice so lahko enake na obeh virtualnih mašinah. Na tem koraku ste se najbrž že uspešno prijavili na drugo virtualno mašino. Po vsej verjetnosti nimate privilegiranega dostopa, zato bo potrebno izvesti »privilege escalation exploit« da pridobite »shadow« datoteko na tem sistemu. Ko pridobite »shadow« datoteko, jo je podobno razbiti in pridobiti še drugo root (HINT: root ni nujno root) geslo. Uspešna prijava v sistem prinese 1 točko, dodatno točko dobite za uspešno izveden »exploit« in pridobitev »shadow« datoteke. Za uspešno razbijanje datoteke in pridobitev ostalih gesel prinaša dodatne točke.

4 nivo: Za vsako dokumentirano poverilnico na katerem koli strežniku (uporabniško ime in pridobljeno geslo) dobite eno točko. Možnih je 5 točk.

Točkovanje – 5 nivo

1. **Oddana dokumentacija se oceni:**
   - Nepopolna/neustrezna – 0 točk
   - Pomanjkljiva/delno ustrezna – 1 točka
   - Popolna/ustrezna – 2 točki
2. **10 min predstavitev rezultatov v PPT:**
   - Neustrezen – 0 točk
   - Ustrezen – 1 točka

5 nivo: Vse postopke, ki ste jih pri izzivu uporabili je potrebno dokumentirati. Pripraviti je potrebno poročilo, ki naj vsebuje naslovnico z naštetimi ekipnimi člani, datum in kraj opravljanja izziva, kazalo, dokumentiranje vsakega koraka, ki ste ga uporabili kot uspešno akcijo pri doseganju nivojskega cilja in na koncu, vaše mnenje o izzivu. Priporočamo uporabo zajemanja ekranskih slik. Za uspešno izvedbo dokumentacije dobite 2 točki, tako kot je predstavljeno v uvodnem kriteriju. Temu sledi še priprava predstavitve s ključnimi ugotovitvami in sama izvedba predstavitve.

Let the HACK begin!