TEST LA SECURITATE CIBERNETICA (Februarie 2023)

* Obligatorii

1

Nume, prenume * (1 punct)

[REDACTED]

2

Care dintre următoarele reprezintă unul dintre avantajele analizei de memorie: * (0.5 puncte)

- (•) Bypass packers
- ( ) Extragere fisiere prefetch
- ( ) Recuperare fișierele șterse
- ( ) Reconstructie fișierele

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

Selectați care din urmatorii vectori definesc o amenintare * (0.5 puncte)

- (●) Capabilitate, Oportunitate si Scop
- ( ) Risk, oportunitate si intentie
- ( ) Capabilitate, probabilitate si impact
- ( ) Vulnerabilitate, probabilitate si scop

4

Selectați 1 principiu de bază pentru asigurarea securității INFOSEC * (0.5 puncte)

- ( ) Separation of environments
- ( ) Due cost
- ( ) Access control list
- (●) Least privilege

5

Alegeti varianta corespunzătoare principiului care asigură prezența datelor la locul, în timpul şi forma potrivită * (0.5 puncte)

- ( ) Confidențialitatea
- (●) Disponibilitatea
- ( ) Integritatea
- ( ) Autenticitatea şi non-repudierea

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

Intre obiectivele securității informatice responsabilă cu păstrarea secretului datelor este * (0.5 puncte)

- (●) Confidențialitatea
- ( ) Disponibilitatea
- ( ) Integritatea
- ( ) Autenticitatea şi non-repudierea

7

Selectați ce tip de control este un firewall * (0.5 puncte)

- ( ) Administrativ
- (●) Tehnic
- ( ) Operational
- ( ) Nu este un control

8

Enumerați în ordinea corectă fazele Kill chain * (0.5 puncte)

- ( ) Reconnaissance, Delivery, Weaponization, Exploitation, Installation, Command and control, Action on objectives
- (●) Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and control, Action on objectives
- ( ) Reconnaissance, Delivery, Weaponization, Installation, Exploitation, Command and control, Action on objectives
- ( ) Reconnaissance, Weaponization, Exploitation, Delivery, Installation, Command and control, Action on objectives

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

Selectați ce conține fișierul Prefetch din cadrul sistemului de operare Windows: * (0.5 puncte)

- ○ numele documentelor rulate pe un SIC;
- ○ lista de DLL utilizate de fiecare document ;
- ◉ numărul de execuții al fiecărui executabil in parte;
- ○ un timestamp care indica data la care executabilul a fost rulat prima data.

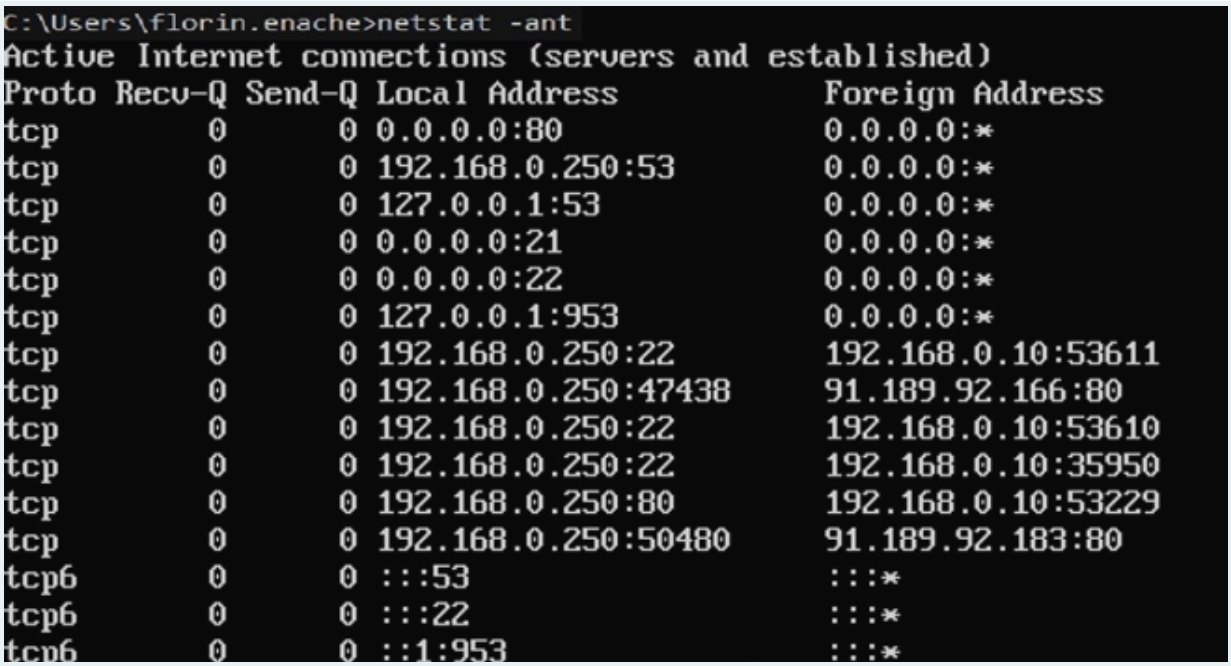
10

Ce reprezintă semnătura unui fișier (magic number)? * (0.5 puncte)

- ○ Bytes din cadrul unui fișier utilizați pentru a identifica formatul fișierului, plasați la finalul fișierului
- ○ Bytes din cadrul unui fișier utilizați pentru a identifica formatul fișierului, plasați în conținutul fișierului
- ◉ Bytes din cadrul unui fișier utilizați pentru a identifica forma fișierului, plasați la începutul fișierului

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

1. Analizati imaginea de mai jos si incercuiti serviciile (server applications) aferente porturilor descoperite. * (0.5 puncte)



```
C:\Users\florin.enache>netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 0.0.0.0:80              0.0.0.0:*
tcp        0      0 192.168.0.250:53        0.0.0.0:*
tcp        0      0 127.0.0.1:53            0.0.0.0:*
tcp        0      0 0.0.0.0:21              0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp        0      0 127.0.0.1:953           0.0.0.0:*
tcp        0      0 192.168.0.250:22        192.168.0.10:53611
tcp        0      0 192.168.0.250:47438     91.189.92.166:80
tcp        0      0 192.168.0.250:22        192.168.0.10:53610
tcp        0      0 192.168.0.250:22        192.168.0.10:35950
tcp        0      0 192.168.0.250:80        192.168.0.10:53229
tcp        0      0 192.168.0.250:50480     91.189.92.183:80
tcp6       0      0 :::53                   :::*
tcp6       0      0 :::22                   :::*
tcp6       0      0 ::1:953                 :::*
```

- [x] HTTP
- [ ] DHCP
- [x] DNS
- [ ] TELNET
- [ ] SNMTP
- [ ] IMAP
- [x] FTP
- [ ]

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

adevărat (A) sau fals (F): Securitate cibernetică - acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice apărării naționale * (0.5 puncte)

- ○ ADEVARAT
- ◉ FALS

13

Enumerați în ordinea corectă volatilitatea datelor in procesul de investigare a probelor digitale * (0.5 puncte)

- ○ Physical configuration, Archival media, network topology, Temporary file systems, Disk, Remote logging data, Registers, cache, Routing table, ARP cache, process table, memory;
- ◉ Registers, cache, Routing table, ARP cache, process table, memory, Temporary file systems, Disk, Remote logging data, Physical configuration, network topology, Archival media;
- ○ Physical configuration, network topology, Registers, cache, Routing table, ARP cache, process table, memory, Temporary file systems, Disk, Remote logging data, Archival media;
- ○ ARP cache, process table, Registers, cache, Routing table, memory, Archival media,Temporary file systems, Disk, Remote logging data, Physical configuration, network topology.

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

Care dintre cele de mai jos nu este o strategie de diminuare a riscului * (0.5 puncte)

- ○ Transferul riscului
- ○ Acceptarea riscului
- ◉ Evaluarea riscului
- ○ Evitarea riscului

15

O schimbare observată în comportamentul (normal) unui SIC, mediu, proces, flux de lucru sau persoană reprezintă? * (0.5 puncte)

- ◉ Un eveniment
- ○ O alertă
- ○ Un incident

16

Dacă un utilizator primește mesaje despre metode specifice utilizate în cadrul băncii ING pentru obținerea de credite imobiliare, acesta este un exemplu de : * (0.5 puncte)

- ○ Spear Phishing
- ○ Hoaxes
- ○ Spoofing
- ◉ Spam

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

Care sunt clasele de jurnale de log existente in sistemele de operare Windows, pe care un analist le-ar putea utiliza pe timpul investigării uni incident de securitate cibernetică? * (0.5 puncte)

- ○ Hardware Events, isaAgentLog, Key Management Services
- ◉ Application, Security, System
- ○ System, Security, Microsoft

18

Selectați o metodă de asigurare a persistenței în cazul unei infecții pe sistemul de operare Windows * (0.5 puncte)

- ○ Fișiere stocare în directorul TEMP
- ○ Task-uri (Schedule task) create de utilizator
- ◉ Registry
- ○ Shortcut Hijacking

Dublați acest formular pentru a-l utiliza ca pe un formular propriu.

In care dintre fazele de răspuns la incidente cibernetice se realizează limitarea extinderii infecției cauzată de execuția unui virus? * (0.5 puncte)

- ○ Preparation
- ○ Identification
- ◉ Containment
- ○ Eradication
- ○ Recovery
- ○ Lessons learned