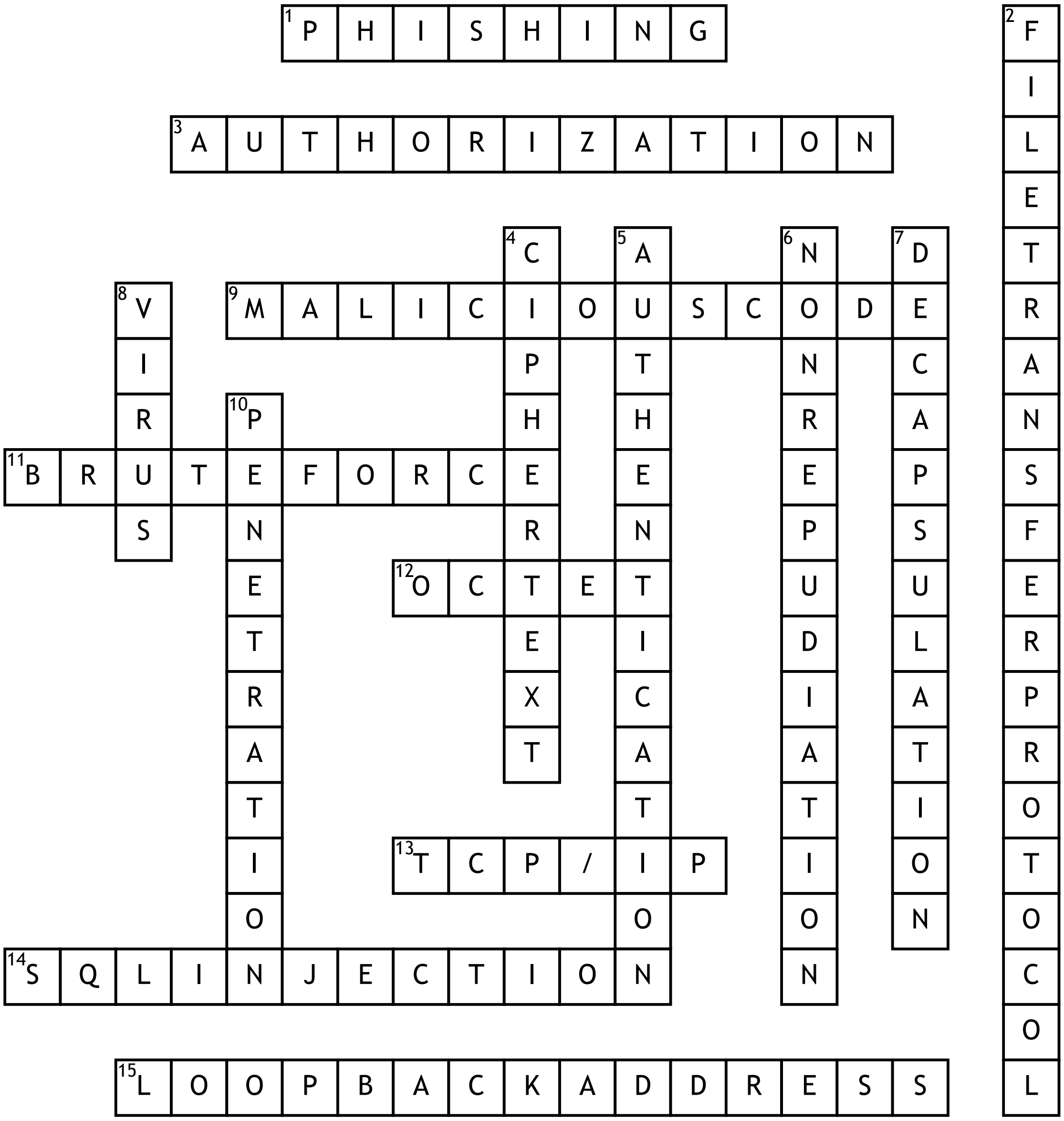
Name: ____ Date: _______

Cyber Security


1 PHISHING
2 FILETRANSFERPROTOCOL
3 AUTHORIZATION
4 CIPHERTEXT
5 AUTHENTICATION
6 NONREPUDIATION
7 DECAPSULATION
8 VIRUS
9 MALICIOUSCODE
10 PENETRATION
11 BRUTEFORCE
12 OCTET
13 TCP/IP
14 SQLINJECTION
15 LOOPBACKADDRESS

Across

1. e-mails that appear to originate from a trusted source to trick a user into entering valid credentials on a fake website

3. approval, permission, or empowerment for someone or something to do something

9. software appearing to perform a useful function but actually tricks a user into executing malicious logic (e.g. Trojan horse)

11. cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one

12. sequence of eight bits

13. basic communication language or "protocol" of the Internet

14. type of input validation attack where SQL code is inserted into application queries to manipulate the database

15. pseudo IP address that always refer back to the local host and never sent out to a network (127.0.0.1)

Down

2. TCP/IP protocol specifying the transfer of text or binary files across the network

4. encrypted form of the message being sent

5. process of confirming the correctness of the claimed identity

6. prove that a user sent a message and the message has not been altered

7. stripping one llayer's headers and passing the rest of the packet up to next higher layer

8. hidden, self-replicating section of computer software that inserts itself and becomes part of the another program

10. gaining unauthorized logical access to sensitive data by circumventing a system's protections