Question 1

When analysing a system compromised by an attacker, there are no off-network connections, but still the attacker is able to leverage the host. What LAN protocols are most likely to provide the attacker access to the system?

A. SMB
B. ICMP
C. RTP
D. ARP
E. XMPP

Answer

A. SMB

Question 2

Which protocol can be used by malware to exfiltrate data over the Internet?

A. ICMP
B. DNS
C. HTTP
D. ARP
E. ICMP, DNS and HTTP

Answer

E. ICMP, DNS and HTTP

Question 3

What is considered an indication of malware beaconing?

A. Anti Malware services stopping.
B. Systems crashing.
C. ICMP unreachable packets received from unknown hosts.
D. BITS Service restarts.
E. Regular SYN requests from unknown services.

Answer

E. Regular SYN requests from unknown services.

Question 4

You have identified a suspicious process. What command will allow you to see the owner of the process?

A. Get-Process -User '<suspicious_process>'
B. Get-Process -Name '<suspicious_process>'
C. Get-Process -Name '<suspicious_process>' -IncludeUserName
D. Get-Process -ProcessOwner '<suspicious_process>'
E. Get-Process -Name '<suspicious_process>' | Get-Property -User

Answer

C. Get-Process -Name '<suspicious_process>' -IncludeUserName

Question 5

What is an indication of DNS C2?

A. Large numbers of sub-domains.
B. Fewer ARP storms.
C. TCP Resets are no longer blocked.
D. The TTL for the record changes.
E. The who is record for the owner lacks personal information.

Answer

A. Large numbers of sub-domains.