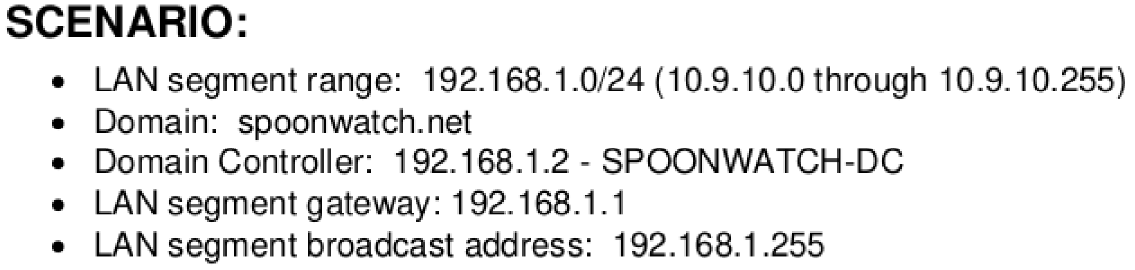
HACKERS SESSION QUESTIONS



SCENARIO:

- LAN segment range: 192.168.1.0/24 (10.9.10.0 through 10.9.10.255)
- Domain: spoonwatch.net
- Domain Controller: 192.168.1.2 - SPOONWATCH-DC
- LAN segment gateway: 192.168.1.1
- LAN segment broadcast address: 192.168.1.255

Q1) What is the host name of the infected device?

Q2) What is the MAC address of the infected device?

Q3) What is the IP address of the infected device?

Q4) What is the Windows user account that was being used at the time of compromise?

Q5) What is the IP of the malicious website accessed?

Q6) What is the SHA256 hash of 1.jpg?

Q7) Run the file command against 1.jpg, what type of file is it?

Q8) What is the name of the php file seen on the malicious site

Bonus:

Find the SHA256 hash, File size, Download location, File Type, and the real file name of every artefact found from the malicious IP.

Bonus Bonus:

OSINT!

Research the IP found, put the hashes into VirusTotal, view the files in Hex editors

Bonus Bonus Bonus:

What Malware family was the IP associated with?