The Ultimate Windows 10 Hardening Guide: What to Do to Make Hackers Pick Someone Else

Paula Januszkiewicz
CQUIRE: CEO, Penetration Tester
CQUIRE Offices: New York, Dubai, Warsaw
MVP: Enterprise Security, MCT
paula@cqure.us | http://cqure.us
1. Network Oriented
2. Learning the Approach
3. System Oriented
4. Summary
Tools!

- Check out the following links:
  - Our tools: http://cquire.pl ➔ Tools

- Knowledge:
Agenda

1. Learning the Approach
2. Network Oriented
3. System Oriented
4. Summary
Step 1: Monitor DNS Queries

- DNS role in security:
  - “Who has DNS has power”
  - DNS Spoofing is easy (WPAD etc.)
  - DNS is a text based protocol

- Monitoring and securing DNS strategy:
  - PTR communication is pretty rare and it depends on the owner of IP
  - Correlate queries and responses
  - DNSSEC is an option

For example: What if RevDNS of Hackers.cn IP says it is Microsoft.com? Nothing if we remember that our DNS has resolved the hackers.cn name!
DNS to Rely On

The **DNS protocol perspective**
Step 2. Sanitize Network Data

- **Shellshock**
  Nothing but an inappropriate data sanitization

- **Data sanitization – know who processes data**
  Black list approach: deny eg. `<script>`, `--`, `;`, `../`
  White list approach: define what you accept
  Regular expressions

- **Examples:**
  SQL Injection, Directory Traversal, escape sequences, XSS

As simple as this: verify data **before** processing...
Shell is shocked

The operating system perspective
Step 3: Actively Monitor Your Servers

- **Applocker and Sysmon are great combo**
  - Applocker blocks unwanted software
  - Sysmon will inform you when someone starts a process or connection or changes the file date

- **How to discover malicious software when Applocker cannot be enabled?**
  - System logs (Process creation details)
  - Sysmon enhances built in functionalities

- **Sysmon stores a hash base**
  - It can be used for malware or unwanted activity discovery
Sysmon Demonstration

The administrator's perspective
Step 4: Web Server Check

- Naturally unpleasant environment
  - Patch and upgrade the Web server application
  - Remove/disable unnecessary services, apps, and sample content
  - Install Web content on a dedicated hard drive or logical partition
  - Limit uploads to filesystem and disable directory browsing
  - Define a single directory for all external scripts or programs executed as part of Web content
  - Disable the use of hard or symbolic links
  - Use service accounts with strictly defined privileges
  - Define a complete Web content access matrix that identifies which folders and files are restricted and which are accessible by whom
  - Use host-based IDS/IPS and/or file integrity checkers
  - Protect backend server (e.g., database server) from command injection attacks at both the Web server and the backend server
How much web could a web-check check?

The *web perspective*
Step 5: Centralize your logs

- It’s quite obvious that losing logs after attack is not in our dreams
  - Logs for critical systems should be stored outside the server

- Log centralization
  - Can help us to correlate different logs and events
  - Helps to maintain the legal proof after attack

- Available solutions
  - Operating system built in: subscriptions, scripts
  - Other products: SCOM, Splunk, SolarWinds, WhatsUpGold, TripWire & other (see: Gartner)

Search for: ‘Top 47 Log Management Tools’
Sysmon Demonstration

The *bad guys perspective*
Step 6A: EMET - Protection From Injection

- **Enhanced Mitigation Experience Toolkit**

- Helps prevent vulnerabilities in software from being successfully exploited

- Protection mechanisms:
  - Data Execution Prevention (DEP)
  - Structured Exception Handler Overwrite Protection (SEHOP)
  - Address Space Layout Randomization (ASLR)
  - Certificate Trust (Pinning)
Step 6B: Code Integrity

- Secure Boot
  - Includes Secure Firmware Updates and Platform Secure Boot
- Kernel Mode Code Integrity (KMCI)
- User Mode Code Integrity (UMCI)
- AppLocker
The workstation perspective
Step 7: Malicious File Review

- Security awareness: Ideally users should recognize malicious .exe, .docx, .pdf etc.
- Malicious files are not digitally signed, but many files are not...

PDF File is comprised of header, objects, cross-reference table (to locate objects), and trailer

- "/OpenAction" and "/AA" defines the script or action to run automatically
- "/Names", "/AcroForm", "/Action" can also specify and launch scripts or actions
- "/JavaScript" specifies JavaScript to run
- "/GoTo*" changes the view to a destination within the PDF or in another PDF file
- "/Launch" launches a program or opens a document
- "/URI" accesses a resource by its URL
- "/RichMedia" can be used to embed Flash in PDF
- "/ObjStm" can hide objects inside an Object Stream

DOCX, DOC – Macro Extracting Techniques
Perfectly Designed File?

The *file* perspective
Step 8: Data Caching

- Idea is simple: no caching
  - Hashes, Passwords from browsers and applications
  - Temporary files, RDP cache
  - Search, browsing history

- Pay attention to the edge servers

- Settings in policies
  - Profile and folder redirection
  - Set cached logon policy
Cache the hash

The *good practice* perspective
Step 9: Use Host-Based Firewall

- For a detailed traffic control
- For internal network protection
- For logging purposes
- For application-based control
  - Edge firewall does not provide that function
- For protection of travelling users
It... is not obvious. It isn't..

The remote connection perspective
Agenda

1. Learning the Approach
2. Network Oriented
3. System Oriented
4. Summary
Summary

- Act proactively: Applocker, EMET
- Isolate infrastructure components so that in case of attack they prevent spreading
- Review servers’ and workstations’ configuration periodically
- Implement log centralization solution
- Implement security awareness campaign
Tools!

- Check out the following links:
  - Our tools: [http://cqure.pl ➔ Tools](http://cqure.pl)