[illegible] CEH [illegible] – 19

[illegible] CEH ([illegible]): [illegible]

[illegible] (Enumeration) [illegible].

[illegible] **CEH** [illegible].

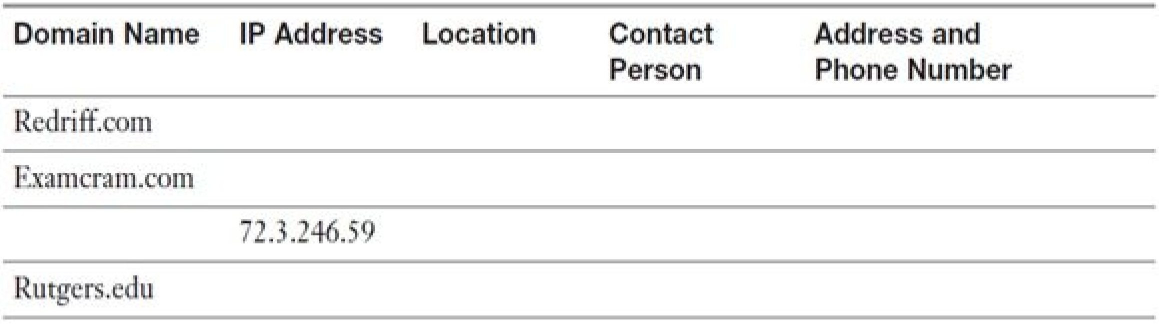
[illegible].

active fingerprinting، CNAMEs، covert channel، demilitarized zone (DMZ)، denial of service (DoS)، echo reply، echo request، EDGAR database، initial sequence number (ISN)، Internet Assigned Numbers Authority (IANA)، intrusion detection system (IDS)، Nslookup، open source، passive fingerprinting، ping sweep، port knocking، scope creep، script kiddie، Simple Network Management Protocol (SNMP)، social engineering، synchronize sequence number، Time To Live (TTL)، traceroute، war dialing، war driving، Whois، written authorization، and zone transfer

[illegible]

[illegible] 20 [illegible].

[illegible] 1[illegible] Rutgers.edu ، Redriff.com ، Redriff.com [illegible] 72.3.246.59 [illegible].



Domain Name	IP Address	Location	Contact Person	Address and Phone Number
Redriff.com				
Examcram.com				
	72.3.246.59			
Rutgers.edu				

[illegible] 2[illegible].

[illegible] 3[illegible] https://www.whois.net [illegible]:

- http:/www.betterwhois.com
- www.allwhois.com
- http://geektools.com
- www.all-nettools.com
- www.dnsstuff.com

[illegible] 4[illegible] traceroute [illegible] r- [illegible].

[illegible] 5[illegible] RIPE ، ARIN ، IANA [illegible].

[illegible] 6[illegible].

[illegible]

[illegible]

[illegible].

[illegible] 1 [illegible] Nmap [illegible] https://nmap.org/download.html [illegible]. [illegible] 7.30 [illegible].

[illegible] 2 [illegible] Nmap [illegible].

[illegible] 3 nmap -h [illegible].

[illegible] 4 [illegible] nmap [illegible]. [illegible]. [illegible]. [illegible].

[illegible] 5 [illegible] UDP [illegible].

[illegible] 6 [illegible] stealth [illegible].

[illegible] 7 [illegible] fingerprint [illegible].

[illegible] 8 [illegible]. [illegible] nmap -sT IP-Address [illegible]. [illegible] IP-Address [illegible].

[illegible] 9 [illegible] stealth [illegible]. [illegible] Nmap -sS IP-Address [illegible]. [illegible] IP-Address [illegible].

[illegible] 10 [illegible] UDP [illegible]. [illegible] nmap -sU IP_address [illegible].

[illegible] 11 [illegible] fingerprint [illegible] namp -O IP-Address [illegible].

[illegible] 12 [illegible]. [illegible] Nmap [illegible]

[illegible]

■ [illegible] (Enumeration): [illegible].

■ [illegible]: [illegible].

[illegible]. [illegible] CEH [illegible] (OS) [illegible]. [illegible]. [illegible]. [illegible]. [illegible] (Enumeration) [illegible]. [illegible]. [illegible].

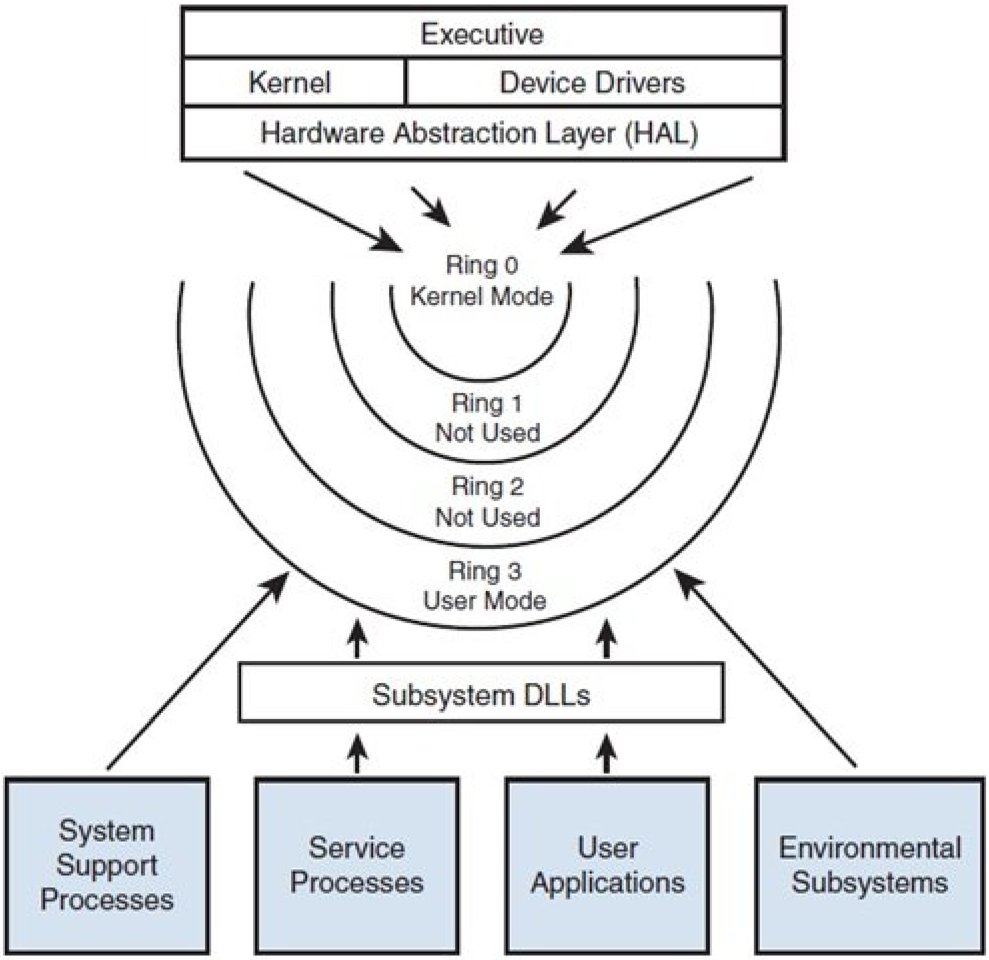
[illegible]

[illegible]

[illegible] UNIX / Linux [illegible] SNMP [illegible] NetBIOS / LDAP [illegible] NTP [illegible] SMTP [illegible] DNS [illegible]

[illegible]

[illegible] 10، 8 و 7 [illegible] 2012، 2016 و 2019 [illegible]



[illegible] (3 [illegible]) [illegible] (0 [illegible]) [illegible]:

■ Security identifiers (SID)

■ Relative identifiers (RID)

SID [illegible] S-1-1-0 SID [illegible]. RID [illegible] SID [illegible].

[illegible]

S-1-5-21-1607980848-492894223-1202660629-500

S for security id

1 Revision level

5 Identifier Authority (48 bit) 5 = logon id

21 Sub-authority (21 = nt non unique)

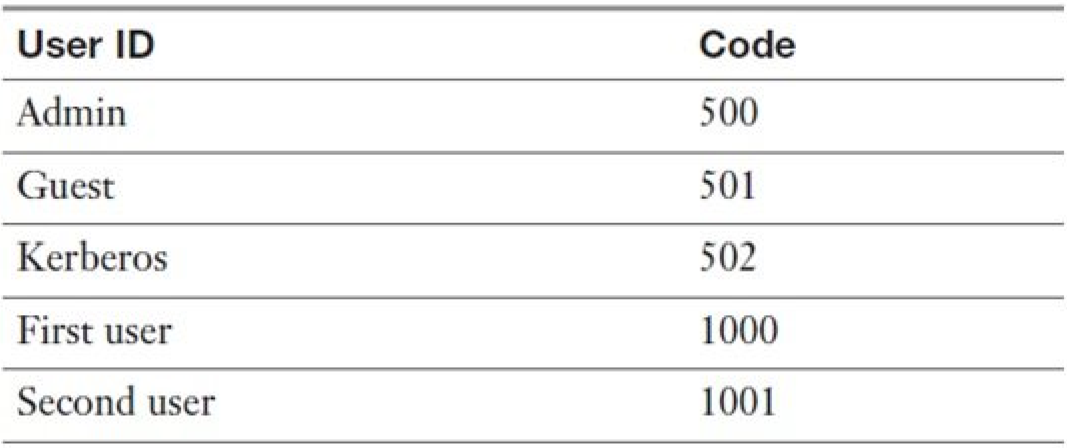
1607980848 SA

492894223 SA domain id

1202660629 SA

500 User id

[illegible] 2 [illegible].



User ID	Code
Admin	500
Guest	501
Kerberos	502
First user	1000
Second user	1001

[illegible] RID 500 [illegible] RID 501 [illegible] RID 1000 [illegible] RID [illegible] (UID) [illegible] (GID) [illegible] etc / passwd / [illegible].

[illegible]

[illegible] (SAM) [illegible] Security Account Manager [illegible] Active Directory [illegible] SAM [illegible] SAM [illegible] Windows / System32 / config [illegible] HKLM \ SAM [illegible].

AD [illegible] AD [illegible] SAM [illegible] NT [illegible] AD [illegible] LDAP [illegible]

[illegible] RFC 2251 [illegible]. [illegible] (LSASS) [illegible]. LSASS [illegible].

[illegible].

[illegible] CEH [illegible]:

[[illegible] CEH]()

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
13:40 - 18/02/1399
[illegible]:
[illegible] CEH - [illegible] CEH - [illegible] CEH - [illegible] - [illegible] CEH v10 - [illegible] - [illegible] CEH10 - [illegible] - [illegible] - [illegible] - [illegible] Nmap - [illegible] SuperScan

---

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/16806/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%B3%D8%B1%D8%B4%D9%85%D8%A7%D8%B1%DB%8C-%D9%88-%D9%87%DA%A9-%DA%A9%D8%B1%D8%AF%D9%86-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7