BruCON 0x0A – Retro Talk

The 99¢ Heart Surgeon Dilemma
Extended Annotated Version

Stefan Friedli
stefan@stefanfriedli.ch
@stfn42

Hi, I’m Stefan


3G
9:41 AM
Messages
Calendar
Thursday
6
Photos
Camera
Videos
Maps
280
Weather
73°
Passbook
Notes
Reminders
Clock
Game Center
Newsstand
iTunes
App Store
Settings
Phone
Mail
Safari
Music

2570 days

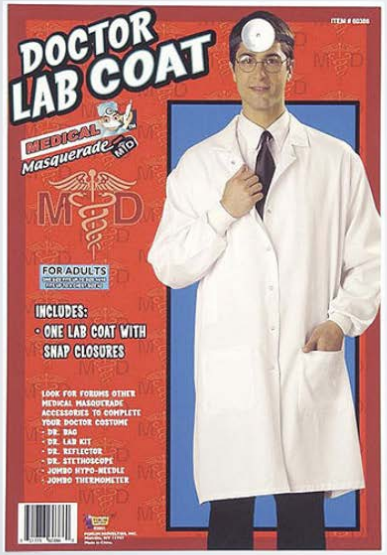

HACK
NAKED
PDF

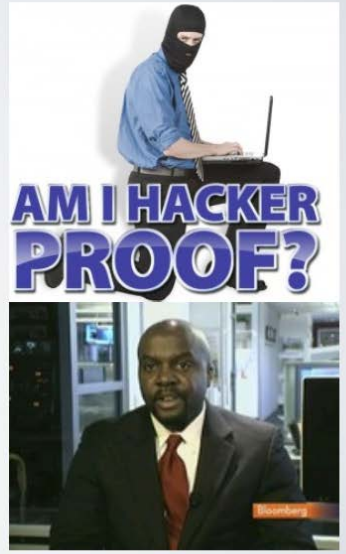
THE 99¢ HEART SURGEON DILEMMA

Stefan Friedli

~~THE 99¢..~~

COMPARE.





Improving Penetration Testing

THIS IS ABOUT BAD EXAMPLES.

«Due to copyright reasons, all of our documents are print-only by default. If you would like to purchase an electronic version at additional cost, please contact our sales staff.»*

WAIT... **BOMBS**?

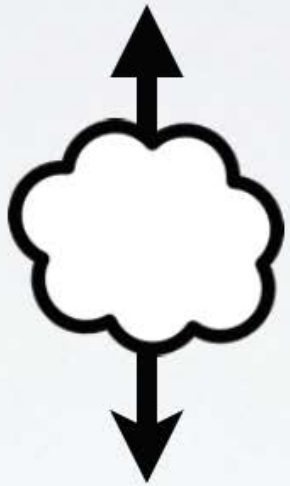
Cross Site Scripting in

„http://intranet.[redacted]/web/search.aspx“

Durch die fehlerhafte Eingabevalidierung des Parameters „s“ kann beliebiger Scriptcode zur Ausführung gebracht werden.

«Due to the incorrect input validation of the parameter ‘s’, arbitrary script code can be executed.»

IMPACT METRICS?



←Magic happens here.

CVSSv2 Base Score = 4.3

Source: nvd.nist.gov | Generated: 2005-12-15 | Disagree?

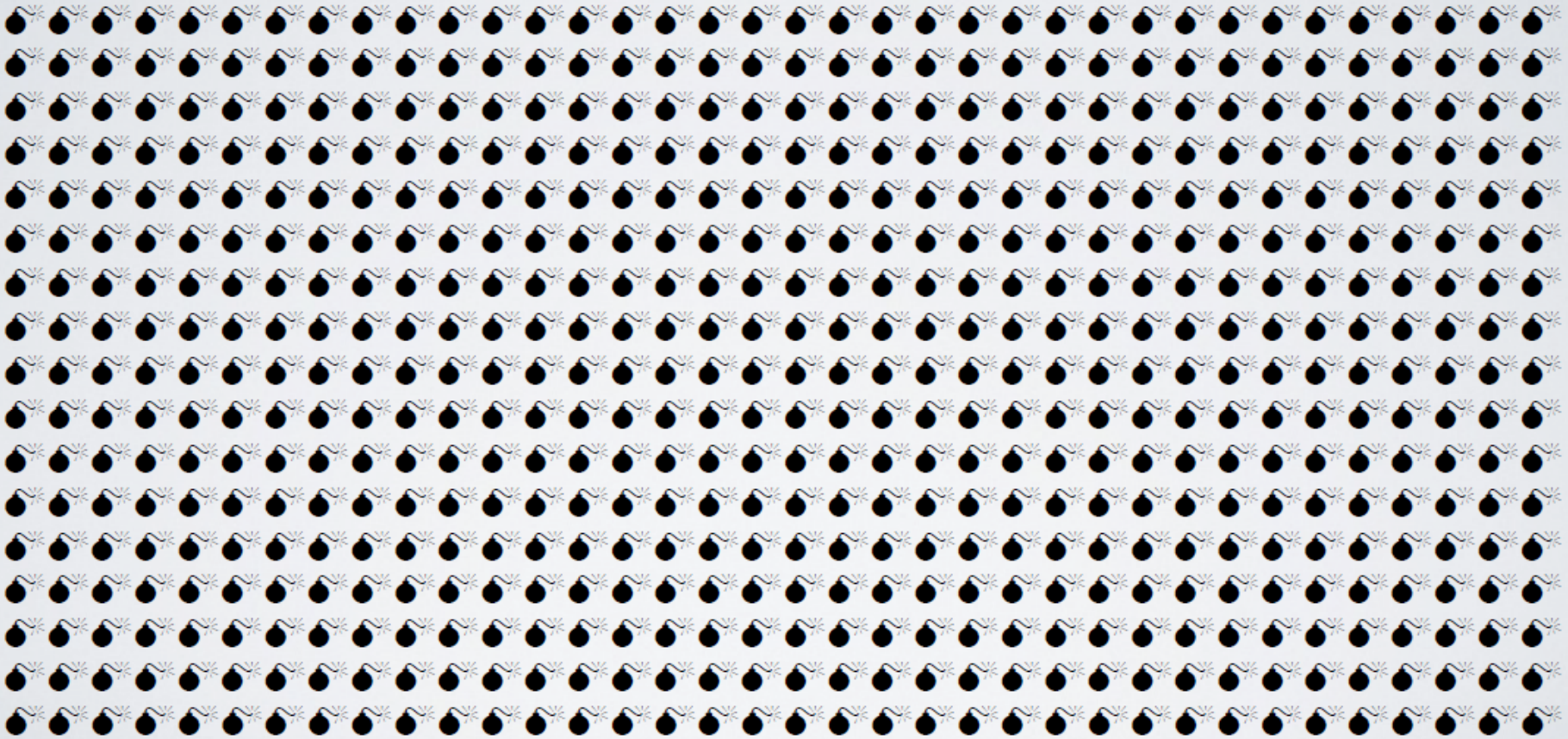
Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability
Local	High	Multiple Instances	None	None	None
Adjacent Network	Medium	Single Instance	Partial	Partial	Partial
Remote	Low	None	Complete	Complete	Complete
1.0	0.61	0.704	0.0	0.275	0.0

YOU'RE ALL WRONG.

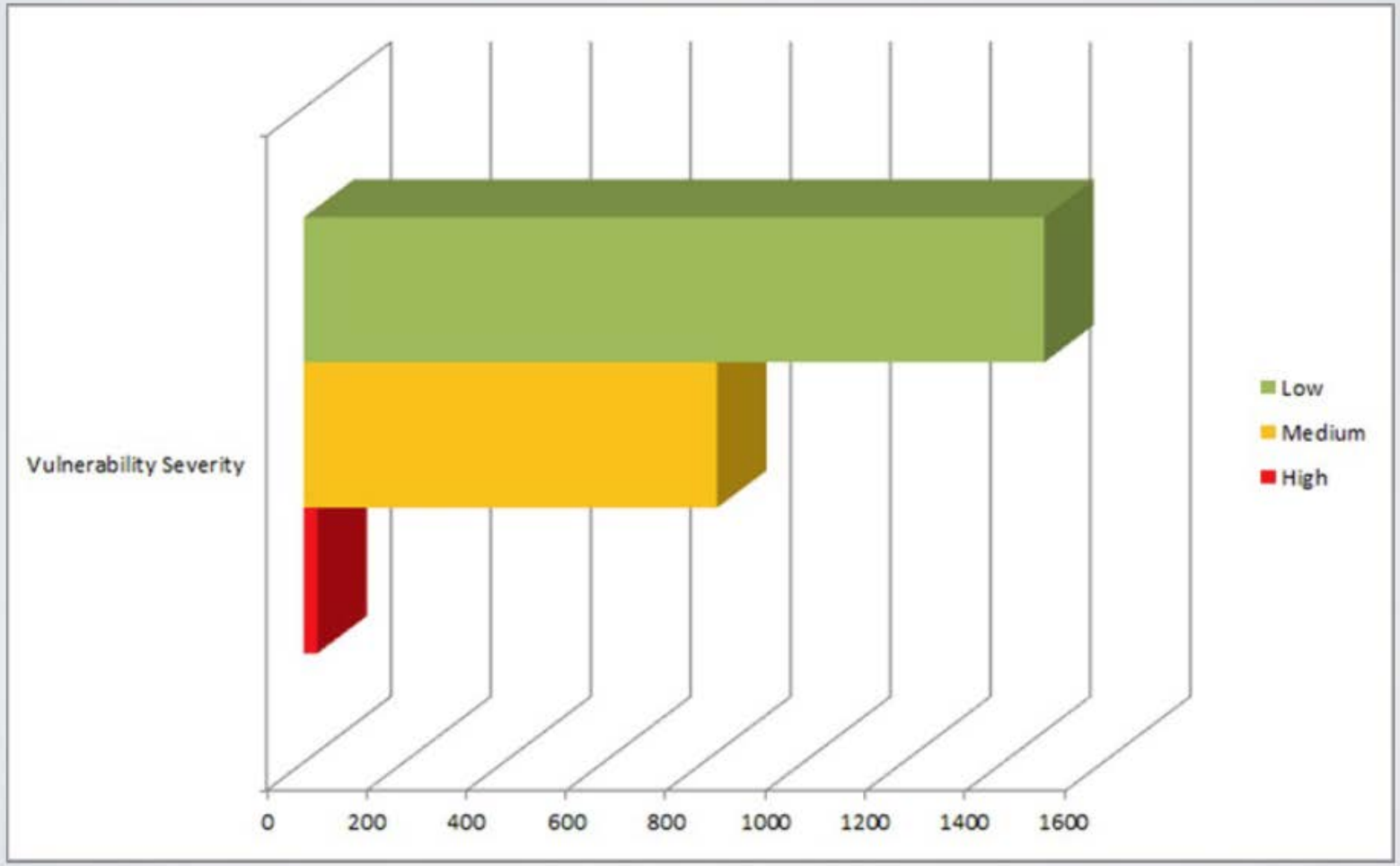
«The amount of bombs depends on the danger the vulnerability causes. (...) There is no upper limit.»*

* Translated from German

MS08-067: Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability



MAKING **IMPORTANT** THINGS INVISIBLE.



SO YOU DIDN'T DO YOUR HOMEWORK?

We tested the complete IP range [redacted].231.[redacted].1/24 supplied by the customer.

Based on the results, we can clearly state that the target range has a high level of security, since no services are supplied and only few hosts are available from the internet.

SO YOU DIDN'T DO YOUR HOMEWORK?

XXX.213.XX.1/24

XXX.231.XX.1/24

We tested the complete IP range [redacted].231.[redacted]1/24 supplied by the customer.

But wait, there is more!

- Accidentally pasting other customer names
- General copy&paste weirdness (Font Mismatch…)
- Spruced up Nessus reports
- Horrible, horrible false positives
- Pentesters beaten by rudimentary obstacles

Management Summary:
«(…) We were unable to complete the task because it [the website] was too big. (…)»

“It’s easy to use cynicism as a protection mechanism for your own insecurities (…)
You might be in a position right now in which you can stand on the sideline and heckle other people’s work without ever having to step up and present a better way to do things, but a time will come when you will be replaced by somebody who does not talk smack about other people’s ideas, but embraces these ideas and *adapts them with his own security mindset* to improve the overall product.”

Me, unfortunately.

Let’s make things better.

“Never attribute to malice that
which is adequately explained by stupidity.”

“Hanlon’s razor”, Robert J. Hanlon

Bad Faith

vs.

Lack of Experience/Knowledge

vs.

Human Error

Let’s talk about charlatans

- Most of them don’t last long.
- Avoiding them is mostly doable
  - Ask about procedures, standards
  - Ask to talk to the testers
  - Check for community participation
  - Look at sample deliverables. Look closely.
  - Be ready to walk away.

The Attacker’s Mindset

Why pentesters are pentesters:

- We like puzzles.
- Nobody ever said “No” to more time.
- We want to exceed expectations.
- We like a broader scope.

The Buyer’s Mindset

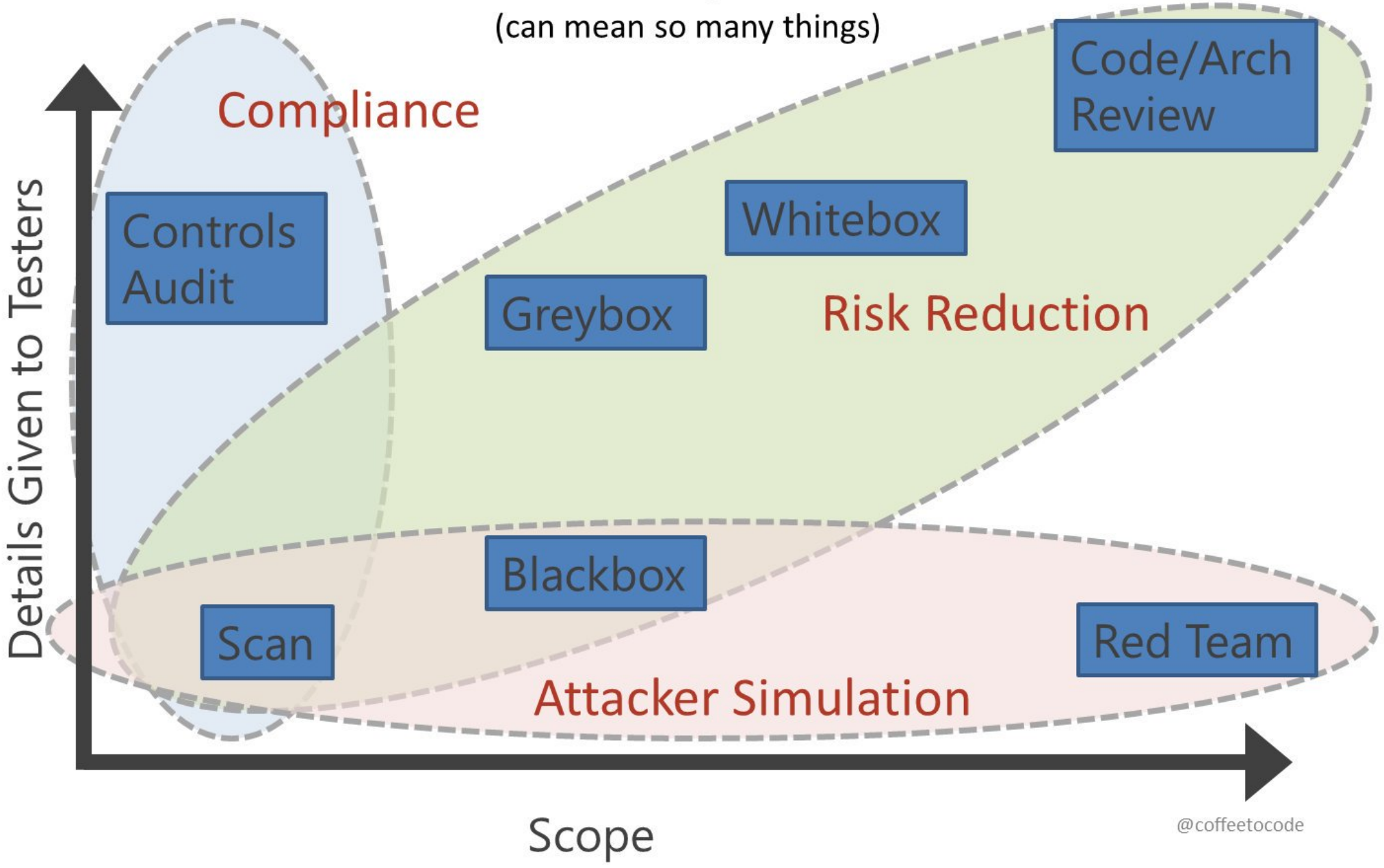
Why people buy pentests

- We want to identify vulnerabilities.
- My boss is making me do it.
- Compliance is making me to it.
- I want to test my blue team.
- I want to simulate a realistic attack.

Taxonomy

“I want a pentest”

(can mean so many things)



twitter.com/coffeetocode

Scope. Scope. Scope.

Pre-Engagement Interactions

Reporting

Intelligence Gathering

Post-Exploitation

Threat Modelling

Exploitation

Vulnerability Analysis

MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

Pentests are more than a report.
Sometimes you barely need one.

How to fix Penetration Testing (One Slide Edition)

Involve more people.
Have more conversations.
Don’t stop at the report.

SAY WHAT?

Management Summary:
«(...) While it was not possible to use a reverse tcp shell to get an outbound connection, we were able to tunnel traffic through ICMP in order to get a shell on the system. (...)»

Thanks for being here,
feel free to ask questions
and have a great night!


SCIP