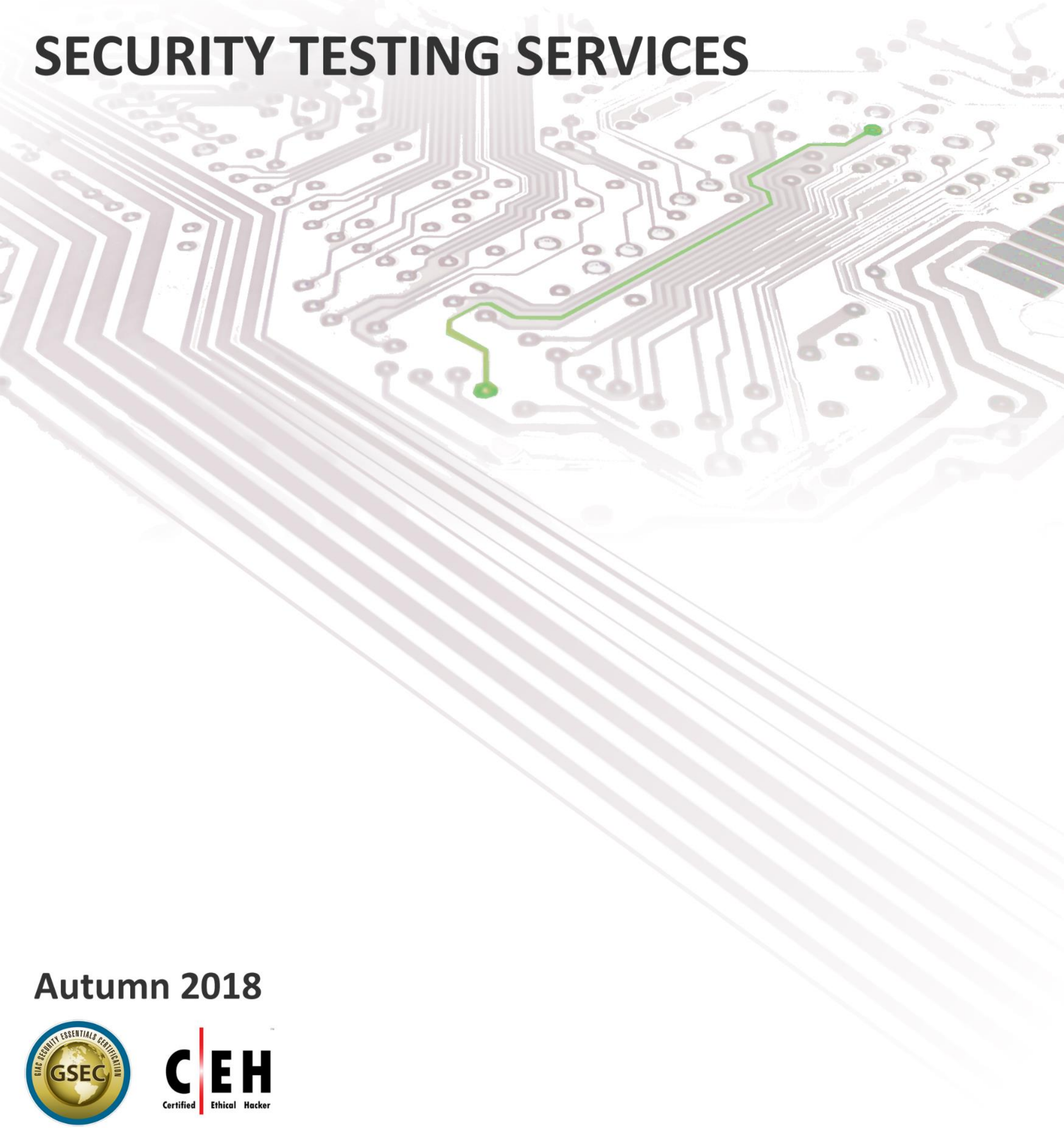
DCT

SECURITY TESTING SERVICES



Autumn 2018

Firewall and External IP Security Assessment

Duration: 2-3 days

Security Tests:

- Scan all available ports to confirm that the services advertised comply with firewall policy and rules.
- Enumerate all available services on the external IP
- Perform (un)authenticated vulnerability scans on public facing servers.
- Provide clear findings and a prioritised list of actions, work efforts, and findings.

Penetration Test for an SME company

Duration: 5-7days depending on scope

The stages listed outline the basic steps that form a penetration test. Each penetration test is different and requires careful planning and scoping

Discovery Phase

- Use DNS enumeration techniques to discover mail servers and public routing information.
- OSINT domain name to discover email address, staff and company details.

Enumeration Phase

- Network discovery scanning and service enumeration.
- Actively trying to obtain user names and application version information for running services.
- Perform vulnerability scans.

Planning Phase

- Map the profile of the environment to publicly known, or, in some cases, unknown vulnerabilities.
- Discover and test possible exploits.

Exploitation Phase

- Attempt to gain privileged access to a target system by exploiting the identified vulnerabilities.
- Carry out password attack against public email accounts

Reporting Phase

- Provide clear findings and a prioritised list matrix actions, work efforts, and findings.