Red Team Tales

Infamous Defaults & Best Practices

23p

Networking Protocols & Services

Use of these protocols should be reviewed and disabled where appropriate

- Link-Local Multicast Name Resolution (LLMNR)
- Server Message Block (SMB)
- Multicast DNS (mDNS)
- IPv6 (Disable / Control)
- Always disable network services that are not actively used in your network

Network Defense

Out of the box, operating systems typically have unnecessary services enabled

- Implement strict segmentation and zero-trust architectures
- Create honey users and monitor for their use
- Seed devices with honey tokens
- Maintain accurate and up-to-date asset inventories
- Test incident response capabilities routinely
- Deploy well-considered honeypot systems and monitoring capabilities

Endpoint Defense

Protecting your endpoint and installed software is a complicated task

- Enable host-based firewalls (all vendors)
- Deploy some combination of endpoint defense capabilities
- Implement application whitelisting wherever possible
- Implement full-disk encryption (don’t forget about layer 8 training, though)
- Implement privilege separation and governance structures
- Disable or otherwise limit PowerShell

Password Guidance

Create a password policy that encourages people to be thoughtful and deliberate

- This is a hot topic among security practitioners
- Password length is arguably the most important factor
- Diversity of characters is less important, but not irrelevant
- Password rotation is very important
- Password uniqueness over time is very important

Mobile Workforce

Keep your mobile workers safe

- Always require the use of a VPN
- Consider the security impact of allowing split VPN configurations
- Your pocket computer is a high-value target
- Disable NFC protocols such as Bluetooth when not in a trusted environment
- Disable wireless (802.11) interfaces when not in use
- Defend against shoulder surfers

General Suggestions

Some general guidelines for operational success

- Test your security posture regularly
- Anchor your offensive testing to governance standards and expectations
- Establish a threat intelligence capability
- Develop policies and communicate them to all of your users regularly
- Perform policy reviews at least annually
- Test your users using a variety of active and passive techniques

Who are 23p?

Your Trusted Cybersecurity Advisor.

- An international cybersecurity services provider based in the United States
- Offering a new approach to your information security services investment
  - Creators of the Rigor Rating™ and Defense Efficacy Report Card™
- Deep knowledge of modern adversarial capabilities
  - In-house research focus results in cutting-edge attack chains to challenge the most mature clients
- Full-spectrum offensive testing
  - Network / Web / API / Cloud / Mobile / Wireless / Ransomware
- Advisory services and training solutions to further develop your security program

Experience

In a service organization, the brand is established by the quality of your people.

- **Decades of experience providing information security services across all client maturity levels**
- **Research-driven approach allows 23p to deliver tailored Red Team services**
- **Sampling of past presentations**
  - Regarding Spectre and Meltdown
  - Securing IoT: Protecting Smart, Connected Systems
  - Refrigerators Hacking Cars: Microservice Security In A Connected World
  - Automotive Security In A Fully Connected World
  - Accelerating Incident Investigations
  - The Attacker’s Mindset
  - Developing A Formal Information Security Program
  - ROSI: Measure with a micrometer, mark with chalk and cut with an axe
  - Practical Exploitation using a Malicious Service Set Identifier (SSID)
  - Metasploit Training

Contact Us

Let’s talk. We’re friendly.

www.23p.com

missy@23p.com

608.212.9927