



FinXTech Connect Executive Briefings:

How to Improve Your Cybersecurity Posture by Partnering with DenSecure by Wolf & Co.

Alex Martirosyan
Wolf & Company, P.C.



LEVERAGING OFFENSIVE SECURITY

How to Improve Your Cybersecurity Posture by Partnering With Densecure by Wolf & Co.

May 10, 2023 • Alex Martirosyan, CRT0, OSCP, GPEN



Alex Martirosyan

CRT0, OSCP, GPEN

Senior Penetration Tester

✉ amartirosyan@wolfandco.com

☎ (617) 261 - 8138

BIOGRAPHY

Alex is a Senior Penetration Tester at Wolf's DenSecure group where he's responsible for coordinating and conducting penetration testing services for clients in a variety of industries, including financial, healthcare, and software.

His expertise consists of internal and external network penetration testing, threat emulation exercises, social engineering, vulnerability assessments, cloud security assessments, and Active Directory security reviews.

Alex has over 5 years experience conducting penetration testing audits and is pursuing ethical hacking certifications from industry-recognized organizations like the SANS Institute and Offensive Security.



MORNING HACKER STORY TIME

AGENDA

- ▀ About Us →
- ▀ Importance of Offensive Security →
- ▀ Understanding Tactics, Techniques, and Procedures (TTPs) →
- ▀ Hacker Story Time →
- ▀ Conclusion →



OFFENSIVE SECURITY ASSESSMENTS



- ▀ Poorly misunderstood exercises
 - Vulnerability Scan or a Penetration Test?
 - Performed by certified individuals from same company?

- ▀ New regulatory requirement (defined broadly)
 - Includes internal and external testing

- ▀ Penetration testing is QA for your controls (human and technical)

ABOUT WOLF & COMPANY, P.C.

1911

WOLF & CO.
ESTABLISHED

300+

PROFESSIONALS

370+

FINANCIAL
INSTITUTION &
FINTECH CLIENTS



3 OFFICES IN:

- ✓ Boston, MA
- ✓ Springfield, MA
- ✓ Princeton, NJ



SERVICES OFFERED IN:

- ✓ Audit
- ✓ Tax
- ✓ Risk Management

WOLF
& COMPANY, P.C.



ABOUT DENSECURE



Wolf & Company's team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.



ADVANCED SECURITY ASSESSMENT

A comprehensive, customized attack methodology combining all the following services into the most relevant tactics, techniques, and procedures (TTPs) used by real-world adversaries against organizations like yours.



NETWORK PENETRATION TESTING

Practical, hands-on testing of your internal, external, and cloud network security to identify and prove the impact of security risks.



SOCIAL ENGINEERING

Testing designed to target your employees and physical infrastructure, alone or in combination with technical attacks.



THREAT EMULATION

A collaborative simulation of the documented attack patterns of real-world attackers, as cataloged by MITRE ATT&CK®, to evaluate your blue team capabilities.

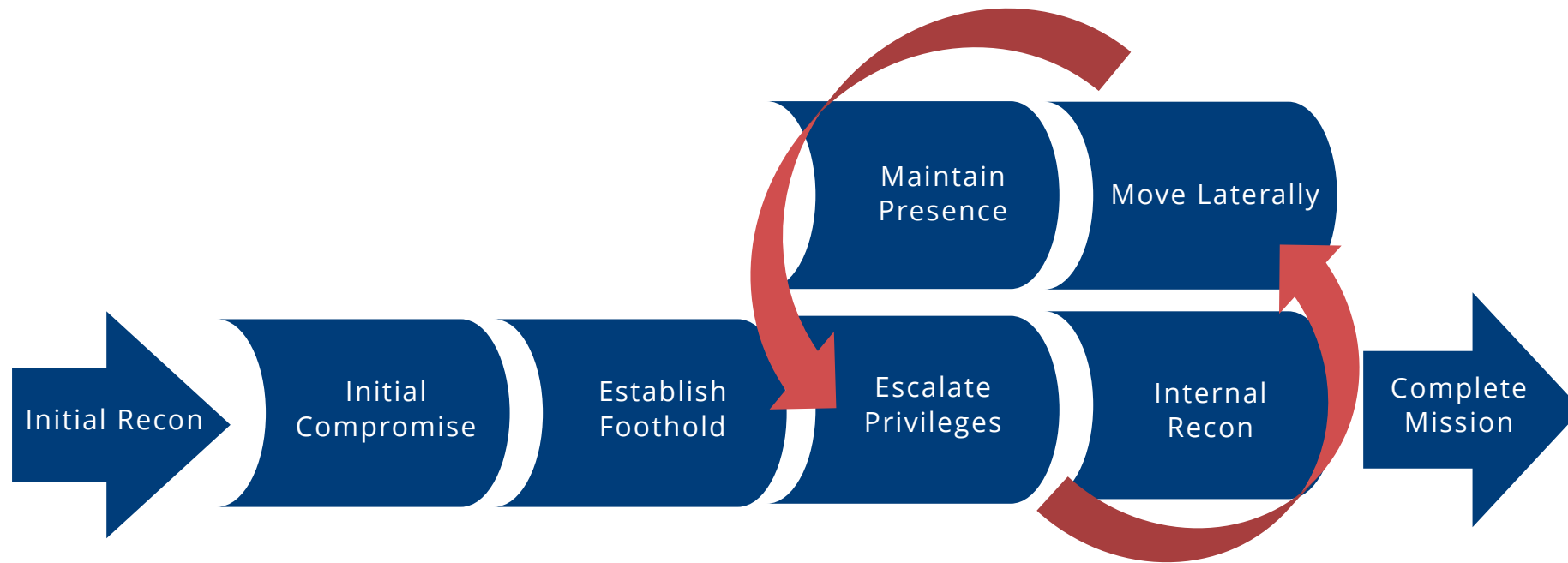


APPLICATION PENETRATION TESTING

Testing specifically designed to uncover flaws in your web- or mobile-based application that could lead to critical exposures.



BASIC METHODOLOGY



SECURITY TESTING DUE DILIGENCE



Do not shop for the lowest cost provider



Look into the vendors you're considering



Ask for references!



Pay attention to communication:

- Did the vendor ask any questions about your environment?
- How are they scoping the exercise?
- Can we see a sample report?

THREAT ACTOR REALITY

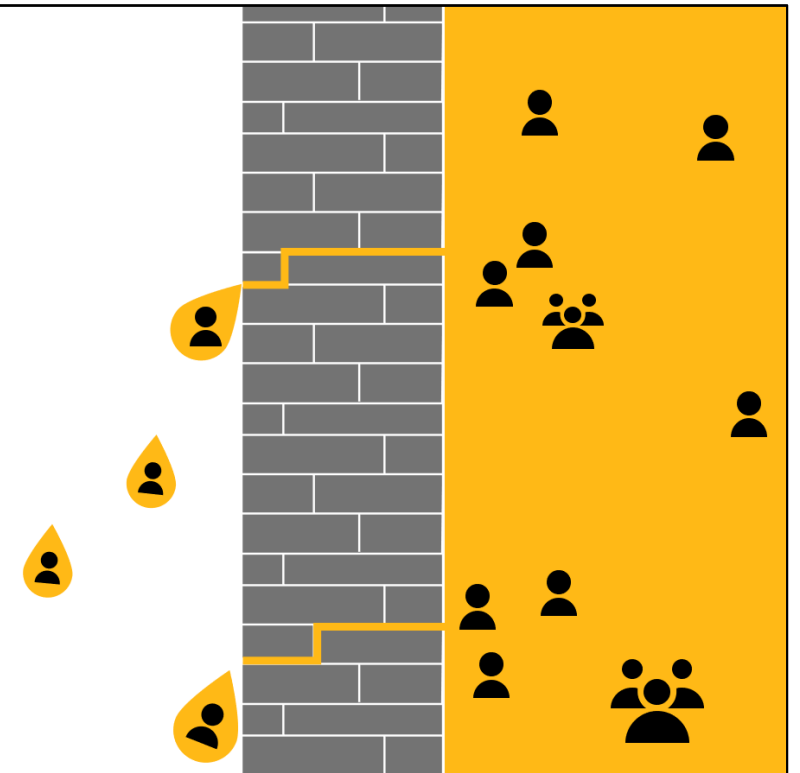
- Threat actors also use commercial tools
 - Cobalt Strike
 - GitHub Open-Source Tools
- Goal: Emulate adversarial actions **FIRST**
- Validate assumptions of your environment

Attackers are like water

Attackers take path of least resistance to achieve objectives

- Established paths/methods
- Easiest new openings

Attackers only bother when they get good **return on investment (ROI)**



<https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-strategy>

[Back to Home](#) →