

Initial Access: Breach Windows Like a Pro! 🚀

HackForest Cybersecurity Academy

Master the Art of Red Team Entry!

Learn how real attackers gain footholds in Windows enterprise environments. From phishing to exploiting mis-configurations, HackForest's hands-on training equips you with cutting-edge techniques to simulate sophisticated attacks ethically. **HackForest guarantees 100% that our students will bypass modern AV and EDR!**

🔍 Why Choose HackForest?

In a rapidly evolving threat landscape, ethical evasion skills are critical for elite pentesters and red teamers. Our course delivers:

- ✓ **Core Insights:** Master Windows and AV internals.
- ✓ **Practical Labs:** Tackle real-world challenges.
- ✓ **Lasting Expertise:** Learn scalable, adaptable techniques.

🔧 What You'll Master

Initial Access Techniques (TTPs)

- 🔪 **Phishing with Weaponized Documents:** Craft malicious Word/Excel files using macros, DDE, or embedded payloads.
- 🔪 **Abusing Free Services:** Leverage GitHub, Discord, CDNs for undetected payload delivery.
- 🔪 **Stealthy File Types:** Use LNK, HTA, ISO, BAT, PS1, OneNote, and chained infection methods.
- 🔪 **Living Off the Land Binaries (LOLBins):** Execute payloads via trusted binaries (mshta, certutil, rundll32).
- 🔪 **Phishing Infrastructure:** Build servers with HTTPS, domain masking, and tracking.
- 🔪 **Securing Infrastructure:** Use geo-fencing, alerts, and hardened configs to avoid detection.
- 🔪 **Bypassing MFA:** Capture session tokens with Evilginx2 to defeat multi-factor authentication.
- 🔪 **Advanced Evasion:** Employ HTML smuggling, SVG loaders, and HTML+JS+CSS chains for sandbox evasion.
- 🔪 **C2 Frameworks:** Set up Cobalt Strike, Sliver, Mythic, Havoc; create listeners and deploy agents.
- 🔪 **C2 Traffic Masking:** Use HTTPS, domain fronting, custom profiles, and redirectors (Apache/IIS/CDN).

Execution Techniques

- User interaction (click-based execution)
- Scheduled Tasks, Startup folder
- Exploiting vulnerable services for code execution

Real-World Case Studies

- 📄 How attackers gained initial access in major breaches
- 📄 APT tactics during initial access
- 🖥️ *Immersive Hands-On Labs!*

📢 Ethical Red Teaming

Initial access is the breach point where a simple click can collapse an empire.

Everything taught is from a Red Team perspective. Use these skills responsibly, never to harm or exploit without authorization. Ethical conduct is the foundation of cybersecurity.

📢 Become an Initial Access Expert!

Register Now!

Limited Seats! Secure Yours Today!

Special Offer: First 10 students get 15% off!