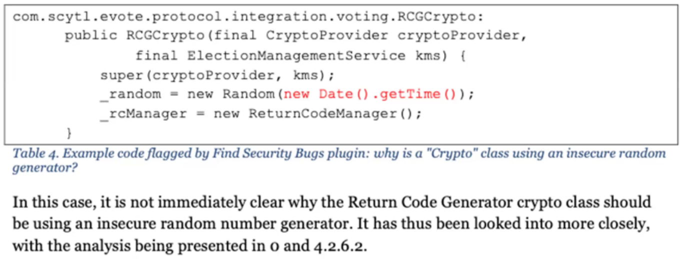
Reporting – Cybersecurity

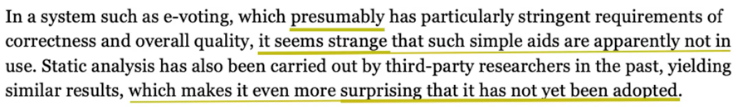
- **REPORT IS ALL YOU HAVE → LIMITED TIME TO WRITE IT**
  - **Make sure to document EVERYTHING DURING TESTING**
- **For your own comfort and safety**
  - Report as you go
    - Online, where you team can see, contribute, or step in if needed
  - Keep a collection of commonly-used sentences and paragraphs
    - Use these to guide your testing, and as anchors in your report
  - But: Never paste from one report into another, even indirectly
    - Write a generic boilerplate *outside of any actual report* → include placeholders as necessary
      - Paste THAT into the report for your current test, then fill in the details
  - **Separation of customer data is a survival skill**
- **Ask yourself as you go…**
  - Have I clearly shown what's important?
  - Am I presenting facts *so clearly they are hard to misunderstand*?
  - Am I presenting opinions clearly as *opinions*?
  - Am I including enough for a read to *intelligently disagree*?
  - Do my words and images support *informed decision-making*?
  - Does my writing *show* respect for *my readers*?
  - Have I *assumed too much* about my readers or their world?
- You can look at past reports for ideas
- Reporting for Pentesters
  - Why are you doing this?
    - To make things better
  - **REPORT**
    - Testing ends → report lives forever
      - Do a good job writing stuff down as you go
    - Report communicates the important parts of the test
      - Vulnerabilities

      - Unique threats and problems in the environment
    - And things that site does well (include the good things)
      - Need to make sure they remember to continue to do the good things → make sure to include positive findings
  - Report is one of many inputs a person will have
    - Part of the story, but not whole story
      - You are a guest → you don't know everything
  - Report is your chance to *guide* improvements in the environment → not to *dictate* (your perspective as a security expert)
  - A **STORY** of the environment as you, a *security expert*, saw it
  - A **tool** for guiding **action**
    - Not just a list of problems → what do we do about those problems
  - A **resource** where interested readers can learn things → more you can teach by showing what you did and why, the better
    - This is what I did, this is how I countered for things that could've gone wrong, this was the output, and this is why it is important
  - **Evidence** of the state of the target at a point in time
    - …and, yes, your skills as a tester → side-effect, not a goal
      - Don't grandstand
- Action makes things better
  - Testing doesn't do it → can't test your way to a secure environment
  - Reporting doesn't do it → it's just a document
  - *Action*, based on the report, which is based on testing and perspective and experience and attention to detail, is what makes things better
    - That's the **goal**
- **The report is THE thing you get to pass on** → make it a good one
- Tone → style or manner of expression
  - Cause for the feelings you get when you read something
  - Determines how you message will be received
    - Partly what you say, what you don't say, and how you say it

- **Make the report actionable, palatable, and usable** → you are telling them what they messed up
- Examples in reports:
    - *This issue can be fixed by simply installing a patch*
        - They are going to hear it as condescending
    - *A small GPO update will quickly solve this problem*
        - Technical fix might be quick, but you don't know everything about the environment → can't imply it is an easy fix (it may not be)
        - Report it in a way that acknowledges the expertise of the people you are reporting it to → be kind and factual
            - Don't **ever** imply they don't know what they are doing
    - *The risk can be resolved by just disabling weak cipher suites*
        - A simple fix can have larger impacts → could disable something you aren't aware of
            - **You don't know**
    - 

      ```
      com.scytl.evote.protocol.integration.voting.RCGCrypto:
            public RCGCrypto(final CryptoProvider cryptoProvider,
                    final ElectionManagementService kms) {
                super(cryptoProvider, kms);
                _random = new Random(new Date().getTime());
                _rcManager = new ReturnCodeManager();
            }
      ```

      Table 4. Example code flagged by Find Security Bugs plugin: why is a "Crypto" class using an insecure random generator?

      In this case, it is not immediately clear why the Return Code Generator crypto class should be using an insecure random number generator. It has thus been looked into more closely, with the analysis being presented in 0 and 4.2.6.2.
        - Why would you ask a negative rhetorical question as a caption? → doesn't tell the story of the environment; doesn't tell how to make things better
    - 

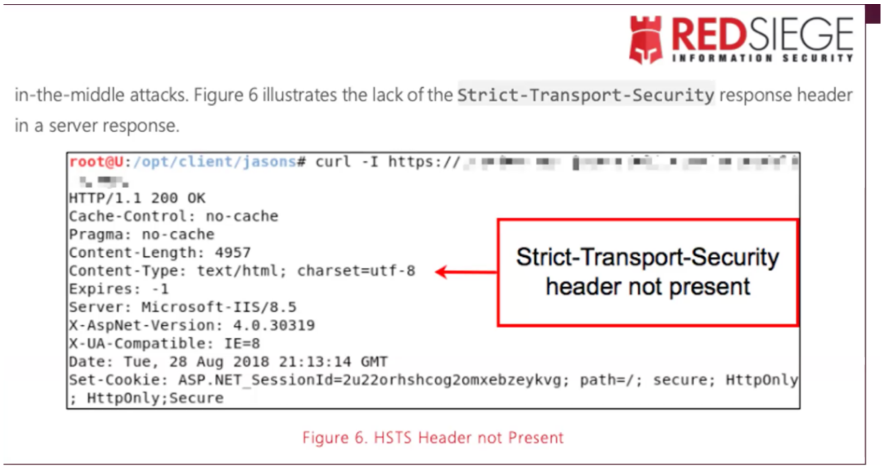
      In a system such as e-voting, which presumably has particularly stringent requirements of correctness and overall quality, it seems strange that such simple aids are apparently not in use. Static analysis has also been carried out by third-party researchers in the past, yielding similar results, which makes it even more surprising that it has not yet been adopted.
        - Bro this is so bad

        - Even if you are correct about all the facts, a bad tone, will make the reader go out of their way NOT to trust you
    - Small thing → big thing
        - How do I describe this issue? → I want them to make changes to fix this issue
    - **Public pentesting reports on github**
- **What is a good report**
    - **Good is NOT perfect**
        - Okay, and important to acknowledge
        - Perfect is not achievable
            - Some point after “good” and before “perfect” you are wasting energy
    - A source of facts → with evidence to back them up
        - Ex. un an environment you had this many systems; this many systems running this; this many systems behind on patches → things you found
    - A source of expert analysis to put facts in context
        - Your analysis → bring to light the significance of the facts
        - **Impact of the vulnerabilities**
            - Show what happens if you exploit it
            - How to make it harder to exploit
    - An opportunity for readers to learn → don’t force learning
        - **Different audiences**
        - Technical: how to *find* problems, *fix* them, and *re-test* them after changes
            - Before next pentest can try and improve their security
        - Business: how technical problems affect “the business”
        - Everyone: why the problems found are worth thinking about
            - You want to scare them → show the bad things that can happen
    - One of the many references for decision-making in an organization
    - The appearance of professionalism
        - Don’t use crayons. Don’t randomly switch fonts. Do pay attention to *appearance*

        - Good, clear summary and introduction → find a friend in an English department to review the report (so, me lmao)
    - **Facts are good**
        - The report: a source of facts, with evidence to back them up
            - Make your facts and your evidence HARD TO MISUNDERSTAND → no other way to interpret what I am saying
        - Facts establish relevant aspects of reality
        - A fact is something that has been verified → something TRUE
        - Evidence, in a report, is usually best provided as a **SCREENSHOT**
            - A screenshot is a real thing that actually happened → led you to believe something to be true
                - Shows readers how you found it
- Facts and expert analysis (opinion based on something) → both are needed but be clear about what is what
    - **Facts first**
        - Fact:
            - Something that is objectively true
            - Something that actually happened
            - Something with a verifiable existence
            - Examples:
                - ~~"The file shares had weak permissions"~~ → "The file share at //fs0I (at this location) allowed any authenticated user to read and write files to it"
                - ~~"The server was running an unsupported version of Nginx"~~ → "The HTTP response headers indicated an unsupported version of Nginx"
        - Establish the facts by including screenshots → pics or it didn't happen
            - Hinges on the idea that we accept visual evidence as fact
            - "Pictures don't lie" (but people can)
            - Goes without saying: don't manipulate the photo (obviously you can underline and highlight what is important)

- Can’t get away from trust: need the reader to trust you → cultivate the appearance of trustworthiness
  - Do NOT doctor your screenshots
    - Cropping, annotating, and redacting are not “doctoring”
    - Omitting important and relevant info → BAD
    - Changing dates or IP addresses or anything else → BAD
- Use screenshots to illustrate any issue → always use when making a claim……
  - That a dishonest person in your position might use to harm or mislead
  - That an inexperienced or rushed person in your position might make a wrong conclusion
    - Highlight important parts, etc.
  - Where interpretation of raw data is key
    - Take screenshot of the response (date and timestamp) → **use HTTP response**
- Good subjects for screenshots
  - Vulnerability scanner or attack configuration details
  - Sensitive data stored insecurely (redact the sensitive parts)
  - Evidence of exploited vulnerability
    - If you got admin access to something, how do you prove it?
      - Ex. show local groups and show your username is in the administrator role
- **Imagine that you must defend this evidence in court**
  - Make it clear where the facts end and your interpretations begin
- Compose the shot first
  - Arrange your display so the screenshot can…
    - Include what you want to show
      - Focus on what is important
    - NOT include anything else
  - Add plain boxes and arrows to direct attention

        - Drop-shadows and embellishments are crayons → don’t use crayons
        - **Find a screenshot editor you like and only use that one**
    - Keep text in the screenshot about the same size as the text around it (body of the report)



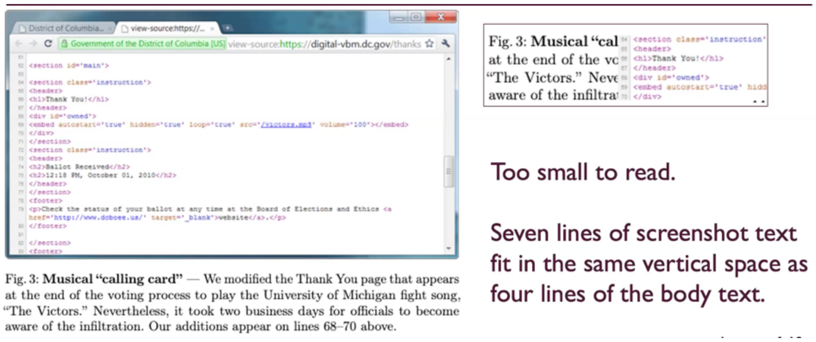
REDSIEGE INFORMATION SECURITY

in-the-middle attacks. Figure 6 illustrates the lack of the `Strict-Transport-Security` response header in a server response.

```
root@U:/opt/client/jasons# curl -I https://[redacted]
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 4957
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-UA-Compatible: IE=8
Date: Tue, 28 Aug 2018 21:13:14 GMT
Set-Cookie: ASP.NET_SessionId=2u22orhshcog2omxebzeykvg; path=/; secure; HttpOnly
; HttpOnly;Secure
```

Figure 6. HSTS Header not Present

        - In real report url probably wouldn’t be redacted
        - Shows evidence of absence
        - Two nitpicks: doesn’t prove that strict-transport-security header is not there; not obvious included all http headers (adjust by a line or two); curl -I (possible, but extremely unlikely that server could respond differently to get requestion → should’ve used get request instead)



District of Columbia...
view-source:https://...
Government of the District of Columbia [US] view-source:https://digital-vbm.dc.gov/thanks

```
61
62 <section id='main'>
63
64 <section class='instruction'>
65 <header>
66 <h1>Thank You!</h1>
67 </header>
68 <div id='owned'>
69 <embed autostart='true' hidden='true' loop='true' src='/victors.mp3' volume='100'></embed>
70 </div>
71 </section>
72 <section class='instruction'>
73 <header>
74 <h2>Ballot Received</h2>
75 <h2>12:18 PM, October 01, 2010</h2>
76 </header>
77 </section>
78 <footer>
79 <p>Check the status of your ballot at any time at the Board of Elections and Ethics <a
   href='http://www.dcboee.us/' target='_blank'>website</a>.</p>
80 </footer>
81
82 </section>
83 <footer>
```

Fig. 3: **Musical “calling card”** — We modified the Thank You page that appears at the end of the voting process to play the University of Michigan fight song, “The Victors.” Nevertheless, it took two business days for officials to become aware of the infiltration. Our additions appear on lines 68–70 above.

Fig. 3: **Musical “cal**
at the end of the vc
“The Victors.” Neve
aware of the infiltrat

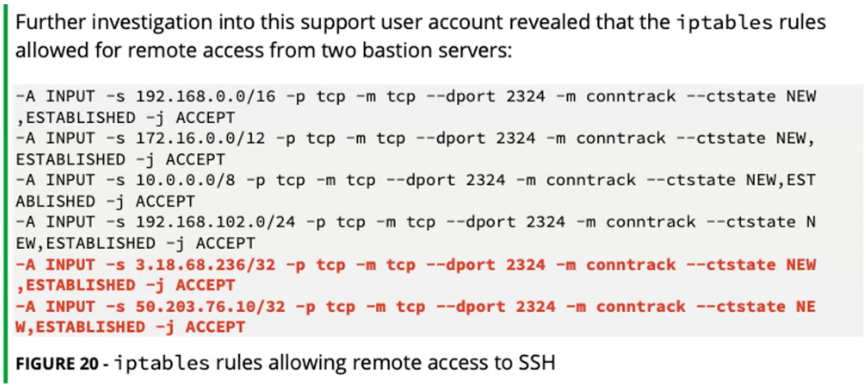
```
64 <section class='instruction'
65 <header>
66 <h1>Thank You!</h1>
67 </header>
68 <div id='owned'>
69 <embed autostart='true' hidd
70 </div>
```

Too small to read.

Seven lines of screenshot text fit in the same vertical space as four lines of the body text.

    -
        - Showing too many lines → should only be about half as tall and half as wide
- Use text when a reader may want to copy-paste it to run the command yu ran

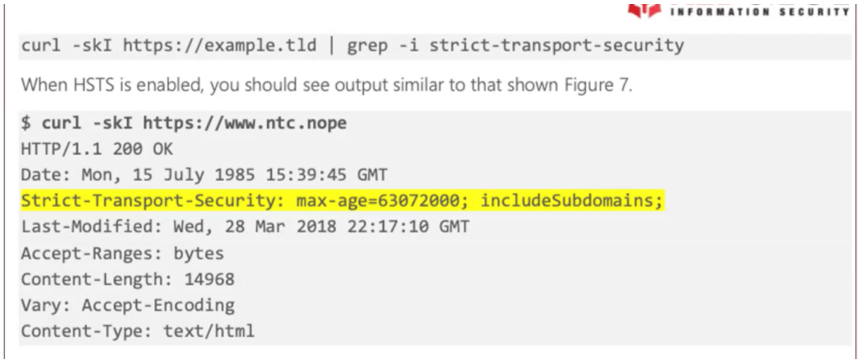
  - Also: make sure the command will run if copy-pasted
    - Ex. when. Operating on a file, does the reader have that file?
    - Ex. command line environment doesn't know what to do with "smart quotes"
      - Make sure word doesn't change you -- to an –
- Use text when you can't get a legible screenshot
- Use text where it's helpful AND where a dishonest person in your position has little incentive to mislead
- Sometimes you will use BOTH text and a screenshot
  - Show it graphically and then with text → make it CLEAR
- Compose the scene first
  - Arrange your text so that it…
    - Includes what you want to show, and
    - As little else as practical
  - Add color or bold or highlighting → direct attention
  - Use a different font than the report's body so that text stands out
    - Convention: use a fixed-width font for these "text screenshots"
  -



Further investigation into this support user account revealed that the `iptables` rules allowed for remote access from two bastion servers:

```
-A INPUT -s 192.168.0.0/16 -p tcp -m tcp --dport 2324 -m conntrack --ctstate NEW
,ESTABLISHED -j ACCEPT
-A INPUT -s 172.16.0.0/12 -p tcp -m tcp --dport 2324 -m conntrack --ctstate NEW,
ESTABLISHED -j ACCEPT
-A INPUT -s 10.0.0.0/8 -p tcp -m tcp --dport 2324 -m conntrack --ctstate NEW,EST
ABLISHED -j ACCEPT
-A INPUT -s 192.168.102.0/24 -p tcp -m tcp --dport 2324 -m conntrack --ctstate N
EW,ESTABLISHED -j ACCEPT
-A INPUT -s 3.18.68.236/32 -p tcp -m tcp --dport 2324 -m conntrack --ctstate NEW
,ESTABLISHED -j ACCEPT
-A INPUT -s 50.203.76.10/32 -p tcp -m tcp --dport 2324 -m conntrack --ctstate NE
W,ESTABLISHED -j ACCEPT
```

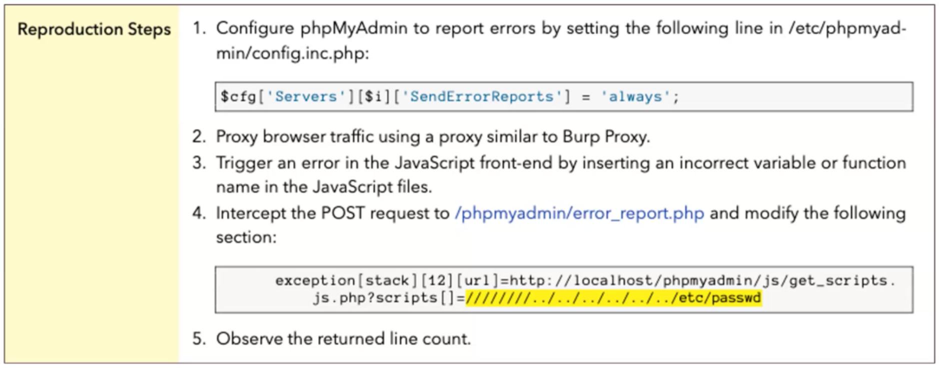
FIGURE 20 - `iptables` rules allowing remote access to SSH

- 
  INFORMATION SECURITY

  ```
  curl -skI https://example.tld | grep -i strict-transport-security
  ```

  When HSTS is enabled, you should see output similar to that shown Figure 7.

  ```
  $ curl -skI https://www.ntc.nope
  HTTP/1.1 200 OK
  Date: Mon, 15 July 1985 15:39:45 GMT
  Strict-Transport-Security: max-age=63072000; includeSubdomains;
  Last-Modified: Wed, 28 Mar 2018 22:17:10 GMT
  Accept-Ranges: bytes
  Content-Length: 14968
  Vary: Accept-Encoding
  Content-Type: text/html
  ```

- 
  Reproduction Steps

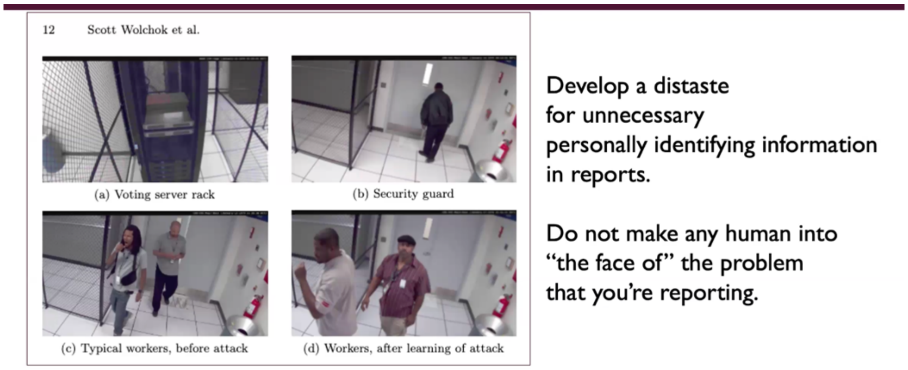
  1. Configure phpMyAdmin to report errors by setting the following line in /etc/phpmyadmin/config.inc.php:

     ```
     $cfg['Servers'][$i]['SendErrorReports'] = 'always';
     ```

  2. Proxy browser traffic using a proxy similar to Burp Proxy.
  3. Trigger an error in the JavaScript front-end by inserting an incorrect variable or function name in the JavaScript files.
  4. Intercept the POST request to /phpmyadmin/error_report.php and modify the following section:

     ```
     exception[stack][12][url]=http://localhost/phpmyadmin/js/get_scripts.
         js.php?scripts[]=///////../../../../../../etc/passwd
     ```

  5. Observe the returned line count.

- 
  12 Scott Wolchok et al.

  (a) Voting server rack

  (b) Security guard

  (c) Typical workers, before attack

  (d) Workers, after learning of attack

  Develop a distaste for unnecessary personally identifying information in reports.

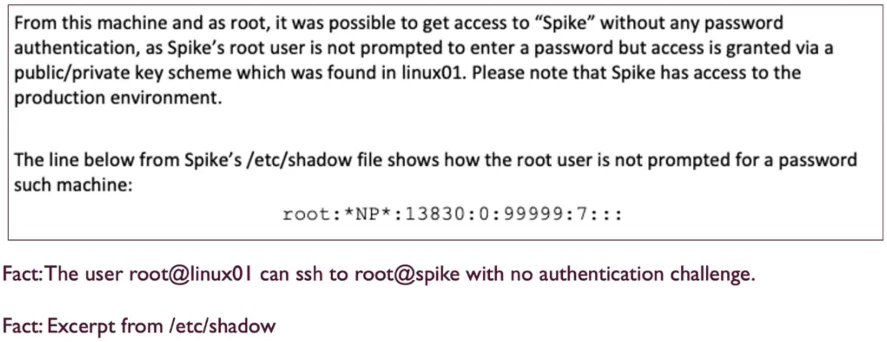
  Do not make any human into "the face of" the problem that you're reporting.

  - Don't show humans → if you need to, redact their faces

- **Imagine something goes wrong** → don't give an opposing legal team anything to go off of (accurate and clear reports)
- Make it obvious which systems or components were involved and when it happened
  - Timestamps, hostname, source IP address, targeted IP address, current username, etc.
- State plainly whether an action had the expected result or not → don't use "success", "unfortunately", "fortunately", etc (means different things to different people)

  - Show any non-trivial command line invocations used
  - If an action was detected, blocked, or otherwise interfered with, say so
    - Call it out when you customer does something right → help them keep doing it
    - Include evidence of detection or interference
- Expert analysis second
  - As security expert, your opinion carries weight → **be clear it is not a fact**
  - Some opinions are facts in disguise → choose words carefully
    - "The 'Domain Users' group should not have write permission on network file shares" (says who?)
      - "Overly-permissive file share permissions can present an attack vector"
    - "This old web server needs to be patched" (says who?)
      - "Outdated systems pose greater risk because they are more likely to include publicly-known vulnerabilities that a low-skilled attacker can exploit"
    - Avoid word "should" or "it is recommended" (specify who recommends) → be clear about where the "should" comes from
      - Convey harm of keeping vs benefits of fixing
      - Use "could"
  - Beware of "unfortunately" and "fortunately"
  - Beware of passive "recommendations"
    - Helps avoid questions
- Expert analysis should be fairly expert
  - Be sure your analysis is correct, or at least not wrong
  - Remember humans work on assumptions → you are human
    - Validate the assumptions you are relying on
      - Does the "enable version 3" setting mean that version 2 is disable?
      - Did your attack fail because the system wasn't vulnerable?
        - Did you make a mistake?

            - Did something block it?
            - A typo?
            - Did you misunderstand the attack?
        - All reasons for “failure” are in play → be humble
        - Do your research in the moment → okay to stop testing
        - Temper your claims of doom and destruction → back them up
        - Allow for unknowns → there are a lot of things you don’t know happening
        - Acknowledge conflicting goals → there’s a reason they haven’t retired Windows 7
            - Still point it out, but do it kindly

- Report summary
    - The report: A source of expert analysis: facts in context
    - *Expert Analysis* is interpreting facts
        - It is not fact
            - Another expert with same facts may produce different analysis
                - Both may provide value
                - Sometimes, neither will be “correct”
        - “Microsoft has recommended disabling SMBv1 since 2016” → give link to where Microsoft says it
            - What way of phrasing it will most likely lead to **action**
        - Analysis lost in translation → choose your words carefully
    - It takes skill to discover facts
    - It takes experience and judgement to do reliable analysis
    - It takes some writing skill to explain it all
    - 

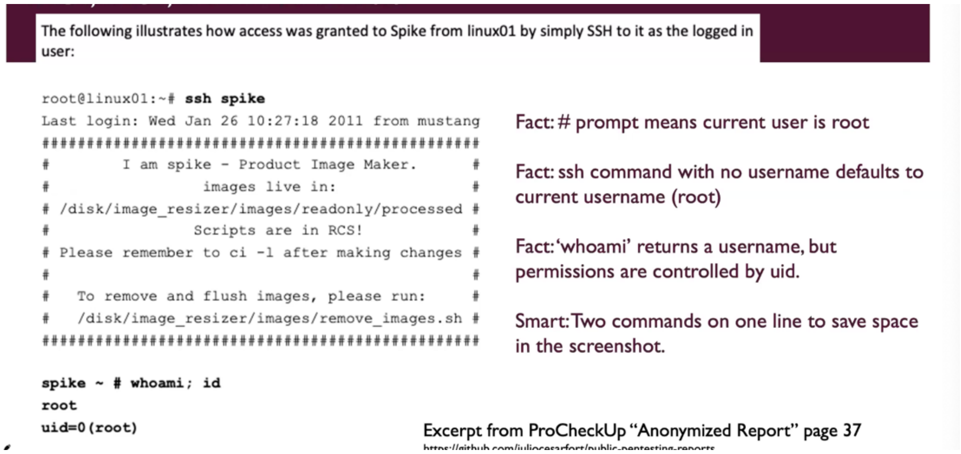
From this machine and as root, it was possible to get access to “Spike” without any password authentication, as Spike’s root user is not prompted to enter a password but access is granted via a public/private key scheme which was found in linux01. Please note that Spike has access to the production environment.

The line below from Spike’s /etc/shadow file shows how the root user is not prompted for a password such machine:

```
root:*NP*:13830:0:99999:7:::
```

Fact: The user root@linux01 can ssh to root@spike with no authentication challenge.

Fact: Excerpt from /etc/shadow

    - 

The following illustrates how access was granted to Spike from linux01 by simply SSH to it as the logged in user:

```
root@linux01:~# ssh spike
Last login: Wed Jan 26 10:27:18 2011 from mustang
################################################
#        I am spike - Product Image Maker.     #
#                 images live in:              #
# /disk/image_resizer/images/readonly/processed #
#                Scripts are in RCS!           #
# Please remember to ci -l after making changes #
#                                              #
#   To remove and flush images, please run:    #
#   /disk/image_resizer/images/remove_images.sh #
################################################

spike ~ # whoami; id
root
uid=0(root)
```

Fact: # prompt means current user is root

Fact: ssh command with no username defaults to current username (root)

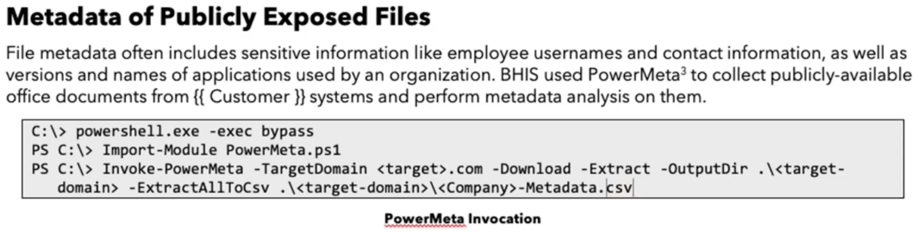
Fact: 'whoami' returns a username, but permissions are controlled by uid.

Smart: Two commands on one line to save space in the screenshot.

Excerpt from ProCheckUp "Anonymized Report" page 37

https://github.com/juliocesarfort/public-pentesting-reports

- Teaching is good → help the reader follow in your footsteps
    - Technical: how to find problems and how to tell when they are fixed
    - Business: how technical problems affect business needs
    - More context you have in common with your readers, the less error-prone the communication → always a gap
    - Assume a *baseline of intelligence, competence,* and *desire* to do the right things
    - Tell them what they need to know to make sense of what you're showing them
    - Baseline of competence….
        - Show them what you did, but not every single step of it
        - Better writing means fewer phone calls and follow up meetings



Metadata of Publicly Exposed Files

File metadata often includes sensitive information like employee usernames and contact information, as well as versions and names of applications used by an organization. BHIS used PowerMeta[3] to collect publicly-available office documents from {{ Customer }} systems and perform metadata analysis on them.

```
C:\> powershell.exe -exec bypass
PS C:\> Import-Module PowerMeta.ps1
PS C:\> Invoke-PowerMeta -TargetDomain <target>.com -Download -Extract -OutputDir .\<target-
   domain> -ExtractAllToCsv .\<target-domain>\<Company>-Metadata.csv
```

PowerMeta Invocation

    -

- Clarity is good → you have 2 audiences
    - Audience = readers
        - Never lose sight of your audience
        - Use terms they'll know, and an approachable tone
        - Use language they're comfortable with
        - Treat them with respect
        - Assume they are your equal in every way….

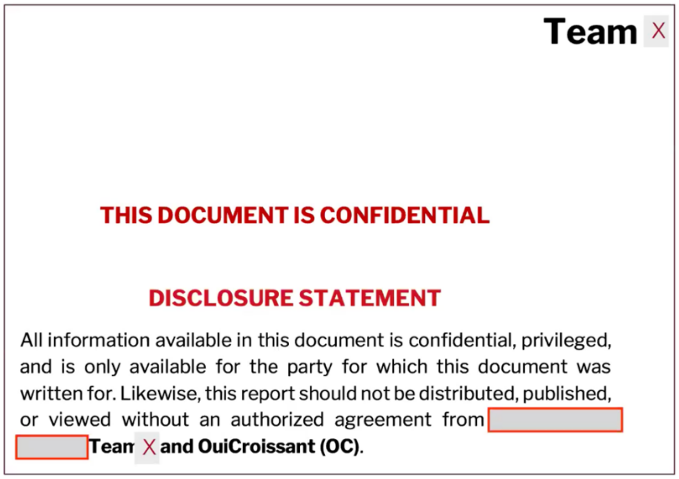
- EXCEPT for your knowledge of the details of pentesting and this particular test
  - Also: let your skills be quietly implied by your report

- Technical audience
  - People who read the bulk of the report → fix the problems
  - Assume they want to learn
  - They need to do what you did and see what you saw → fix it and rerun the problem
  - Set priorities (ex. of what to fix) within their area of responsibility
  - The more you teach them, the better they do
    - And the more they’ll like your work
    - AND the less they’ll call you later for explanations
- Business audience
  - Decide whether to hire you again, based on report
  - Will allocate resources and set priorities
  - Need to know how the technical stuff affects the business
  - Need to know which managerial levels they can pull → process oriented; root cause of the process
    - Is it a technical fix, personnel fix, policy fix, etc?
  - The report is an Executive Summary for them
- Both audiences:
  - Are smart
  - May not share your priorities or domain knowledge
  - Anticipate their questions: don’t ask them
  - Neither of them will understand all the jargon you might want to use
  - Write clearly and simply
  - Read out load what you wrote → if it sounds awkward, it is, so rephrase it
    - Especially the executive summary
- **Strategic guidance:**
  - “It is recommended that the organization carefully manage the membership of the local administrators group and avoid adding domain

users to this group unless absolutely necessary. Routine audits of local administrator groups should also be preformed.”

      - It is recommended (says who) that the organization carefully manage the membership of the local administrator group (why just that one?)…
      - …and avoid adding *the Doman Users group* to this group unless absolutely necessary (what would be a good justification for doing it?)
        - [and … that ship has sailed: the group is already in there. What do we do now?]
      - Routine audits of local administrator groups should also be performed
        - [Who should do that? What should they look for?] → **passive voice can be a killer**
  - The report is your contribution
    - One of the many sources of input for decision-making in an organization
    - You will never know the whole story
    - Describe your part of the story clearly, accurately, and fairly
    - Trust the reader to have the *business context* you do not
    - Help them make informed decisions
    - Remind yourself that good decisions require info you will not have → if you have communicated your part clearly, you’re done
      - They won’t always fix what you think needs fixing → okay as long as they understand the facts
- Learning from experience of others → let yourself be influenced
  - Things that do not work
    - Folder of screenshots → choose good ones later
    - Screenshots in the report → add words later
    - Words in a note-taking app → write report later
    - *Fill-in-the blanks* report templates or over-reliance on find/replace

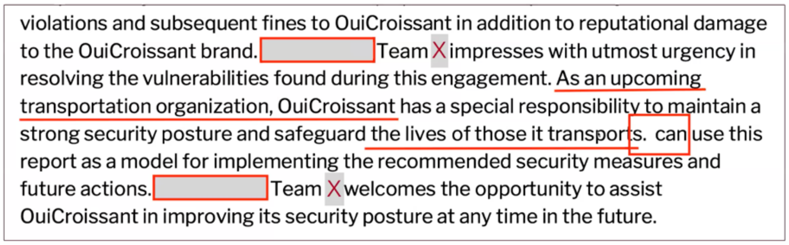
            - Some of this is wonderful, too much is terrible: better none than too much
        - “May contain one or more of the follow” kinds of phrases
            - “…support for NBNS, LLMNR **and/or** other legacy protocols”
            - “…on the in-scope domain**(s).**”
    - **Do the report as you go**
        - Take notes in the report, save screenshots in the report, etc
- Automation is good (has it’s limits) → can’t automate reporting with a shell script
    - Automation comes later
        - First, you should know clearly what your goal is
        - Then…
            - Word templates
            - Boilerplate text
            - Findings database
            - Checklists
            - Word macros
            - Shell scripts
- If are redacting report to share have multiple people redact → better way to do it is via CTF
    - Both make list of what they are redacting
    - Then go through the list and report
    - At least 4 people redacting
    - Redacted report: want someone who knows what the company is can’t prove it

- Example team report:
    - 

      Team X

      THIS DOCUMENT IS CONFIDENTIAL

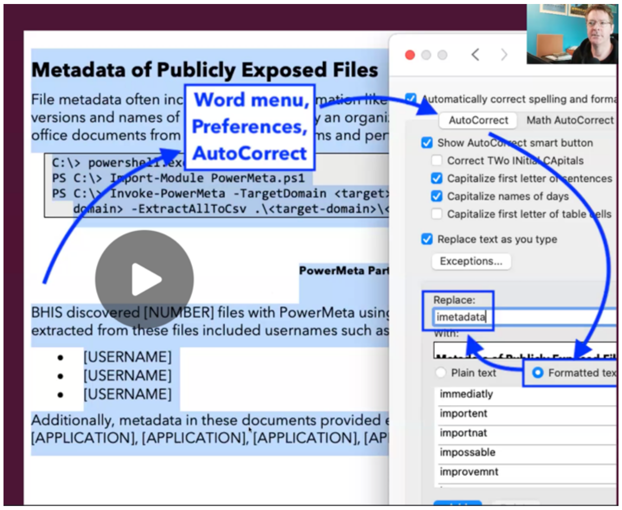
      DISCLOSURE STATEMENT

      All information available in this document is confidential, privileged, and is only available for the party for which this document was written for. Likewise, this report should not be distributed, published, or viewed without an authorized agreement from [redacted] [redacted] **Team X and OuiCroissant (OC).**
    - 

      violations and subsequent fines to OuiCroissant in addition to reputational damage to the OuiCroissant brand. [redacted] Team X impresses with utmost urgency in resolving the vulnerabilities found during this engagement. As an upcoming transportation organization, OuiCroissant has a special responsibility to maintain a strong security posture and safeguard the lives of those it transports. can use this report as a model for implementing the recommended security measures and future actions. [redacted] Team X welcomes the opportunity to assist OuiCroissant in improving its security posture at any time in the future.
        - Can see where issues arose from copy and pasting from past report
    - **Always start clean**

Using Word

- **For competition may have to use web version of word**
    - It is worse → and doesn't have all the same things available (much of these notes may not apply)
- Make word do all the work
    - Autocorrect → not just for typos
        - Replaces a series of characters with different characters
            - Could have key character combos that get replaced with entire paragraphs of text
            - **Have to memorize abbreviations**
        - How to:

- 

  Metadata of Publicly Exposed Files

  File metadata often inc mation like versions and names of y an organi office documents from ms and per

  ```
  C:\> powershell.ex
  PS C:\> Import-Module PowerMeta.ps1
  PS C:\> Invoke-PowerMeta -TargetDomain <target>
     domain> -ExtractAllToCsv .\<target-domain>\<
  ```

  PowerMeta Part

  BHIS discovered [NUMBER] files with PowerMeta using extracted from these files included usernames such as

  - [USERNAME]
  - [USERNAME]
  - [USERNAME]

  Additionally, metadata in these documents provided e [APPLICATION], [APPLICATION], [APPLICATION], [AP

  Word menu, Preferences, AutoCorrect

  ☑ Automatically correct spelling and forma

  AutoCorrect | Math AutoCorrect

  ☑ Show AutoCorrect smart button
  □ Correct TWo INitial CApitals
  ☑ Capitalize first letter of sentences
  ☑ Capitalize names of days
  □ Capitalize first letter of table cells

  ☑ Replace text as you type

  Exceptions...

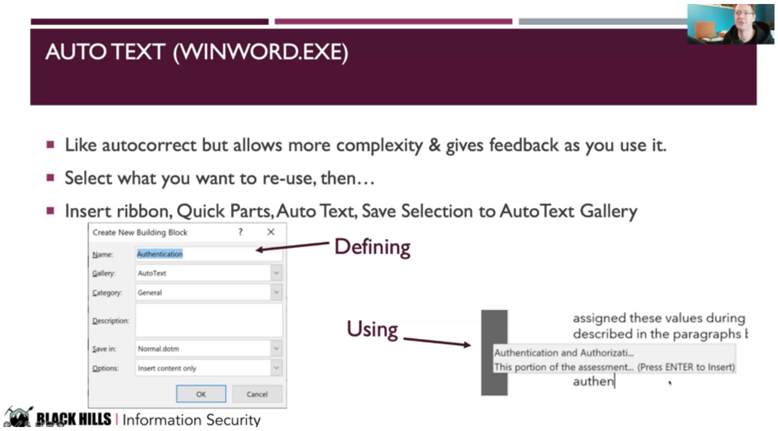
  Replace: imetadata

  With: Metadata of Publicly Exposed Fil

  ○ Plain text ● Formatted tex

  immediatly
  importent
  importnat
  impossable
  improvemnt

  - Quick parts and auto text

    - 

      AUTO TEXT (WINWORD.EXE)

      - Like autocorrect but allows more complexity & gives feedback as you use it.
      - Select what you want to re-use, then…
      - Insert ribbon, Quick Parts, Auto Text, Save Selection to AutoText Gallery

      Create New Building Block

      Name: Authentication
      Gallery: AutoText
      Category: General
      Description:
      Save in: Normal.dotm
      Options: Insert content only

      Defining

      Using

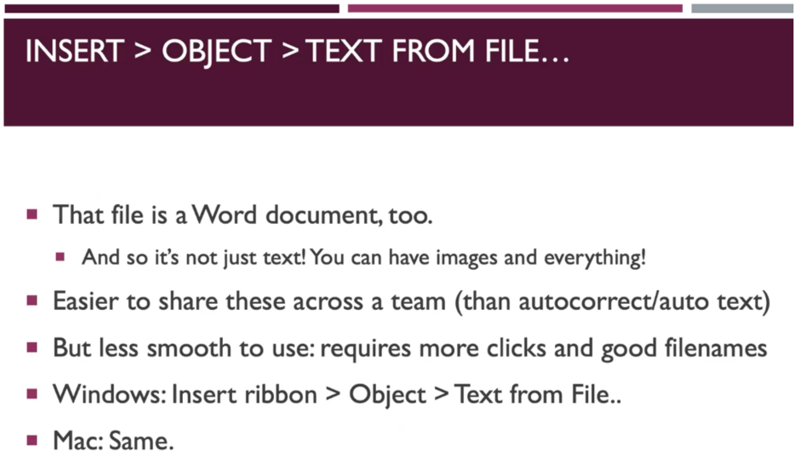
      assigned these values during
      described in the paragraphs b

      Authentication and Authorizati…
      This portion of the assessment… (Press ENTER to Insert)

      authen

      BLACK HILLS | Information Security

  - Custom dictionaries

    - 

      INSERT > OBJECT > TEXT FROM FILE…

      - That file is a Word document, too.
        - And so it's not just text! You can have images and everything!
      - Easier to share these across a team (than autocorrect/auto text)
      - But less smooth to use: requires more clicks and good filenames
      - Windows: Insert ribbon > Object > Text from File..
      - Mac: Same.

    -

  - Styles and sections

  - A structured document is easier to read (and write) than an unstructured one
  - Use Heading styles and you can have a Table of Contents for free
    - Insert table of contents
  - Use styles, never* the “bold” or “italic” or “change font size” buttons
  - Use other styles for things that should be consistent:
    - Screenshot captions
    - Monospaced terminal text
    - Finding titles
    - Remediation advice
    - Severity words
- Macros
- Quick access toolbar and keyboard shortcuts
- Form fields and variables
- Can open a separate view so you can see consistency of document → two different views of doc at the same time
- Paragraph setting → can force there to be a page break before a heading
- Select list, go to columns, and hit 2 and it will make it into 2 columns (can do 3, 4, etc)
- Insert table → convert text
- View menu → navigation pane will let you see the headings in a way that is easy to navigate
- Can click on the dots and choose insert and add whatever commands you want
- Access tool bar → macros → apply style
- Most common color blind is red/green color blind → make sure you have a symbol as well as colors so that it is still accessible