DUMPSARENA

Certified Network Security Practitioner ()

The SecOps Group CNSP

Version Demo

Total Demo Questions: 7

Total Premium Questions: 78

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

If you find the 111/TCP port open on a Unix system, what is the next logical step to take?

A. Run "rpcinfo -p " to enumerate the RPC services.

B. Telnet to the port to look for a banner.

C. Telnet to the port, send "GET / HTTP/1.0" and gather information from the response.

D. None of the above.

ANSWER: A

Explanation:

Run `rpcinfo -p <hostname>` to enumerate the RPC services. TCP port 111 is conventionally used by the RPC bind service (also called `rpcbind` or portmapper). Its role is to maintain a registry of Remote Procedure Call programs and identify the transport ports on which those programs are available. Finding this service exposed is therefore a strong indication that the next useful reconnaissance step is to query the RPC registry rather than treat the port as a generic interactive or web service.

The `rpcinfo -p` command requests the target's portmapper program list and reports registered RPC program numbers, versions, protocols, and mapped ports. This can reveal services such as NFS, NIS, mountd, or status-monitoring components and provides the information needed to perform focused, authorized enumeration of the services actually available. The RPC documentation describes `rpcinfo -p` as displaying the programs registered with the portmapper, while the Nmap service reference identifies 111 as the standard port for RPC bind/portmapper. Use the hostname or IP address of the Unix host and conduct this activity only within the defined assessment scope. References: rpcinfo(8) manual page; Nmap RPC scanning documentation.

QUESTION NO: 2

Which of the following represents a valid Windows Registry key?

A. HKEY_LOCAL_MACHINE

B. HKEY_INTERNAL_CONFIG

C. HKEY_ROOT_CLASSES

D. HKEY_LOCAL_USER

ANSWER: A

Explanation:

HKEY_LOCAL_MACHINE is a valid predefined Windows Registry root key, commonly abbreviated as HKLM. It stores configuration data that applies to the computer as a whole rather than to one particular signed-in user. Its contents include system-wide hardware information, installed software configuration, Windows services, drivers, security policies, and operating-system settings. Because these values can affect every user and the overall security posture of a device, registry analysis and monitoring frequently examine HKLM locations during system administration, incident response, and security assessments. Windows presents HKLM as one of its standard predefined registry handles, and many administrative tasks use paths under it, such as `HKEY_LOCAL_MACHINE\SOFTWARE` and `HKEY_LOCAL_MACHINE\SYSTEM`. Microsoft documents the predefined registry keys and describes HKEY_LOCAL_MACHINE as containing configuration information local to the computer. For further technical details, see Microsoft's Predefined Registry Keys documentation and Microsoft's Registry Hives documentation.

QUESTION NO: 3

Which of the following commands will work on a Microsoft operating system to add a new domain admin user?

A. net group "Domain Admins" John /add /domain

B. net user John "Domain Admins" /add /domain

C. net user John /add /domain /admin

D. net group "Administrator" John /add

ANSWER: A

Explanation:

The command `net group "Domain Admins" John /add /domain` is the appropriate legacy Windows command for adding the existing domain account `John` to the Active Directory domain global group named `Domain Admins`. The `net group` command manages domain groups; specifying the group name first, followed by the user name and `/add`, requests that the user be added as a member. The `/domain` switch directs the operation to the domain rather than the computer's local Security Accounts Manager database. Membership in Domain Admins grants highly privileged administrative access throughout an Active Directory domain, so the command must be run by an account with authority to modify that group, and the specified user must already exist in the domain. Microsoft documents the `net group` syntax as accepting member names with `/add` and supporting the `/domain` switch for operations on the primary domain controller. In modern administrative workflows, equivalent membership changes can also be performed through Active Directory Users and Computers or PowerShell, but this command remains valid for the stated purpose. See Microsoft's net group command reference and Microsoft's Active Directory security groups overview.

QUESTION NO: 4

Which of the following services use TCP protocol?

A. SNMP

B. NTP

C. HTTP

D. IKE

ANSWER: C

Explanation:

HTTP is the correct answer because traditional HTTP web traffic is carried over TCP. TCP provides a reliable, connection-oriented byte stream: it establishes a session between client and server, acknowledges received data, retransmits data when necessary, and preserves the order of the delivered stream. Those characteristics support dependable transfer of web resources such as HTML documents, style sheets, scripts, and images. In the conventional HTTP deployment model, web servers listen on TCP port 80 for HTTP, while encrypted HTTP traffic, commonly called HTTPS, is typically carried over TCP port 443 with TLS layered above TCP. This is the protocol-and-port association generally expected when identifying services during network security operations, firewall-rule review, packet analysis, and service enumeration. The Internet Assigned Numbers Authority lists HTTP as assigned to port 80 over TCP, and the current HTTP specification describes HTTP/1.1 messaging over a reliable transport such as TCP. Modern HTTP can also be deployed through HTTP/3 over QUIC, which uses UDP; however, that newer transport does not change the standard foundational exam association of HTTP with TCP. See the IANA Service Name and Port Number Registry and RFC 9112: HTTP/1.1.

QUESTION NO: 5

How many usable TCP/UDP ports are there?

A. 65536

B. 65535

C. 63535

D. 65335

ANSWER: B

Explanation:

65535 is the correct practical count of usable TCP or UDP port numbers. Both TCP and UDP encode source and destination ports in 16-bit fields, giving a numeric namespace from 0 through 65535. Although this represents 65,536 possible numeric values, port 0 is reserved and is not a normal service port to which an application should bind for network communication. Consequently, the standard usable range is ports 1–65535 inclusive, which contains 65,535 ports.

Port numbers identify the application endpoint within a host and transport protocol. TCP and UDP maintain separate port spaces, so a service may use the same numeric port under each protocol where appropriate; for example, a TCP listener and a UDP listener can both use the same port number. For operational security work, the 1–65535 range is the conventional scope when discussing service exposure, firewall rules, enumeration, and port scanning. IANA's registry also treats port 0 as reserved, reinforcing the distinction between the full 16-bit numerical range and ports available for ordinary application services.

See the TCP specification in RFC 9293 and IANA's Service Name and Transport Protocol Port Number Registry.

QUESTION NO: 6

Which built-in Windows utility can be used to verify the validity of a Kerberos ticket?

A. Klist

B. Kerbtray

C. Netsh

D. Kerberos Manager

ANSWER: A

Explanation:

Klist is the built-in Windows command-line utility used to inspect Kerberos tickets held in a user's credential cache. Running `klist` displays cached ticket-granting tickets and service tickets, including the client and service principals, encryption type, ticket flags, start time, end time, and renewal time. These fields allow an administrator or security practitioner to establish whether a ticket is currently within its valid lifetime, whether it can be renewed, and which service identity it applies to. The command is useful when investigating Active Directory authentication behavior, diagnosing access failures, or validating the Kerberos context under which a process or user is operating. Windows also provides related Klist operations, such as `klist purge` to clear cached tickets and commands for viewing or managing tickets in specific logon sessions. Because it is included with supported Windows client and server systems, Klist is the standard native utility for examining Kerberos ticket status. Microsoft documents Klist and its available commands at Klist | Microsoft Learn. For background on ticket-based Kerberos authentication in Windows domains, see Kerberos authentication overview | Microsoft Learn.

QUESTION NO: 7

Which one of the following services is not a UDP-based protocol?

A. SNMP

B. NTP

C. IKE

D. SSH

ANSWER: D

Explanation:

SSH is the correct answer because Secure Shell uses the Transmission Control Protocol (TCP), conventionally on port 22. SSH provides encrypted remote administration, command execution, tunneling, and file-transfer capabilities. These activities require a reliable, ordered, connection-oriented transport so that authentication exchanges, commands, and returned data are delivered accurately and in sequence. TCP supplies these properties through connection establishment, acknowledgements, retransmission of lost segments, and flow control. The Internet Assigned Numbers Authority registers the `ssh` service on TCP port 22, which confirms the standard transport association. This transport choice is also relevant to network security operations: SSH sessions can be identified by examining TCP connections to port 22, although administrators may configure SSH to listen on an alternative TCP port. Understanding the standard port and transport protocol helps analysts build accurate firewall policies, monitoring rules, and intrusion-detection signatures. See the IANA Service Name and Transport Protocol Port Number Registry and the SSH Transport Layer Protocol specification (RFC 4253).