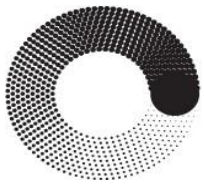
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



МОСКОВСКИЙ
ПОЛИТЕХ

Лабораторная работа №1

по дисциплине

«Основы сетевых технологий»

Группа 231-351

Студент Павлюченко М.С

Москва – 2024

Cyber Security Resources

www.sans.org/security-resources/

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

SANS

Contact Sales

Train and Certify

For Organizations

Security Awareness

Resources

Get Involved

About

Search SANS...

SANS Sites

Log In

Join

New Resource to Help Secure Your Organization

SANS Institute offers free and exclusive access to a variety of online cybersecurity resources, including this ICS Strategy Guide, news updates, tools, and more.

https://www.sans.org/security-resources/?msc=main-nav

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 1 / 4 100%

презентаций.

Часть 1: Изучение веб-сайта SANS

В части 1 вам нужно открыть веб-сайт SANS и изучить доступные ресурсы.

Шаг 1: Найдите ресурсы SANS.

Перейдите по ссылке www.SANS.org. На главной странице наведите указатель мыши на меню **Resources** (Ресурсы).

Назовите три доступных ресурса.

Шаг 2: Найдите основные средства контроля безопасности.

Список **основных средств контроля безопасности** на веб-сайте SANS был составлен в результате совместной работы государственных и частных компаний при участии Министерства обороны, Ассоциации национальной безопасности, Центра интернет-безопасности и Института SANS. Его задачей было определить приоритетность средств контроля кибербезопасности и связанных с ними расходов для Министерства обороны. На основе этого списка правительство США разработало эффективные программы обеспечения безопасности. В меню **Resources** (Ресурсы) выберите пункт **Critical Security Controls** (Основные средства контроля безопасности) (название может отличаться).

Лабораторная работа. Изучение угроз сетевой безопасности

Выберите одно из средств контроля и назовите три предложения по его реализации.

11° Поиск РУС 11:28 01.10.2024

Cyber Security Resources

www.sans.org/security-resources/

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

Resources

- Overview
- Webcasts
- Free Cybersecurity Events
- Content
- Internet Storm Center
- Research
- Tools
- Focus Areas

New Resource to Help Secure Your Organization

SANS Institute offers free and exclusive access to a variety of online cybersecurity resources, including this ICS Strategy Guide, news updates, tools, and more.

Download Strategy Guide

https://www.sans.org/security-resources/

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 1 / 4 100%

презентаций.

Часть 1: Изучение веб-сайта SANS

В части 1 вам нужно открыть веб-сайт SANS и изучить доступные ресурсы.

Шаг 1: Найдите ресурсы SANS.

Перейдите по ссылке www.SANS.org. На главной странице наведите указатель мыши на меню **Resources** (Ресурсы).

Назовите три доступных ресурса.

Шаг 2: Найдите основные средства контроля безопасности.

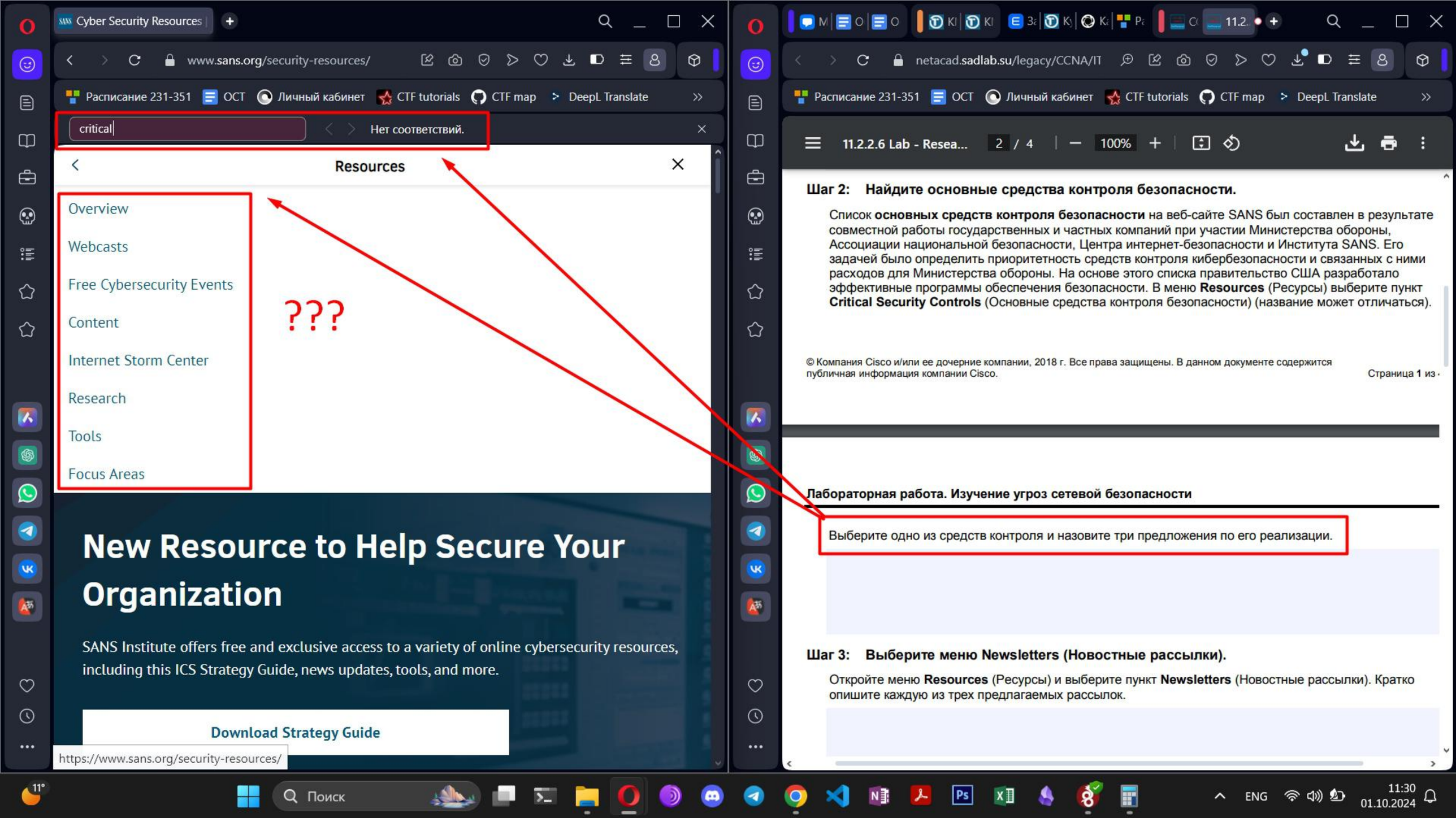
Список **основных средств контроля безопасности** на веб-сайте SANS был составлен в результате совместной работы государственных и частных компаний при участии Министерства обороны, Ассоциации национальной безопасности, Центра интернет-безопасности и Института SANS. Его задачей было определить приоритетность средств контроля кибербезопасности и связанных с ними расходов для Министерства обороны. На основе этого списка правительство США разработало эффективные программы обеспечения безопасности. В меню **Resources** (Ресурсы) выберите пункт **Critical Security Controls** (Основные средства контроля безопасности) (название может отличаться).

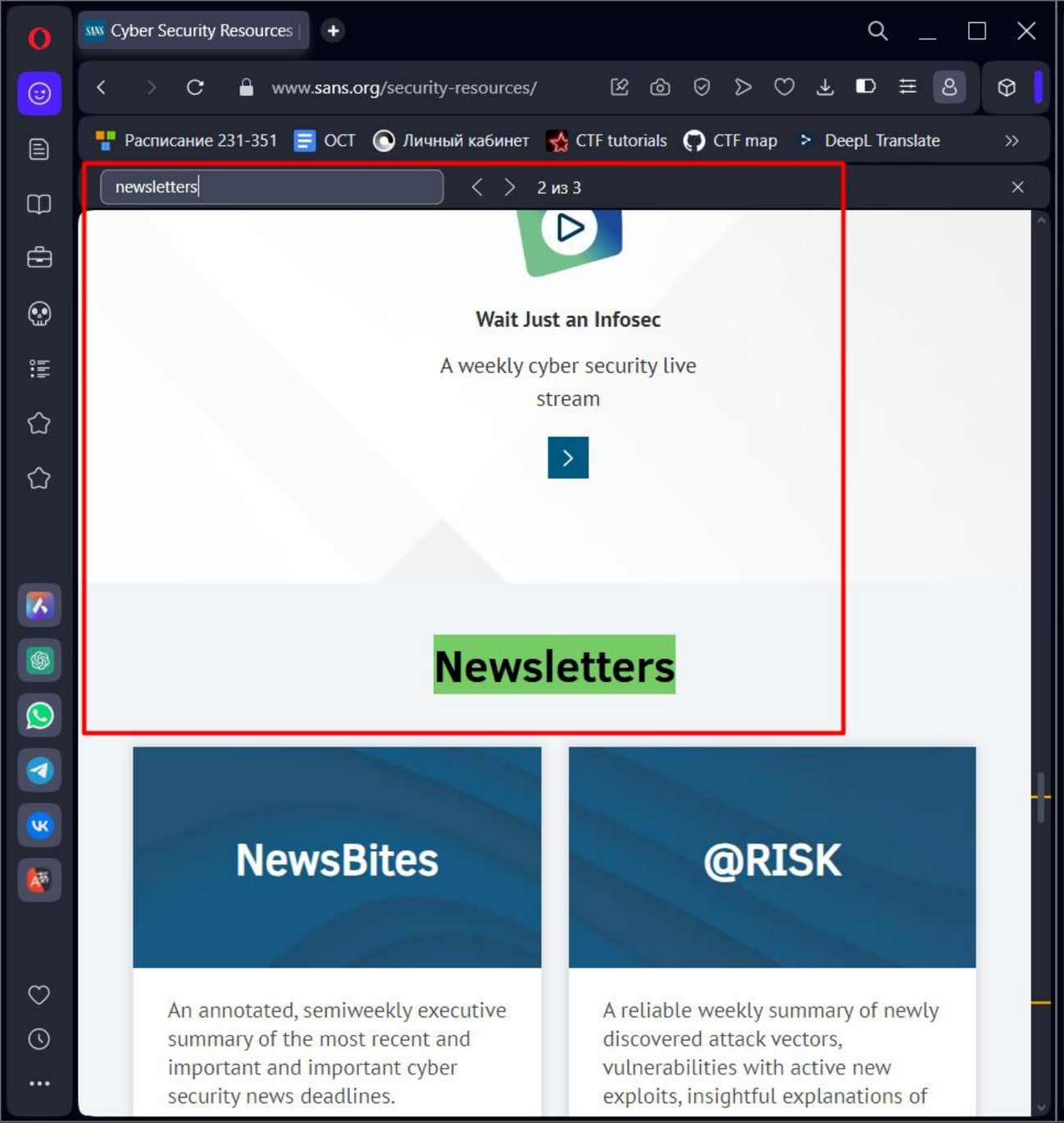
Лабораторная работа. Изучение угроз сетевой безопасности

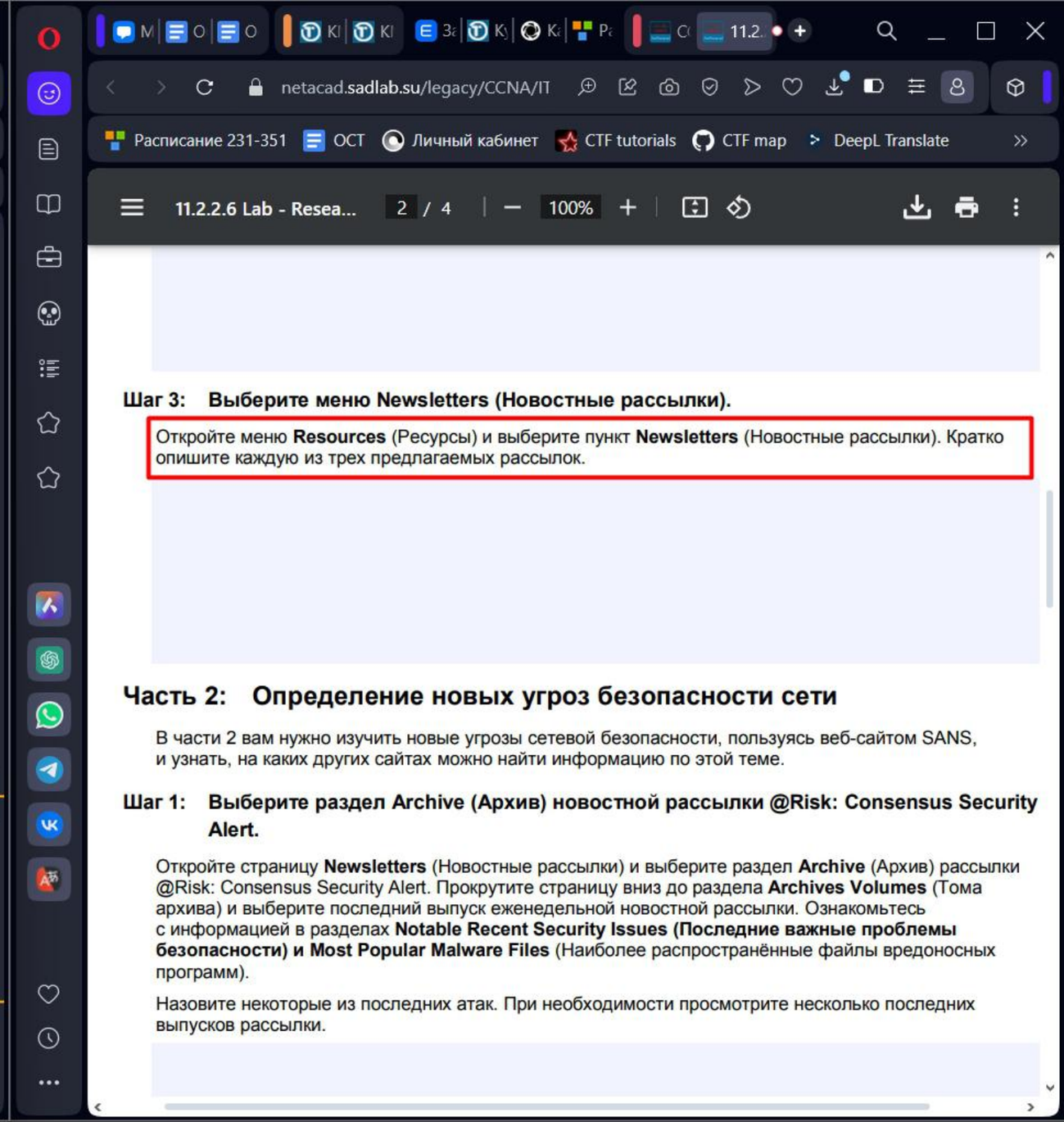
Выберите одно из средств контроля и назовите три предложения по его реализации.

Поиск

РУС 11:28 01.10.2024


Cyber Security Resources
www.sans.org/security-resources/
Расписание 231-351
ОСТ
Личный кабинет
CTF tutorials
CTF map
DeepL Translate
critical
Нет соответствий.
Resources
Overview
Webcasts
Free Cybersecurity Events
Content
Internet Storm Center
Research
Tools
Focus Areas
???
New Resource to Help Secure Your Organization
SANS Institute offers free and exclusive access to a variety of online cybersecurity resources, including this ICS Strategy Guide, news updates, tools, and more.
Download Strategy Guide
https://www.sans.org/security-resources/
netacad.sadlab.su/legacy/CCNA/IT
11.2.2.6 Lab - Resea...
2 / 4
100%
Шаг 2: Найдите основные средства контроля безопасности.
Список основных средств контроля безопасности на веб-сайте SANS был составлен в результате совместной работы государственных и частных компаний при участии Министерства обороны, Ассоциации национальной безопасности, Центра интернет-безопасности и Института SANS. Его задачей было определить приоритетность средств контроля кибербезопасности и связанных с ними расходов для Министерства обороны. На основе этого списка правительство США разработало эффективные программы обеспечения безопасности. В меню Resources (Ресурсы) выберите пункт Critical Security Controls (Основные средства контроля безопасности) (название может отличаться).
© Компания Cisco и/или ее дочерние компании, 2018 г. Все права защищены. В данном документе содержится публичная информация компании Cisco.
Страница 1 из
Лабораторная работа. Изучение угроз сетевой безопасности
Выберите одно из средств контроля и назовите три предложения по его реализации.
Шаг 3: Выберите меню Newsletters (Новостные рассылки).
Откройте меню Resources (Ресурсы) и выберите пункт Newsletters (Новостные рассылки). Кратко опишите каждую из трех предлагаемых рассылок.
Поиск
ENG
11:30
01.10.2024





Шаг 3: Выберите меню Newsletters (Новостные рассылки).

Откройте меню **Resources** (Ресурсы) и выберите пункт **Newsletters** (Новостные рассылки). Кратко опишите каждую из трех предлагаемых рассылок.

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

Cyber Security | SANS NewsBites - Cyber | SANS @RISK | www.sans.org

www.sans.org/newsletters/newsbites/

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

SANS

Contact Sales

1. Home >
2. Newsletters >
3. SANS NewsBites

NewsBites - Cyber Security News

SANS NewsBites is a semiweekly executive summary of the most important cyber security news articles published recently. Each news item is annotated with important context provided by respected subject matter experts within the SANS community.

Filters:

Clear All

Dates

- (•) All Dates
- ( ) Select a Date Range

30.09.2023

30.09.2024

Apply

10 per page

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 2 / 4 100%

Шаг 3: Выберите меню Newsletters (Новостные рассылки).

Откройте меню **Resources** (Ресурсы) и выберите пункт **Newsletters** (Новостные рассылки). Кратко опишите каждую из трех предлагаемых рассылок.

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

11° | Поиск | ENG | 11:35 01.10.2024

Cyber Security | SANS NewsBit | SANS @RISK | SANS OUCH!

www.sans.org/newsletters/ouch/

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

SANS

Contact Sales

OUCH! Newsletters

OUCH! is the world's leading, free security awareness newsletter designed for everyone. Published every month in multiple languages, each edition is carefully researched and developed by the SANS Security Awareness team, instructors and community members.

Each OUCH! is developed through a rigorous process involving numerous community volunteers, including translators, subject matter experts, and editors.

Our Volunteers

Security Awareness Products & Services

Filters:

10 per page

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 2 / 4 100%

Шаг 3: Выберите меню Newsletters (Новостные рассылки).

Откройте меню **Resources** (Ресурсы) и выберите пункт **Newsletters** (Новостные рассылки). Кратко опишите каждую из трех предлагаемых рассылок.

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

11° Поиск ENG 11:36 01.10.2024

Cyber Security | SANS NewsBit | SANS @RISK | SANS OUCH!

www.sans.org/newsletters/at-risk/

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

SANS

Contact Sales

SANS @RISK

A weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, insightful explanations of how recent attacks worked, and other valuable data.

Filters:

10 per page

Vol. 24, Num. 38 · 2024-09-26

The Consensus Security Vulnerability Alert

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 2 / 4 100%

Шаг 3: Выберите меню Newsletters (Новостные рассылки).

Откройте меню **Resources** (Ресурсы) и выберите пункт **Newsletters** (Новостные рассылки). Кратко опишите каждую из трех предлагаемых рассылок.

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

11° Поиск ENG 11:37 01.10.2024

Cyber Security | SANS NewsBit | SANS @RISK | SANS OUCH!

www.sans.org/newsletters/at-risk/

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

archive

Нет соответствий.

10 per page

Vol. 24, Num. 38 · 2024-09-26

The Consensus Security Vulnerability Alert

Vol. 24, Num. 37 · 2024-09-19

The Consensus Security Vulnerability Alert

Vol. 24, Num. 36 · 2024-09-12

The Consensus Security Vulnerability Alert

Vol. 24, Num. 35 · 2024-09-05

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 2 / 4 100%

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

Шаг 2: Найдите веб-сайты, которые содержат информацию о новых угрозах безопасности.

Выясните, на каких еще сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.

Поиск

ENG 11:38 01.10.2024

INTERNET STORM CENTER SPOTLIGHT

ISC provides a free analysis and warning service to thousands of Internet users and organizations, and is actively working with Internet Service Providers to fight back against the most malicious attackers. https://isc.sans.edu/about.html

DNS Reflection Update and Odd Corrupted DNS Requests

Published: 2024-09-25.

Last Updated: 2024-09-25 16:33:15 UTC

by Johannes Ullrich (Version: 1)

Occasionally, I tend to check in on what reflective DNS denial of service attacks are doing. We usually see steady levels of attacks. Usually, they attempt to use spoofed requests for ANY records to achieve the highest possible amplification. Currently, I am seeing these two records used (among others):

ANY nlrb<.>gov

The response for this query may be up to 5,826 bytes in size. With a query payload size of 37 bytes, this leads to a rather impressive implication. The original name server appears to do the right thing, and it ignores EDNS0, but that, of course, doesn't help with open resolvers.

ANY ncca<.>mil

This domain is a bit odd. I only receive empty responses for ANY, NS, or other queries I tried. Maybe this domain was fixed after it got abused for DDoS attacks.

ANY fnop<.>net

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

Шаг 2: Найдите веб-сайты, которые содержат информацию о новых угрозах безопасности.

Выясните, на каких еще сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.

Read the full entry:

https://isc.sans.edu/diary/DNS+Reflection+Update+and+Odd+Corrupted+DNS+Requests/31296/

Fake GitHub Site Targeting Developers

Published: 2024-09-19. Last Updated: 2024-09-19 20:14:39 UTC

by Johannes Ullrich (Version: 1)

Our reader "RoseSecurity" forwarded received the following malicious email:

Hey there!

We have detected a security vulnerability in your repository. Please contact us at https:[//]github-scanner[.]com to get more information on how to fix this issue. Best regards,

Github Security Team

GitHub has offered free security scans to users for a while now. But usually, you go directly to GitHub.com to review results, not a "scanner" site like suggested above.

The github-scanner website first displays what appears to be some form of Captcha to make sure you are "Human" (does this exclude developers?) ...

Read the full entry:

https://isc.sans.edu/diary/Fake+GitHub+Site+Targeting+Developers/31282/

Phishing links with @ sign and the need for effective security awareness building

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

Шаг 2: Найдите веб-сайты, которые содержат информацию о новых угрозах безопасности.

Выясните, на каких еще сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.

https://isc.sans.edu/diary/Fake+GitHub+Site+Targeting+Developers/31282/

Phishing links with @ sign and the need for effective security awareness building

Published: 2024-09-23.

Last Updated: 2024-09-23 07:40:22 UTC

by Jan Kopriva (Version: 1)

While going over a batch of phishing e-mails that were delivered to us here at the Internet Storm Center during the first half of September, I noticed one message which was somewhat unusual. Not because it was untypically sophisticated or because it used some completely new technique, but rather because its authors took advantage of one of the less commonly misused aspects of the URI format – the ability to specify information about a user in the URI before its "host" part (domain or IP address).

RFC 3986 specifies[1] that a "user information" string (i.e., username and – potentially – other contextual data) may be included in a URI in the following format:

[userinfo "@"] host [":" port]

In this instance, the threat actors used the user information string to make the link appear as if it was pointing to facebook.com, while it actually lead to an IPFS gateway[2] ipfs.io.

Read the full entry:

https://isc.sans.edu/diary/Phishing+links+with+sign+and+the+need+for+effective+security+awareness+building/31288/

Internet Storm Center Entries

Часть 2: Определение новых угроз безопасности сети

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

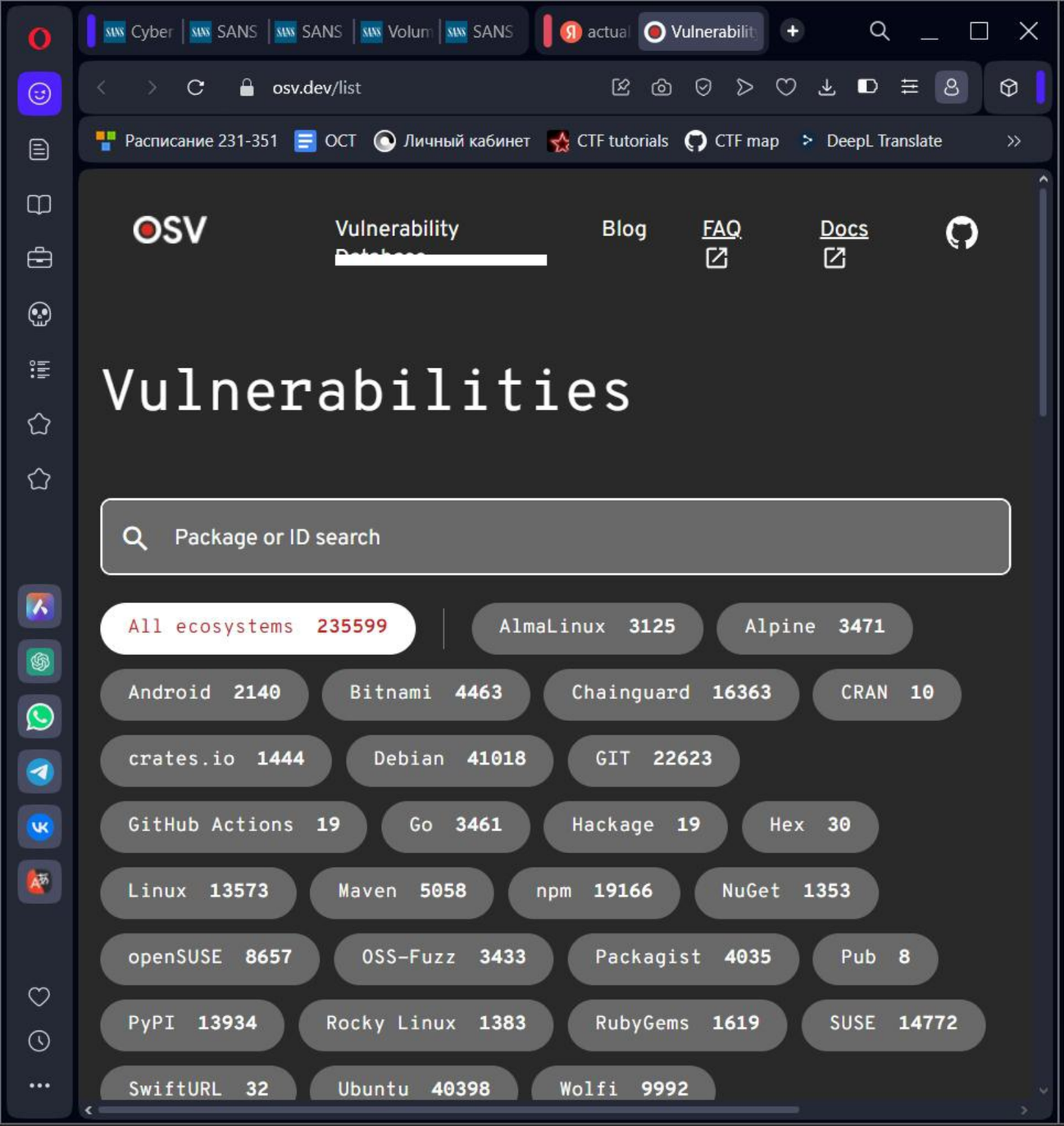
Шаг 1: Выберите раздел Archive (Архив) новостной рассылки @Risk: Consensus Security Alert.

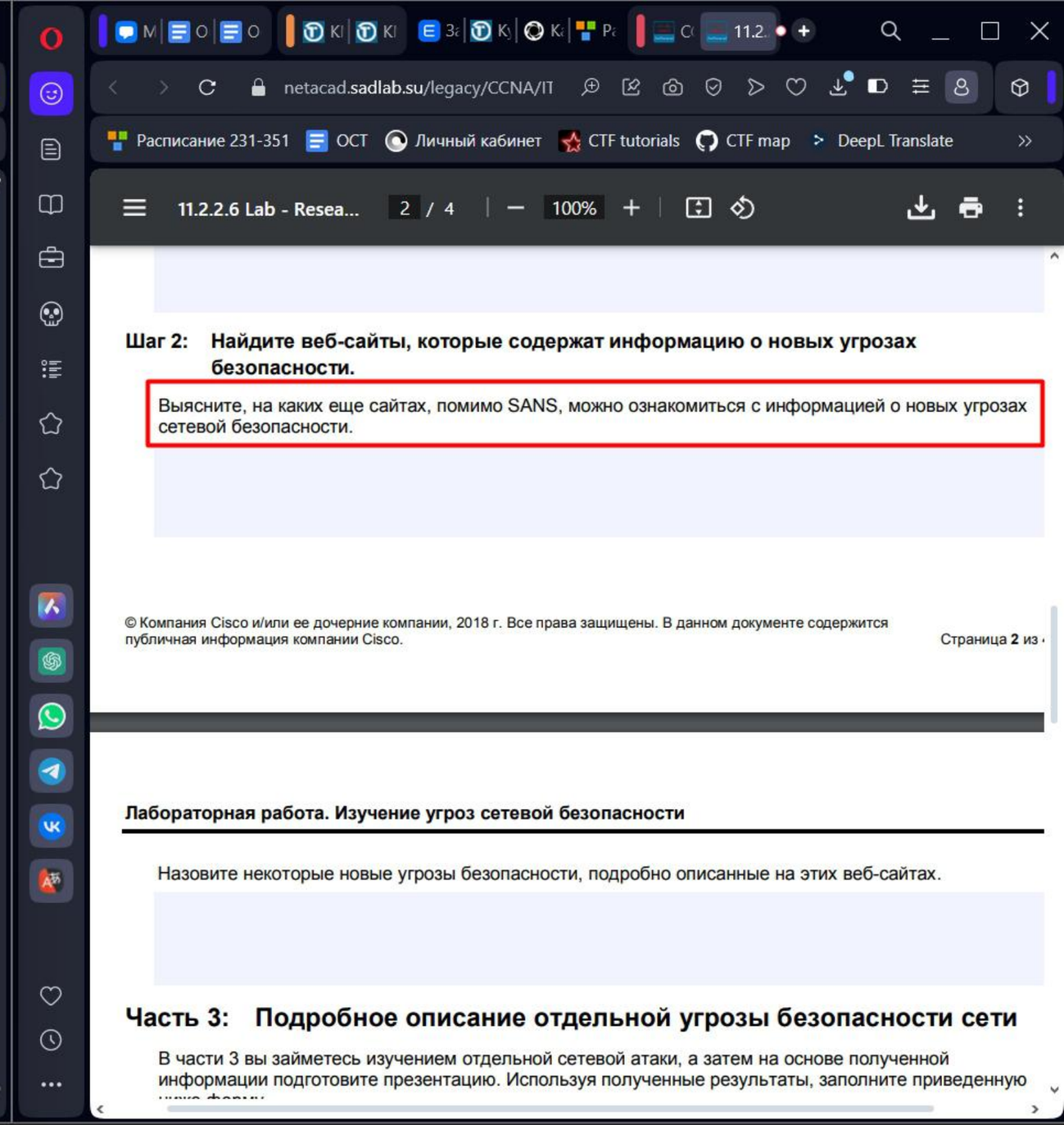
Откройте страницу **Newsletters** (Новостные рассылки) и выберите раздел **Archive** (Архив) рассылки @Risk: Consensus Security Alert. Прокрутите страницу вниз до раздела **Archives Volumes** (Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесь с информацией в разделах **Notable Recent Security Issues (Последние важные проблемы безопасности) и Most Popular Malware Files** (Наиболее распространённые файлы вредоносных программ).

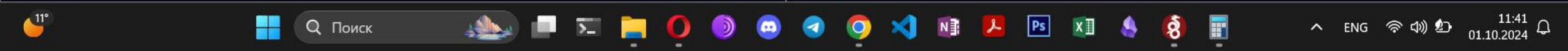
Назовите некоторые из последних атак. При необходимости просмотрите несколько последних выпусков рассылки.

Шаг 2: Найдите веб-сайты, которые содержат информацию о новых угрозах безопасности.

Выясните, на каких еще сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.


osv.dev/list
Расписание 231-351
ОСТ
Личный кабинет
CTF tutorials
CTF map
DeepL Translate
OSV
Vulnerability Database
Blog
FAQ
Docs
Vulnerabilities
Package or ID search
All ecosystems 235599
AlmaLinux 3125
Alpine 3471
Android 2140
Bitnami 4463
Chainguard 16363
CRAN 10
crates.io 1444
Debian 41018
GIT 22623
GitHub Actions 19
Go 3461
Hackage 19
Hex 30
Linux 13573
Maven 5058
npm 19166
NuGet 1353
openSUSE 8657
OSS-Fuzz 3433
Packagist 4035
Pub 8
PyPI 13934
Rocky Linux 1383
RubyGems 1619
SUSE 14772
SwiftURL 32
Ubuntu 40398
Wolfi 9992


netacad.sadlab.su/legacy/CCNA/IT
Расписание 231-351
ОСТ
Личный кабинет
CTF tutorials
CTF map
DeepL Translate
11.2.2.6 Lab - Resea...
2 / 4
100%
Шаг 2: Найдите веб-сайты, которые содержат информацию о новых угрозах безопасности.
Выясните, на каких еще сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.
© Компания Cisco и/или ее дочерние компании, 2018 г. Все права защищены. В данном документе содержится публичная информация компании Cisco.
Страница 2 из
Лабораторная работа. Изучение угроз сетевой безопасности
Назовите некоторые новые угрозы безопасности, подробно описанные на этих веб-сайтах.
Часть 3: Подробное описание отдельной угрозы безопасности сети
В части 3 вы займетесь изучением отдельной сетевой атаки, а затем на основе полученной информации подготовите презентацию. Используя полученные результаты, заполните приведенную


11°
Поиск
ENG
11:41
01.10.2024

osv.dev/list

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

Packagist 4035 | Pub 8 | PyPI 13934 | Rocky Linux 1383 | RubyGems 1619

SUSE 14772 | SwiftURL 32 | Ubuntu 40398 | Wolfi 9992

ID	Packages	Summary	Published
ASB-A-261721900	Android/platform/frameworks/base	Bypass CVE-2022-20338	01 Sep
ASB-A-293199910	Android/platform/packages/apps/Settings	Android 13 Factory Reset Protection (FRP) Bypass - Hang/Crash Settings App > Share Feedback	01 Sep
ASB-A-300904123	Android/platform/packages/services/Telecomm	App can keep its while in use permission forever even if it is in background.	01 Sep
ASB-A-324321147	Android/platform/build/soong Android/platform/frameworks/base Android/platform/hardware/interfaces Android/platform/system/sepolicy	Device administration API factory reset can be interrupted by an attacker with physical access (long-term fix)	01 Sep
ASB-A-327749022	Android/platform/packages/apps/Settings	(Split 5) (Step 27) - FRP Bypass January 2024 (Android 14)	01 Sep
ASB-A-329058967	Android/platform/packages/services/Telecomm	Conference StatusHints allow cross-user image access	01 Sep
ASB-A-329641908	Android/platform/frameworks/av	[Out of Bounds Write in kDescribeHdr10PlusInfoIndex case in getConfig in SoftVideoDecoderOMXComponent.cpp in libstagefright_softomx]	01 Sep
ASB-A-333364513	Android/platform/packages/apps/Settings	Spoofing getCallingPackage or getCallingActivity with FLAG_ACTIVITY_FORWARD_RESULT: Discussion on vulnerability pattern	01 Sep

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 3 / 4 100%

Лабораторная работа. Изучение угроз сетевой безопасности

Назовите некоторые новые угрозы безопасности, подробно описанные на этих веб-сайтах.

Часть 3: Подробное описание отдельной угрозы безопасности сети

В части 3 вы займетесь изучением отдельной сетевой атаки, а затем на основе полученной информации подготовите презентацию. Используя полученные результаты, заполните приведенную ниже форму.

Шаг 1: Заполните приведенную ниже форму для выбранной сетевой атаки.

Имя атаки:	
Тип атаки:	
Даты атак:	
Пострадавшие компьютеры или организации:	

11° | Поиск | ENG | 11:42 01.10.2024

osv.dev/list

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

Packagist 4035 | Pub 8 | PyPI 13934 | Rocky Linux 1383 | RubyGems 1619

SUSE 14772 | SwiftURL 32 | Ubuntu 40398 | Wolfi 9992

ID	Packages	Summary	Published
ASB-A-261721900	Android/platform/frameworks/base	Bypass CVE-2022-20338	01 Sep
ASB-A-293199910	Android/platform/packages/apps/Settings	Android 13 Factory Reset Protection (FRP) Bypass - Hang/Crash Settings App > Share Feedback	01 Sep
ASB-A-300904123	Android/platform/packages/services/Telecomm	App can keep its while in use permission forever even if it is in background.	01 Sep
ASB-A-324321147	Android/platform/build/soong Android/platform/frameworks/base Android/platform/hardware/interfaces Android/platform/system/sepolicy	Device administration API factory reset can be interrupted by an attacker with physical access (long-term fix)	01 Sep
ASB-A-327749022	Android/platform/packages/apps/Settings	(Split 5) (Step 27) - FRP Bypass January 2024 (Android 14)	01 Sep
ASB-A-329058967	Android/platform/packages/services/Telecomm	Conference StatusHints allow cross-user image access	01 Sep
ASB-A-329641908	Android/platform/frameworks/av	[Out of Bounds Write in kDescribeHdr10PlusInfoIndex case in getConfig in SoftVideoDecoderOMXComponent.cpp in libstagefright_softomx]	01 Sep
ASB-A-333364513	Android/platform/packages/apps/Settings	Spoofing getCallingPackage or getCallingActivity with FLAG_ACTIVITY_FORWARD_RESULT: Discussion on vulnerability pattern	01 Sep

netacad.sadlab.su/legacy/CCNA/IT

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

11.2.2.6 Lab - Resea... 3 / 4 100%

Выясните, на каких еще сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозах сетевой безопасности.

Лабораторная работа. Изучение угроз сетевой безопасности

Назовите некоторые новые угрозы безопасности, подробно описанные на этих веб-сайтах.

Часть 3: Подробное описание отдельной угрозы безопасности сети

В части 3 вы займетесь изучением отдельной сетевой атаки, а затем на основе полученной информации подготовите презентацию. Используя полученные результаты, заполните приведенную ниже форму.

Шаг 1: Заполните приведенную ниже форму для выбранной сетевой атаки.

Имя атаки:	

11° | Поиск | ENG | 11:46 01.10.2024

Введите запрос для поиска или веб-адрес

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

Осло | Выберите свой город

6 °C

Найти в интернете

YouTube | vk.com | Личный кабинет | GitHub | СДО Московского По... | lichess.org • Бесплатн...

netacad.sadlab.su/legacy/CCNA/IT

11.2.2.6 Lab - Resea... 3 / 4 100%

Шаг 1: Заполните приведенную ниже форму для выбранной сетевой атаки.

Имя атаки:	WannaCry
Тип атаки:	Эксплойт
Даты атак:	2017
Пострадавшие компьютеры или организации:	300 000 пользователей в 150 странах мира

Механизм атаки и ее последствия:

Вредоносная программа сканирует диапазон IP-адресов локальной сети и случайно выбранные IP-адреса сети Интернет в поисках компьютеров с открытым TCP-портом 445, который отвечает за обслуживание протокола SMBv1. Обнаружив такой компьютер, программа предпринимает несколько попыток проэксплуатировать на нём уязвимость EternalBlue и, в случае успеха, устанавливает бэкдор DoublePulsar, через который загружается и запускается исполняемый код программы WannaCry. При каждой попытке эксплуатации вредоносная программа проверяет наличие на целевом компьютере DoublePulsar, и в случае обнаружения загружается непосредственно через этот бэкдор

Способы устранения:

Переустановка системы

Источники и ссылки на информационные ресурсы:

https://ru.wikipedia.org/wiki/WannaCry

Поиск

РУС 11:58 01.10.2024

Введите запрос для поиска или веб-адрес

Расписание 231-351 | ОСТ | Личный кабинет | CTF tutorials | CTF map | DeepL Translate

Осло | Выберите свой город

6 °C

Найти в интернете

YouTube | vk.com

Личный кабинет | GitHub

СДО Московского По... | lichess.org • Бесплатн...

netacad.sadlab.su/legacy/CCNA/IT

11.2.2.6 Lab - Resea... 4 / 4 100%

Лабораторная работа. Изучение угроз сетевой безопасности

Вопросы для повторения

1. Какие меры можно предпринять для защиты собственного компьютера?

Антивирус, внимательность, параноидальность, межсетевой экран, правильно настроенный фаервол, безопасная ОС (linux)

2. Какие важные меры могут предпринимать компании для защиты своих ресурсов?

фаервол, скрипты работы сотрудников, СКУД, пароли на сетевые устройства, защищенные помещения

Поиск

РУС

11:58
01.10.2024