Penetration Testing Packages Pivot Point Security	Investigative Assessment	Intentioned Assessment	Tenacious Assessment
Assurance Level	The Investigative Attacker doesn't have a lot of time, and doesn't have a lot of tools, and may not even be targeting you specifically. He may stumble upon your external IP during a sweep and will pay you little mind unless you have an obvious security problem. Attackers that get in through a blank or default password on an administrative account are Investigative Attackers.	The Intentioned Attacker has more time, and a few more tools than the Investigative attacker. More importantly, she has intent. She wants to find a weakness in your network specifically. Attackers that get in by exploiting an unpatched vulnerability in an operating system or network service are Intentioned Attackers.	The Tenacious Attacker has time, tools, intent, and determination. He is willing to go the extra mile to make it past your defenses. He may even attempt social engineering to find a way beyond your perimeter defenses. He will do it quietly, though, and take care to go unnoticed. Attackers who convince your help desk to reset an account password for them are Tenacious Attackers.
Extent/Rigor	Moderate	High (~1.4x Investigative)	Extensive (~2.5x Investigative)
Reconnaissance Phase			
Google Hacking	No	No	Yes
ARIN/DNS	No	Yes	Yes
News Groups	No	Yes	Yes
Social Media	No	No	Yes
Foot Printing Phase (Vulnerability Assessment)			
IP Definition	By Client	By Client or Discovery Scan (< 4X the number of contracted IP's)	By Client or Discovery Scan (< 24X the number of contracted IP's)
Network Sniffing	No	Yes	Yes
Ports Analyzed	~1,000 Top Ports	65,000 Ports	65,000 Ports
Protocols	TCP & UDP	TCP & UDP	TCP, UDP, & selected layer 2 protocols
# Scans	Single	Single	Dual (separated by time) on request
Points of Origin	Single	Single	Dual (as necessary)
~ Public Sampling	100%	100%	100%
~ Server Sampling	40 -> 100%	50 -> 100% VA	60 -> 100%
~ Host Sampling	20 -> 100%	25 -> 100%	30 -> 100%
Network Devices	Yes	Yes	Yes
Printers	No	Performed on request	Not performed on request
Sensitive Hosts	No	Performed on request	Not performed on request
Privileged Scanning	No	Optional (see below)	Optional (see below)
Content Scanning	No	Optional (see below)	Optional (see below)
Perspective	White	White/Grey	White/Grey/Black
IDS/IPS Evasion	IPS must be disabled	IPS disabled or enabled (with assurance related to objective)	IPS disabled or enabled or both (with assurance related to objective)
Visibility	Quiet	Quiet/Stealth	Quiet/Stealth/Black Ops
Allowable Impact	Do no harm	Do no harm	Do no/minimal harm (client defined)
Active Exploit / Intrusion Phase			
~ Public Sampling Rate (based on #)	2 -> 66%	4 -> 100%	5 -> 100%
~ Server Sampling Rate (based on #)	2 -> 66%	4 -> 100%	5 -> 100%
~ Host Sampling Rate (based on #)	1 -> 33%	2 -> 100%	2.5-> 100%
Exploits Utilized	Known exploits	Exploit research as required	Exploit research as required
Password Cracking	None	None	On request
Network Exploits	None	Directed ARP poisoning attacks	Directed ARP poisoning attacks
Encryption Attacks	None	SSL Attacks	SSL Attacks, SSL Stripping
Command & Control Tactics	No	No	Yes
Leap-Frogging	No	No	Yes
General			
Test Team	Engagement Manager & Security Consultant	Engagement Manager, Sr. Security Consultant, & Security Consultant	Engagement Manager, Practice Lead, & Sr. Security Consultant
Test End	Victory Condition or Scope Exhaustion	Victory Condition, Surrender, or Scope Exhaustion	Victory Condition, Surrender, or Scope Exhaustion

Optional Assessment Activities

Social Engineering	Provides assurance that Security Awareness training is effective by employing scenario based Social Engineering activities
Physical Security Testing	Provides assurance that Physical Security Controls are operating as intended. Commonly performed in concert with scenario based Social Engineering.
Privileged VA	Provides much more thorough and accurate Vulnerability Assessment reports as the scans are run with administrative level of privilege.
Content Scanning	Detects sensitive information (e.g., Personally Identifiable Information, Credit Cards, Medical Data) on hosts/servers to provide assurance that data confidentiality controls are operating as intended. Generally performed in concert with a Privileged Vulnerability Assessment.
Incident Response Testing	Provides a mechanism to determine whether monitoring and incident response procedures are operating as intended. Security Assessments (e.g., Vulnerability Assessment/Penetration Testing/Social Engineering) are conducted from a covert perspective with the intention of slowly
War Driving	Also called: WLAN Assessment. Provides verification that Wireless Local Area Networking is aligned with prevailing good practices.