5 PHASES OF ETHICAL HACKING

1. RECONNAISSANCE
2. SCANNING
3. GAINING ACCESS
4. MAINTAINING ACCESS
5. COVERING TRACKS

1. RECONNAISSANCE

JUST LIKE IN MALICIOUS HACKING, ETHICAL HACKERS START BY GATHERING INFORMATION ABOUT THE TARGET. THEY COLLECT PUBLICLY AVAILABLE DATA, SUCH AS IP ADDRESSES, DOMAIN NAMES, EMPLOYEE NAMES, AND OTHER RELEVANT INFORMATION, TO UNDERSTAND THE SCOPE OF THE ASSESSMENT.

2. SCANNING

IN THIS PHASE, ETHICAL HACKERS USE SCANNING TOOLS AND TECHNIQUES TO IDENTIFY POTENTIAL VULNERABILITIES IN THE TARGET'S SYSTEMS OR NETWORK. THEY LOOK FOR OPEN PORTS, KNOWN VULNERABILITIES, AND WEAK POINTS THAT COULD BE EXPLOITED.

3. GAINING ACCESS

ETHICAL HACKERS ATTEMPT TO EXPLOIT THE IDENTIFIED VULNERABILITIES TO GAIN ACCESS TO THE TARGET SYSTEM OR NETWORK. HOWEVER, UNLIKE MALICIOUS HACKERS, THEY DO THIS WITH THE PERMISSION AND AUTHORIZATION OF THE SYSTEM OWNER. THIS PHASE OFTEN INVOLVES TRYING TO EXPLOIT KNOWN VULNERABILITIES, WEAK PASSWORDS, OR MISCONFIGURED SYSTEMS.

4. MAINTAINING ACCESS

AFTER GAINING ACCESS, ETHICAL HACKERS WORK TO MAINTAIN THEIR PRESENCE ON THE SYSTEM OR NETWORK. THIS MAY INVOLVE CREATING BACKDOORS, ESTABLISHING USER ACCOUNTS, OR INSTALLING MONITORING TOOLS TO ASSESS THE EXTENT OF THE VULNERABILITY.

5. COVERING TRACKS

UST LIKE MALICIOUS HACKERS, ETHICAL HACKERS MAY COVER THEIR TRACKS TO SOME EXTENT TO MIMIC THE ACTIONS OF REAL ATTACKERS. HOWEVER, IN ETHICAL HACKING, THIS IS PRIMARILY DONE TO TEST THE TARGET ORGANIZATION'S DETECTION AND RESPONSE CAPABILITIES RATHER THAN TO AVOID DETECTION. AFTER COMPLETING THE ASSESSMENT, ETHICAL HACKERS DOCUMENT THEIR FINDINGS AND PROVIDE RECOMMENDATIONS FOR REMEDIATION.

TEST YOUR HACKING KNOWLEDGE!

Q: WHICH PHASE OF ETHICAL HACKING INVOLVES IDENTIFYING VULNERABILITIES?

LET US KNOW YOUR ANSWER IN THE COMMENTS!