

Rules of Engagement (ROE) for Penetration Testing

Contents

[Introduction 3](#_Toc46494073)

[Purpose 3](#_Toc46494074)

[Services 3](#_Toc46494075)

[Objectives 3](#_Toc46494076)

[Approach 4](#_Toc46494077)

[Scope 4](#_Toc46494078)

[Assumptions and Responsibilities 4](#_Toc46494079)

[Assumptions 4](#_Toc46494080)

[Responsibilities 5](#_Toc46494081)

[Confidentiality 5](#_Toc46494082)

[Risks 6](#_Toc46494083)

[Logistics 7](#_Toc46494084)

[Personnel 7](#_Toc46494085)

[Dates and Locations 7](#_Toc46494086)

[Testing Equipment 7](#_Toc46494087)

[Communication Strategy 8](#_Toc46494088)

[General Communications 8](#_Toc46494089)

[Incident Handling and Response 8](#_Toc46494090)

[Security Assessment Execution 9](#_Toc46494091)

[Data Handling 9](#_Toc46494092)

[Reporting 9](#_Toc46494093)

[Signatures 10](#_Toc46494094)

[Appendix A: List of Personnel 11](#_Toc46494095)

[IP Addresses, Subnets, and Hosts 12](#_Toc46494096)

[Web / Mobile Application Testing 12](#_Toc46494097)

[Appendix C: Limitations and Special Handling 13](#_Toc46494098)

[IP Address, Host, and Service Exclusions 13](#_Toc46494099)

[Web Application and Service Exclusions 13](#_Toc46494100)

[Appendix D: Security Assessment Methodology 14](#_Toc46494101)

[Testing Methodology 14](#_Toc46494102)

[Appendix E: Testing Tools 15](#_Toc46494103)

[Reconnaissance Tools 15](#_Toc46494104)

[Foot printing and Enumeration Tools 15](#_Toc46494105)

[Vulnerability Scanners 15](#_Toc46494106)

[Exploitation Tools 15](#_Toc46494107)

[Web Application Tools 15](#_Toc46494108)

[Password Attacking Tools 16](#_Toc46494109)

[Sniffers 16](#_Toc46494110)

[Appendix F: Acronyms 17](#_Toc46494111)

**Table of Figures**

[Figure 1: Services 3](#_Toc3180412)

[Figure 2: Locations and Expected IP Addresses 4](#_Toc3180413)

[Figure 3: Dates and Locations 7](#_Toc3180414)

[Figure 4: In-Scope Assets 12](#_Toc3180415)

[Figure 5: In-Scope URLs 12](#_Toc3180416)

[Figure 6: Host and Service Exclusions 13](#_Toc3180417)

[Figure 7: Web Service Exclusions 13](#_Toc3180418)

# Introduction

## Purpose

The purpose of this document is to define the rules under which an efficient, accurate, and non-disruptive Security Assessment of HAP/MyRounding will be performed.

The approach involves an active analysis of for any potential vulnerabilities that could present risk to assets, systems, infrastructure, customer held data and business processes.

Common categories of vulnerabilities include poor or improper system configuration, hardware or software flaws, and operational weaknesses in processes or technical countermeasures.

The analysis will be conducted from the perspective of a potential attacker and/or a malicious insider with access to HAP/MyRounding’s computing assets and infrastructure.

The assessment will involve a comprehensive analysis and correlation of findings on one or more systems or applications. All discovered vulnerabilities will be documented and provided to HURON CONSULTING GROUP (HURON) through detailed reporting and either an in-person or remote out-brief.

Remediation information and recommendations will also be delivered.

## Services

The following services have been agreed to by HAP Security and HURON per the signed Statement of Work (SOW):

|  |  |  |
| --- | --- | --- |
| **Service** | **Description** | **Comments** |
| Internal Black-Box Penetration Testing | HAP / MyRounding | See SOW |
|

Figure 1: Services

## Objectives

The objectives of the Security Assessment consist of the following:

* Assessment of Business Risk faced by HURON due to inadequate or missing Information Security controls
* Providing HURON with accurate information on the state of information computing systems, applications, and underlying infrastructure
* Providing HURON with a roadmap to improve the state of their information security posture
* Assisting HURON with any Information Security needs they may have

## Approach

Test procedures will include non-destructive test techniques to include manual analysis of discovered vulnerabilities and flaws.

Procedures may include but are not limited to network scanning as well as operating system, database, and application vulnerability scans, and exploitation of discovered vulnerabilities.

Once a vulnerability has been identified, the assessment team will document the vulnerability, attempt to establish whether it affects systems risk, and provide guidance to HURON on how to remediate the vulnerability.

## Scope

The scope for this Security Assessment will include testing of systems, applications, and assets as provided by HURON **.**

A complete list of in-scope IP addresses and applications is contained in Appendix B of this document.

An IP address is considered “live” if a computing asset is communicating at a unique IPv4/IPv6 address and is discoverable by the Security Assessment Team (SAT). Common protocols used for discovery and testing include TCP, UDP, and ICMP.

# Assumptions and Responsibilities

## Assumptions

HAP Security assumes all management and technical staff members related to the systems under test will fully cooperate to maximize the opportunity of success for the Security Assessment.

Prior to the Security Assessment, HURON’sleadership and staff members will be notified, unless employee interaction is considered in-scope for the security assessment.

All Security Assessment activities will be coordinated by HURON’s POC to avoid interference with ongoing business operations.

If at any time HAP Security or HURON determines testing activities have crossed the boundary of a system not identified as in-scope for testing, the Security Assessment team shall immediately pause testing activities and notify all responsible parties.

Before the Security Assessment begins, HURON will provide HAP Security with the following resources (**if applicable**):

1. The expected number of unique, “live” IP addresses for each location
2. A complete list of all IP addresses that will be considered “in-scope” for testing
3. A list of any IP addresses/services that should not be tested (outside of scope)
4. If applicable, on-site logistics support to include:
   1. An escort into secure spaces
   2. Technical support to assist with identification of communication equipment racks, data switches, data switch ports, default gateways, and IP addresses for pen tester use
   3. A work surface (e.g.: table or desk), chair, access to AC power, power strips, and network cables (on site testing only)
5. HURON will notify any hosting providers, vendors, service providers, or any other entities with the potential to be affected by testing activities
6. If the Security Assessment is to be performed remotely but includes internal (non-internet accessible) IP addresses, HURON will provide the assessment team with a method to reach those resources (VPN tunnels, firewall rules, etc.).

## Responsibilities

1. HAP Security will provide skilled and knowledgeable personnel to conduct the Security Assessment.
2. HAP Security will provide all necessary hardware and software to complete the assessment.
3. Customer shall provide a knowledgeable Point of Contact dedicated to this project and make available any other key resources and information reasonably necessary to successfully complete these Services.
4. Customer will provide target identification data prior to testing.
5. Customer shall make necessary any security arrangements to allow HAP Security access to equipment, buildings, and rooms, if applicable.
6. Upon completion of the Services provided by HAP Security, responsibility for administering the environment or addressing any out of scope issues or gaps identified by the HAP Security testing team.
7. Customer will communicate any issues or concerns with respect to the Services, including any Deliverables, in a timely manner to the Project Representatives

## Confidentiality

Information gained through a Security Assessment is sensitive in nature. As such, HAP Security or its contractors will not share any information gathered through testing with parties other than authorized customer representatives.

In addition, HAP Security will delete all test data from testing systems once the final report has been delivered and accepted. This ensures that vulnerability information is not inadvertently disclosed to 3rd parties.

HAP Security and HURON will be bound by any Non-Disclosure Agreements (NDA) signed prior to testing activities.

## Risks

There are inherent risks to conducting any type of Information Security Assessment, including Penetration Testing.

Common Risks that can be encountered include:

* Denial of Service (DoS) of the entire system or specific components
* System performance degradation
* Temporary loss of connections with customers, business partners, vendors, employees, and others with access to client computer systems

In the event adverse impacts are observed due to testing actives, HURON will contact HAP Security immediately so that testing can be halted. Analysis will be conducted to determine which activities caused an adverse reaction, which may in and of itself identify a vulnerability.

It is strongly advised that HURON has a functional and tested backup/recovery process in place for all systems that will be in scope for the Security Assessment. This is especially important for Web Application testing. HAP Security and its consultants will not be held liable for any business losses due to the lack of a functional and tested backup/recovery system.

# Logistics

## Personnel

Only personnel agreed to by HAP Security andHURON will have knowledge of and participate in testing activities. This includes 3rd party personnel such as service providers, contractors, and business partners.

A complete list of personnel involved in the Security Assessment is contained in [Appendix A](#_Appendix_A:_List) of this document.

## Dates and Locations

The following table contains desired testing dates for each location. HAP Security will notify affected personnel before and after testing activities are performed.

|  |  |  |
| --- | --- | --- |
| Dates | Location | Description |
|
| 27 July 2020 – 31 July 2020 | Remote | Conduct Interviews of Huron CG Staff |
| 3 Aug 2020 – 21 Aug 2020 | Remote | 3PAO Conducts Pen Test Assessment |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Figure 3: Dates and Locations

## Testing Equipment

All hardware and software used by the testing team will be wholly owned and/or licensed to HAP Security or it’s approved contractors.

The assessment team may also use resources hosted on internet resources such as Amazon Web Services (AWS), as well as other cloud hosted services. Notification of testing activities is typically provided to hosting providers before testing begins.

Prior to beginning test activities, the assessment team will provide its source IP addresses so HURON is aware of the origin of traffic that may appear malicious.

A list of software that may be used during the Security Assessment is provided in [Appendix E](#_Appendix_E:_Testing) of this document.

# Communication Strategy

## General Communications

Effective communication is critical to the success of the Security Assessment.

An initial kick off meeting will be conducted virtually or by phone conference. The purpose of the meeting will be to introduce the involved parties and to discuss the process, schedule, and to understand HURON’s goals and concerns for the Security Assessment.

Prior to any testing activities, HURON’s representatives will be notified to coordinate the testing scope.

If at any time the testing team feels they have discovered a significant vulnerability that has an immediate impact on the confidentiality, integrity, or availability of the systems being assessed, HAP Security will notify HURON.

Likewise, if at any time during the test HURON staff feels like the system is being adversely affected by testing activities, they may inform the assessment team members to halt testing.

If testing activities are found to adversely impact operations, HURON has the option to halt or stop testing, conduct an analysis of activities, then schedule an alternative time to complete testing, as applicable

## Incident Handling and Response

There may be times when a system under test is the target of an actual attack, is being maliciously scanned, or is infected by malware or a virus. In these cases, testing activities will be halted to facilitate investigation and restoration any affected systems.

To aid incident response and management activities, the assessment team will provide HURON with their source IP addresses (both internal and external), to ensure the Security Assessment is not misinterpreted as an actual attack.

Should it be discovered that testing activities are adversely impacting the functionality of a system or causing a service disruption, the assessment team will immediately halt testing activities upon notification by HURON**.**

# Security Assessment Execution

## Data Handling

Information generated about HURON**’s** assets as part of the Security Assessment activities may contain sensitive information that could be damaging were it to be disclosed.

HAP Security shall handle any information collected as Sensitive/Confidential and will not release any information to any entity outside HURON, unless prior approval is granted in writing.

HAP Security shall comply with HURON’s policies regarding the protection of this information.

Standard data handling procedures include:

* Using “clean” systems and virtual machines for testing
* Securing laptops and testing systems using disk encryption
* Transferal of test data using secured transmission mediums, to include HTTPS, IPSEC, etc.
* Removing test data from testing systems at the conclusion of testing activities
* Erasing test data using secure methods, such as crypto-shredding, secure wipe, etc.

After records are accepted byHURON , any copies held by HAP Security will be destroyed.

## Reporting

The final deliverable for the Security Assessment is the Final Report. This report will document the test and will include findings, vulnerabilities, and mitigation strategies.

It is not uncommon for the report to undergo several revisions, and reasonable modifications will be made as requested by HURON.

An in person or remote out-brief to stakeholders can also be requested.

# Signatures

IN WITNESS WHEREOF, HAP Security and HURON have executed this Rules of Engagement as of the date of the signature below by their duly authorized representatives.

HAP Security and HURON, by their respective signatures below, expressly acknowledge and agree they have carefully read this Rules of Engagement and agree to the terms within.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **HAP Security Security** | |  | **HURON** | |
| **Name:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | **Name:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Signature:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | **Signature:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Position:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | **Position:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Date:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | **Date:** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |  |  |

# Appendix A: List of Personnel

The following people will play a role in the Security Assessment for HURON .

|  |  |
| --- | --- |
| **Name:** | Tyler Masters |
| **Company:** | Huron Consulting Group |
| **Phone:** | 123.456.7890 |
| **Email:** | [tyler.masters@huronconsultinggroup.com](mailto:tyler.masters@huronconsultinggroup.com) |
| **Role:** | FedRAMP Project Manager |

|  |  |
| --- | --- |
| **Name:** | Andrew Fox |
| **Company:** | Huron Consulting Group |
| **Phone:** | 123.456.7890 |
| **Email:** | [tyler.masters@huronconsultinggroup.com](mailto:tyler.masters@huronconsultinggroup.com) |
| **Role:** | FedRAMP ISSM / Security Testing Team Lead |

|  |  |
| --- | --- |
| **Name:** | Phillip Harrell |
| **Company:** | Access Data Consulting Group |
| **Phone:** | 123.456.7890 |
| **Email:** | [tyler.masters@huronconsultinggroup.com](mailto:tyler.masters@huronconsultinggroup.com) |
| **Role:** | FedRAMP Deputy ISSM / Security Testing Engineer |

Appendix B: List of In-Scope IP Addresses and URLs

The assets below will be considered “in-scope” for the Security Assessment. Addresses and hosts that are not listed here will not be included in testing activities.

## IP Addresses, Subnets, and Hosts

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address/Range | Host/Domain Name | CSP | Internal/External |
| 123.123.123.123 | 123.123.123.123 | Huron Consulting Group |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Figure 4: In-Scope Assets

For Web Application testing, the following URLs will be considered in-scope:

## Web / Mobile Application Testing

Figure 5: In-Scope URLs

|  |  |  |
| --- | --- | --- |
| IP Address | URL | Comments |
| To be discovered and validated |  |  |
|  |  |  |
|  |  |  |

# Appendix C: Limitations and Special Handling

In the event HURON does not want an asset, service, port, etc. tested, notification will be provided before testing begins.

## IP Address, Host, and Service Exclusions

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address/Range | Host/Domain Name | Host/Component Excluded | Comments |
|
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Figure 6: Host and Service Exclusions

## Web Application and Service Exclusions

|  |  |  |
| --- | --- | --- |
| IP Address/Range | URL | Comments |
|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Figure 7: Web Service Exclusions

# Appendix D: Security Assessment Methodology

## Testing Methodology

The Security Assessment for HURON will consist of the following phases:

* **Scoping**: determining the customer’s goals and expectations for the Security Assessment
* **Reconnaissance**: using open source/publicly available information to determine the Customer’s attack surface from the viewpoint of an external attacker
* **Scanning**: using open source and proprietary tools to map in-scope subnets, systems, services, and discover potential vulnerabilities
* **Exploitation (Penetration Testing Only):** targeted exploitation of discovered vulnerabilities to demonstrate that they represent Business Risk. This can include “pivoting” to other systems that may be vulnerable
* **Reporting**: providing the customer with a detailed report of all vulnerability findings, successful exploitation vectors, and recommendations to remediate all discovered findings

# Appendix E: Testing Tools

The following tools *may be used* in the Security Assessment/Penetration Test. In addition, custom or publicly shared scripts may be written used to meet specific testing objectives.

### Reconnaissance Tools

**Arptool**: ARP and ICMP scanner

**Bing**: estimates bandwidths between network hosts and routers

**Firewalk**: employs traceroute-like techniques to analyze IP packet responses to determine gateway ACL filters and map networks

**Fragrouter**: network tool to send custom ICMP/UDP/TCP packets and to display target replies

**ipsend**: generates TCP/IP packets with a scripting language

**nemesis**: command-line UNIX network packet injection suite based on libnet

**Netdiscover**: tool that can discover TCP/IP hosts on multiple network segments

**SendIP**: command Line IP Packet Generator

### Foot printing and Enumeration Tools

**Nmap**: network and host scanner that reveals live hosts, port status, operating system and service information.

**Superscan**: GUI network and host scanner that runs under a Microsoft Windows environment

**UDPprobe**: sends and receives UDP Packets

**Flatline**: web server vulnerability scanner. Options include mass host scanning, scanning through proxies, detection evasion, and quick banner grab scans

**Ftpscan**: Searches FTP sites for world writeable directories

**LDAPminer**: Scans for LDAP vulnerabilities

**Scowl**: A CGI vulnerability scanner

**Snmpscan**: scans hosts or routers running SNMPD for common communities (passwords)

**Whisker**: A 'next generation' CGI scanner

**Zodiac**: A portable, extensible and multithreaded DNS tool

### Vulnerability Scanners

**Nessus Professional**: a widely used commercial vulnerability scanner

**Tenable.io**: cloud-based version of Nessus and Tenable Security Center

**Qualys Vulnerability Scanner**: a widely used commercial vulnerability scanner

**Qualys SSL Labs:** online SSL/TLS scanner geared towards protocols, ciphers, and X.509 certificates

### Exploitation Tools

**CANVAS**: a commercial exploitation toolkit

**Metasploit Framework**: a collection of open-source, community vetted exploit code

**Poweshell Empire**: An open source collection of post exploitation tools for Windows

### Web Application Tools

**Burp Suite Professional**: commercial Web Application scanner.

**NetSparker**: commercial Web Application scanner

**OWASP Tools**: a collection of tools used for analyzing web application security

**Samurai Web Testing Framework**: live Linux environment pre-configured to function as a web pen-testing environment

**Teneable.io**: cloud-based vulnerability scanner

**ZAP (ZED Attack Proxy):** interception proxy released by the OWASP project

### Password Attacking Tools

**Hydra**: a multi-threaded online password guesser

**John the Ripper**: A widely used password cracker

**L0phtcrack**: A Windows NT password sniffer and cracker

**Mimikatz**: an open-source application that allows users to view and save authentication credentials like Kerberos tickets and password hashes

**OCL Hashcat**: a versatile GPU hash and password cracker. Known for its speed

**Pandora**: An offline password auditing and Online attack for the X Windows platform on Linux

**Rainbow Crack**: A Windows password cracker uses pre-generated hashes

### Sniffers

**Dsniff**: A collection of tools for network auditing and Penetration Testing

**Netmon**: network sniffer/packet analyzer released by Microsoft

**TCPdump**: Unix/Linux based network sniffer

**Wireshark**: a widely network capture and analysis tool

# Appendix F: Acronyms

* **A&A**: Assessment and Authorization
* **ACK**: Acknowledgment
* **ACL**: Access Control List
* **AO**: Authorizing Official
* **AODR**: Authorizing Officials’ Designated Representative
* **ARP**: Address Resolution Protocol
* **BGP**: Border Gateway Protocol
* **CASL**: Custom Auditing Scripting Language
* **CGI**: Common Gateway Interface
* **CIRT**: Computer Incident Response Team
* **CISO**: Chief Information System Officer
* **CSO**: Chief Security Officer
* **CSPSB**: Cyber Security Program and Solutions Branch
* **DCS**: Data Collection System
* **DCE/RPC**: Distributed Computing Environment/Remote Procedure Call
* **DNS**: Domain Name Service
* **DoS**: Denial of Service
* **DMZ**: De-Militarized Zone
* **EDT**: Eastern Daylight Time
* **FIN**: Finish
* **FTP**: File Transfer Protocol
* **GPL**: Government Project Lead
* **GRE**: Generic Routing Encapsulation
* **HTTP**: Hypertext Transfer Protocol
* **HTTPS**: Secure Hypertext Transfer Protocol
* **ICMP**: Internet Control Message Protocol
* **ICS**: Industrial Control System
* **IOC**: Indicator of Compromise
* **IP**: Internet Protocol
* **IPSec**: Internet Protocol Security
* **IPX/SPX**: Internetwork Packet Exchange / Sequenced Packet Exchange
* **POC**: Information System Security Officer
* **L2TP**: Layer 2 Tunneling Protocol
* **LAN**: Local Area Network
* **LDAP**: Lightweight Directory Access Protocol
* **LSA**: Link State Advertisement
* **MAC**: Mission Assurance Category or Media Access Control
* **MOD**: Mission Operations Department
* **NBT**: NetBIOS over TCP
* **NCA**: No Configured Address
* **NetBIOS**: Network Basic Input/Output System
* **NTP**:Network Time Protocol
* **NIDS**: Network Intrusion Detection System
* **ORB**: Operational Review Board
* **OS**: Operating System
* **OSPF**: Open Shortest Path First
* **OSI**: Open System Interconnection
* **Pentest**: Penetration Test
* **POA&M**: Plan of Action and Milestones
* **POC**: Point of Contact
* **PPTP**: Point-to-Point Tunneling Protocol
* **RADIUS**: Remote Authentication Dial-In User Service
* **RFID**: Radio Frequency Identification
* **RIP**: Routing Information Protocol
* **ROE**: Rules of Engagement
* **RPC**: Remote Procedure Call
* **SAT**: Security Assessment Team
* **SMB**: Server Message Block
* **SNMP**: Simple Network Management Protocol
* **SO**: System Owner
* **SSL**: Secure Socket Layer
* **SYN**: Synchronize
* **TCP**: Transmission Control Protocol
* **TDS**: Top-level DNS Scanner
* **TLS**: Transport Layer Security
* **UDP**: User Datagram Protocol
* **VA**: Vulnerability Assessment
* **WAN**: Wide Area Network