

კიბერუსაფრთხოება

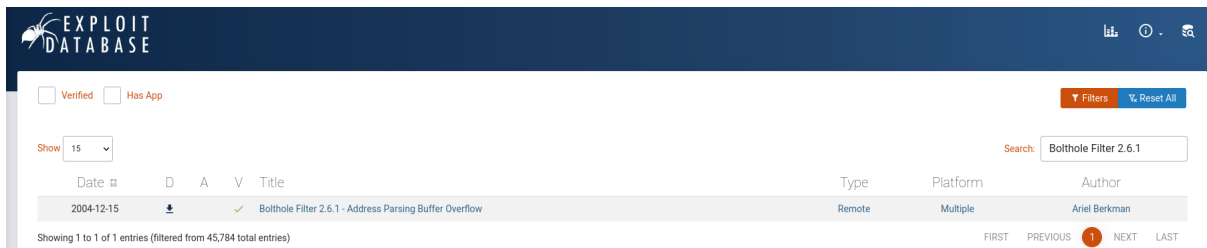
პრაქტიკული დავალება N1:

1. Exploit-db-ის გამოყენებით იპოვნეთ ინფორმაცია და დაწერეთ რეპორტი **Bolthole Filter 2.6.1**:

1. ექსპლოიტის სახელი.
2. მოწყვლადობის მოკლე აღწერა და მისი პოტენციური გავლენა.
3. პროგრამული უზრუნველყოფის ვერსია.
4. გამოვლენის თარიღი და Exploit-DB-ში მისი დამატების თარიღი.
5. ექსპლოიტის ავტორის სახელი.

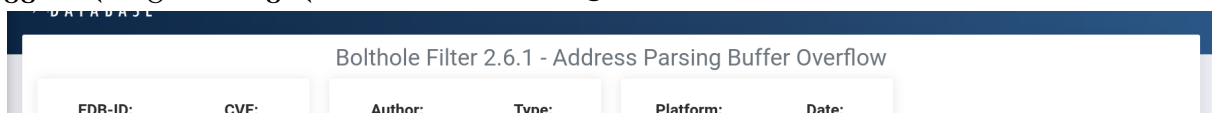
ამოხსნა:

შევდიართ exploit-db.com ზე, ზემოთ მარჯვნივ სერჩში ვწერთ სახელს რომელიც იქნება მოცემული, ამ შემთხვევაში **Bolthole Filter 2.6.1**:

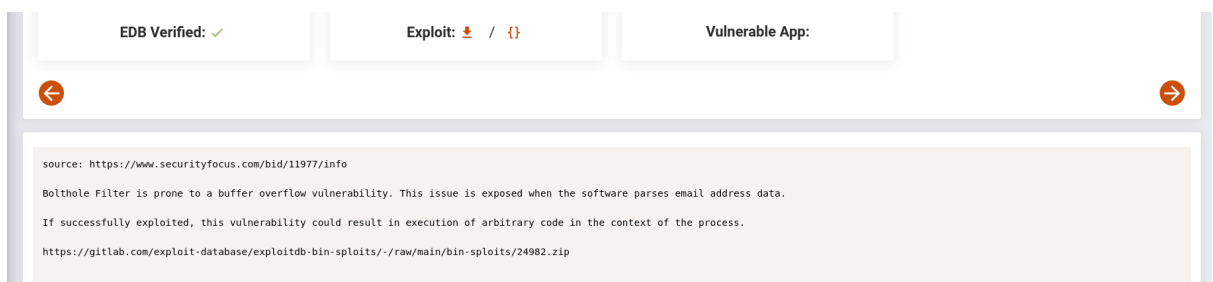


იქნება ერთი შედეგი, ვხსნით მაგას.

1. ექსპლოიტის სახელი - Address Parsing Buffer Overflow



2. მოწყვლადობის მოკლე აღწერა და მისი პოტენციური გავლენა. - ქვემოთ აღწერაში უწერია ყველას და უნდა გადმოთარგმნო უბრალოდ



Bolthole Filter-ს აქვს Buffer Overflow-ს სისუსტე.ეს სისუსტე აქვს მეილების გაპარსვის დროს. წარმატებულად გამოყენებული ექსპლოიტის შემთხვევაში შემტევს შეუძლია თავისი მავნე კოდის გაშვება.

3. პროგრამული უზრუნველყოფის ვერსია. - ეს სახელშივე წერია, Bolthole Filter 2.6.1
4. გამოვლენის თარიღი და Exploit-DB-ში მისი დამატების თარიღი -
Date: ველში წერია სახელის ქვემოთ.

Address Parsing Buffer Overflow

Platform:

MULTIPLE

Date:

2004-12-15

Vulnerable App:

2004-12-15

5. ექსპლოიტის ავტორის სახელი. - შუაში წერია პირდაპირ **Author** -
ARIEL BERKMAN

Bolthole Filter 2.6.1 - Address I

Author:

ARIEL BERKMAN

Type:

REMOTE

Exploit:  / 

პირველი პრაქტიკული მარტო ესაა, უნდა დასერჩო ერთი რაღაც და ამოიწერო იქიდან, სხვებიც იგვევება უბრალოდ სახელებია შეცვლილი მარტივად იბამ გადმოთარგმნა მოგიწევს უბრალოდ აღწერის. თუ აღწერაში რამეს ვერ გაიგებ დაგუგლავ კონკრეტულ შეტევაზე რას ნიშნავს და ეგეც შეგიძლია მიახამრო მაგრამ არარის საჭირო.

პრაქტიკული დავალება N2:

1. Google dorking-ის მეშვეობით მოიძიეთ შემდეგი ინფორმაცია და დაწერეთ რეპორტი:

- PDF დოკუმენტები, რომლებიც დაკავშირებულია „გარემოს დაცვასთან“
 - იპოვეთ ინფორმაცია ვიკიპედიას ვებ-საიტის შესახებ.
 - იპოვეთ ვებ გვერდები URL-ში “Download-ით”;
 - იპოვეთ ვებ გვერდები სათაურში „theconomy”;
1. PDF დოკუმენტები, რომლებიც დაკავშირებულია „გარემოს დაცვასთან“ - pdf დოკუმენტების მოსაძებნად გუგლში შემდეგი ღორკია - filetype:pdf და მარტო pdf ებს ამოგიგდებს, გვერდზე უბრალოდ გარემოს დაცვას მიუწერ და ეგარის. პირველი

The screenshot shows a Google search interface with the query "filetype:pdf \"გარემოს დაცვა\"". Below the search bar, there are tabs for "სურათები", "ვიდეოები", "ვაჭრობა", "Maps", "წიგნები", "ავიაბილეთები", and "ფინანსები". The search results show 25,000 results in 0.23 seconds. The first result is from "საქართველოს ახალგაზრდა იურისტთა ასოციაცია" with the URL "https://gyla.ge › files › GetFileAttachment-14". The title is "გარემოს დაცვა და ადამიანის უფლებები" and it is dated 27 აგვ. 2021. The second result is from "სსიპ \"საქართველოს საკანონმდებლო მაცნე\"" with the URL "https://matsne.gov.ge › download › pdf". The title is "საქართველოს კანონი გარემოს დაცვის შესახებ" and it is dated 27 აგვ. 2021.

2. იპოვეთ ინფორმაცია ვიკიპედიას ვებ-საიტის შესახებ.
- თუ გვინდა საიტის შესახებ ინფორმაციის მოძებნა ვწერთ info: და საიტს, ამშემთხვევაში info:wikipedia.org ან ვიკიპედიას მაგივრად რაციქნება იმას ჩაწერდა ეგარის, მთავარია წინ ინფო: გეწეროს რო ინფორმაცია მოგცეს.


Google

info:wikipedia.org

სურათები ვიდეოები წიგნები ვაჭრობა Maps ავიაბილეთები ფინანსები

ყველა ფილტრი ▾ ხელსაწყოები

დაახლოებით 10 100 000 000 შედეგი (0.41 წამი)


 Wikipedia
https://www.wikipedia.org

Wikipedia
Wikipedia is a free online encyclopedia, created and edited by volunteers around the world and hosted by the Wikimedia Foundation.



ადამიანები ასევე კითხულობენ

- Who runs and owns Wikipedia?
- How trustworthy is Wikipedia 2023?
- What organization is behind Wikipedia?
- Who is the owner of Wikipedia?

გამოხმაურება

 Wikipedia
https://en.wikipedia.org › wiki › Wikipedia

Article Talk
Wikipedia is a free-content online encyclopedia written and maintained by a community of volunteers, collectively known as Wikipedians, through open ...
Wikipedia:About · History · English Wikipedia · Wikipedia (disambiguation)

ვიკიპედია (Wikipedia)

ვიკიპედია — მრავალენოვანი, თავისუფალი ვიკი-ენციკლოპედია. გაიშვა 2001 წლის 15 იანვარს, როგორც ინგლისურენოვანი პროექტი ონლაინ-ენციკლოპედიისა, რომელშიც ნებისმიერ ადამიანს შეუძლია შეიტანოს ცვლილებები და დამატებები. პროექტს მართავს ამერიკული არამომგებიანი ფონდი ვიკიმედია. Wikipedia

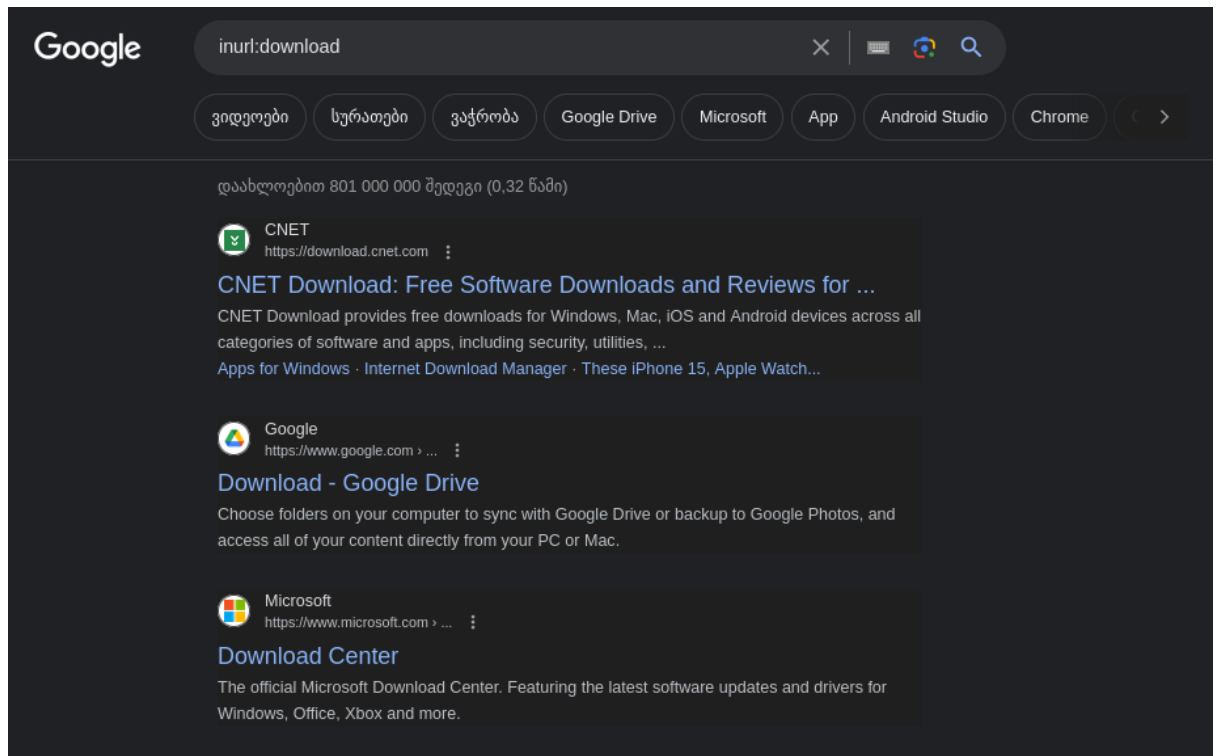
ჯილდოები: Princess of Asturias Award for International Cooperation, Free Software Award for Projects of Social Benefit

მფლობელი: ფონდი ვიკიმედია

რეგისტრაცია: არასავალდებულო

შემქნელი: ჯიმი ველზი

3. იპოვეთ ვებ გვერდები URL-ში “Download-ით”; - თუ გინდა სპეციფიური ფრაზა ან რაზე მოძებნო ურლში და მარცო ეგეტები გამოიგანო შედეგად, უნდა დაწერო inurl:Download ამ შემთხვევაში.



Google

intitle:technology

სურათებივიდეოებიAdvantages ofვაჭრობაMapsნიგნებიავიბილიტებიფინანსები

ყველა ფილტრიხელსაწყოები

დაახლოებით 171 000 000 შედეგი (0,44 წამი)

Technology is the application of scientific knowledge to the practical aims of human life or, as it is sometimes phrased, to the change and manipulation of the human environment.

16 ოქტ. 2023

Britannica
https://www.britannica.com › ... › Earth Sciences

Technology | Definition, Examples, Types, & Facts | Britannica

ადამიანები ასევე კითხულობენ :

What is the definition of technology?

What is example of technology?

What are three examples of technology?

What technology does in our life?

გამომზადება

ტექნოლოგია (Technology)

ტექნოლოგია — მეცნიერება იმ იარაღების, პროცესებისა და მეთოდების შესახებ, რომელიც გამოიყენება სხვადასხვა საგნების და ობიექტების დამზადებისათვის, რაიმეს წარმოების მიზნით. სხვაგვარად, ტექნოლოგია ეს არის ნივთიერების, ენერგიისა და ინფორმაციის გადამუშავების ხერხი.

Wikipedia

სხვები ასევე ეძებენ

იხილეთ კიდევ 10+

მეცნიერება

ფინანსები

Innovation

საზოგადო.

პრაქტიკული დავალება N3:

1. მოძებნეთ Nmap ხელსაწყოს ოპერატორები შემდეგი სკანირებისთვის:

1. პორტის მითითება;
2. TCP სკანირება;
3. ოპერაციული სისტემის ოპერატორი.

აქ ცოცხა დაგუგლვა მოგიწევს სავარაუდოდ, კალი ლინუქსის ვირტუალური მანქანა გექნებათ და იქიდან უნდა გააკეთო იდეაში man ბრძანებით ეს ყველაფერი მარა დაგუგლვაც შეგიძლია როდამე.

ლინუქსში თუ დააპრიებ პატარა tricks გასწავლი man ში.

ჯერ უნდა ჩაწერო man nmap ბრძანება რო nmap-ის მეხუალი გაგისხნას ანუ როგორუდნა მოიხმარო



მერე რო გაგისხნის მეხუალს, / “დახრილი ხაზი” ანუ - / ეს უნდა დაწერო და მერე რასაც ეძებ, მაგალითად თუ ვეძებ პორტების სკანირებას დავწერ /port

და სადაც ეგ სიგევა იქნება ანხსენები მაგას გამილურჯებს და უკეთ ნახავ ყველაფერი როარ წაიკითხო. Q - ს უნდა დააჭირო რო man იდან გამოხვიდე.

```
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options]
/port
```

ასე იქნება ქვევით, მერე ენთერს დააჭერ და ამოგიგდებს ყველაფერს. ამის გამოყენება არარის აუცილებელი უბრალოდ გაგიმარგივებს ალბათ და იცოდე მაინც

1. პორტის მითითება: -p <port ranges>

```
-sU: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
```

2. TCP სკანირება: -sT

```
-sT (TCP connect scan)
TCP connect scan is the default scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, POP clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt.

When SYN scan is available, it is usually a better choice. Nmap has less control over the high level connect call than with raw packets, making it less efficient. The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does. Not only does this take longer and require more packets to obtain the same information, but target machines are more likely to log the connection. A decent IDS will catch either, but most machines have no such alarm system. Many services on your average Unix system will add a note to syslog, and sometimes a cryptic error message, when Nmap connects and then closes the connection without sending data. Truly pathetic services crash when this happens, though that is uncommon. An administrator who sees a bunch of connection attempts in her logs from a single system should know that she has been connect scanned.
```

3. ოპერაციული სისტემის ოპერატორი: -O

```
-O (Enable OS detection)
Enables OS detection, as discussed above. Alternatively, you can use -A to enable OS detection along with other things.
```

ბოლო თემებია და მაგის წერა არცისე კარგად გამომდის მგონი შენუკეთ იბამ ისედაც გყუილად არ დაეწიყებ ახლა. დაგუგლავ ნაწილს იქვე რაც ამოგივა და გადმოთარგმნი თან, მარტივი თემებია. უბრალოდ 2 ნაწილს გამოვყოფ მოკლედ.

Malware-ს გავრცელების გზები - Malware-ს გავრცელების ძალიან ბევრი გზა არსებობს და ყველაზე უბრალოდ ვერ ვისაუბრებთ, თუმცა გამოვყოფ რამოდენიმე ჩემი აზრით ყველაზე გავრცელებულ და მნიშვნელოვან მეთოდს, პირველი ეს არის ფიშინგი. ფიშინგით მალვეარის გავრცელება ულაპარაკოდ ყველაზე ხშირი შემთხვევაა. მეორე ალბათ პირატული პროგრამები იქნება

სიხშირით. ასევე სისტემებში არსებული სისტემების ექსპლოიტაციის შემდეგად დატოვებული მალვეარი და კიდევ ბევრი სხვა.

რა არის Malware და როგორ ხდება მისი ანალიზი - Malware-ს
ანალიზის ძირითადი ორი ტიპი არსებობს, ესენია: დინამიური და სტატიკური. დინამიური მალვეარის ანალიზის დროს გამოიყენება ისეთი ხელსაწყოები როგორიცაა მაგალითად sandbox. დინამიური ანალიზი დამოკიდებულია მალვეარის ქცევაზე და არა მის Signature-ზე ანუ ჰეშზე. ამ დროს ხდება მავნე კოდის იზოლირებულ სისტემაში გაშვება და ამ სისტემის დინამიურად მონიტორინგი და დაკვირვება თუ რას აფუჭებს ეს მავნე კოდი. სტატიკური ანალიზის დროს კი ხდება Signature based detection, ანუ ჰეშის შედარება ცნობილ მალვეარებთან და ასე დადგენა თუმა არის ბევრად უფრო სწრაფი.