Name:

NAU login ID (e.g. adg326 for me):

1. Which of the following involves the “I” in “CIA”?

A Protecting a website against denial of service attacks
B Ensuring that doctors at a hospital, other than those treating you, cannot read your medical history
C Using very strong cryptography to discourage the NSA
D Preventing a student from changing the timestamp on an assignment submission

2. A general description of the high-level approach of many static analysis tools is:

A Parse; build annotated CFG; walk CFG to check properties; prioritize/compress results and present to user
B Compile; compute product of CFG and specification automata; determine if language intersection is empty
C Mark variable initializations as “def”s; mark variables in expressions as “use”s; check all defs are before uses
D Check for proper coding style; check for tainted user input; check for use of deprecated functions

3. The end-goal of a security protocol is essentially to:

A Authenticate data received from an unreliable source over the Internet
B Force the use of sufficiently strong cryptography, even in embedded systems with low compute power
C Formulate a security policy that is agreed on by users of a software system
D Instill in various participants certain justfied beliefs about other participants or data

4. A major cause for a large number of security vulnerabilities over the last 30 years is:

A Open source software is not developed using a highly-disciplined waterfall approach
B Low-level systems software is usually written in C, a language in which it is easy to write vulnerable code
C Modern computer architectures make the order of operations hard for programmers to predict
D Cloud computing is inherently insecure, because you do not have physical control of the machine

5. The following tools are all widely used in finding and exploiting software vulnerabilities:

A fuzzer like afl, SQL database for SQL injection attacks, and disassembler like IDA Pro
B fuzzer like afl, debugger like gdb, and natural language processing tool to scan for suspicious comments
C fuzzer like afl, debugger like gdb, and disassembler like IDA Pro
D fuzzer like afl, debugger like gdb, and code coverage tool to check test suite quality

6. What is the MIG-in-the-middle attack?

A Using a Russian fighter jet to intimidate an employee into giving away secret data
B An example of a World War II era cryptographic system
C An example of not using good timestamps to make sure that a message is fresh
D An instance of phishing to obtain a response to a challenge-response in authentication

7. SQL injection does NOT involve which of the following:

A Defense using static analysis of taint in the flow of data
B Enforcing of quotation rules to make sure that data is parsed correctly in database queries
C Exploitation of a timing or electromagnetic side channel
D Execution of code provided by an untrusted user

8. The end goal of most attempts to exploit software bugs is:

A To introduce nondeterminism into the behavior of a software system
B To corrupt the heap and cause a crash due to a null pointer
C To decrypt encrypted email messages
D To be able to take control of the instruction pointer/program counter

9. Symbolic execution is

A The simplest kind of software vulnerability analysis
B Not considered a useful technique in security, only in performance analysis
C Static analysis of the symbol table of a compiled program
D Executing a program with some values left partly undetermined (solved for)

10. American Fuzzy Lop works by

A Injecting new faults into a software system and seeing if it can detect them
B Mutating inputs that it has found to cover interesting code paths
C Watching network traffic for passwords and plaintext data
D Using valgrind to look for memory-safety problems