eSENTIRE

DATA SHEET

Penetration Test

eSentire certified security testers perform a myriad of penetration tests on a yearly basis across a variety of industries and organizations of all sizes. Whether an organization is deploying a new service, meeting compliance mandates or assessing network weaknesses, our testers use the latest tactics, techniques and procedures to emulate what attackers are doing in the real world.

Leveraging intelligence from our Managed Detection and Response (MDR) platform which identifies attacks that bypass traditional security controls, we are uniquely equipped to conduct testing that other vendors cannot. Once we achieve the goal, vulnerabilities are prioritized by risk and the eSentire Advisory Services team provides remediation consultation to reduce the potential window of exploitation and avoid regulatory fines.

WHAT CAPABILITIES ARE WE TESTING?

✓	✗	✗
PREVENTION	DETECTION	RESPONSE

WHAT DOES IT HELP YOU ANSWER?

- What are my most critical security gaps that could be exploited?
- How would my prevention and detection capabilities stand up to the latest threat tactics?
- What methods would an attacker use to bypass my security controls?
- Are my IT Admins and security personnel making good choices?
- If a user or system is compromised, how will the rest of the network withstand the attacker?

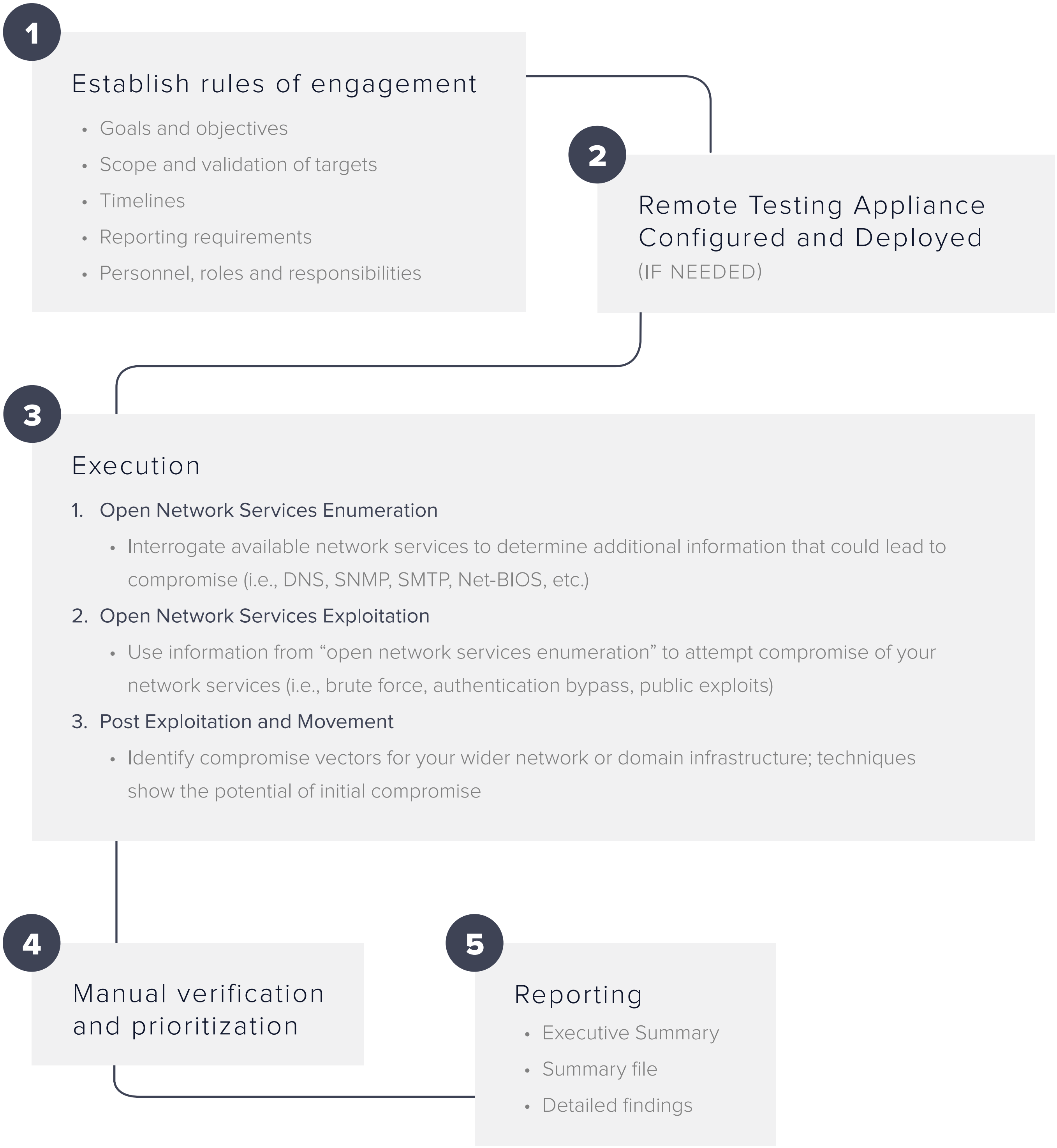
BENEFITS

- Risk identification
- Prioritization of remediation efforts
- Validation of internal and/or external security controls
- Satisfies compliance needs, including HIPAA, SEC, NYCRR, PCI 3.x.

SOLUTIONS AT A GLANCE

	Vulnerability Assessment (Internal or External)	Phishing	Web App Test	Wireless Pen Test	**Penetration Test (Internal or External)**	Red Team
Stealth	Low	Low	Low	Low	Low	High
Scoping	Reports on all systems and vulnerabilities found on in-scope systems	Reports on all target users	Reports on all web applications and vulnerabilities found on in-scope web applications	Threat modeling (from a wireless perspective)	Threat modeling (includes suitable testing scenario)	Customized engagement goals
Target Users		●				●
Objective	Broad scan	Test users	Goal seeking	Goal seeking	Goal seeking	Goal seeking/ Test response
Can be performed on premise				●	●	●
Can be performed remotely	●	●	●		●	●
Vulnerability Scanning	●		●		● (as necessary)	● (as necessary)
Detailed Report	●	●	●	●	●	●
Post-exploitation			●		●	●
Recon on in-scope targets					●	●
Manual testing to simulate attacker methods and techniques			●	●	●	●
Review compromised system for any data that allows further compromise					●	●
Port scanning	●				●	●
Exploitation			●	●	●	●
Escalation			●	●	●	●
Pivoting					●	●
Continue post-exploitation as necessary					●	●
Review compromised or target systems for business-critical data			●		●	●
Report narrative			●	●	●	●
Attack planning and preparation					●	●
Crack "decrypt" any obtained passwords				●	●	●
Phishing		●				●
Vishing						●
OSINT to gather additional targets					●	●
Perimeter breach: Wireless (as necessary)						● (as necessary)
Perimeter breach: Physical testing and drop box placement (as necessary)						● (as necessary)

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

(IF NEEDED)

3

Execution

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.)
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)
3. Post Exploitation and Movement
   - Identify compromise vectors for your wider network or domain infrastructure; techniques show the potential of initial compromise

4

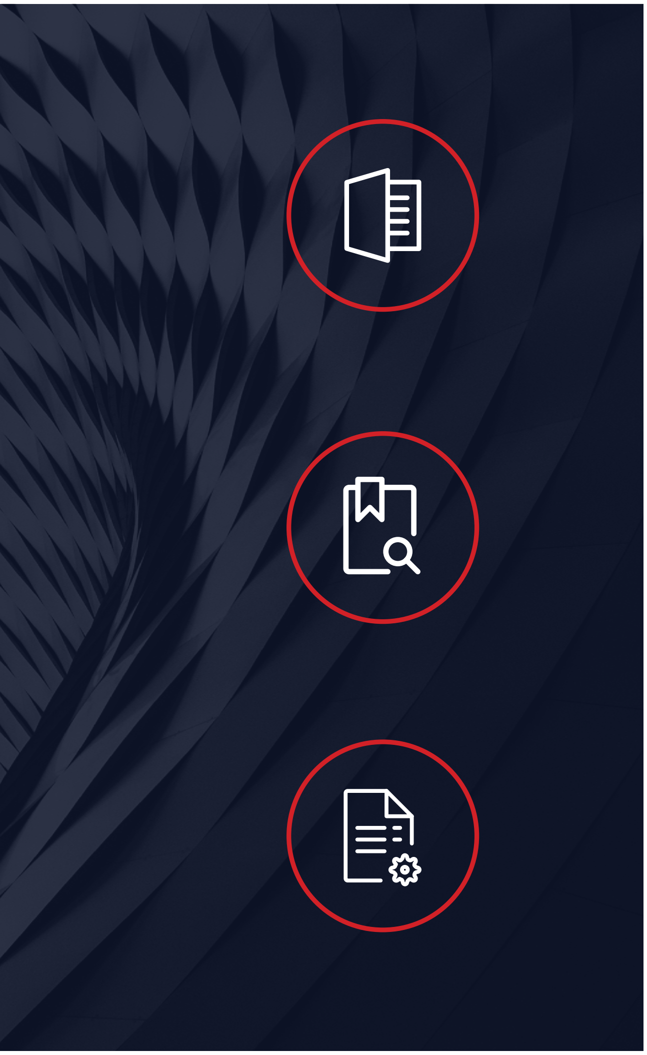
Manual verification and prioritization

5

Reporting

- Executive Summary
- Summary file
- Detailed findings

WHAT TO EXPECT IN YOUR REPORT



EXECUTIVE SUMMARY REPORT

Targeted toward a non-technical audience so they are apprised of risks and mitigation strategies as a result of the test:

Executive Summary: Brief description of the results of the engagement

Findings and Recommendations: Describes scope, approach, findings, high-risk and systemic issues, and recommendations to remedy issues or reduce risk

DETAILED TECHNICAL REPORT

Targeted toward technical staff and provides detailed findings and recommendations:

- Methodology employed
- Positive security aspects identified
- Detailed technical findings
- An assignment of a risk rating for each vulnerability exploited
- Supporting detailed exhibits when appropriate
- Technical remediation steps

After the reports are created, we can set up a meeting to share and discuss the findings.

> *If you're performing Penetration Testing infrequently or have commissioned a large scope of work, keep in mind the requirements of the "post-test" phase. Often, the report will describe remediation measures that could take considerable time and money to implement. Avoid the temptation to just file away the reports that specify challenging or time-consuming remediation.*
>
> Gartner

MAKE THE CASE FOR AN ESENTIRE PENETRATION TEST

- ✓ Testers leverage intelligence from our MDR platform to understand attackers' tactics and apply them in the penetration test
- ✓ Continuous and clear communication and establishment of goals
- ✓ Testing conducted via experienced and certified professionals (CEH, OSCP, CISSP, etc.)
- ✓ Clear reporting with risk prioritization and detailed findings
- ✓ Includes detailed discussion with eSentire Advisory Services team members on findings and remediation

NEXT STEPS

- Test your response capabilities
- Manage your vulnerabilities
- Assess your cybersecurity maturity and chart a measurable course for the future
- Put eSentire Managed Detection and Response to the test

eSENTIRE®

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $5 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements.

For more information, visit **www.eSentire.com** and follow **@eSentire**.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.