# Red Team Exercise

eSentire will, through a variety of means (for example, social engineering or penetration testing) selected by eSentire, attempt to infiltrate Client's network at the frequency indicated on the applicable Partner Order Form. A Red Team Exercise may include the following:

i. Attempt to establish an undetected persistent foothold in Client's network that could be used to pivot to other internal systems;
ii. Attempt to compromise and gain privileges on workstations, servers and Client-specified systems;
iii. Attempt to escalate privileges and gain administrative privileges on workstations, servers and Client-specified systems (including attempting to gain top domain admin access);
iv. Attempt to obtain access to key systems and information defined by Client (known as a Capture the Flag exercise);
v. Attempt to compromise high profile users (for example, accounts and credentials);
vi. Attempt to bypass security controls on workstations and servers to execute eSentire controlled code;
vii. Attempt to use custom, non-destructive malware and other technology (custom websites, executable web applets);
viii. Open source intelligence gathering whereby through the use of custom tools and a variety of services data is collected related to Client's employees and their external network (OSINT). This data is used to generate lists of potential usernames and passwords, discover publicly available email addresses, and generate a snapshot of open ports and services for use in penetration testing and Red Team Exercises;
ix. External penetration testing whereby eSentire identifies the services running on each host, and identifies the service versions running on each host, as well as:
    a. Penetration attempts on hosts and/or services identified by Client and which have known vulnerabilities;
    b. Attempt external infrastructure attacks (excluding denial of service attacks);
    c. Attempt external data access attacks (including brute force attacks);
    d. Attempt basic technical security violations of external facing applications (including cross site scripting attacks, cross site referencing, and SQL injection attacks); and
    e. Attempt a deep dive exploitation of identified weaknesses in external systems into internal systems.
x. Social engineering whereby:
    a. eSentire identifies Client employees using publicly available information and, at eSentire's discretion, targets such employees for social engineering campaigns based on such employee's role at Client,
    b. eSentire potentially conducts phishing campaigns to attempt to access and/or gather confidential information of Client or to exploit other vulnerabilities to compromise Client's data and/or infrastructure security;
    c. eSentire potentially conducts vishing campaigns to attempt to access and/or gather confidential information of Client or to exploit other vulnerabilities to compromise Client's data and/or infrastructure security; and
    d. eSentire attempts to install custom, non-destructive malware on a Client system, including use of USB dongles, flash drives, etc. or use other technology (custom websites, executable web applets, etc.) in connection with telephone calls to Client employees or phishing emails to access and/or gather confidential information of Client.