The 99¢ Heart Surgeon Dilemma
Extended Annotated Version

Stefan Friedli
stefan@stefanfriedli.ch
@stfn42
Hi, I’m Stefan
THE 99¢ HEART SURGEON DILEMMA

Stefan Friedli
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.[*]/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: null.net.gov | Generated: 2008-12-16 | Disagree?
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 231.1/24 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 231.1/24 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)

Compliance

Controls Audit

Whitebox

Greybox

Risk Reduction

Scan

Blackbox

Red Team

Attacker Simulation

Code/Arch Review

Scope

Details Given to Testers
## MITRE ATT&CK

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td>10</td>
</tr>
<tr>
<td>Execution</td>
<td>31</td>
</tr>
<tr>
<td>Persistence</td>
<td>56</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>28</td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>59</td>
</tr>
<tr>
<td>Credential Access</td>
<td>20</td>
</tr>
<tr>
<td>Discovery</td>
<td>10</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>17</td>
</tr>
<tr>
<td>Collection</td>
<td>21</td>
</tr>
<tr>
<td>Exfiltration</td>
<td>9</td>
</tr>
<tr>
<td>Command And Control</td>
<td>21</td>
</tr>
</tbody>
</table>

### Initial Access
- AppleScript
- CMSTK
- Command-Line Interface
- Control Panel Items
- Dynamic Data Exchange
- Execution through API
- Execution through Module Load
- Exploitation for Client Execution
- Graphical User Interface
- InstallUtil
- LaunchEtl
- Local Job Scheduling
- LSASS Driver
- Metasploit
- PowerShell
- Regrss/Regasm
- Registry
- Rundll32
- Scheduled Task
- Scripting
- Service Execution
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Source
- Szone after Filename

### Execution
- .bash_profile and .bashrc
- Accessibility Features
- AppCert DLLs
- Application Shimming
- Authorization Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association
- Components Firmware
- Component Object Model Hijacking
- Create Account
- DLL Search Order Hijacking
- Dylib Hijacking
- External Remote Services
- File System Permissions Weakness
- Hidden Files and Directories
- Hacking
- Hypervisor
- Image File Execution Options Injection
- Kernel Modules and Extensions
- Hooks
- Launch Agent

### Persistence
- Account Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTK
- Code Signing
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decompile Files or Information
- Disable Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Execution Interception
- File System Logical Overwrites
- File System Permissions Weakness
- Filesystem Bypass
- Hidden Files and Directories
- Hidden Users
- HiddenWindow
- HISTCONTROL
- Image File Execution Options Injection

### Privilege Escalation
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery of Vulnerability
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Process Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery

### Defense Evasion
- Account Manipulation
- Binary Padding
- BITS Jobs
- Bypass User Account Control
- Clear Command History
- CMSTK
- Code Signing
- Component Firmware
- Component Object Model Hijacking
- Control Panel Items
- DCShadow
- Deobfuscate/Decompile Files or Information
- Disable Security Tools
- DLL Search Order Hijacking
- DLL Side-Loading
- Exploitation for Defense Evasion
- Extra Window Memory Injection
- File Execution Interception
- File System Logical Overwrites
- File System Permissions Weakness
- Filesystem Bypass
- Hidden Files and Directories
- Hidden Users
- HiddenWindow
- HISTCONTROL
- Image File Execution Options Injection

### Credential Access
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery of Vulnerability
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Process Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery

### Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery of Vulnerability
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Process Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery

### Lateral Movement
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Discovery of Vulnerability
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Process Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery

### Collection
- Audio Capture
- Automated Exfiltration
- Clipboard Data
- Data from Informational Resources
- Data from Local System
- Data from Network
- Data from Shared Drive
- Data from Remote Media
- Data Staged
- Email Collection
- Input Capture
- Input Prompt
- KerbKerbeat
- Keychain
- LLMNR/NT-NS
- Logon Script
- Malicious Code
- Network Enumeration
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

### Exfiltration
- Audio Capture
- Automated Exfiltration
- Clipboard Data
- Data from Informational Resources
- Data from Local System
- Data from Network
- Data from Shared Drive
- Data from Remote Media
- Data Staged
- Email Collection
- Input Capture
- Input Prompt
- KerbKerbeat
- Keychain
- LLMNR/NT-NS
- Logon Script
- Malicious Code
- Network Enumeration
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

### Command And Control
- Audio Capture
- Automated Exfiltration
- Clipboard Data
- Data from Informational Resources
- Data from Local System
- Data from Network
- Data from Shared Drive
- Data from Remote Media
- Data Staged
- Email Collection
- Input Capture
- Input Prompt
- KerbKerbeat
- Keychain
- LLMNR/NT-NS
- Logon Script
- Malicious Code
- Network Enumeration
- Password Filter DLL
- Private Keys
- Replication Through Removable Media
- Shared Webroot
- SSH Hijacking
- Taint Shared Content
- Third-party Software
- Windows Admin Shares
- Windows Remote Management

### Commonly Used Port
- Communication Through Remote Media
- Connection Proxy
- Custom Command and Control Protocol
- Command And Control
- Cybersecurity
- Domain Fronting
- Feedback Channels
- Multi-Step Proxy
- Multi-Staged Channel
- Multi-Band Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service
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.
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!