SYNERCOMM

Adversary Simulation

A technical audit, controls validation, SIEM tuning & training all in one!

Fact: Regular internal and external penetration testing is the best way to validate your security program. But, you often wonder, "how did the pentester find that flaw?", or "what tool did they use to execute that attack?" In hopes of helping our clients understand and improve their controls, SynerComm is pleased to offer Adversary Simulations. Work side by side with our penetration testers and collaborate with them as they demystify pentesting and share their tools, tactics, and techniques.

How it Works

- Allow defenders to test control and configuration changes until simulated attacks can be prevented and/or logged
- Help defenders discover and attempt to fix control gaps and weaknesses
- Train defenders to recognize dangerous attack sequences within their own networks and systems
- Allow SOC and SIEM staff to tune and validate logging, monitoring, and alerting systems
- Proof of concept or product evaluations (ex. Endpoint Detection and Response software "bakeoff")
- Validate effectiveness of firewall rules, intrusion/threat prevention systems, Active Directory settings, and end-point controls against simulated, safe attacks

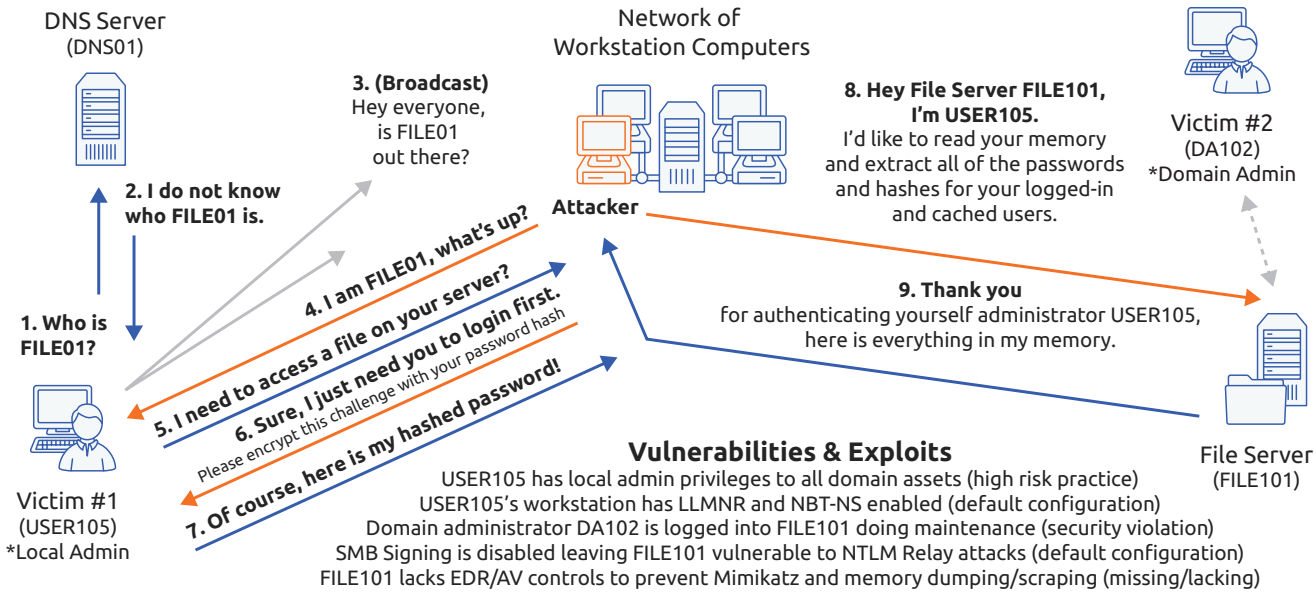
Companies that benefit most:

Looking to validate, tune, and improve their security information and event management system (SIEM)

Wishing to train staff who monitor security or work in a security operations center (SOC)

Have mature security programs and conduct regular internal penetration testing

LLMNR Poisoning → NTLM Relay → Memory Scrape



Vulnerabilities & Exploits

USER105 has local admin privileges to all domain assets (high risk practice)
USER105's workstation has LLMNR and NBT-NS enabled (default configuration)
Domain administrator DA102 is logged into FILE101 doing maintenance (security violation)
SMB Signing is disabled leaving FILE101 vulnerable to NTLM Relay attacks (default configuration)
FILE101 lacks EDR/AV controls to prevent Mimikatz and memory dumping/scraping (missing/lacking)

There is no replacement for the validation provided by a thorough, skilled, and human-led penetration test. External and internal pentests with social engineering demonstrate precisely how a skilled intruder could breach your company's systems and data. Adversary Simulations take your security program to the next level by collaborating with pentesters to learn their attacks and precisely evaluate your controls. Building on a recent penetration test, we simulate common and often sophisticated adversary attacks. Adversary simulations are typically performed remotely in 1-day sessions with both the pentester and defenders sharing their screens. AdSim engagements follow "Pentest Playbooks" based on recent pentest findings and observations, common exploits and late-breaking attacks.

Partner with SynerComm to find out what your penetration test's have been missing.

SYNERCOMM