Zero to OSCP

Thank You to Our Sponsors and Hosts!

OWASP
NEW
ZEALAND
owasp.org.nz

Without them, this Conference couldn't happen

whoami

Poll

Growing Up

Screensaver lock by-pass via the virtual keyboard #354

Closed **ghost** opened this issue on 29 Dec 2020 · 49 comments

ghost commented on 29 Dec 2020

```
* Cinnamon version:  Cinnamon 4.6.7
* Distribution: Fedora 32
* Graphics hardware *and* driver used: 03:00.0 VGA compatible controller: Advanced Micro Devices, Inc. [AMD/ATI
* 32 or 64 bit: 64bit
```

Issue
Screensaver lock by-pass. It is possible to crash the screensaver and unlock the desktop via the virtual keyboard.

Steps to reproduce
Lock the system
Click on the virtual keyboard
Type at the real keyboard while typing at the virtual keyboard, both at the same time, as many keys as possible.

Expected behaviour
No crash.

Other information
A few weeks ago, my kids wanted to hack my linux desktop, so they typed and clicked everywhere, while I was standing behind them looking at them play... when the screensaver core dumped and they actually hacked their way in! wow, those little hackers... 🦌

I thought it was a unique incident, but they managed to do it a second time. So I'd consider this issue... reproducible... by kids 😄

I tried to recreate the crash on my own with no success, maybe because it required more than 4 little hands typing and using the mouse on the virtual keyboard.

Maybe not the best bug report, but I've seen the screenlock crash twice already with my own eyes, so its pretty real.

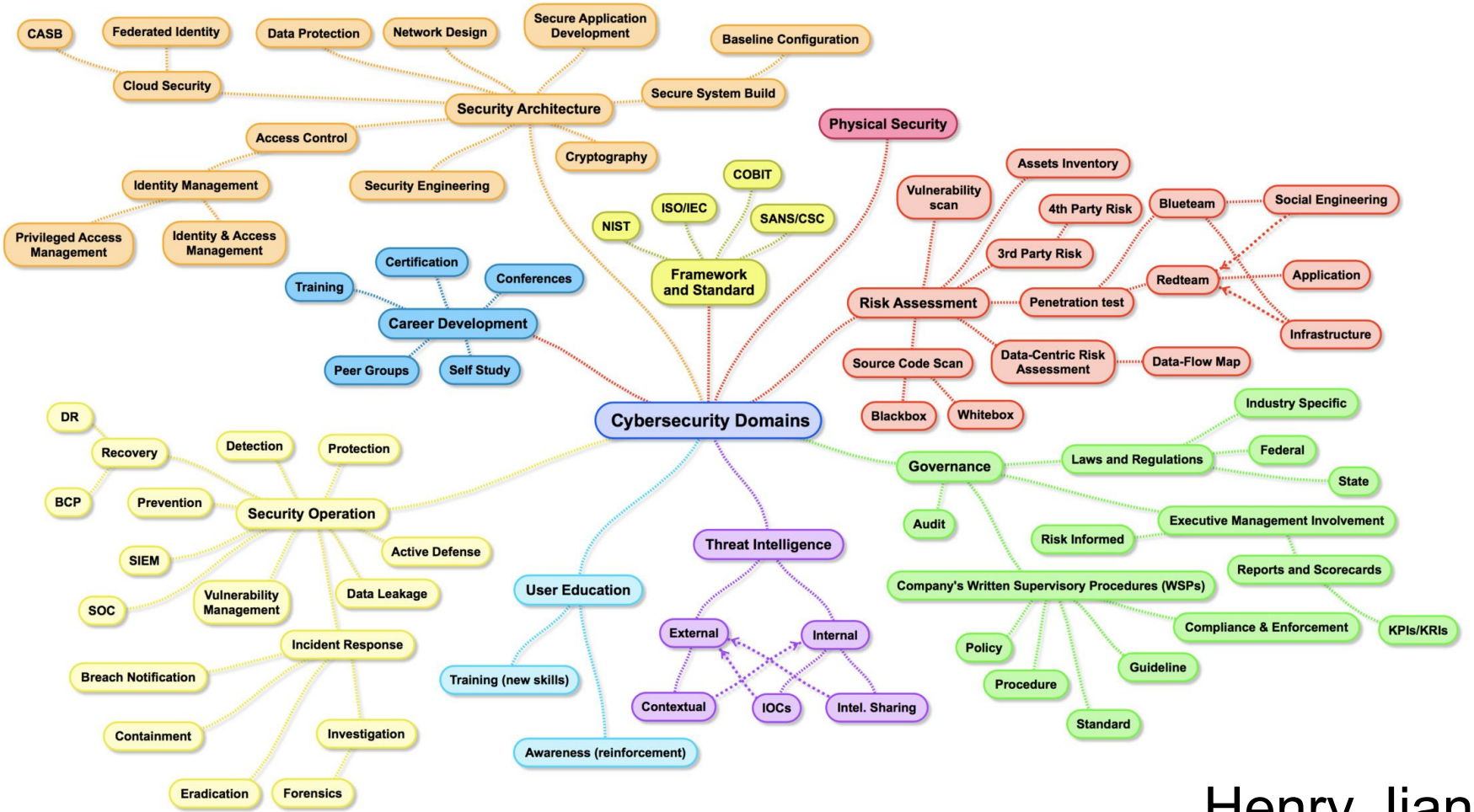
One last thing, after the desktop is unlocked, I can't re-lock it again, the screensaver process is pretty dead and requires me to open a shell and run 'cinnamon-screensaver' manually to get it working.

👍 318 😄 668 🎉 36 ❤️ 186 🚀 33 👀 39

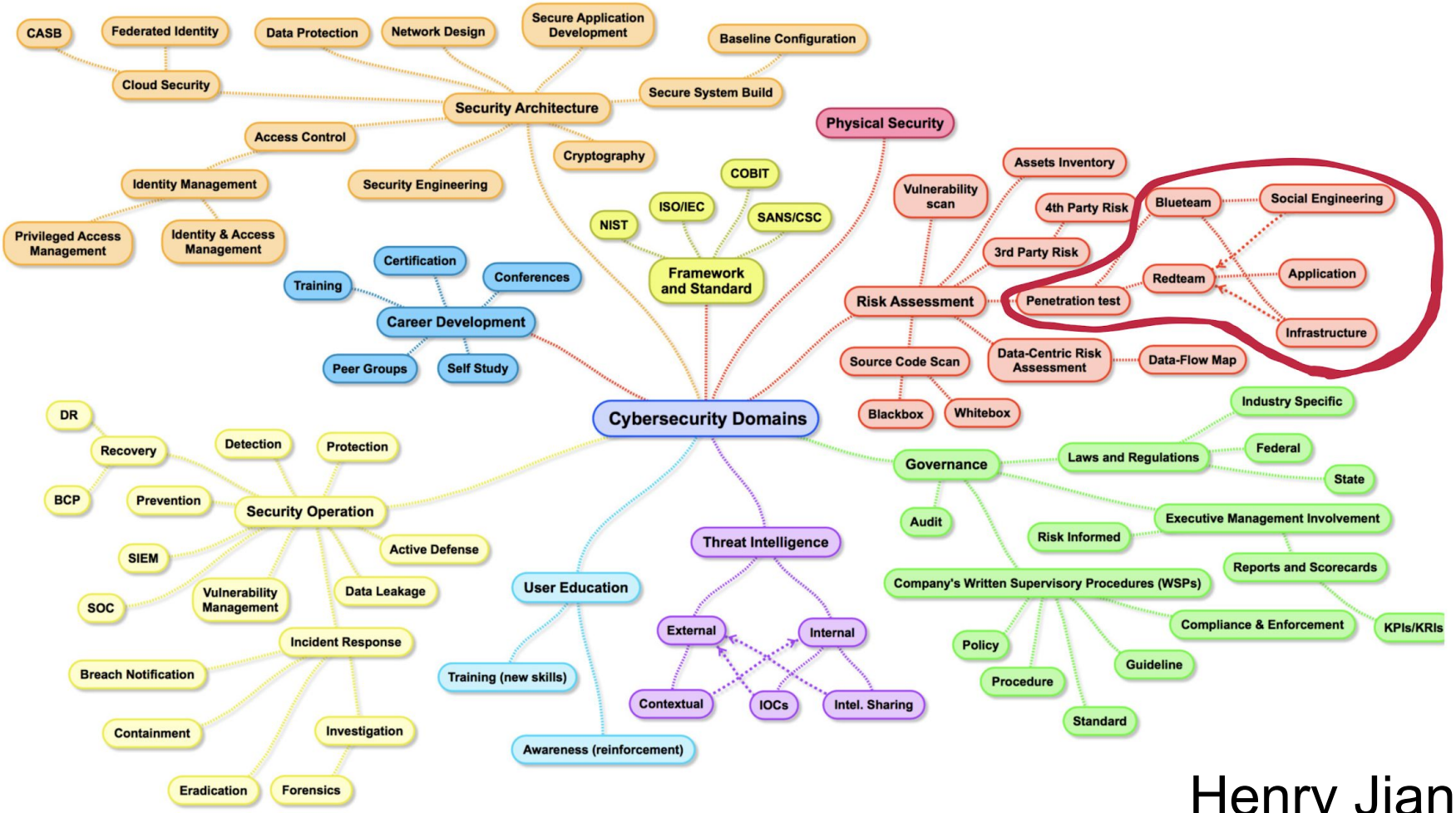
University


Job

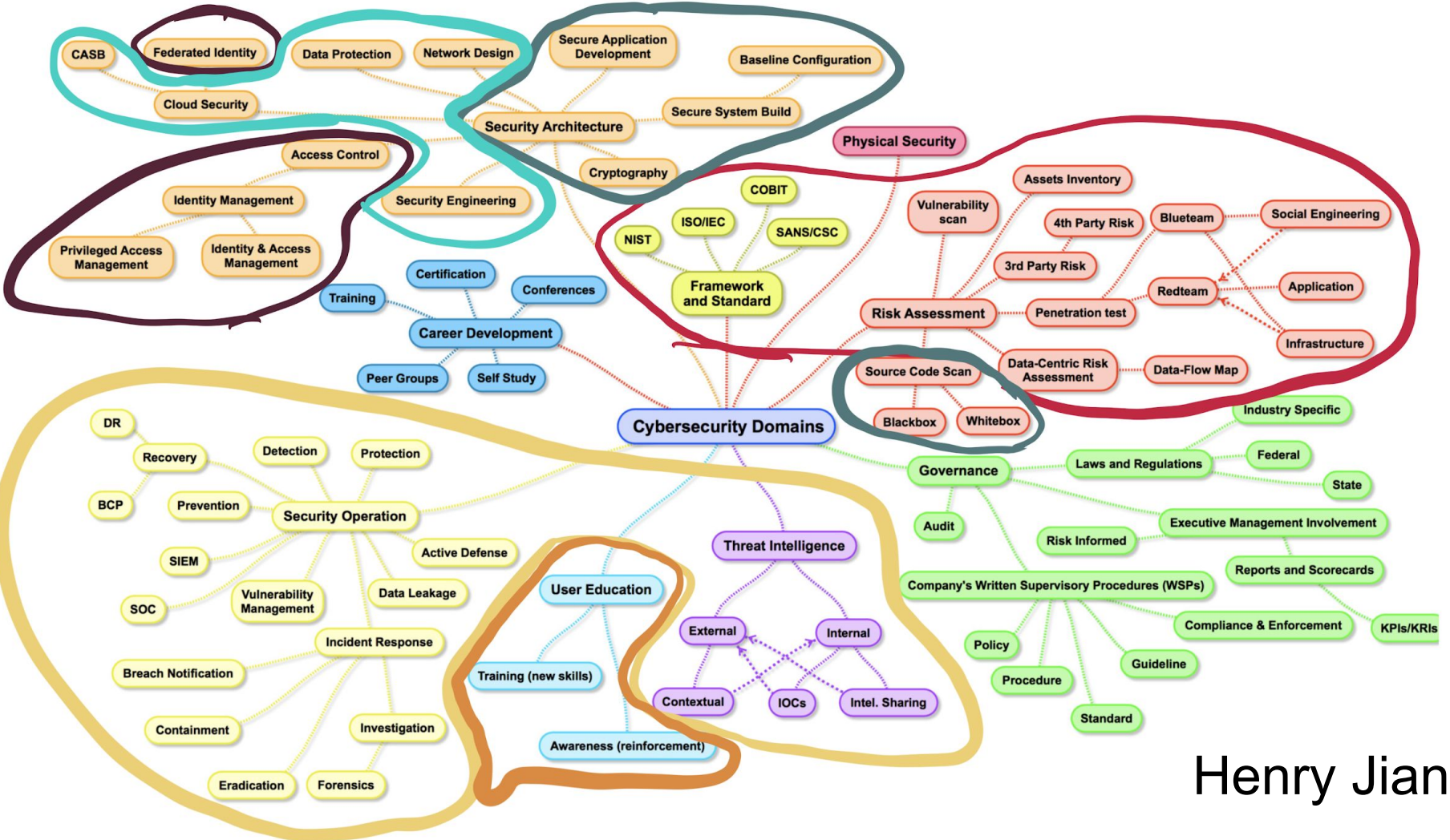

1011100
100111


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Cryptography
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Framework and Standard
COBIT
ISO/IEC
SANS/CSC
NIST
Career Development
Certification
Conferences
Training
Peer Groups
Self Study
Physical Security
Risk Assessment
Assets Inventory
Vulnerability scan
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Redteam
Social Engineering
Application
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Governance
Industry Specific
Laws and Regulations
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics

Henry Jiang


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Framework and Standard
COBIT
ISO/IEC
SANS/CSC
NIST
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Physical Security
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics

Henry Jiang


CASB
Federated Identity
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Cloud Security
Secure System Build
Security Architecture
Cryptography
Access Control
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Physical Security
COBIT
ISO/IEC
NIST
SANS/CSC
Framework and Standard
Assets Inventory
Vulnerability scan
4th Party Risk
Blueteam
Social Engineering
3rd Party Risk
Redteam
Application
Risk Assessment
Penetration test
Infrastructure
Data-Centric Risk Assessment
Data-Flow Map
Source Code Scan
Blackbox
Whitebox
Certification
Training
Conferences
Career Development
Peer Groups
Self Study
Cybersecurity Domains
Industry Specific
Governance
Laws and Regulations
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Guideline
Procedure
Standard
DR
Recovery
Detection
Protection
BCP
Prevention
Security Operation
Active Defense
SIEM
SOC
Vulnerability Management
Data Leakage
Incident Response
Breach Notification
Containment
Investigation
Eradication
Forensics
User Education
Training (new skills)
Awareness (reinforcement)
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing

Henry Jiang


OSCP

Offensive
Security
Certified
Professional

If you want to be a pentester OSCP is worth more than a degree

- Dom Rapp ("Reformed" Pentester)

Alternatives

Where to Start?

@rana__khalil

@0xTib3rius

@ippsec

@TJ_Null

HACKTHEBOX VM LIST:

Do not forget to

Curated by: TJnull at Netsec Focus

Disclaimer: The boxes that are contained in this list should be used as a way to get started, to build your practical skills, or brush up on any weak points that you may have in your pentesting methodology. This list is not a substitute to the actual lab environment that is in the PWK/OSCP course. When you are taking the course, It is encouraged that you try to go through every system that is in the PWK/OSCP lab environment, as they will provide better insight for when you attempt to the exam itself. This list is not exhaustive, nor does it guarantee a passing grade for the OSCP Exam.

Linux Boxes:	Windows Boxes:	More challenging than OSCP, but good practice:	Updated Boxes for February 2021:
Lame	legacy	Jeeves [Windows]	Buff [Windows]
brain	Blue	Bart [Windows]	SneakyMailer [Linux]
shocker	Devel	Tally [Windows]	Omni [Windows]
bashed	Optimum	Kotarak [Linux]	Worker [Windows]
nibbles	Bastard	falafel [Linux]	
beep	granny	Devops [Linux]	
cronos	Arctic	Hawk [Linux]	
nineveh	grandpa	Netmon [Windows]	
sense	silo	Lightweight [Linux]	
solidstate	bounty	La Casa De Papel [Linux]	
node	jerry	Jail [Linux]	
valentine	conceal	Safe [Linux]	
poison	chatterbox	Bitlab [Linux]	
sunday	Forest	Sizzle [Windows]	
tartarsauce	BankRobber	Sniper [Windows]	
Irked	secnotes	Control [Windows]	
Friendzone	Bastion	October [Linux]	
Swagshop	Buff	Mango [Linux]	
Networked	Servmon	Nest [Windows]	
jarvis	Active	Book [Linux]	
Mirai	Remote	Sauna [Windows]	
Popcorn	Fuse	Cascade [Windows]	

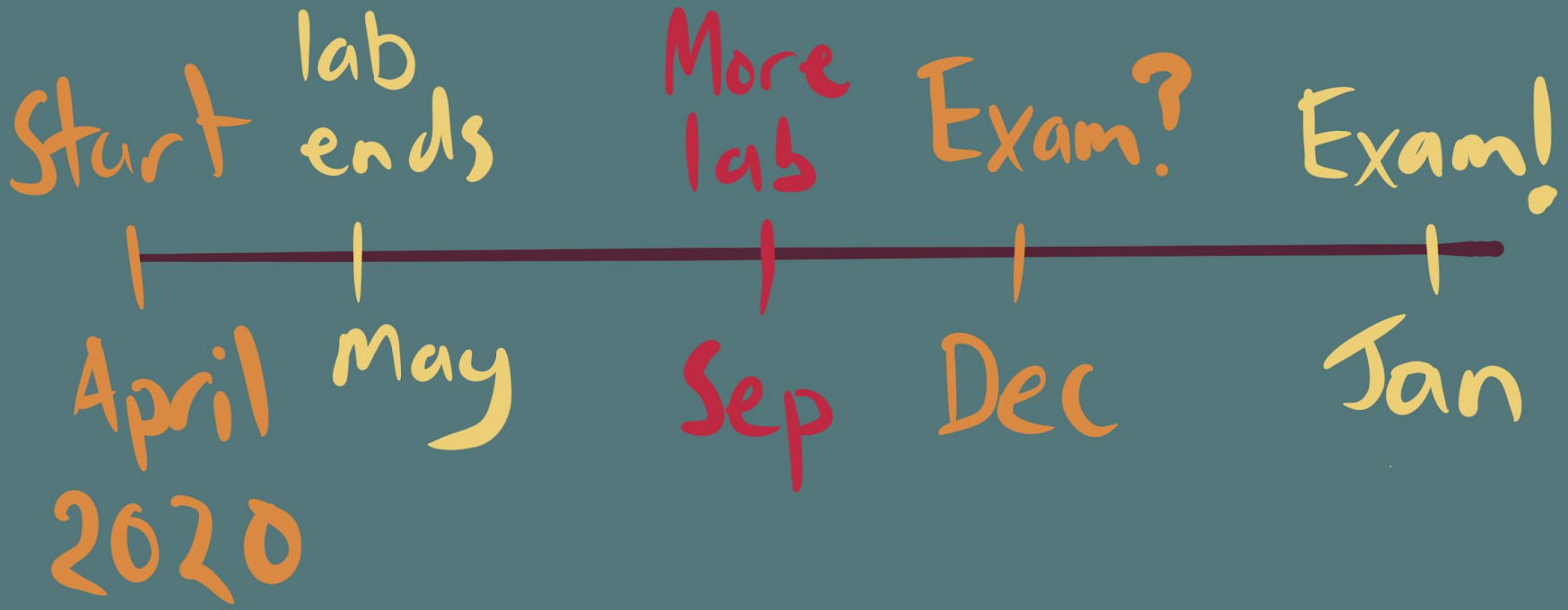
IPPSEC

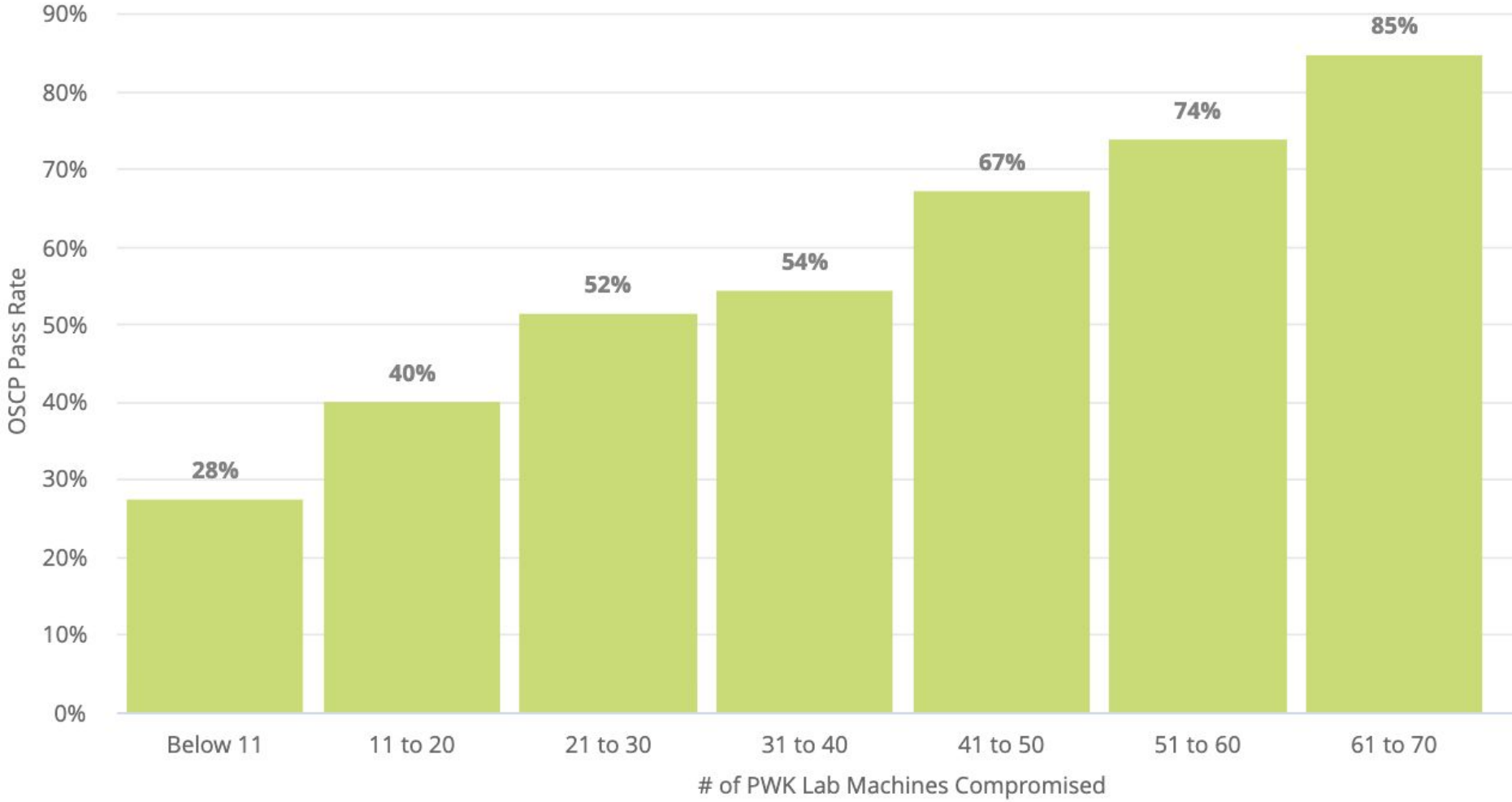
Twitter • Patreon • Youtube

kerbero

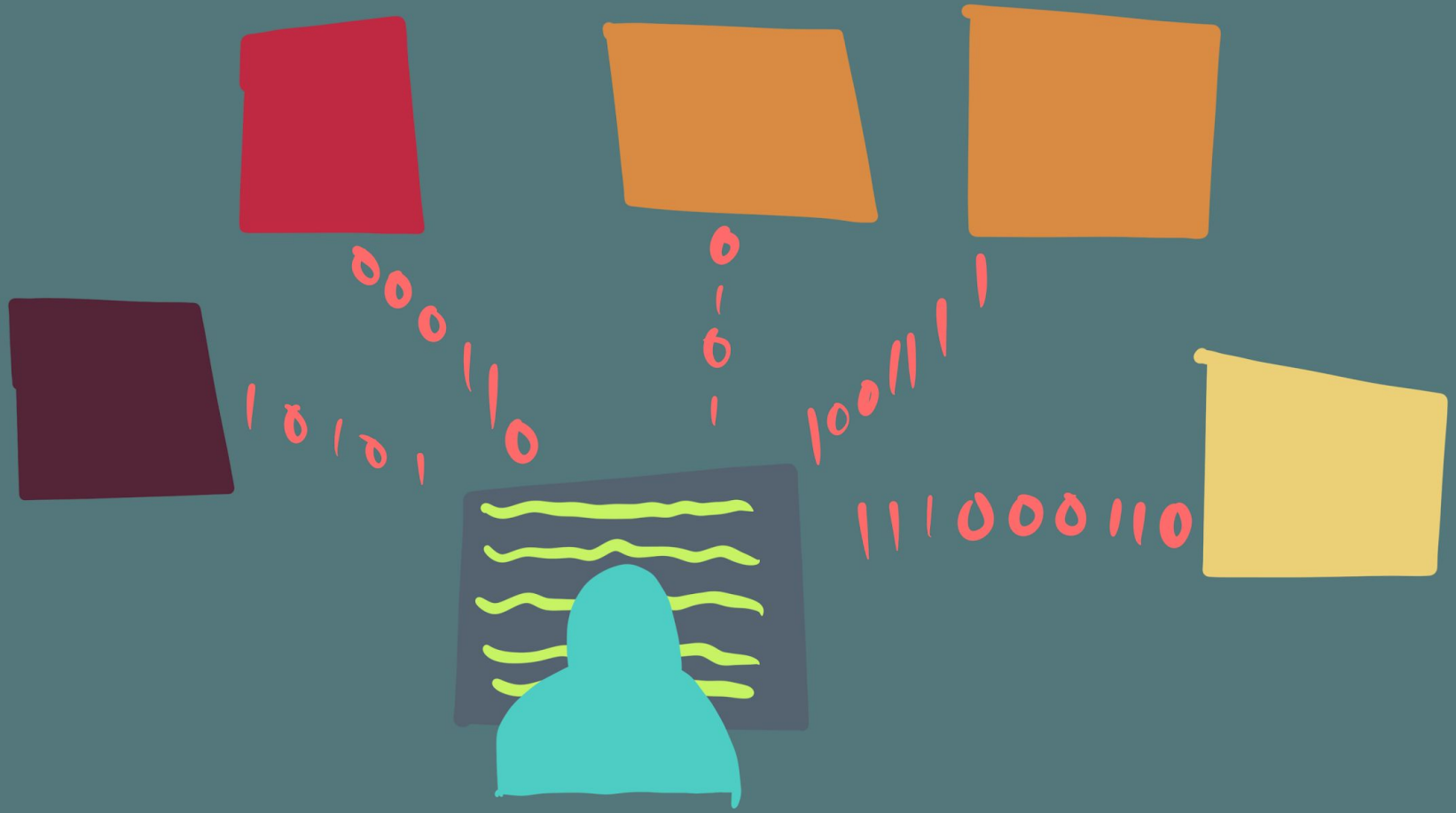
Video/Course	Description
Forest	Using GetNPUsers to perform an ASREP Roast (Kerberos PreAuth) with Null Authentication to extract SVC-ALFRESCO's hash. Then Cracking it.
Sizzle	Cannot kerberoast because of the Double Hop Problem, create token with MakeToken
Sizzle	Cracked the Kerberoasted Hash, doing maketoken with mrlky and running DCSYnc
Active	Analyzing BloodHound Output to discover Kerberostable user
Active	Performing Kerberoast attack from linux with Impacket GetUsersSPNs
Mantis	Intended Route - Forging a Kerberos Ticket MS14-068


NMAP
Impacket
Exploit DB
Python
Bash
WinPEAS
Gobuster
Github
Google


Start
lab ends
More lab
Exam?
Exam!
April 2020
May
Sep
Dec
Jan


90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
OSCP Pass Rate
28%
40%
52%
54%
67%
74%
85%
Below 11
11 to 20
21 to 30
31 to 40
41 to 50
51 to 60
61 to 70
# of PWK Lab Machines Compromised

Exam


000110
0
1
10101
100111
111000110

Recap