აირჩიეთ სწორი პასუხი:

* შესაძლებელია თუ არა Ethernet ტიპის ტექნოლოგიით მონაცემების უსადენოდ გადაცემა?(0.5 ქულა)
* დიახ, შესაძლებელია, რადგან ამ დროს ხდება რადიოტალღების მოდულაცია,
* **არა, შეუძლებელია, რადგან აღნიშნული ტექნოლოგია მხოლოდ სადენიან ქსელებს ემსახურება,**
* დიახ, შესაძლებელია, რადგან აღნიშნული ტექნოლოგია განიხილება, როგორც IEEE 802.11 AC ტიპის ქსელის ალტერნატივა,
* არა, შეუძლებელია, რადგან აღნიშნული ტექნოლოგია იყენებს ინფრაწითელ ტალღებს ინფორმაციის გადასაცემად.
* OSI მოდელის რომელ დონეზე მუშაობენ Firewall-ები?(0.5 ქულა)
* OSI მოდელის 3 დონეზე,
* OSI მოდელის 4 დონეზე,
* **OSI მოდელის როგორც 3, ასევე 4 დონეზე,**
* ყველა პასუხი სწორია.
* რისთვის გამოიყენება OSINT ? (0.5 ქულა)
* **OSINT გამოიყენება სამიზნე პირზე ან ორგანიზაციაზე ინფორმაციის შესაგროვებლად, საჯარო ინფორმაციის გამოყენებით.**
* OSINT გამოიყენება სამიზნე პირზე ან ორგანიზაციაზე ინფორმაციის შესაგროვებლად, როგორც საჯარო, ისე კონფიდენციალური ინფორმაციის გამოყენებით.
* OSINT გამოიყენება სამიზნე პირზე ან ორგანიზაციაზე ინფორმაციის შესაგროვებლად, მხოლოდ ნაბეჭდი პრესის გამოყენებით.
* OSINT გამოიყენება სამიზნე პირზე ან ორგანიზაციაზე ინფორმაციის შესაგროვებლად, კერძო დეტექტივის გამოყენებით.
* რა ტიპის სისუსტეა ცნობილი, როგორც “Zero day Vulnerability” ? (0.5 ქულა)
* სისუსტე, რომლის შესახებაც შეტევამდე არაფერი იყო ცნობილი, თუმცა არსებობდა მისი საწინააღმდეგო კონტროლები,
* სისუსტე, რომლის შესახებაც შეტევამდე არაფერი იყო ცნობილი, ასევე, არ არსებობდა მისი საწინააღმდეგო კონტროლები,
* სისუსტე, რომლის შესახებაც შეტევამდე არაფერი იყო ცნობილი, თუმცა არსებობდა მისი საწინააღმდეგო პროგრამული უზრუნველყოფის განახლებები(software patches),
* **სისუსტე, რომლის შესახებაც შეტევამდე არაფერი იყო ცნობილი, ასევე, არ არსებობდა მისი საწინააღმდეგო პროგრამული უზრუნველყოფის განახლებები(software patches).**
* ჩამოთვლილთაგან როგორი ტიპის ჰაკერები არსებობენ?(0.5 ქულა)
* Orange hat,
* Green hat,
* **Gray hat,**
* Silver hat.
* MAN ტიპის ქსელის მაგალითად გამოდგება: (0.5 ქულა)
* კომპიუტერული ქსელი, რომელიც აკავშირებს საქართველოსა და თურქეთს,
* კომპიუტერული ქსელი, რომელიც აკავშირებს ზესტაფონსა და თელავს,
* **კომპიუტერული ქსელი, რომელიც აკავშირებს ნაძალადევსა და ვარკეთილს,**
* კომპიუტერული ქსელი, რომელიც აკავშირებს საქართველოსა და სომხეთს.
* რომელი დებულებაა სწორი OSI მოდელის შესახებ?(0.5 ქულა)
* აღნიშნული მოდელი გამოიყენება ქსელში პაკეტების ანალიზისათვის,
* აღნიშნული მოდელი შეიქმნა ჰუბერტ ქნირშის მიერ 1978 წელს,
* **აღნიშნული მოდელით ხდება მონაცემთა ენკაპსულაცია/დეკაპსულაცია,**
* აღნიშნული მოდელის ამერიკული ანალოგი არის UDP stack.
* Ransomware ტიპის მავნე პროგრამული უზრუნველყოფა: (0.5 ქულა)
* შიფრავს მსხვერპლ კომპიუტერში ყველაფერს და დეშიფრაციის გასაღებს ანადგურებს,თუმცა გამოსასყიდს მაინც ითხოვს,
* **შიფრავს მსხვერპლ კომპიუტერში ყველაფერს, დეშიფრაციის გასაღებს შემტევ მხარეს უგზავნის და ლოკალურ გასაღებს ანადგურებს, ასევე, ითხოვს გამოსასყიდს,**
* შიფრავს მსხვერპლ კომპიუტერში ყველაფერს, დეშიფრაციის გასაღებს შემტევ მხარეს უგზავნის და ლოკალურ გასაღებს შიფრავს, თუმცა არ ანადგურებს. ასევე, ითხოვს გამოსასყიდს,
* არც ერთი პასუხი არ არის სწორი.

უპასუხეთ შეკითხვებს:

* რა არის და რისთვის გვჭირდება AAA კონცეფცია? ჩამოთვალეთ მისი სამივე შემადგენელი ნაწილი, მოკლედ აღწერეთ მათი არსი და მნიშვნელობა.(2 ქულა)

AAA – Authentication, Authorization,Accounting კონცეფცია წარმოადგენს მიდგომას, რომლის თანახმადაც ორგანიზაციაში უსაფრთხოებისათვის გვჭირდება მომხმარებლების:

ავთენთიფიკაცია - დადასტურება იმისა, რომ ნამდვილად ლეგიტიმურ თანამშრომელთან/კონტრაქტორთან გვაქვს საქმე,

ავტორიზაცია - ავთენტური მომხმარებლისათვის სხვადასხვა როლებისა თუ უფლებების მინიჭებას მოიცავს,

ანგარიშგება - მუდმივი მონიტორინგი იმისა, თუ რას აკეთებს მომხმარებელი.

* ვინ შეიძლება იყოს Malicious Insider, რის გაკეთება შეუძლია და როგორ შეიძლება ასეთი ტიპის საფრთხესთან გამკლავება ორგანიზაციაში? მოიყვანეთ არგუმენტები თქვენი პოზიციის დასადასტურებლად. ( 2 ქულა)

Malicious Insider - ეს არის თანამშრომელი, რომელიც პოლიტიკური, ეკონომიკური, რელიგიური ან ნებისმიერი სხვა მოტივით მოქმედებს ორგანიზაციის წინააღმდეგ, როგორც წესი, საბოტაჟის გზით. მაგალითად, ედვარდ სნოუდენი იყო ინსაიდერი CIA შემთხვევაში: <https://www.infosecurity-magazine.com/magazine-features/top-ten-insider-threat/>

დავალება 1 (6 ქულა)

დავუშვათ, გვაქვს კომპანია “X trading Limited”, რომელსაც სჭირდება ქსელური მონიტორინგის გამარტივებისათვის SIEM-ის შესყიდვა. კომპანიას აქვს შემდეგი სახის ინვენტარი:

3 ცალი მარშრუტიზატორი(Router) - თითოეული აგენერირებს 850 Syslog ტიპის შეტყობინებას წამში.

5 ცალი კომუტატორი(Switch) - თითოეული მათგანი აგენერირებს 500 Syslog ტიპის შეტყობინებას წამში.

4 ცალი HP-ის წარმოების სერვერი, რომელიც არ აგენერირებს Syslog ტიპის შეტყობინებას, თუმცა გვაძლევს 250 შეტყობინებას წამში.

4 ცალი IBM წარმოების სერვერი, თითოეული აგენერირებს 300 Syslog ტიპის შეტყობინებას წამში.

ჩათვალეთ, რომ ერთი Syslog არის ერთი EPS, ხოლო ერთი Smart Connector ნებისმიერი სახის შეტყობინებას გარდაქმნის ამავე ოდენობის Syslog ტიპის შეტყობინებად. ერთი EPS-ის ფასი გახლავთ 2 ლარი, ხოლო ერთი Smart Connector-ის 1500 ლარი.

ამოხსნა:

SIEM - ის ღირებულება გახლავთ EPS-ების ღირებულებისა და Smart Connector-ების ღირებულების ჯამი, გამომდინარე აქედან, დავთვალოთ თითოეული ცალკ-ცალკე და შემდგომ შევკრიბოთ.

რადგან ამოცანა გვეუბნება, რომ ერთი Syslog არის ერთი EPS, 3 ცალი მარშრუტიზატორი(Router) დააგენერირებს 850 \* 3 = 2550 EPS-ს.

5 ცალი კომუტატორის შემთხვევაში(Switch) გვექნება 500 \* 5 = 2500 EPS,

HP წარმოების სერვერის შემთხვევაში, რადგან Syslog არ გვაქვს, დაგვჭირდება Smart Connector იმისთვის, რომ ჩანაწერები გადავაქციოთ Syslog-ებად. სულ სერვერი 4 ცალია, ამიტომ დაგვჭირდება 4 Smart Connector, მათი ჯამური ღირებულება იქნება 1500 \* 4 = 6000 ლარი. კონექტორების დაყენების შემდეგ თითოეული სერვერი მოგვცემს 250 Syslog-ს, რაც სულ იქნება 250\*4 = 1000 EPS ჯამურად.

IBM წარმოების სერვერის შემთხვევაში, სულ გვექნება 300 \* 4 = 1200 EPS.

მაშასადამე, სულ გვაქვს: 2550 + 2500 + 1000 + 1200 = 7250 EPS, ასევე, 4 ცალი Smart Connector.

სულ იქნება (7250\*2) + (4\*1500) = 20500 ლარი

დავალება 2 (6 ქულა)

კომპანია „Ernest & Sons AG”-ის შიდა ქსელზე განხორციელდა კიბერშეტევა, რომლის დროსაც რამდენიმე საათის განმავლობაში კომპანიის ვებ-სერვერი იყო გათიშული, დიდი რაოდენობით HTTPS Request-ების მიღების გამო, რომელთა ჯამურმა მოცულობამ მიაღწია 4 ტბ/წმ-ს(ტერაბაიტი წამში). სერვისის აღდგენის შემდეგ კომპანიის უსაფრთხოების სპეციალისტებმა შეამჩნიეს, რომ ინტრანეტში დაახლოებით 4 ჯერ გაეზარდათ UDP პროტოკოლის წილი ქსელურ ტრეფიკში, რაც ნიშნავდა იმას, რომ გამოიყენებოდა სტრიმინგ-სერვისები. 2 კვირიანი ძიების შემდეგ სპეციალისტებმა დაადგინეს, რომ სტრიმინგის პროცესს აწარმოებდა სერვისი dllexecute2germany.exe. აღნიშნული სერვისი აკონტროლებდა კლავიატურას და თუ მომხმარებელი შეიყვანდა სიტყვებს: „war”, “Oil”, “Sanctions” ავტომატურად რთავდა კამერას, მიკროფონს და მომხმარებელს უთვალთვალებდა 4 საათის მანძილზე, შემდგომ კი კომპანიის ვებ-სერვერის გამოყენებით აღნიშნულ ჩანაწერებს აგზავნიდა IP მისამართზე 12.12.10.10.

კომპანიის უსაფრთხოების სპეციალისტებმა მოახერხეს dllexecute2germany.exe სერვისის ბლოკირება ყველა ინფიცირებულ კომპიუტერზე, თუმცა მათ მოხსენების დაწერისათვის სჭირდებათ დახმარება, გთხოვთ დაუზუსტეთ მათ, თუ რა ტიპის კიბერშეტევა მოხდა მათ ვებ-სერვერზე, როგორ შეიძლება მოხვედრილიყო მავნე სერვისი dllexecute2germany.exe. მათი კომპანიის კომპიუტერებზე. ასევე, დააზუსტეთ თუ რა ტიპის მავნე პროგრამულ უზრუნველყოფას წარმოადგენდა აღნიშნული dllexecute2germany.exe. თქვენი დებულებები და მოსაზრებები აუცილებლად გაამყარეთ არგუმენტებით.

აუცილებლად უნდა ითქვას, რომ კოპმანიის წინააღმდეგ რეალურად განხორციელდა 2 ტიპის კიბერშეტევა. პირველ რიგში შემტევმა მხარემ განახორციელა მასშტაბური DoS ან DDoS შეტევა, რამაც გადატვირთა კომპანიის შიდა ქსელში არსებული დაცვის სისტემები და დიდი ალბათობით, შანსი მისცა შემტევ მხარეს გაევრცელებინა Spyware ტიპის მავნე კოდი, რომელიც თავის მხრივ უთვალთვალებდა ინფიცირებულ კომპიუტერებს, აკონტროლებდა რა კლავიატურას შემდეგ სიტყვებზე: „war”, “Oil”, “Sanctions”.