



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



SCNP-EN Dumps
SCNP-EN Braindumps
SCNP-EN Real Questions
SCNP-EN Practice Test
SCNP-EN Actual Questions



Exin

SCNP-EN

SCNP Strategic Infrastructure Security

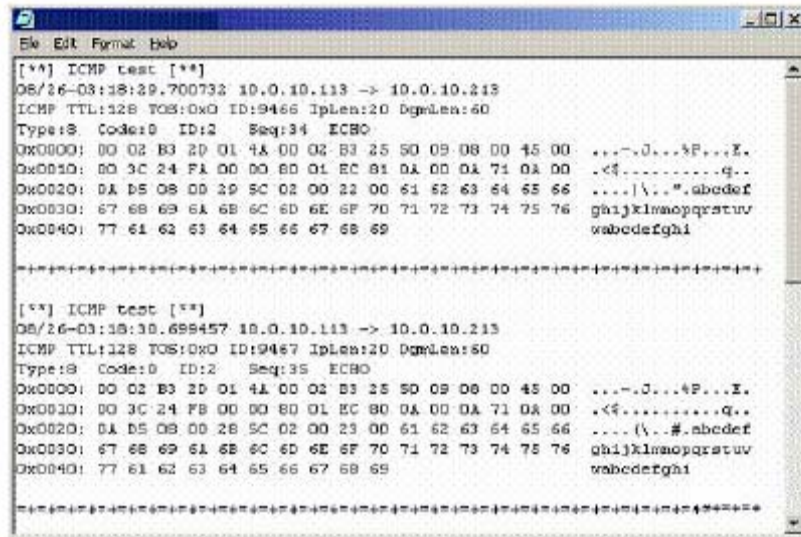


<https://killexams.com/pass4sure/exam-detail/SCNP-EN>

Answer: B

QUESTION: 225

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?



```
File Edit Format Help
[**] ICMP test [**]
08/26-03:18:29.700732 10.0.10.113 -> 10.0.10.213
ICMP TTL:128 TOS:0x0 ID:9466 Iplen:20 Dgmlen:60
Type:8 Code:0 ID:2 Seq:34 ECHO
0x0000: 00 02 B3 20 01 4A 00 02 B3 25 50 09 08 00 45 00  ...-.J...P...X.
0x0010: 00 3C 24 FA 00 00 80 01 EC 81 0A 00 0A 71 0A 00  <$.-----q..
0x0020: 0A D5 08 00 2D 5C 02 00 22 00 61 62 63 64 65 66  ....|\..".abedef
0x0030: 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
0x0040: 77 6A 62 63 64 65 66 67 68 69                      wabedefghi

+-----+
[**] ICMP test [**]
08/26-03:18:30.699457 10.0.10.113 -> 10.0.10.213
ICMP TTL:128 TOS:0x0 ID:9467 Iplen:20 Dgmlen:60
Type:8 Code:0 ID:2 Seq:35 ECHO
0x0000: 00 02 B3 20 01 4A 00 02 B3 25 50 09 08 00 45 00  ...-.J...P...X.
0x0010: 00 3C 24 FA 00 00 80 01 EC 80 0A 00 0A 71 0A 00  <$.-----q..
0x0020: 0A D5 08 00 28 5C 02 00 23 00 61 62 63 64 65 66  ....(\..#.abedef
0x0030: 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
0x0040: 77 6A 62 63 64 65 66 67 68 69                      wabedefghi

+-----+
```

- A. Linux Ping Reply
- B. Windows 2000 Ping Reply
- C. Windows NT 4.0 Ping Request
- D. Linux Ping Request
- E. Windows 2000 Ping Request

Answer: E

QUESTION: 226

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```

10/28-01:52:16.879681 0:80:9:7E:ES:ES -> 0:DO:9:7F:C:9S ctype:0x800 len:0x3E
10.0.10.237:1674 -> 10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5277 Iplen:20 Dglen:40
*****S* Seq: 0x3F2FE2CC Ack: 0x0 Win: 0x4000 Toplen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====

10/28-01:52:16.899652 0:80:9:7E:ES:ES -> 0:2:D3:2D:1:4A type:0x800 len:0x3E
10.0.10.237:1675 -> 10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5278 Iplen:20 Dglen:40
*****S* Seq: 0x3F30DB1F Ack: 0x0 Win: 0x4000 Toplen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====

10/28-01:52:17.019680 0:80:9:7E:ES:ES -> 0:DO:9:7E:F9:DB type:0x800 len:0x3E
10.0.10.237:1675 -> 10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5279 Iplen:20 Dglen:40
*****S* Seq: 0x3F31B3AE Ack: 0x0 Win: 0x4000 Toplen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====

10/28-01:52:17.039669 0:80:9:7E:ES:ES -> 0:DO:9:6B:87:2C type:0x800 len:0x3E
10.0.10.237:1678 -> 10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5282 Iplen:20 Dglen:40
*****S* Seq: 0x3F332EC2 Ack: 0x0 Win: 0x4000 Toplen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====

10/28-01:52:17.079621 0:80:9:7E:ES:ES -> 0:DO:9:69:48:E9 type:0x800 len:0x3E
10.0.10.237:1679 -> 10.0.10.235:31337 TCP TTL:128 TOS:0x0 ID:5283 Iplen:20 Dglen:40
*****S* Seq: 0x3F3436FA Ack: 0x0 Win: 0x4000 Toplen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====

```

- A. Trojan Horse Scan
- B. Back Orifice Scan
- C. NetBus Scan
- D. Port Scan
- E. Ping Sweep

Answer: B

QUESTION: 227

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```

10/28-17:26:06.234410 0:DO:9:7E:F9:DB -> 0:2:D3:2D:1:4A type:0x000 len:0x62
10.0.10.233 -> 10.0.10.235 ICMP TTL:64 TOS:0x0 ID:0 Iplen:20 Dglen:84 DF
Type:8 Code:0 ID:2116 Seq:0 ECHO
F1 9B DC 3E E7 13 02 00 0B 09 0A 0B 0C 0D 0E 0F ...f.....
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F .....
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#$%&'()*+,-./
30 31 32 33 34 35 36 37 01234567

=====

10/28-17:26:07.231774 0:DO:9:7E:F9:DB -> 0:2:D3:2D:1:4A type:0x000 len:0x62
10.0.10.233 -> 10.0.10.235 ICMP TTL:64 TOS:0x0 ID:0 Iplen:20 Dglen:84 DF
Type:8 Code:0 ID:2116 Seq:1 ECHO
F2 9B DC 3E 6D 0A 02 0D 0B 09 0A 0B 0C 0D 0E 0F ...fB.....
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F .....
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F !"#$%&'()*+,-./
30 31 32 33 34 35 36 37 01234567

```

- A. Linux Ping Response
- B. Linux Ping Request
- C. Windows 2000 Ping Request
- D. Windows 2000 Ping Response
- E. Windows NT 4.0 Ping Request

Answer: B

QUESTION: 228

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```

10/28-19:09:07.307953 0:00:0:7E:F9:DB -> 0:2:33:2D:1:4A type:0x000 len:0x0C
10.0.10.236:57228 -> 10.0.10.235:1 TCP TTL:44 TOS:0x0 ID:24652 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+
10/28-19:09:07.320917 0:00:0:7E:F9:DB -> 0:2:33:2D:1:4A type:0x000 len:0x0C
10.0.10.236:57228 -> 10.0.10.235:2 TCP TTL:44 TOS:0x0 ID:52330 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+
10/28-19:09:07.377933 0:00:0:7E:F9:DB -> 0:2:33:2D:1:4A type:0x000 len:0x0C
10.0.10.236:57228 -> 10.0.10.235:3 TCP TTL:44 TOS:0x0 ID:10807 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+
10/28-19:09:07.328200 0:00:0:7E:F9:DB -> 0:2:33:2D:1:4A type:0x000 len:0x0C
10.0.10.236:57228 -> 10.0.10.235:4 TCP TTL:44 TOS:0x0 ID:40192 IpLen:20 DgmLen:40
***** Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20

+-----+

```

- A. Nmap SYN/FIN Scan
- B. Nmap ACK Scan
- C. Nmap NULL Scan
- D. Nmap XMAS Scan
- E. Nmap SYN Scan

Answer: C

QUESTION: 229

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?


```
10/28-16:05:45.378701 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:1 TCP TTL:57 TOS:0x0 ID:52554 EplLen:20 DgmLen:40
*****S* Seq: 0x2A9F61BD Ack: 0x0 Win: 0x800 TcpLen: 20

10/28-16:05:45.922227 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:2 TCP TTL:57 TOS:0x0 ID:574117 EplLen:20 DgmLen:40
*****S* Seq: 0x2A9F61BD Ack: 0x0 Win: 0x800 TcpLen: 20

10/28-16:05:45.907360 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:3 TCP TTL:57 TOS:0x0 ID:57895 EplLen:20 DgmLen:40
*****S* Seq: 0x2A9F61BD Ack: 0x0 Win: 0x800 TcpLen: 20

10/28-16:05:45.921634 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:34145 -> 10.0.10.235:4 TCP TTL:57 TOS:0x0 ID:14182 EplLen:20 DgmLen:40
*****S* Seq: 0x2A9F61BD Ack: 0x0 Win: 0x800 TcpLen: 20
```

- A. Nmap SYN/FIN Scan
- B. Nmap NULL Scan
- C. Nmap ACK Scan
- D. Nmap SYN Scan
- E. Nmap XMAS Scan

Answer: D

QUESTION: 230

Recently, you have seen an increase in intrusion attempts and in network traffic. You decide to use Snort to run a packet capture and analyze the traffic that is present. Looking at the example, what type of traffic did Snort capture in this log file?

```
10/28-16:17:37.437225 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:40465 -> 10.0.10.235:1 TCP TTL:40 TOS:0x0 ID:4473 EplLen:20 DgmLen:40
**F*P**F Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0

10/28-16:17:37.434667 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:40465 -> 10.0.10.235:2 TCP TTL:40 TOS:0x0 ID:28435 EplLen:20 DgmLen:40
**F*P**F Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0

10/28-16:17:37.434443 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:40465 -> 10.0.10.235:3 TCP TTL:40 TOS:0x0 ID:21003 EplLen:20 DgmLen:40
**F*P**F Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0

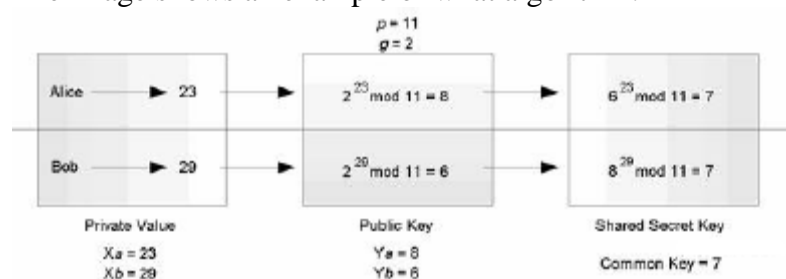
10/28-16:17:37.353755 0:10:9:7E:F9:D8 -> 0:2:B3:2D:1:4A type:0x000 len:0x3C
10.0.10.236:40465 -> 10.0.10.235:4 TCP TTL:40 TOS:0x0 ID:45668 EplLen:20 DgmLen:40
**F*P**F Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20 UrgPtr: 0x0
```

- A. Nmap XMAS Scan
- B. Nmap NULL Scan
- C. Nmap SYN Scan
- D. Nmap ACK Scan
- E. Nmap SYN/FIN Scan

Answer: A

QUESTION: 231

The image shows an example of what algorithm?

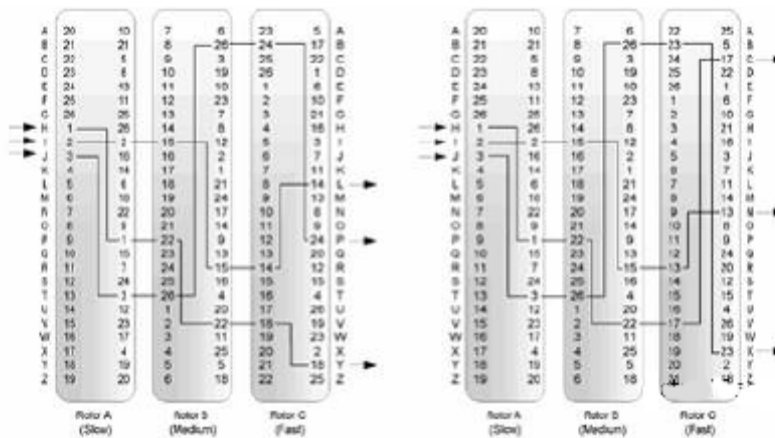


- A. DES
- B. Triple-DES
- C. Blowfish
- D. DH
- E. IDEA

Answer: D

QUESTION: 232

What type of cryptographic system is represented in this image?



- A. Caesar
- B. Vingre
- C. Polybius
- D. Purple
- E. Enigma

Answer: E

QUESTION: 233

What classic cipher is shown in this image?

- A. Feistel Cipher
- B. Caesar Cipher
- C. Vingre Cipher
- D. Polybius Cipher
- E. Enigma Cipher

Answer: A



SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>
Kill your exam at First Attempt....Guaranteed!