Wykrywanie ataków sieciowych - lab 7

Created	@April 16, 2022 5:01 PM
Class	WAS

Wykrywanie ataków sieciowych - lab 6

Zadanie 1

Format CVD (ClamAV Virus Database) jest formatem plików używanym przez `ClamAV`. Pliki te zawierają definicje wirusów dla zaktualizowania listy rozpoznawalnych wirusów w `ClamAV`. Popularne pliki CVD to `daily.cvd` oraz `main.cvd`.

Najwygodniejszym sposobem na dodawanie nowych sygnatur jest wykorzystanie sum kontrolnych funkcji skrótu. Można je utworzyć za pomocą narzędzia `sigtool` z opcją `--md5`, np.

```
sigtool --md5 test.exe > test.hdb
```

Zadanie 2

Najbardziej polecanym sposobem na przetestowanie programu `ClamAV` jest stworzenie pliku zawierającego ciąg znaków wykrywany przez każdy skaner wirusów jako wirus, niezawierający jednak prawdziwego wirusa:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Wyjście z programu `clamscan` po wywołaniu go na tym pliku wygląda następująco:

```
┌──(kali㉿kali)-[~]
└─$ clamscan -v clamav-testfile.txt
Scanning /home/kali/clamav-testfile.txt
/home/kali/clamav-testfile.txt: Eicar-Signature FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8610523
Engine version: 0.103.5
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 19.292 sec (0 m 19 s)
Start Date: 2022:04:16 15:04:03
End Date:   2022:04:16 15:04:22
```

Zadanie 4

W pliku `/var/lib/suricata/rules/local.rules` należy dodać własną regułę, np.

```
alert http any any -> any any (msg:"Black list checksum match and extract MD5"; filemd5:fileextraction-chksum.list; filestore; sid:28;
```

Za każdym razem po przesłaniu pliku z funkcja skrótu, która znajduje się na czarnej liście wywołany zostanie alarm.

Zadanie 5

Uruchomiono pasywny skan na domenie http://201.191.205.60/dvwa/, gdzie pod publicznym adresem dostępna jest aplikacja Damn Vulnerable Web Application. Z ciekawszych wyników zostało zwrócone 235 wyników po wywołaniu `db query` na tabeli `contacts`.

```
[recon-ng][dvwa][resolve] > spool start /tmp/names
[*] Spooling output to '/tmp/names'.
[recon-ng][dvwa][resolve] > db query SELECT DISTINCT last_name,first_name,title FROM contacts WHERE last_name IS NOT NULL ORDER BY las
```

```
+-----------------------------------------------------------------------------+
|      last_name       |  first_name |                title                 |
+-----------------------------------------------------------------------------+
| Adlakhiya            | Arpan       | Graduate Engineering Trainee        |
| Allen                | Bayden      | Penetration Tester                  |
| Alves                | Anderson    | SysAdmin                            |
| Ameyaw               | Justice     |                                     |
| Anbari               | Omar        |                                     |
| Annavajjula          | Dinesh      |                                     |
| Avhad                | Pooja       | Security Engineer II                |
| Avulov               | Daniel      | Fullstack Academy                   |
| Awan                 | Rashid      | Local Web Projects                  |
| Bachu                | Sushmitha   | Architect                           |
| Bagga                | Harsimar    |                                     |
| Bagheri              | Somayeh     | Technical Officer                   |
| Bajis                | Jason       | Assistant Production Manager        |
| Banks                | Stuart      | anaerobic digestion operative       |
| Bathla               | Akshay      | Security Ops Analyst II             |
| Bava                 | Anmol       | Technology Consultant Cyber         |
| Bedi                 | Vishal      | Offensive Security Engineer         |
| Bennett              | Daniel      | Senior Systems Analyst              |
| Bhoir                | Vaibhav     | Ethical Hacker                      |
| Biglari              | Sara        | Team Lead Cyber Security Analyst    |
| Bilavin              | Shafeer     |                                     |
| Birdine              | Carey       | Security Operations Center Analyst  |
| Bonnette             | Jeremy      |                                     |
| Bounouar             | Celia       |                                     |
| Bowman               | Richard     | Quantity Surveyor                   |
| Brisco               | Katie       |                                     |
| Byford               | James       |                                     |
| C Gonzales Jr        | Juan        | Senior Network Systems Analyst      |
| Carroll              | Matthew     |                                     |
| Cashmore             | Huw         | Estimator                           |
| Castillo             | Len         |                                     |
| Ch                   | Nina        |                                     |
| Chafkaoui            | Yassine     |                                     |
| Chakraborty          | Arindam     | Risk Management Advisor             |
| Chanchal             | Raj         |                                     |
| Chandratre           | Samruddhi   | Wireless Network Engineer           |
| Chaudhary            | Shubham     |                                     |
| Chhabra              | Lovejot     | SYSTEM SECURITY AUDITOR             |
| Crawshaw             | Gary        | Field Operations Excellence Manager |
| Dave                 | Parv        | Adani Institute of Infrastructure   |
| Davies               | Emma        | Project Manager                     |
| Delgado              | Jhon        |                                     |
| Dewhurst             | Ryan        |                                     |
| Dhagadi              | Mahesh      | Associate Consultant                |
| Dhaliwal             | Khem        |                                     |
| Dhar                 | Manisa      | Associate                           |
| Dhiman               | Aman        |                                     |
| Duggal               | Abhinav     | Software Engineer                   |
| Duller               | Preston     | General Associate                   |
| Edwards              | Jonathon    | System Analyst                      |
| Eleie                | Abdi        |                                     |
| Ermakov              | Kirill      | Chief Security Officer              |
| Evangelio            | Lawrence    | Security Engineer                   |
| Everingham           | Guy         | Associate Consultant                |
| Fairbairn            | Trudi       |                                     |
| Fancher              | Angelique   |                                     |
| Faragher             | Steve       | Remote Site Services IT Analyst     |
| Farmer               | Levi        | Senior Guest Advisor                |
| Fernandes            | Bruna       |                                     |
| Francisco            | Austin      |                                     |
| Franks               | Elizabeth   |                                     |
| Gailey               | Johnny      | Owner                               |
| Galgat               | Abhinav     |                                     |
| Gandhi               | Vivek       |                                     |
| Gangjiyot            | Ashok       |                                     |
| Gaur                 | Yatharth    |                                     |
| Gephart              | Steven      |                                     |
| Goddard              | Jason       | Regulations                         |
| Gonzalez             | Joe         | Greater Chicago Area                |
| Grant                | Tiffany     | Registered Dental Hygienist         |
| Gupta                | Ajit        | Company Owner                       |
| Gupta                | Shivam      |                                     |
| Gurjar               | Niharika    |                                     |
| Hajiali              | Abdillahi   |                                     |
| Hames Tech IOSH MCGI | Alan        | SHEF Auditor                        |
| Hannaby              | Sue         | Work Flow Management Technician     |
| Harry                | Aalokit     | Ethical Hacker                      |
| Hatton               | Tomos       |                                     |
| Hayes                | Chris       | Project Manager                     |
| Hernandez            | Demetrio    |                                     |
| Herrera              | Yerko       |                                     |
| Hidayat              | Dhody       | DevOps Engineer                     |
| Highberg             | Mickey      |                                     |
```

```
| Hughes              | Daniel      |                                  |
| Hukkeri             | Afrin       | Software Engineer                |
| Iglesias            | Ademir      |                                  |
| Iwen                | Christopher |                                  |
| Jarraya             | Molka       | SI Administrator                 |
| Jasbi               | Alireza     | IT Manager                       |
| Jaubert             | Vincent     | Pentester                        |
| Jones               | David       | Leakage Technician               |
| Jones               | Mark        | Developer Services ICS Project   |
| Jones               | Matt        | Project Manager                  |
| Jones               | Phil        | Senior Project Manager           |
| Karpe               | Nikhil      | Technical Consultant             |
| Kassabi             | Othmane     |                                  |
| Kaur                | Pardeep     | Portioning Team Member           |
| Kedia               | Mukund      | Cyber Security Analyst           |
| Keny                | Nirav       |                                  |
| Khanna              | Abhinav     |                                  |
| Khanna              | Jitesh      | Cyber Security Analyst           |
| Kheni               | Urvashi     | Software Engineer                |
| Kim                 | Nathaniel   | Supervisor                       |
| Kotaidis            | Vasileios   | Cyber Security Specialist -      |
| Kowal               | Penny       |                                  |
| Kumar               | Ashish      |                                  |
| Kumar               | Avijit      | Information Security Analyst     |
| Kumar               | Himanshu    |                                  |
| Kumar               | Siddharth   |                                  |
| Kumar               | Sumit       | QA Engineer                      |
| Kumar               | Vishal      |                                  |
| Kuratti             | Vishal      | System Engineer                  |
| Kuriakose           | Abhilash    | Threat Analyst                   |
| Kyoung              | Haeri       | Rochester Institute of Technology|
| Lahtinen            | Tuomo       |                                  |
| Laszkiewicz         | David       | Digital Marketing Co-ordinator   |
| Leal da Silva       | Eliane      |                                  |
| Lemarechal          | Kris        | Senior Server Engineer           |
| Lohore              | DJahi       |                                  |
| Louali              | Farouk      |                                  |
| Machhour            | Elmostafa   |                                  |
| Malki               | Anas        |                                  |
| Martinez            | Andy        | Senior Tech Associate            |
| Mehta               | Nikhar      | Security Software Engineer       |
| Mendiratta          | Roy         |                                  |
| Merner              | Patrick     | Junior Developer                 |
| Miranda             | Ronaldo     |                                  |
| Mmonu               | Ugochukwu   | Managed Care Specialist          |
| Mohamadi            | Amir        |                                  |
| Mohamed             | Amad        |                                  |
| Mohanty             | Sukanya     |                                  |
| Mokni               | Souha       | Cyber Security Engineer          |
| Monasterial         | Carlo       | IT Specialist                    |
| Moore               | Rachel      | DIRECTOR                         |
| Morrison            | Duncan      |                                  |
| Moule               | Steve       | Senior Project Manager           |
| Mounir              | Fairouz     |                                  |
| Moussaoui           | Badr        |                                  |
| Neves               | Mauricio    | Cyber Security Analyst           |
| Nickerson           | Rachel      | Customer Care Professional       |
| Nizam               | Nihal       |                                  |
| Obeahon             | Oti         | Cloud Compliance Analyst         |
| Owen                | Steffan     | Project Manager                  |
| Pacheco             | Michael     | Technology Associate             |
| Pan                 | Walter      | Senior Airport Technician        |
| Pandey              | Abhishek    | Analyst                          |
| Panorios            | Michael     | Junior Software Developer        |
| Patel               | Nirmohi     |                                  |
| Patton              | Tyler       | Network Analyst                  |
| Peres               | Yoan        | Cyber Security Consultant        |
| Petrick             | Stephen     |                                  |
| Phdwork             | Sonia       |                                  |
| Pichotier           | Mickael     | Ressource humaine                |
| Pinches             | Gemma       | Health and Safety Administrator  |
| Pole                | Mrudulla    | Analyst                          |
| Punjani             | Anuj        |                                  |
| Quispe              | Alexander   | CyberSecurity Consultant         |
| Rached              | Roger       | Cyber Practitioner               |
| Rajput              | Ankur       | Training and Enablement Manager  |
| Rajwania            | Laksh       | Information Security Consultant  |
| Rao                 | Shruti      | Senior Software Engineer         |
| Rastogi             | Kavita      | Developer                        |
| Ravichandran        | Divakar     | Programmer Analyst Trainee       |
| Reef                | Giorgi      | Rail Engineer                    |
| Rees-slawson        | Cathryn     |                                  |
| Roberts             | Darren      |                                  |
| Roberts             | Gareth      | Control Room Operator            |
| Roblin              | Huw         | Asset Manager                    |
| Rodriguez           | Reece       | Security Engineer                |
| Romero              | Jason       | Technical Account Manager        |
```

```
  | Rowland              | Michael     | Knights Construction Group Ltd      |
  | Roy                  | Andrew      |                                     |
  | Rybak                | Tomasz      | Self Taught Pen Testing Enthusiast  |
  | SAHA                 | Pramesh     | Scholar Trainee                     |
  | Sahu                 | Nitesh      | Business Owner                      |
  | Sahu                 | Shrikant    |                                     |
  | Saini                | Abhishek    |                                     |
  | Salazar              | Johanna     |                                     |
  | Sathe                | Roopa       |                                     |
  | Saunderson           | David       | Project Manager                     |
  | Saxena               | Money       | Information Security Analyst        |
  | Sayers               | Kiera       |                                     |
  | Schofield            | Dave        | General Manager                     |
  | Schoof               | Lane        | Cyber Security Analyst              |
  | Selvakumar           | Anjana      |                                     |
  | Shaabani             | Abolfazl    | Developer                           |
  | Shafer               | Syd         |                                     |
  | Shaikh               | Ebad        | Ethical Hacker                      |
  | Sharma               | Anushka     | Client Services Engineer            |
  | Sharma               | Rupali      | Information Security Engineer       |
  | Sheahan              | Zac         | Telemetry Technician                |
  | Sherkhane            | Snehal      |                                     |
  | Shete                | Ayur        | Ethical Hacker                      |
  | Shevgaonkar          | Mansi       |                                     |
  | Shinde               | Gajanan     |                                     |
  | Silverstein          | Michael     | Post Production Engineer            |
  | Singano              | Enoch       |                                     |
  | Singh                | Jasneet     | Data Analyst                        |
  | Singh                | Lokesh      | Royal Bank of Scotland Business     |
  | Singh                | Priya       |                                     |
  | Sivakumar            | Suresh      |                                     |
  | Smith                | Chris       |                                     |
  | Solarczyk            | Piotr       |                                     |
  | Sprague              | Jason       |                                     |
  | Srivastava           | Ayush       | Associate Consultant                |
  | Starling             | Kevin       | Non Executive Chairman              |
  | Steward              | Kaden       | Technical Operations Analyst        |
  | Sulkamo              | Ville       | Senior Integration Engineer         |
  | Sun                  | Jiangfeng   |                                     |
  | Tagliafierro         | Alessandro  |                                     |
  | Taleb                | Anne        | Sales Manager                       |
  | Tamarapalli          | Karthik     | Team Lead                           |
  | Tan                  | Andrew      | Auston Inst                         |
  | Tapiawala            | Parth       | Servic Desk Analyst                 |
  | Tayoro               | Hugo        | DGA                                 |
  | Tesh                 | Tame        | IT Specialist                       |
  | Thi Hong Phuc        | Nguyen      |                                     |
  | Tripathi             | Fagun       |                                     |
  | Twydell              | Oliver      |                                     |
  | Verner               | Trametra    |                                     |
  | Walia                | Bhavnoor    | Network Engineer                    |
  | Wall                 | Casey       | Security Services Northwest         |
  | Wanguba              | Evans       |                                     |
  | Wedley               | Leigh       | Managed Services Analyst            |
  | Weerasinghe          | Sithum      | Associate Security Analyst          |
  | Wilga                | Corey       | Security Analyst                    |
  | Williams             | Brad        | Call Center Representative          |
  | Williams             | Keith       |                                     |
  | Williams             | Rapheal     | Simulation Lab Software Engineer    |
  | Yadav                | Dharam      |                                     |
  | Yadav                | Samarjeet   | Cyber Security Analyst              |
  | Yap                  | Jerome      | Saudi Electricity Company           |
  | Zaigum               | Asad        |                                     |
  | Zeh                  | Christopher | Network Analyst                     |
  | katam                | Sai         | Security Analyst                    |
  +----------------------------------------------------------------------------+

[*] 235 rows returned
```

Komplety log zapisany jest w pliku `discover-log.txt`.