PREPARED FOR :
OLIVIA THOMPSON

INTERVIEW QUESTIONS

Task 4

1. WHAT IS A FIREWALL?

A FIREWALL IS ESSENTIALLY A SECURITY GUARD OR FILTER FOR A NETWORK. IT'S A SYSTEM—EITHER HARDWARE, SOFTWARE, OR BOTH—THAT CONTROLS INCOMING AND OUTGOING NETWORK TRAFFIC BASED ON A SET OF PREDETERMINED SECURITY RULES. MY JOB WAS TO DEFINE WHICH TRAFFIC GETS TO PASS AND WHICH DOESN'T, ACTING AS A CRUCIAL BARRIER BETWEEN A TRUSTED INTERNAL NETWORK AND UNTRUSTED EXTERNAL NETWORKS, LIKE THE INTERNET.

2. DIFFERENCE BETWEEN STATEFUL AND STATELESS FIREWALLS?

THIS WAS A KEY DISTINCTION I LEARNED:

STATELESS FIREWALL: THIS ONE'S SIMPLE BUT DUMB. IT EXAMINES EACH DATA PACKET INDIVIDUALLY AND MAKES A BLOCKING/ALLOWING DECISION BASED ONLY ON THE PACKET'S CURRENT INFORMATION (SOURCE/DESTINATION IP, PORT). IT HAS NO MEMORY OF PAST PACKETS OR THE CONNECTION'S CONTEXT. IT'S FAST BUT LESS SECURE.

STATEFUL FIREWALL: THIS IS THE SMARTER OPTION. IT MONITORS THE STATE OF ACTIVE CONNECTIONS. IT REMEMBERS THE CONTEXT OF THE CONNECTION—MEANING ONCE I ALLOW AN OUTGOING CONNECTION (SAY, BROWSING A WEBSITE), IT AUTOMATICALLY ALLOWS THE RETURN TRAFFIC WITHOUT NEEDING AN EXPLICIT RULE FOR THE INBOUND RESPONSE. THIS OFFERS MUCH BETTER SECURITY AND PERFORMANCE FOR DYNAMIC TRAFFIC.

3. WHAT ARE INBOUND AND OUTBOUND RULES?

THESE RULES DEFINE THE DIRECTION OF THE TRAFFIC BEING CONTROLLED:

INBOUND RULES: THESE GOVERN TRAFFIC TRYING TO ENTER MY PROTECTED NETWORK OR HOST FROM AN EXTERNAL SOURCE. FOR EXAMPLE, IF I HOST A WEB SERVER, AN INBOUND RULE MUST BE CREATED TO ALLOW TRAFFIC TO PORT 80/443. I GENERALLY AIM TO BE VERY STRICT WITH INBOUND TRAFFIC.

OUTBOUND RULES: THESE GOVERN TRAFFIC TRYING TO LEAVE MY NETWORK OR HOST AND GO TO AN EXTERNAL DESTINATION. WHILE OFTEN MORE PERMISSIVE THAN INBOUND, THESE ARE IMPORTANT FOR PREVENTING MALWARE FROM "CALLING HOME" OR CONTROLLING WHICH SERVICES USERS CAN ACCESS EXTERNALLY.

4. HOW DOES UFW SIMPLIFY FIREWALL MANAGEMENT?

UFW (UNCOMPLICATED FIREWALL), WHICH I USED ON MY LINUX SYSTEM, IS BASICALLY A USER-FRIENDLY WRAPPER FOR THE COMPLEX IPTABLES UTILITY. IT MASSIVELY SIMPLIFIES FIREWALL MANAGEMENT BY:

USING SIMPLE, INTUITIVE COMMANDS (LIKE SUDO UFW ALLOW 80) INSTEAD OF LONG, CONFUSING IPTABLES CHAINS AND FLAGS.

MAKING IT EASY TO MANAGE RULES BY SERVICE NAME (LIKE SSH OR HTTP) INSTEAD OF JUST PORT NUMBERS.

REDUCING THE CHANCE OF CONFIGURATION ERRORS THAT PLAGUE MANUAL IPTABLES MANAGEMENT.

5. WHY BLOCK PORT 23 (TELNET)?

I LEARNED THAT PORT 23 (TELNET) SHOULD BE BLOCKED BECAUSE THE TELNET PROTOCOL TRANSMITS DATA, INCLUDING LOGIN CREDENTIALS, IN PLAIN, UNENCRYPTED TEXT. THIS MEANS ANYONE "SNIFFING" THE NETWORK CAN EASILY CAPTURE USERNAMES AND PASSWORDS. WE BLOCK IT AND USE SSH (SECURE SHELL) ON PORT 22 INSTEAD, AS SSH ENCRYPTS ALL COMMUNICATIONS, MAKING IT SECURE.

6. WHAT ARE COMMON FIREWALL MISTAKES?

WHILE WORKING ON THE TASK, I IDENTIFIED A FEW EASY-TO-MAKE MISTAKES:

TOO PERMISSIVE DEFAULTS: LEAVING THE DEFAULT POLICY AS ALLOW INSTEAD OF CHANGING IT TO THE SECURE "DENY ALL, ALLOW ONLY WHAT'S NECESSARY" PRINCIPLE.

FORGETTING CONNECTION TRACKING: NOT REALIZING THAT ALL CONNECTIONS NEED BOTH AN INBOUND AND OUTBOUND COMPONENT TO WORK, ESPECIALLY WITH STATELESS FIREWALLS.

IGNORING LOGS: NOT CHECKING FIREWALL LOGS TO SEE WHAT TRAFFIC IS ACTUALLY HITTING THE SYSTEM AND IF ANY ATTEMPTS ARE BEING BLOCKED.

OPENING PORTS TEMPORARILY AND FORGETTING: OPENING A PORT FOR TESTING AND THEN FAILING TO CLOSE IT LATER, LEAVING A PERMANENT SECURITY HOLE. 😬

7. HOW DOES A FIREWALL IMPROVE NETWORK SECURITY?

A FIREWALL IS FOUNDATIONAL TO NETWORK SECURITY BECAUSE IT ACTS AS THE PRIMARY ENFORCEMENT POINT FOR MY SECURITY POLICY. IT IMPROVES SECURITY BY:

CONTROLLING ACCESS: IT ENSURES ONLY AUTHORIZED SERVICES (PORTS) AND SOURCES (IP ADDRESSES) CAN INTERACT WITH THE NETWORK.

PREVENTING INTRUSIONS: IT BLOCKS MALICIOUS TRAFFIC, LIKE PORT SCANS OR COMMON EXPLOIT ATTEMPTS, BEFORE THEY CAN REACH INTERNAL SYSTEMS.

LOGGING AND AUDITING: IT RECORDS BLOCKED AND ALLOWED TRAFFIC, PROVIDING A CRUCIAL TRAIL FOR MONITORING SECURITY THREATS AND ANALYZING NETWORK BEHAVIOR.

8. WHAT IS NAT IN FIREWALLS?

NAT (NETWORK ADDRESS TRANSLATION) IS A CRUCIAL FUNCTION PERFORMED BY MANY FIREWALLS/ROUTERS THAT ALLOWS MULTIPLE DEVICES ON A PRIVATE INTERNAL NETWORK TO SHARE A SINGLE PUBLIC IP ADDRESS WHEN COMMUNICATING WITH THE INTERNET.

WHEN AN INTERNAL DEVICE SENDS A PACKET OUT, THE FIREWALL TRANSLATES ITS PRIVATE IP AND PORT INTO THE FIREWALL'S PUBLIC IP AND A NEW PORT.

THIS NOT ONLY SAVES PUBLIC IP ADDRESSES BUT ALSO ADDS A LAYER OF SECURITY BECAUSE EXTERNAL ENTITIES ONLY SEE THE FIREWALL'S PUBLIC IP ADDRESS, EFFECTIVELY HIDING THE INTERNAL NETWORK STRUCTURE AND MAKING DIRECT ATTACKS ON INTERNAL HOSTS MUCH HARDER.