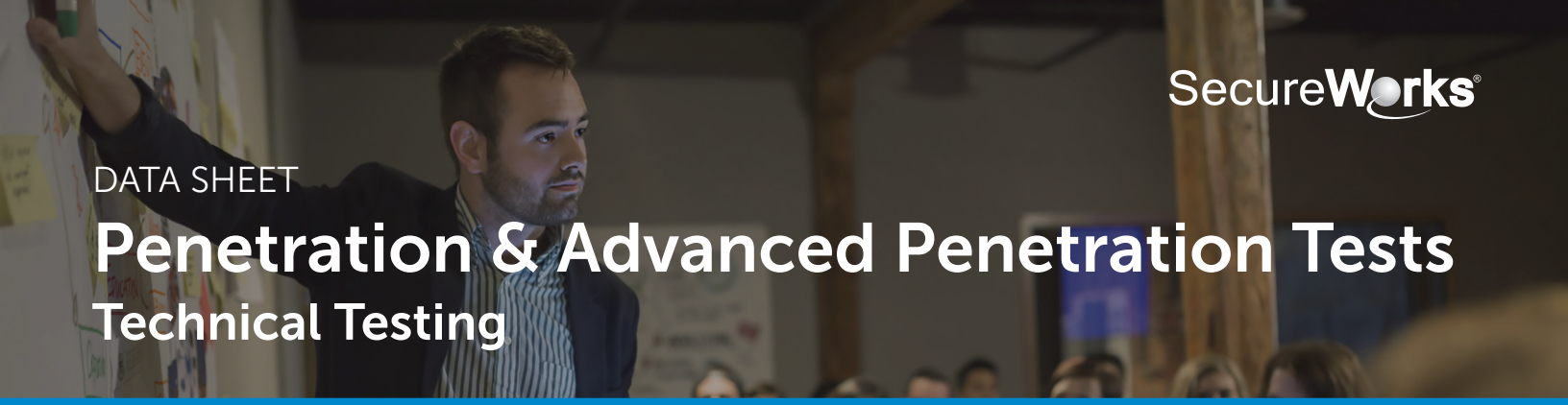

SecureWorks

DATA SHEET

Penetration & Advanced Penetration Tests

Technical Testing

The Challenge

Unauthorized access to company resources using existing and new vulnerabilities is a serious security concern. Verifying that new and existing applications, networks and systems are not vulnerable to a security risk is key to addressing these vulnerabilities before they can be utilized by unauthorized users. While vulnerability assessments are a "light touch" evaluation to identify gaps and vulnerabilities in your network, further testing is required to show how an attacker would gain access to your environment and use those systems as a base for attacks deeper into the network.

The Solution

SecureWorks approaches every penetration test as unique to every organization. Our methodology is performed by the industry's top security testers, leveraging our proprietary tactics and intelligence from the SecureWorks Counter Threat Unit™. Both Penetration and Advanced Penetration Tests are designed to show how an attacker would gain unauthorized access to your environment by compromising in-scope systems and highlight pivoting opportunities from compromised hosts. Based on the findings, SecureWorks will discuss the findings with all relevant audiences and provide a customized course of action for both leadership and technical audiences.

Solution at a Glance

	Vulnerability Assessment	Penetration Test	Advanced Penetration Test	Remote Red Team	On-site Red Team
Scoping	Reports on all systems and vulnerabilities found on in-scope systems.	Threat Modeling (includes suitable testing scenario)	Threat Modeling (includes suitable testing scenario)	Customized engagement goals	Customized engagement goals
Skill level required	Low	High	High	High	High
Targets users			✓	✓	✓
Objective	Broad Scan	Goal Seeking	Goal Seeking	Goal Seeking	Goal Seeking
Can be performed on premise	✓	✓	✓		✓
Can be performed remotely	✓	✓	✓	✓	
Vulnerability scanning	✓	✓ (as necessary)	✓ (as necessary)		
Detailed report	✓	✓	✓	✓	✓
Repetition performed until goal is met		✓	✓	✓	✓
Post-exploitation		✓	✓	✓	✓
Manual testing to simulate attacker methods and techniques		✓	✓	✓	✓
Phishing			✓	✓	✓
Vishing				✓	✓
OSINT to gather additional targets				✓	✓
Wireless (as necessary)					✓ (as necessary)
Physical testing and drop box placement					✓ (as necessary)

	Penetration Test	Advanced Penetration Test
What Does the Test Help Me Answer?	• How would my network stand up to a skilled attacker? • How are my security controls protecting my critical data? • What ways can an attacker defeat my security controls? • Are my IT Admins making good security choices? • If a user is compromised, how will the rest of my network withstand an internal attacker?	• Can I defend against a dedicated attacker with minimal scope restraints? • Which attacks could we see, and which attacks did we miss? • Could someone phish my employees and gain internal network access? • Once a system is compromised, what additional access can be gained?
Benefits	• Validate internal and/or external security controls, including protections around high-value systems • Manual testing that simulates current threats, including pivoting and post-exploitation • Satisfy compliance needs, including PCI 3.x, FFIEC, HIPAA • Confidence in the assessment knowing that the latest threat intelligence and tactics from the SecureWorks Counter Threat Unit™ were utilized	• Tests users in conjunction with your external and internal networks • Simulates a common real-world threat; spear phishing + external testing that segues into an Internal foothold • Tests your response and detection capabilities
Who Should Use the Test?	• Have a security baseline and want to test it • Need to meet compliance needs for penetration testing, including PCI 3.x • Are concerned that there may be deeper security issues that their vulnerability assessments are not finding • Have a successful Vulnerability Management program and want to take the next step • Attempting to protect a subset of critical systems • Need to find deeper, systemic issues that can span systems, domains, or security zones • Concerned about external attack surface • Concerned about internal threats like rogue employees or attackers that have gained physical access to the internal network	• Have a mature security program and want to test people as well as the network • Need a more advanced threat simulation that more-closely matches attack vectors seen in the wild (phishing + endpoint compromise) • Need to mix phishing engagements with network penetration testing

Methodology

1 Establish Rules of Engagement

- Goals and objectives
- Scope and validation of targets
- Timelines
- Reporting requirements
- Personnel, roles and responsibilities

2 Remote Testing Appliance Configured and Deployed

3 Execution

Step 1: Open Network Services Enumeration

- Interrogate available network services to determine additional information that could lead to compromise (i.e., DNS, SNMP, SMTP, Net-BIOS, etc.)

Step 2: Open Network Services Exploitation

- Use information from "open network services enumeration" to attempt compromise of your network services (i.e., brute force, authentication bypass, public exploits)

Step 3: Post Exploitation and Movement

- Identify compromise vectors for your wider network or domain infrastructure; techniques show the potential of initial compromise

Step 4: Phishing – Email Social Engineering (Advanced Pen Test Only)

- Test user security awareness by manipulating target individuals (scenarios range from generic, spam-like messages to customer-specific emails)
- Any credentials captured or systems compromised will be leveraged during the external and internal penetration test portions of engagement

4 Manual Verification and Prioritization

5 Final Report

What to Expect in Your Report

Executive Summary is targeted toward a nontechnical audience — senior management, auditors, board of directors, and other concerned parties.

- **Engagement summary:**
  Brief description of the results of the engagement
- **Summary of findings and recommendations:**
  Describes systemic issues and high-risk findings, and our recommendations to remedy issues or reduce risk

Detailed Findings are targeted toward technical staff and provides detailed findings and recommendations:

- **Engagement methodology:**
  Details of what was performed during the engagement
- **Narrative:**
  Describes the sequence of events the testers took in their attempts to achieve the goals of the engagement to assist in understanding blended threats and/or dependent phases
- **Detailed findings and recommendations:**
  Describes any findings, web page links for further reading, and recommendations for remediation or risk reduction. Evidence of the findings is supplied where applicable and, if possible, sufficient information is supplied to replicate the findings using publicly available tools.
- **Phishing Results (Advanced Pen Test Only)**
  A section detailing the phishing attacks used and their success rate

Why SecureWorks

Our Testers

SecureWorks hires only the best and brightest. From our in-depth technical hiring process, to our continued investment in our consultants through generous training programs, we seek to find and cultivate technical excellence. Our consultants can be found speaking at industry conferences and releasing cutting-edge security research.

SecureWorks Global Threat Intelligence

Threat intelligence is the fuel that powers the engine of the security solutions we provide. With more than 65 of the world's most highly regarded security researchers, SecureWorks' distinguished Counter Threat Unit™ research team (CTU) is what sets us apart. Our researchers analyze threat data across our global client base and actively monitor the cyber threat landscape to provide a globalized view of emerging threats that is integrated into every security solution we provide.

Proven Methodology

SecureWorks has performed thousands of assessments and tests for a wide array of companies from small business to Fortune 500. Our methodology is a combination of proven, public industry methodology (NIST and PTES), in conjunction with our experts' advice and years of experience. Our methodology is updated on a regular basis to match current industry and attack trends.

Next Steps

- **Advanced Pen Test**
- **Incident Management Retainer**
- **Threat Intelligence**

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com