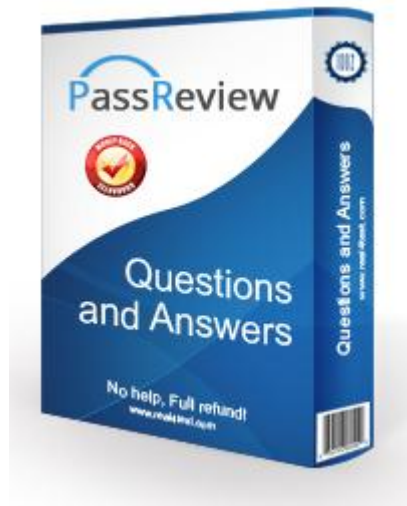


# PassReview



<http://www.passreview.com>

PassReview - IT Certification Exams Pass Review

**Exam** : **GSEC**

**Title** : **GIAC Security Essentials  
Certification**

**Vendor** : **GIAC**

**Version** : **DEMO**

**NO.1** Which of the following applications would be BEST implemented with UDP instead of TCP?

- A. A multicast streaming application.
- B. A file transfer application.
- C. A DNS zone transfer.
- D. A web browser.

**Answer:** A

**NO.2** What is a limitation of deploying HIPS on a workstation?

- A. Requires an HIDS to Identify an attack
- B. Runs as a non-privileged user
- C. Requires more frequent system patching
- D. Restricted support for custom applications

**Answer:** D

**NO.3** When using Pretty Good Privacy (PGP) to digitally sign a message, the signature is created in a two-step process. First, the message to be signed is submitted to PGP's cryptographic hash algorithm. What is one of the hash algorithms used by PGP for this process?

- A. Blowfish
- B. SHA-1
- C. DES
- D. Cast

**Answer:** B

**NO.4** In PKI, when someone wants to verify that the certificate is valid, what do they use to decrypt the signature?

- A. X.509 certificate CA's private key
- B. CA's public key
- C. Receiver's digital signature
- D. Secret passphrase

**Answer:** B

**NO.5** Which Linux command could a systems administrator use to determine if an attacker had opened up a new listening port on her system?

- A. vrnstat
- B. nfsstat
- C. netstat
- D. netreport
- E. ps

**Answer:** C

**NO.6** What is a recommended defense against SQL injection, OS injection, and buffer overflows?

- A. Use a secure protocol like HTTPS
- B. Validate user input

- C. Use stored procedures
- D. Put in an application layer

**Answer:** B

**NO.7** In preparation to do a vulnerability scan against your company's systems. You've taken the steps below:

You've notified users that there will be a system test.

You've prioritized and selected your targets and subnets.

You've configured the system to do a deep scan.

You have a member of your team on call to answer questions.

Which of the following is a necessary step to take prior to starting the scan?

- A. Clear relevant system log files.
- B. Scheduling the scan to run before OS updates.
- C. Getting permission to run the scan.
- D. Placing the incident response team on call.

**Answer:** C

**NO.8** Use sudo to launch Snort with the, /etc /snort /snort.conf file In full mode to generate alerts based on incoming traffic to echo. What is the source IP address of the traffic triggering an alert with a destination port of 156?

Note: Snort is configured to exit after it evaluates 50 packets.

A blue rectangular button with rounded corners and a white border. The text "View VM" is written in white, sans-serif font, centered within the button.

```

110 client (Footprint)
111 client (Footprint)
113 client (Footprint)
119 client (Footprint)
135 client (Footprint)
136 client (Footprint)
137 client (Footprint)
139 client (Footprint)
143 client (Footprint)
161 client (Footprint)
additional ports configured but not printed.
Stream UDP Policy config:
Timeout: 180 seconds
Portscan Detection Config:
Detect Protocols: TCP UDP ICMP IP
Detect Scan Type: portscan portsweep decoy_portscan distributed_portscan
Sensitivity Level: Low
Memcap (in bytes): 10000000
Number of Nodes: 19569
httpInspect Config:
GLOBAL CONFIG
Detect Proxy Usage: NO
IIS Unicode Map Filename: /etc/snort/unicode.map
IIS Unicode Map Codepage: 1252
Memcap used for logging URI and Hostname: 150994944
Max Gzip Memory: 104857600
Max Gzip Sessions: 201649
Gzip Compress Depth: 65535
Gzip Decompress Depth: 65535
DEFAULT SERVER CONFIG:
Server profile: All

Continue to check encrypted data: YES
TELNET CONFIG:
Ports: 23
Are You There Threshold: 20
Normalize: YES
Detect Anomalies: YES
FTP CONFIG:
FTP Server: default
Ports (PAF): 21 2100 3535
Check for Telnet Cnds: YES alert: YES
Ignore Telnet Cnd Operations: YES alert: YES
Ignore open data channels: NO
FTP Client: default
Check for Bounce Attacks: YES alert: YES
Check for Telnet Cnds: YES alert: YES
Ignore Telnet Cnd Operations: YES alert: YES
Max Response Length: 256
SMTP Config:
Ports: 25 465 587 691
Inspection Type: Stateful
Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESNL ESOM ETRN EVFY EXPN
HELO HELP IDENT MAIL NOOP ONEX QUEUE RCPT RSET SAHL SEND STARTTLS SOML TICK
TIME TURN TURNV X-EXPS XADR XAUTH XCIA XEXCHS XGEN XLICENSE X-LINK2
STATE XQUE XSTA XTRN XUSR CHUNKING X-ADAT X-DRCP X-ERCP X-EXCHSD
POP Memcap: 838860
MIME Max Mem: 838860
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted-Printable Decoding: Enabled
Quoted-Printable Decoding Depth: Unlimited
Unix-to-Unix Decoding: Enabled
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
Ibus config:
Ports:
502
I3 config:
Memcap: 262144
Check Link-Layer CRCs: ENABLED
Ports:
20000

Number of patterns truncated to 20 bytes: 0 ]
ap DAQ configured to passive.
quitting network traffic from "eth0".
load thread starting...
load thread started, thread 0x7fc399f79700 (1880)
coding Ethernet

--= Initialization Complete =--

o'')- -> Snort! <-
****
Version 2.9.7.0 GRE (Build 149)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
  UDP6: 0 ( 0.000%)
  TCP6: 0 ( 0.000%)
  Teredo: 0 ( 0.000%)
  ICMP-IP: 0 ( 0.000%)
  IP4/IP4: 0 ( 0.000%)
  IP4/IP6: 0 ( 0.000%)
  IP6/IP4: 0 ( 0.000%)
  IP6/IP6: 0 ( 0.000%)
  GRE: 0 ( 0.000%)
  GRE Eth: 0 ( 0.000%)
  GRE VLAN: 0 ( 0.000%)
  GRE IP4: 0 ( 0.000%)
  GRE IP6: 0 ( 0.000%)
  GRE IP6 Ext: 0 ( 0.000%)
  GRE PPTP: 0 ( 0.000%)
  GRE ARP: 0 ( 0.000%)
  GRE IPX: 0 ( 0.000%)
  GRE Loop: 0 ( 0.000%)
  MPLS: 0 ( 0.000%)
  ARP: 10 (20.000%)
  IPX: 0 ( 0.000%)
  Eth Loop: 0 ( 0.000%)
  Eth Disc: 0 ( 0.000%)
  IP4 Disc: 0 ( 0.000%)
****
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SDP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SFTP Version 1.1 <Build 9>
Preprocessor Object: SF_DCE/RPC2 Version 1.0 <Build 3>

Commencing packet processing (pid=1875)

```

- A. 10.11.10.11
- B. 10.72.101.210

- C. 192.168..30
- D. 10.10.28.19
- E. 10.11.12.13
- F. 10.10.199.146
- G. 192.168.87.68
- H. 10.10.10.66
- I. 10.10.201.150
- J. 10.12.10.112

**Answer:** I

**NO.9** Which of the following is the FIRST step in performing an Operational Security (OP5EC) Vulnerabilities Assessment?

- A. Assess the threat
- B. Conduct risk versus benefit analysis
- C. Implement appropriate countermeasures
- D. Assess vulnerabilities of critical information to the threat
- E. Identification of critical information

**Answer:** E

**NO.10** Why would someone use port 80 for deployment of unauthorized services?

- A. Google will detect the service listing on port 80 and post a link, so that people all over the world will surf to the rogue service.
- B. If someone were to randomly browse to the rogue port 80 service they could be compromised.
- C. This is a technique commonly used to perform a denial of service on the local web server.
- D. HTTP traffic is usually allowed outbound to port 80 through the firewall in most environments.

**Answer:** D

**NO.11** When file integrity checking is enabled, what feature is used to determine if a monitored file has been modified?

- A. One-way hash
- B. File change notifications in the Application Event Log
- C. Last modified date
- D. file size

**Answer:** A

**NO.12** What is log, pre-processing?

- A. Removing known bad log event entries
- B. Moving log entries of unknown status to an analyst's queue
- C. Converting logs from one format to another
- D. Transferring logs to short-term storage

**Answer:** C

**NO.13** SSL session keys are available in which of the following lengths?

- A. 40-bit and 64-bit.
- B. 128-bit and 1,024-bit.
- C. 64-bit and 128-bit.
- D. 40-bit and 128-bit.

**Answer:** D

**NO.14** You are doing some analysis of malware on a Unix computer in a closed test network. The IP address of the computer is 192.168.1.120. From a packet capture, you see the malware is attempting to do a DNS query for a server called iamabadservr.com so that it can connect to it. There is no DNS server on the test network to do name resolution. You have another computer, whose IP is 192.168.1.115, available on the test network that you would like for the malware connect to it instead. How do you get the malware to connect to that computer on the test network?

- A. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.120 iamabadservr iamabadservr.com
- B. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.115 iamabadservr iamabadservr.com
- C. You modify the HOSTS file on the Unix computer your malware is running on and add an entry that reads: 192.168.1.115 iamabadservriamabadservr.com
- D. You modify the HOSTS file on the computer you want the malware to connect to and add an entry that reads: 192.168.1.120 iamabadservr iamabadservr.com

**Answer:** C

**NO.15** What is a characteristic of iOS security?

- A. Less restrictive architecture than macOS
- B. Most security features are user configurable
- C. Forbids mobile operator (MO) software
- D. Flaw disclosures are sent to the Open Handset Alliance (OHA)

**Answer:** B

**NO.16** Your system has been infected by malware. Upon investigation, you discover that the malware propagated primarily via email. The malware attacked known vulnerabilities for which patches are available, but due to problems with your configuration management system you have no way to know which systems have been patched and which haven't, slowing your progress in patching your network. Of the following, which solution would you use to protect against this propagation vector?

- A. Separate the email server from the trusted portions of the network
- B. Install a firewall between the email server and the Internet
- C. Scan and block suspect email attachments at the email server
- D. Encrypt the emails on the server

**Answer:** C

**NO.17** Training an organization on possible phishing attacks would be included under which NIST Framework Core guidelines?

- A. Protect

- B. Identify
- C. Respond
- D. Detect

**Answer:** A

**NO.18** Which Defense-in-Depth principle starts with an awareness of the value of each section of information within an organization?

- A. Perimeter layering
- B. Uniform information protection
- C. General information protection
- D. Information centric defense

**Answer:** D

**NO.19** On an NTFS file system, what will happen when a conflict exists between Allow and Deny permissions?

- A. The resolution depends on the user's machine rights.
- B. Allow permission will take precedence over the Deny permission.
- C. Deny permission will take precedence over the Allow permission.
- D. The resolution depends on the groups that the user belongs to.

**Answer:** C

**NO.20** Which of the following should be implemented to protect an organization from spam?

- A. Auditing
- B. E-mail filtering
- C. Packet filtering
- D. System hardening

**Answer:** B

**NO.21** Validating which vulnerabilities in a network environment are able to be exploited by an attacker is called what?

- A. Perimeter assessment
- B. Vulnerability scanning
- C. Penetration testing
- D. Anomaly detection

**Answer:** B

**NO.22** What Windows log should be checked to troubleshoot a Windows service that is failing to start?

- A. Security
- B. Application
- C. Setup
- D. System

**Answer:** D

**NO.23** Which of the following services resolves host name to IP Address?

- A. DHCP
- B. DNS
- C. Computer Browser
- D. WINS

**Answer:** B

**NO.24** You work as a Network Administrator for McNeil Inc. You are installing an application. You want to view the log file whenever a new entry is added to the /var/log/messages log file. Which of the following commands will you use to accomplish this?

- A. TAIL -show /var/log/messages
- B. TAIL -50 /var/log/messages
- C. TAIL -f /var/log/messages
- D. TAIL -view /var/log/messages

**Answer:** C

**NO.25** A folder D:\Files\Marketing has the following NTFS permissions:

- \* Administrators: Full Control
- \* Marketing: Change and Authenticated
- \* Users: Read

It has been shared on the server as "MARKETING", with the following share permissions:

- \* Full Control share permissions for the Marketing group

Which of the following effective permissions apply if a user from the Sales group accesses the \\FILESERVER\MARKETING shared folder?

- A. Read
- B. No access
- C. Full Control
- D. Change

**Answer:** A

**NO.26** A simple cryptosystem that keeps the same letters and shuffles the order is an example of what?

- A. Substitution
- B. Monolithic
- C. Rotation
- D. Permutation

**Answer:** D

**NO.27** An organization keeps its intellectual property in a database. Protection of the data is assigned to one system administrator who marks the data, and monitors for this intellectual property leaving the network. Which defense-in-depth principle does this describe?

- A. Protected Enclave
- B. Threat-Vector Analysis

- C. Uniform Protection
- D. Information Centric

**Answer:** D

**NO.28** Which Linux file lists every process that starts at boot time?

- A. netsrv
- B. initd
- C. inittab
- D. inetd

**Answer:** C

**NO.29** Which of the following quantifies the effects of a potential disaster over a period of time?

- A. Disaster Recovery Planning
- B. Risk Assessment
- C. Business Impact Analysis
- D. Lessons Learned

**Answer:** C

**NO.30** Which of the following statements about buffer overflow is true?

- A. It manages security credentials and public keys for message encryption.
- B. It is a condition in which an application receives more data than it is configured to accept.
- C. It is a collection of files used by Microsoft for software updates released between major service pack releases.
- D. It is a false warning about a virus.

**Answer:** B