T12
Security Testing
2019-05-02 11:15

Security Partners or Security Police?

Presented by:

Janna Loeffler, Carnival Corp.
Yesenia Yser, Ultimate Software

Brought to you by:

888-268-8770 ·· 904-278-0524 - info@techwell.com - http://www.stareast.techwell.com/

Janna Loeffler

Janna Loeffler has more than fifteen years of software quality experience. She holds a bachelor's degree in computer engineering and a master's degree in business administration. Working in a variety of software engineering roles, including development, testing, quality assurance, and DevOps, has provided her with a holistic view of software engineering. She has worked on a wide variety of products, such as industrial controls, embedded medical devices, websites, mobile applications, and theme park attractions. Janna has a passion for helping people build high2   quality software more efficiently.

Yesenia Yser

Yesenia Yser has over eight years in Information Technology and Software Security. She holds a bachelor's degree in computer science and a master's degree in digital forensics. Her professional background is composed of security software development and incident response, with emphasis on customer support, communication, training, security, and leadership awareness. She has managed and worked on a wide range of tools, such as certificate authority, encryption service, detection and alerting, mobile applications, and risk evaluation tools on a global scale. Yesenia is also passionate learner who studies Brazilian jiu jitsu and yoga in her free time.

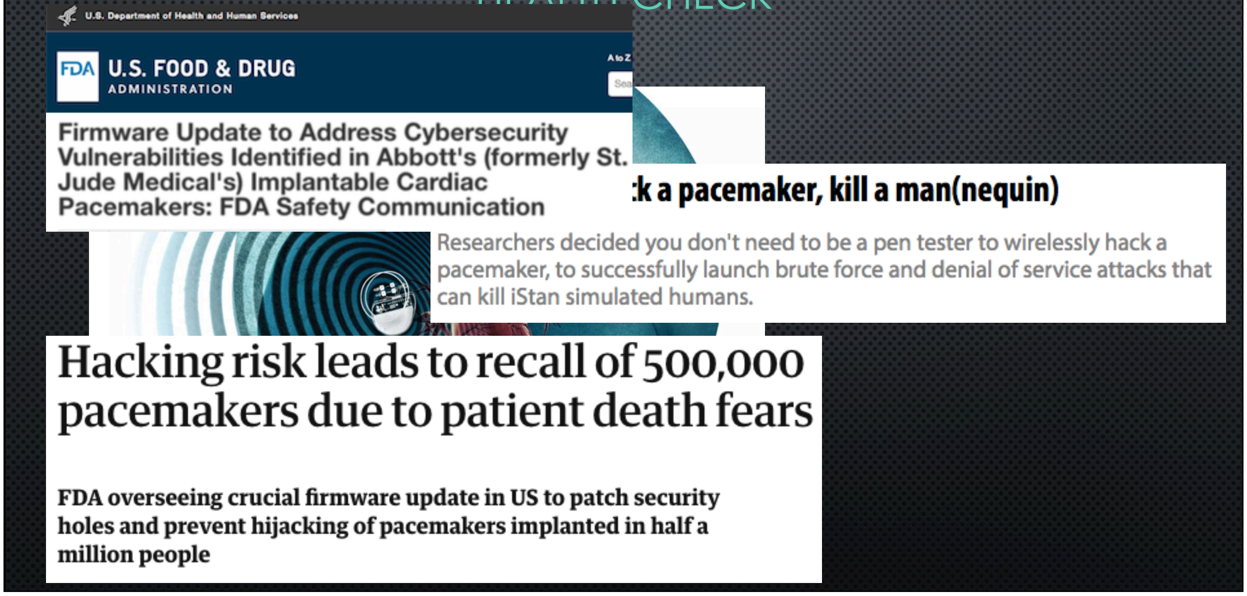
SECURITY POLICE OR SECURITY PARTNERS?

REALITY CHECK

- Tesla Model S
- Upgraded Autopilot, full self-driving capability, and the works (~10k)
- Spent over 70k
- Arrived very late yesterday
- You decide to drive it tomorrow

WATCH THIEVES STEAL YOUR CAR WITH ONLY A MOBILE PHONE AND A TABLET!

HEALTH CHECK



U.S. Department of Health and Human Services

FDA U.S. FOOD & DRUG ADMINISTRATION

Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication

k a pacemaker, kill a man(nequin)

Researchers decided you don't need to be a pen tester to wirelessly hack a pacemaker, to successfully launch brute force and denial of service attacks that can kill iStan simulated humans.

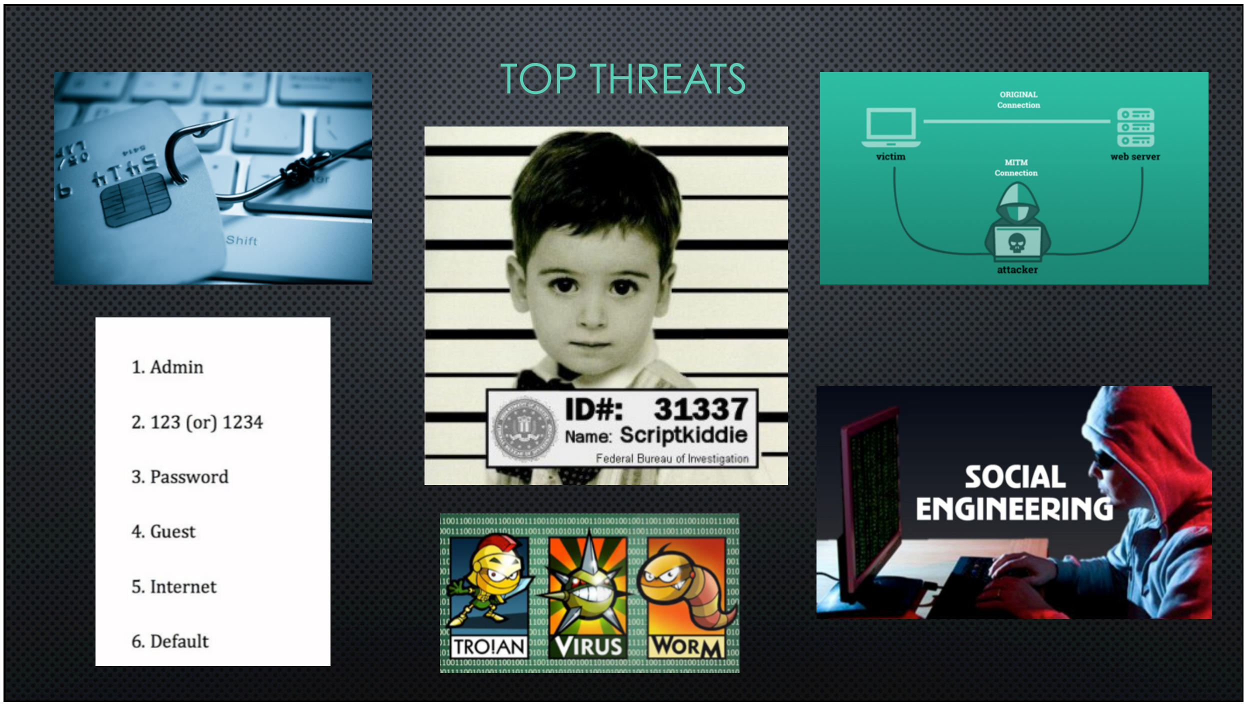
Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

WHAT ARE TOP CYBERSECURITY THREATS FACING THE ENTERPRISE?

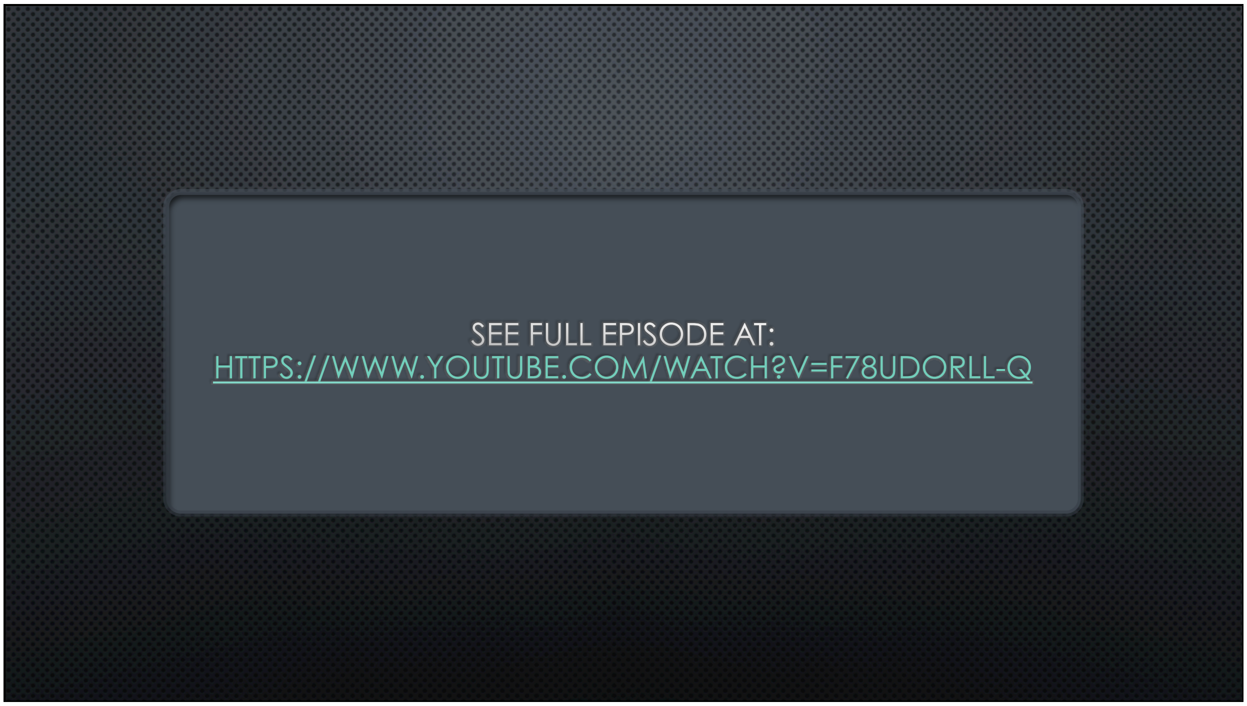
OWASP TOP TEN

- Top Ten Web Vulnerabilities 2017
  - Injection
  - Broken Authentication
  - Sensitive Data Exposure
  - XML External Entities (XXE)
  - Broken Access Control
  - Security Misconfiguration
  - Cross-Site Scripting (XSS)
  - Insecure Deserialization
  - Using Components with Known Vulnerabilities
  - Insufficient Logging & Monitoring
- Top Ten Mobile Securities 2018
  - Improper Platform Usage
  - Insecure Data Storage
  - Insecure Communication
  - Insecure Authentication
  - Insufficient Cryptography
  - Insecure Authorization
  - Client Code Quality
  - Code Tampering
  - Reverse Engineering
  - Extraneous Functionality



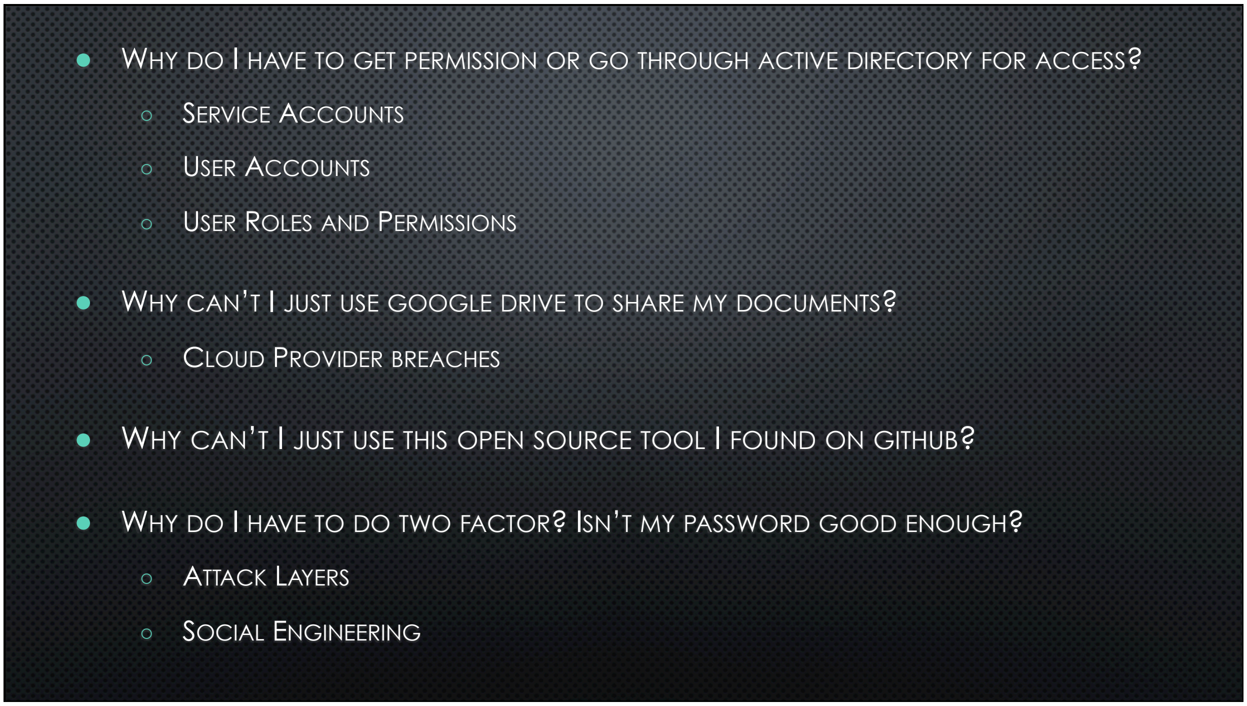
TOP THREATS

1. Admin
2. 123 (or) 1234
3. Password
4. Guest
5. Internet
6. Default



SEE FULL EPISODE AT:
HTTPS://WWW.YOUTUBE.COM/WATCH?V=F78UDORLL-Q

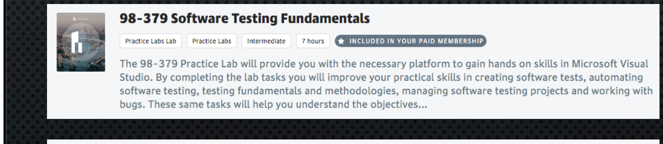
TOP COMPLAINTS ABOUT SECURITY



- Why do I have to get permission or go through active directory for access?
  - Service Accounts
  - User Accounts
  - User Roles and Permissions
- Why can't I just use google drive to share my documents?
  - Cloud Provider breaches
- Why can't I just use this open source tool I found on github?
- Why do I have to do two factor? Isn't my password good enough?
  - Attack Layers
  - Social Engineering

HOW CAN YOU BECOME A SECURITY PARTNER?

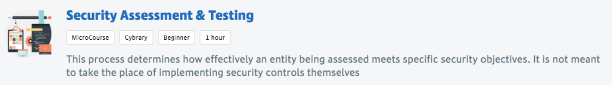
TRAINING



98-379 Software Testing Fundamentals

Practice Labs Lab | Practice Labs | Intermediate | 7 hours | ★ INCLUDED IN YOUR PAID MEMBERSHIP

The 98-379 Practice Lab will provide you with the necessary platform to gain hands on skills in Microsoft Visual Studio. By completing the lab tasks you will improve your practical skills in creating software tests, automating software testing, testing fundamentals and methodologies, managing software testing projects and working with bugs. These same tasks will help you understand the objectives...

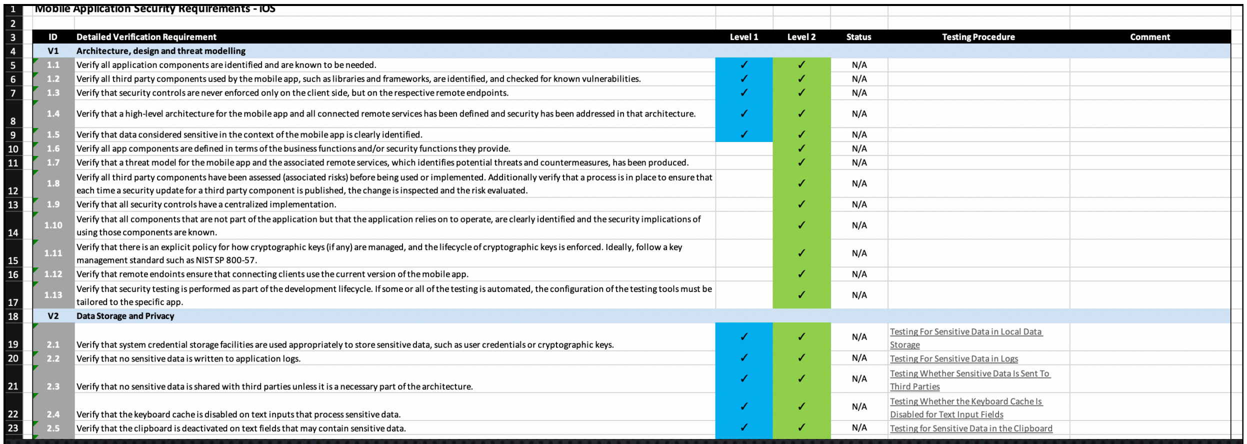


Security Assessment & Testing

MicroCourse | Cybrary | Beginner | 1 hour

This process determines how effectively an entity being assessed meets specific security objectives. It is not meant to take the place of implementing security controls themselves

- Security +
- Certified Information Systems Security Professional (CISSP)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Cloud Security Based Certificate
  - Google
  - Amazon
- HTTPS://APP.CYBRARY.IT/BROWSE
  - Free Account
  - Earn CPEs
  - Learn and Read the latest Cyber Security
  - Network with Security Professionals
  - Become an Instructor



1	Mobile Application Security Requirements - iOS						
2							
3	ID	Detailed Verification Requirement	Level 1	Level 2	Status	Testing Procedure	Comment
4	V1	Architecture, design and threat modelling					
5	1.1	Verify all application components are identified and are known to be needed.	✓	✓	N/A		
6	1.2	Verify all third party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.	✓	✓	N/A		
7	1.3	Verify that security controls are never enforced only on the client side, but on the respective remote endpoints.	✓	✓	N/A		
8	1.4	Verify that a high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	✓	✓	N/A		
9	1.5	Verify that data considered sensitive in the context of the mobile app is clearly identified.	✓	✓	N/A		
10	1.6	Verify all app components are defined in terms of the business functions and/or security functions they provide.		✓	N/A		
11	1.7	Verify that a threat model for the mobile app and the associated remote services, which identifies potential threats and countermeasures, has been produced.		✓	N/A		
12	1.8	Verify all third party components have been assessed (associated risks) before being used or implemented. Additionally verify that a process is in place to ensure that each time a security update for a third party component is published, the change is inspected and the risk evaluated.		✓	N/A		
13	1.9	Verify that all security controls have a centralized implementation.		✓	N/A		
14	1.10	Verify that all components that are not part of the application but that the application relies on to operate, are clearly identified and the security implications of using those components are known.		✓	N/A		
15	1.11	Verify that there is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.		✓	N/A		
16	1.12	Verify that remote endoints ensure that connecting clients use the current version of the mobile app.		✓	N/A		
17	1.13	Verify that security testing is performed as part of the development lifecycle. If some or all of the testing is automated, the configuration of the testing tools must be tailored to the specific app.		✓	N/A		
18	V2	Data Storage and Privacy					
19	2.1	Verify that system credential storage facilities are used appropriately to store sensitive data, such as user credentials or cryptographic keys.	✓	✓	N/A	Testing For Sensitive Data in Local Data Storage	
20	2.2	Verify that no sensitive data is written to application logs.	✓	✓	N/A	Testing For Sensitive Data in Logs	
21	2.3	Verify that no sensitive data is shared with third parties unless it is a necessary part of the architecture.	✓	✓	N/A	Testing Whether Sensitive Data Is Sent To Third Parties	
22	2.4	Verify that the keyboard cache is disabled on text inputs that process sensitive data.	✓	✓	N/A	Testing Whether the Keyboard Cache Is Disabled for Text Input Fields	
23	2.5	Verify that the clipboard is deactivated on text fields that may contain sensitive data.	✓	✓	N/A	Testing for Sensitive Data in the Clipboard	

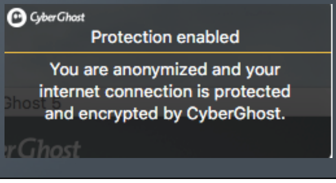
WHEN IS ENOUGH GOOD ENOUGH?

PASSWORD

- 15-20 Character +
- Mixture of Lower, Upper, and accepted Symbols
- Use a one time secret Tool/Method
  - Ask Security Team
- No
  - Sticky Notes
  - Emailing/ Iming Passwords
  - Children/Pet/Identifiable Data
  - Same Password across accounts
- Password Management System:
  - Keeper
  - 1Password
  - LastPass
  - Dashline
  - More ++

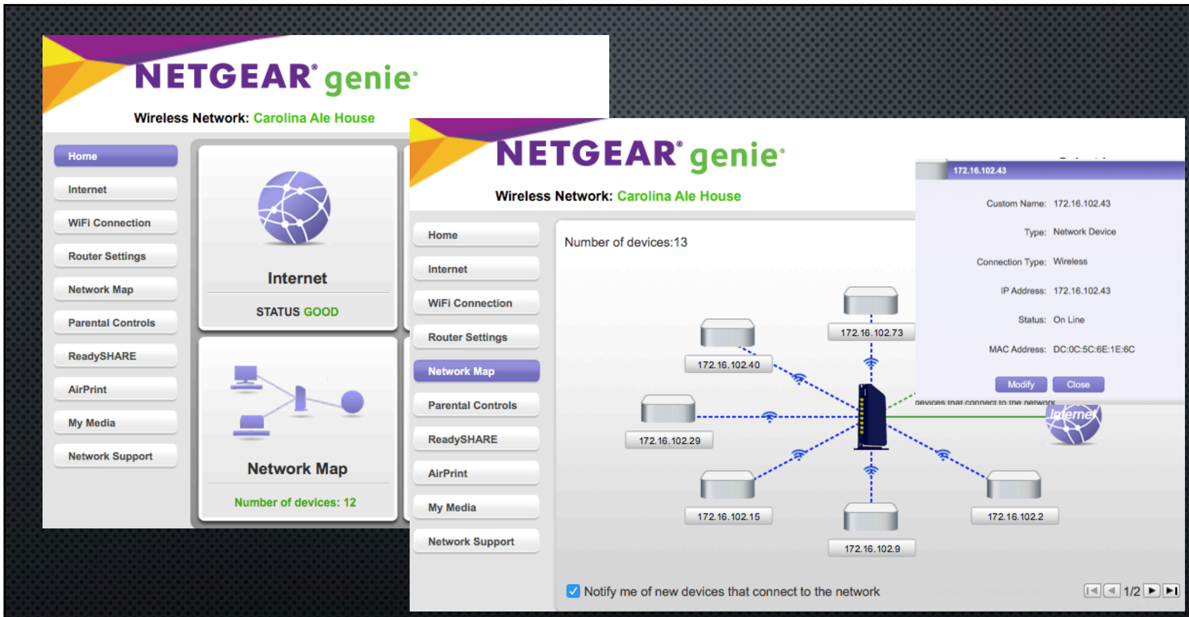
VIRTUAL PRIVATE NETWORK (VPN)

- Encrypts and protects your network traffic
- Free and Paid versions
  - CyberGhost
  - HotSpot Shield
  - IPVanish
  - ExpressVPN
  - More ++



Protection enabled

You are anonymized and your internet connection is protected and encrypted by CyberGhost.



Wireless Network: Carolina Ale House

Internet

STATUS GOOD

Network Map

Number of devices: 12

Wireless Network: Carolina Ale House

Number of devices:13

172.16.102.43

Custom Name: 172.16.102.43

Type: Network Device

Connection Type: Wireless

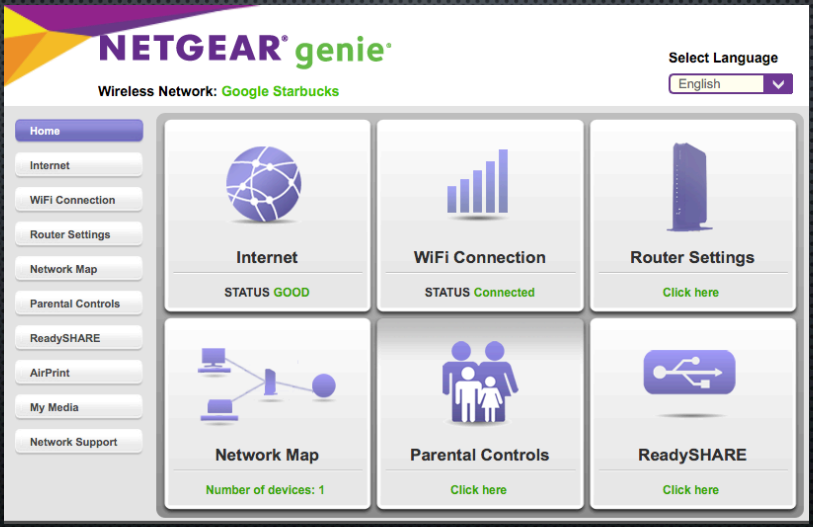
IP Address: 172.16.102.43

Status: On Line

MAC Address: DC:0C:5C:6E:1E:6C

☑ Notify me of new devices that connect to the network

1/2



Wireless Network: Google Starbucks

Select Language: English

Internet STATUS GOOD

WiFi Connection STATUS Connected

Network Map Number of devices: 1

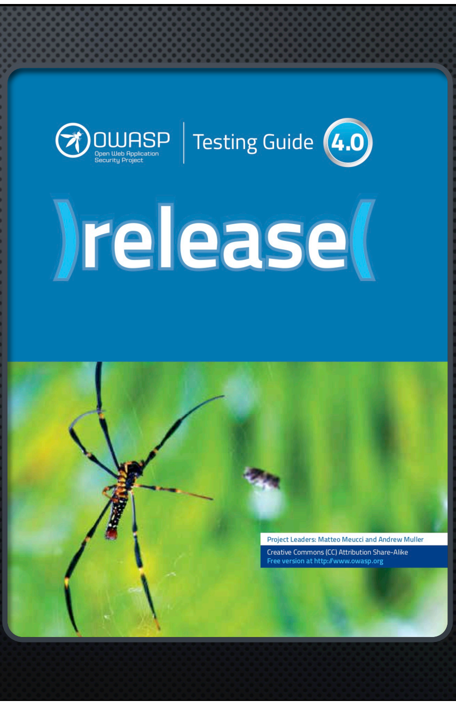
SSL / TLS CERTIFICATES

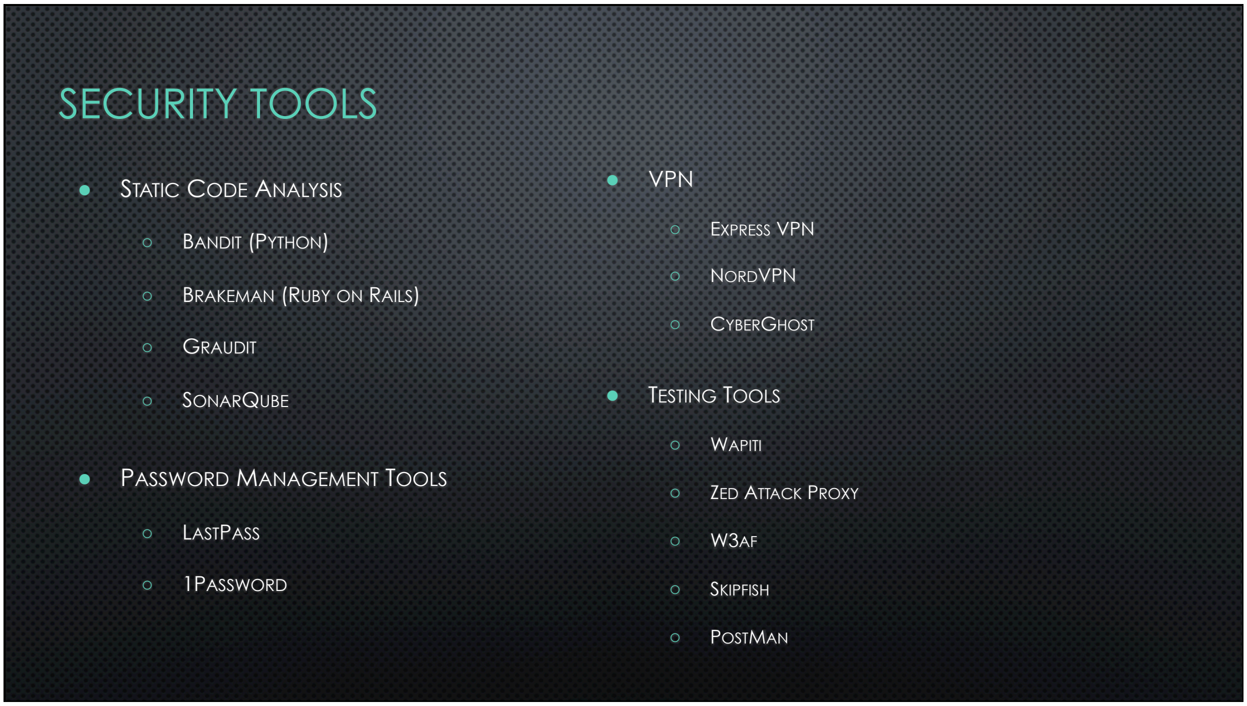
TWO-FACTOR AUTHENTICATION AND IAM SERVICES

- Two-Factor authentication
  - Yubikey or U2F
  - Push Notification
  - Time-based One Time Password (TOTP)
  - SMS / Email (Not Recommended)
- TOTP Tools
  - Google Authenticator
  - Amazon Authenticator
  - Facebook Authenticator
- IAM Services
  - Service Accounts
  - Role-Based Access Control
  - Third Party SAML Auth
    - Amazon
    - Google
    - Facebook

TESTING

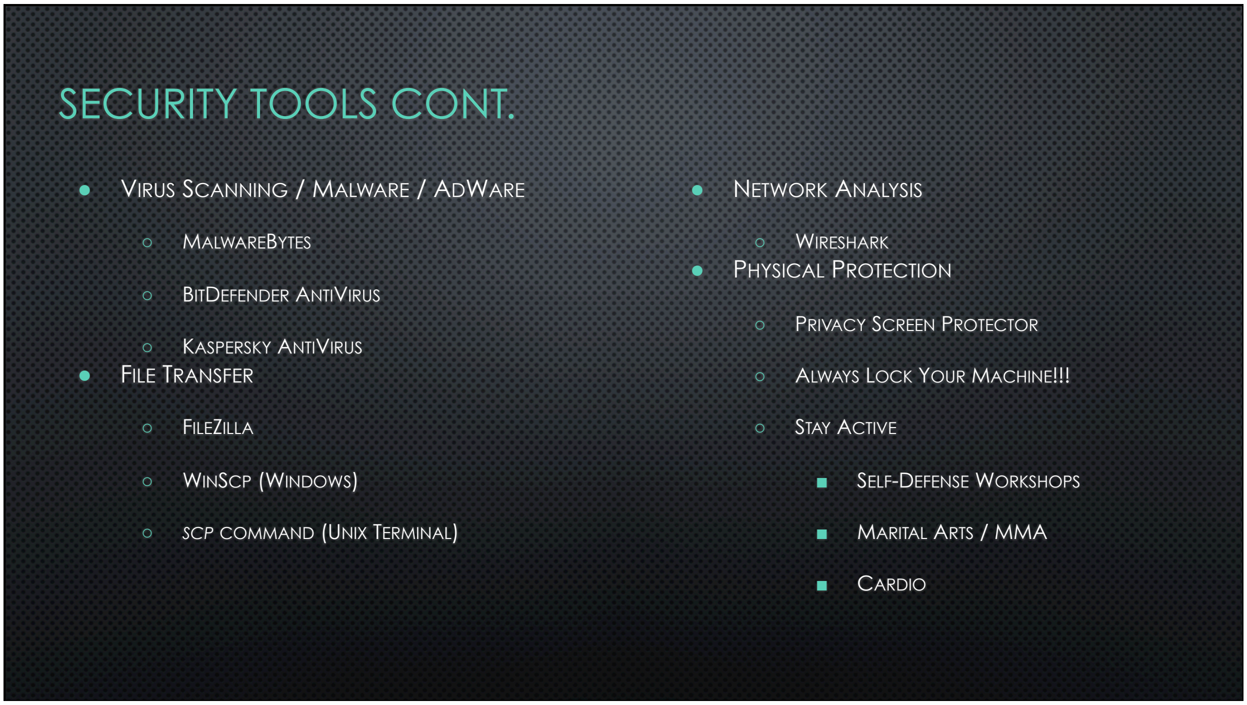
- Fuzzy testing
  - Rainbow tables for brute forcing authentication
- Sanitize and Validate your inputs
- If a user can write text, they can exploit it
  - Inject SQL and XSS during your testing
- Encryption in transition and at rest
  - Encrypt PII Databases
    - Business define PII
- Proper environment configurations, such as
  - Threshold
  - Load balancing
  - Throttle
  - Caching


OWASP
Open Web Application Security Project
Testing Guide 4.0
)release(
Project Leaders: Matteo Meucci and Andrew Muller
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org



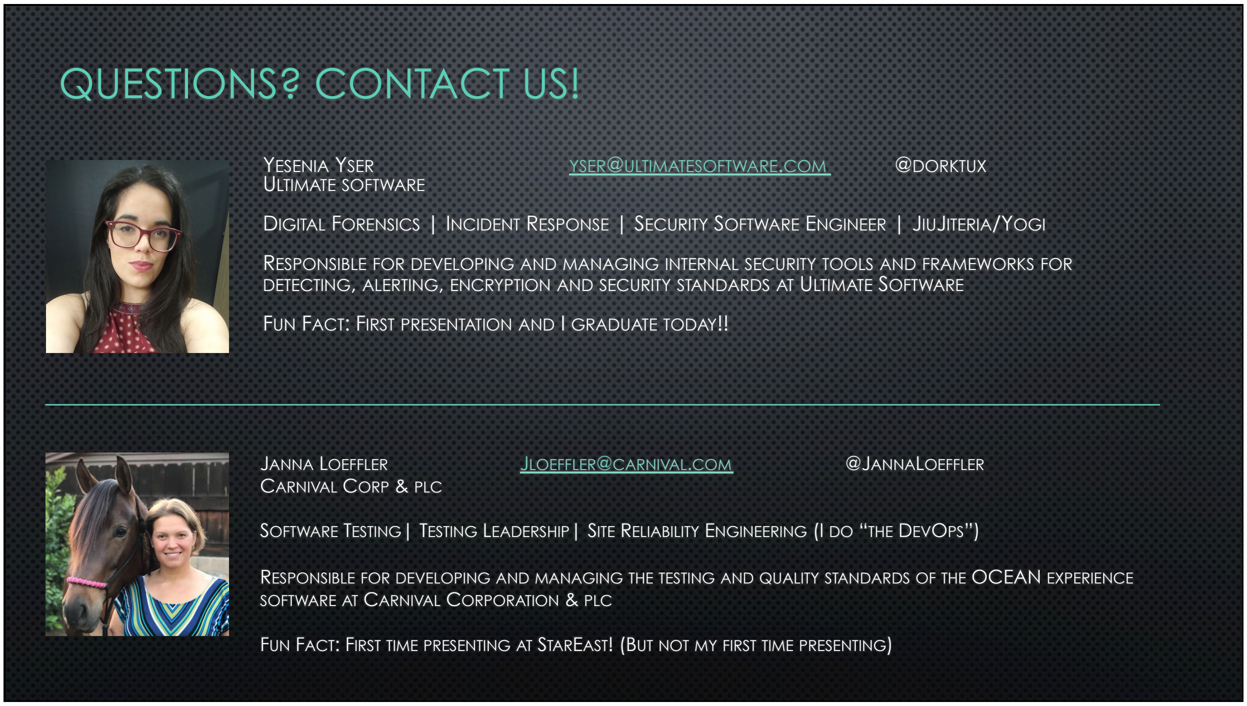
Security Tools

- Static Code Analysis
  - Bandit (Python)
  - Brakeman (Ruby on Rails)
  - Graudit
  - SonarQube
- Password Management Tools
  - LastPass
  - 1Password
- VPN
  - Express VPN
  - NordVPN
  - CyberGhost
- Testing Tools
  - Wapiti
  - Zed Attack Proxy
  - W3af
  - Skipfish
  - PostMan



Security Tools Cont.

- Virus Scanning / Malware / AdWare
  - MalwareBytes
  - BitDefender AntiVirus
  - Kaspersky AntiVirus
- File Transfer
  - FileZilla
  - WinScp (Windows)
  - *scp* command (Unix Terminal)
- Network Analysis
  - Wireshark
- Physical Protection
  - Privacy Screen Protector
  - Always Lock Your Machine!!!
  - Stay Active
    - Self-Defense Workshops
    - Marital Arts / MMA
    - Cardio



Questions? Contact us!

Yesenia Yser yser@ultimatesoftware.com @dorktux
Ultimate software

Digital Forensics | Incident Response | Security Software Engineer | JiuJiteria/Yogi

Responsible for developing and managing internal security tools and frameworks for detecting, alerting, encryption and security standards at Ultimate Software

Fun Fact: First presentation and I graduate today!!

Janna Loeffler Jloeffler@carnival.com @JannaLoeffler
Carnival Corp & plc

Software Testing| Testing Leadership| Site Reliability Engineering (I do “the DevOps”)

Responsible for developing and managing the testing and quality standards of the OCEAN experience software at Carnival Corporation & plc

Fun Fact: First time presenting at StarEast! (But not my first time presenting)