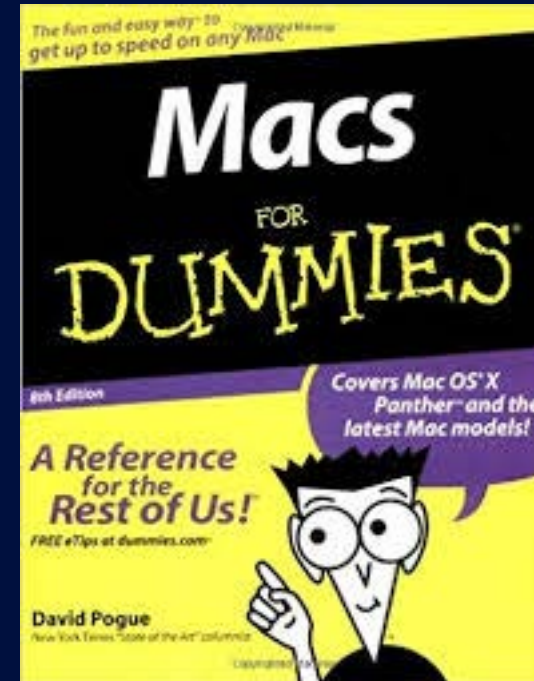


Macs for *this* Dummy

Date: 12.04.2019

Jigsaw24



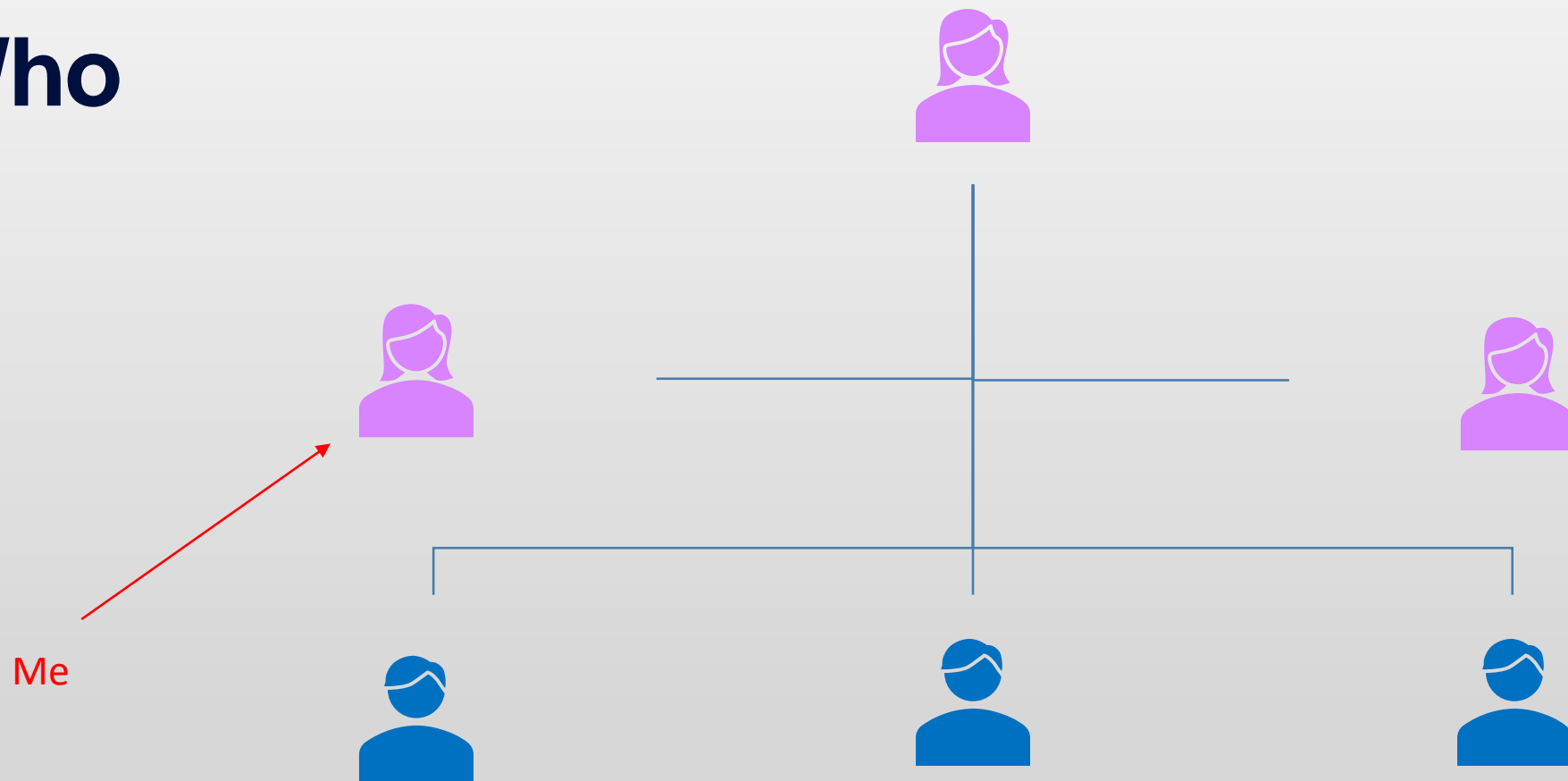
Nadine Ripley

Infrastructure Lead

Slack: @nadine.ripley

Who?
What?
Where?
When?
Why?
How?

Who



Relationship with Macs



What

Things that I'm good at:

- Organization
 - Procrastination
 - Troubleshooting
 - Error checking
 - Documentation
 - Procedure
 - Not letting go
 - Not saying no
-

What The F_____

Things I do that would look embarrassing in front of an audience

- Mac clients
 - Windows clients and servers
 - Fortigate firewall
 - HP Aruba switches
 - Frankenstein scripts you'd think your grandmother made
-

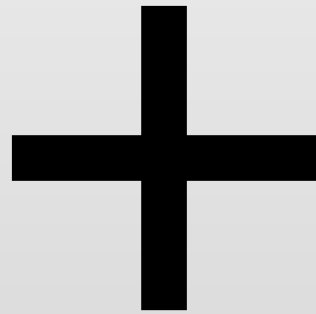
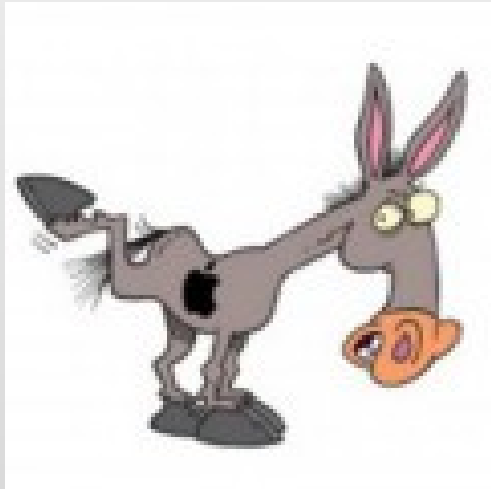
Where – Here



When – Now



Why



How

- Mostly from the hip –
“Why do today what you can put off to tomorrow”
- With a little help from a friend



Cyber Essentials Plus



CYBER
ESSENTIALS

<https://www.cyberessentials.ncsc.gov.uk>





Part of UK Government's National Cyber Security Strategy

First launched in 2014

Preceded by the “10 Steps to Cyber Security” in 2012

The benefits of certification

Cyber Essentials can help your organisation in many ways

-  Reassure customers that you take cyber security seriously
 -  Be listed on our Directory of organisations awarded Cyber Essentials
 -  Attract new business with the promise you have cyber security measures in place
- 

CyberEssentials Plus process

1. Selecting a Certification body
2. Verify your IT is suitably secure
3. Complete the self-assessment questionnaire

PLUS = independent verification

The Self Assessment Questionnaire

- Remote Vulnerability Scan
- Gold Build Assessment
- Cloud & Shared Services
- Security Controls Questionnaire

Remote Vulnerability Scan...

"URL (inc http, https, or both and full path to application entry point)

IP v4 and v6 addresses (or range)"

"Nature & Description of System (eg, firewall, website, cms)"

"System Ownership and Hosting
(eg internal system, dedicated external hosted, dedicated cloud system, shared platform)"

Do you have administrative control at the operating system level?

If out of scope, organisation should cite a reason why

"Number of authentication interfaces e.g. SSH, Telnet, Remote Desktop, Web Login Forms, SNMP, etc."

Does this service give access only to information that is both public and read-only?

...Remote Vulnerability Scann

- Do network controls restrict access to a defined, limited set of end points?
- "Number of authentication interfaces e.g. SSH, Telnet, Remote Desktop, Web Login Forms, SNMP, etc."
- Does this service give access only to information that is both public and read-only?
- Do network controls restrict access to a defined, limited set of end points?
- Is authentication based on two or more factors? (e.g username/password AND a single use code)
- Does the authentication interface throttle login attempts (to defend against brute force password guessing)?
- Does the authentication interface lockout user accounts after a maximum of 10 failed login attempts (to defend against brute force password guessing)?
- Valid credentials for the service

Cloud & Shared Services

Cloud / Shared Services Assessment

Help to complete this section

Ensure all shared services are included.

Cloud services are classified as in scope for the remote vulnerability scan where the service is a dedicated instance and there is administrative responsibility for the operating system layer and above.

All other Cloud services which are used should be listed, although they will not form part of the remote vulnerability scan. Details should be provided for any security controls which are implemented by the third party, such as ISO27001.

Notes:

- 1) This table should only be completed for shared services – dedicated platforms should be included within the hands on testing
- 2) Note remote services such as email or document stores should be included in Stage 1 but remote desktop (VDI) solutions are also relevant at Stage 2

Description of the service (with unique customer ID where relevant)	Supplier	Independent audit standards to which the suppliers has been previously assessed.	Evidence of certification provided to CB (website URLs, certificate numbers, name of independent audit bodies etc)
--	----------	--	---

Security Controls Questionnaire

- Boundary firewalls and Internet Gateways
- Secure configuration
- Access Control
- Malware protection
- Patch management

CyberEssentials Plus vs Sarbanes-Oxley

CyberEssentials Plus	Sarbanes Oxley
Makes sure you have obvious policies in place	Makes sure you have ridiculous policies in place
Skims the surface to make sure you comply at a basic level	Delves deep to make sure you can jump through hoops, while whistling, and patting your stomach



Every Little Helps Freebies from Apple

So how do we can get a free repair? - Current Apple Freebies

- Apple MacBook Keyboard Service Program
 - 13-inch MacBook Pro (non Touch Bar)
-

Thank you