Source | Rich Text | Ω

Recompile 336

```
organizational approval before proceeding.\\
89 As businesses collect, process and store increasingly large
amounts of data, the need for ethical hackers as part of their
cybersecurity programs will grow. The demand for ethical hackers
has already far outstripped supply, and that's not going to
change anytime soon.
90 Ethical hackers use their knowledge to secure and improve the
technology of organizations. They provide essential services to
these organizations by looking for vulnerabilities that can lead
to a security breach. An ethical hacker reports the identified
vulnerabilities to the organization. Additionally, they provide
remediation advice. In many cases, with the organization's
consent, the ethical hacker performs a re-test to ensure the
vulnerabilities are fully resolved.  Malicious hackers intend to
gain unauthorized access to a resource (the more sensitive the
better) for financial gain or personal recognition. Some
malicious hackers deface websites or crash backend servers for
fun, reputation damage, or to cause financial loss. The methods
used and vulnerabilities found remain unreported. They aren't
concerned with improving the organizations security posture.\\
91 To conclude, Ethical hacking covers all methods and techniques of
hacking and cyber attacks. This is a long-term assessment
conducted by ethical hackers with the necessary privileges to
explore the IT infrastructure more broadly. Moreover, it uses a
wide range of attack vectors and types to break into systems and
help uncover vulnerabilities and security flaws.
92
93 \subsection{Penetration Testing }
94 Whereas ethical hacking gives actors the freedom to use whatever
attack methods they have at their disposal, penetration testing
```

(a) Perimeter device:

A network perimeter device is the boundary between an organization's secure internal network and the Internet or other uncontrolled external networks. In other words, a network edge device is an edge that an organization can control.

(b) Operating System:

Many hackers are interested in finding out what operating system is supported and what vulnerabilities it can present.

(c) Services :

Services have as a purpose serving as a communication endpoint.

(d) Web Services:

Web Services is a standardized framework for extending communication between client and server applications to the WWW. More specifically, it is a software module that is designed to perform a certain set of tasks. It is also by definition a server running on a computer device, listening for requests at a particular port

over a network, serving web documents.

I.4.1.2 Scanning