

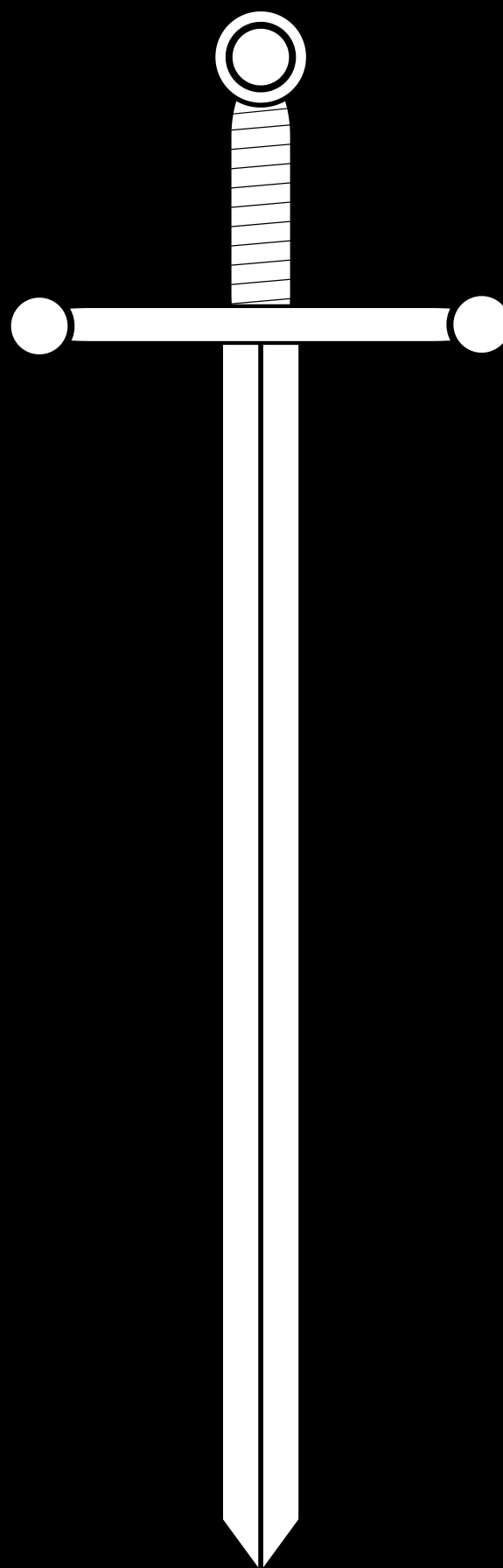


RED TEAM

GETTING TO KNOW ABOUT
ADVANTAGES AND DISADVANTAGES



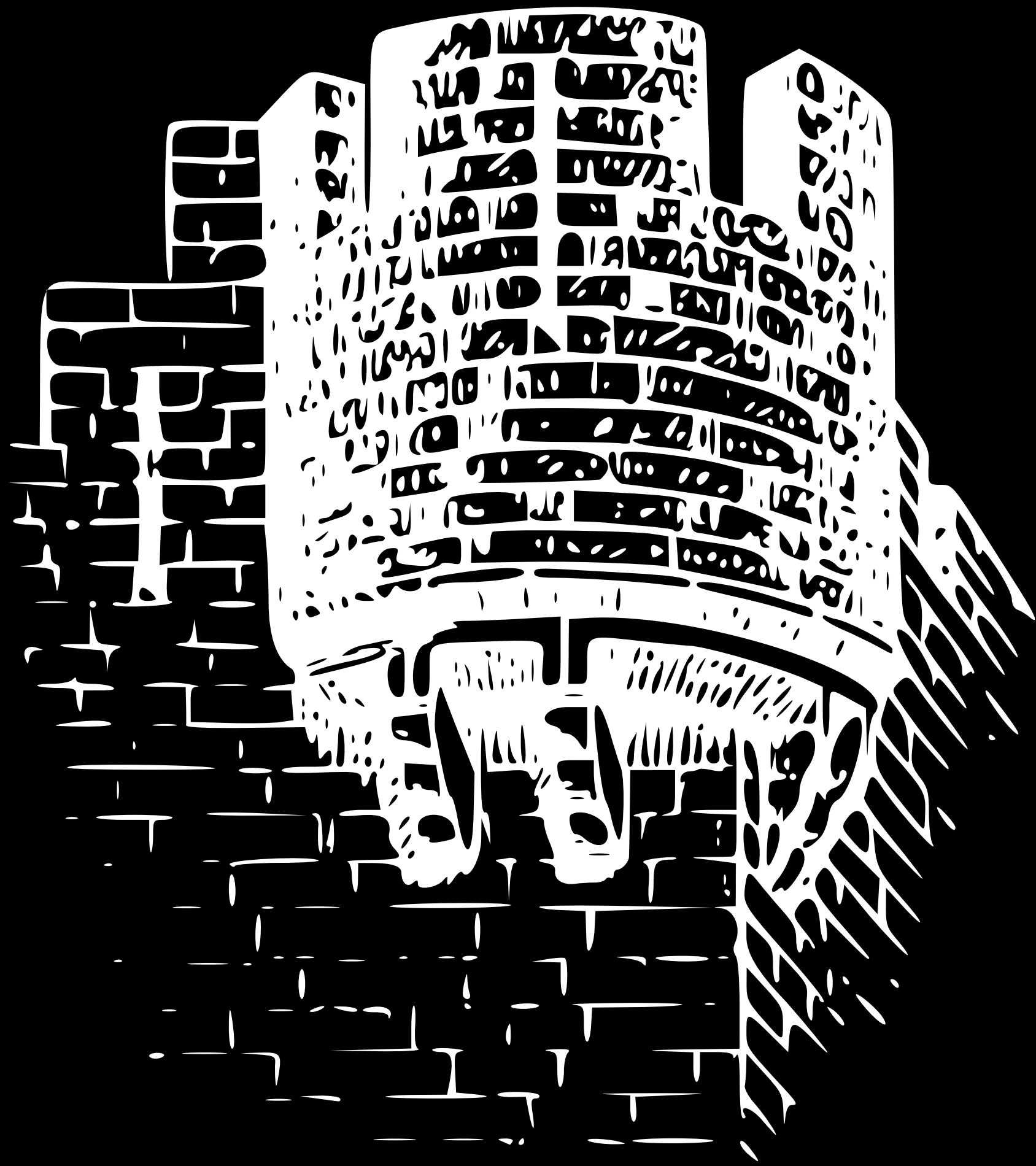
WWW.HADESS.IO



IN SIMPLE WORDS **RED TEAMING** IS AN
ETHICAL HACKING EXERCISE TO TEST YOUR
DEFENSE SYSTEM.



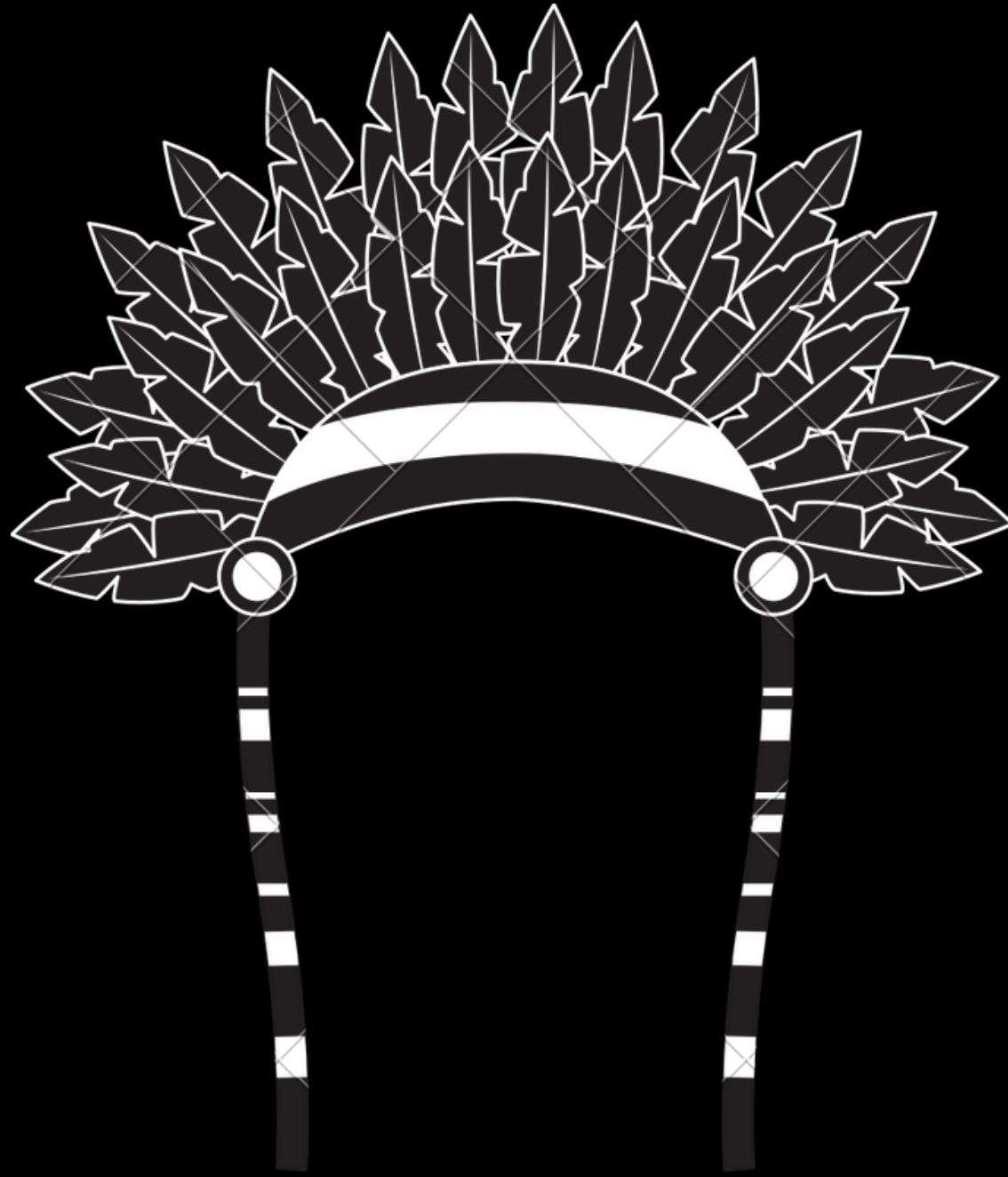
HADESS



RED TEAM IS PERFORMED BY ETHICAL
HACKERS LIKE **HADESS** WHO MIRROR THE
CONDITIONS OF A REAL-WORLD ATTACK
USING TTPS THAT IS USED BY REAL
ADVERSARIES.



HADESS

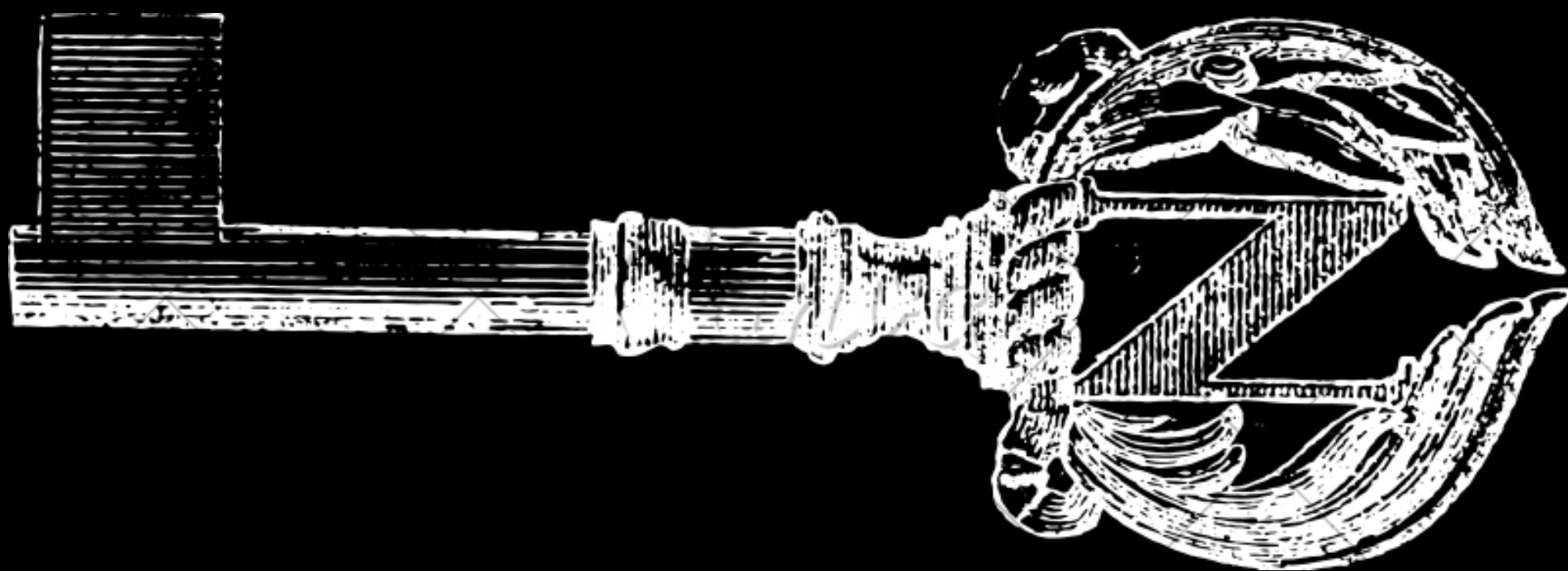


WHAT IS THE ADVANTAGE OF USING RED-TEAM

**TRADITIONAL PENETRATION TEST HAS SOME
CONSTRAINTS, SUCH AS A LIMITED
ASSESSMENT TIME WINDOW AND A
REQUIREMENT TO GET FULL COVERAGE OF
ALL IN-SCOPE SYSTEMS.**



HADESS



THE KEY IS FULL SYSTEM COVERAGE

YOU NEED TO KNOW ABOUT

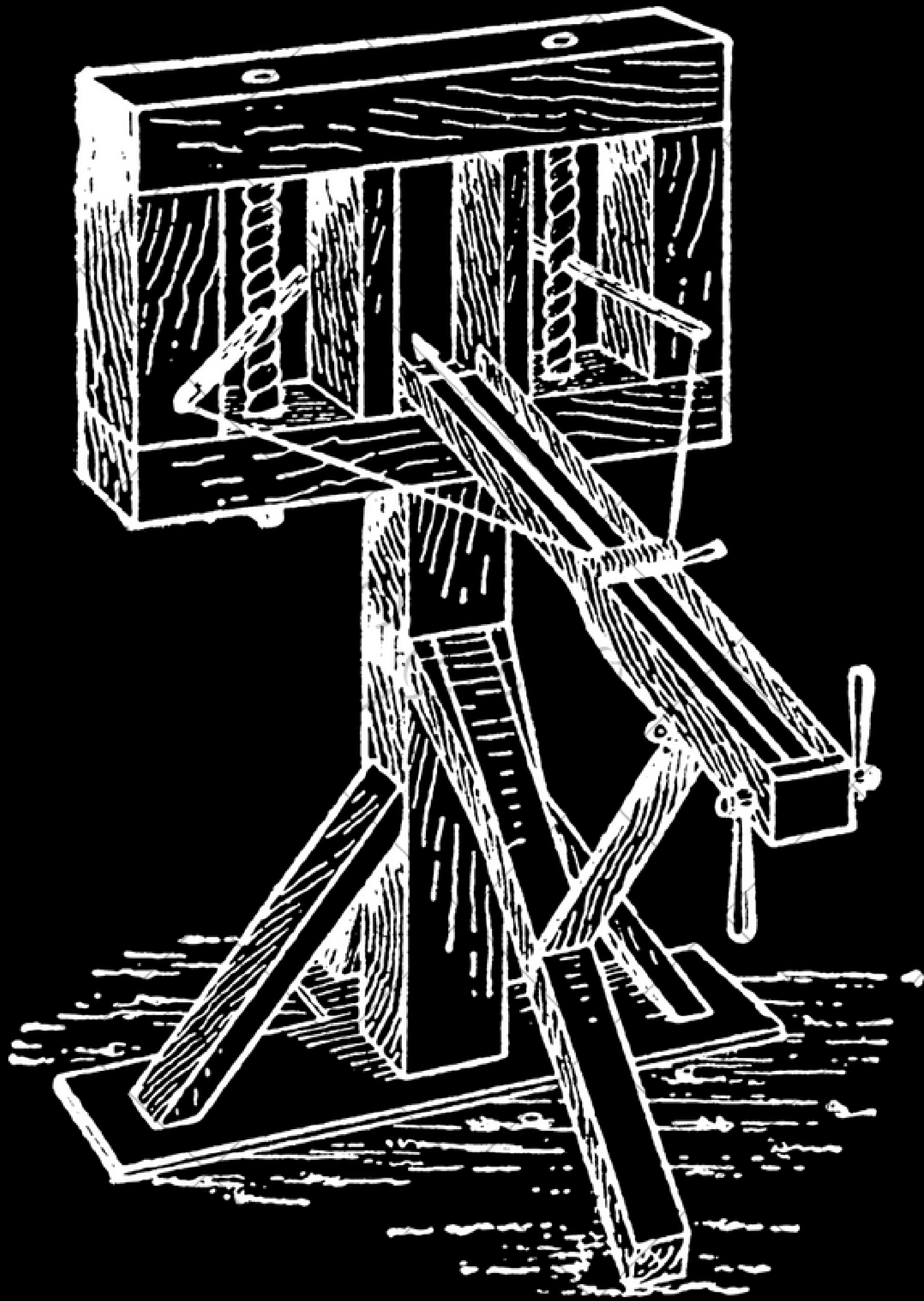
ALL YOUR RISKS, NOT JUST SOME OF THEM

AND A COMPLIANCE PERSPECTIVE

**TYPICAL PENETRATION TESTS ARE NOT A TRUE
REPRESENTATION OF AN ACTUAL ATTACK**



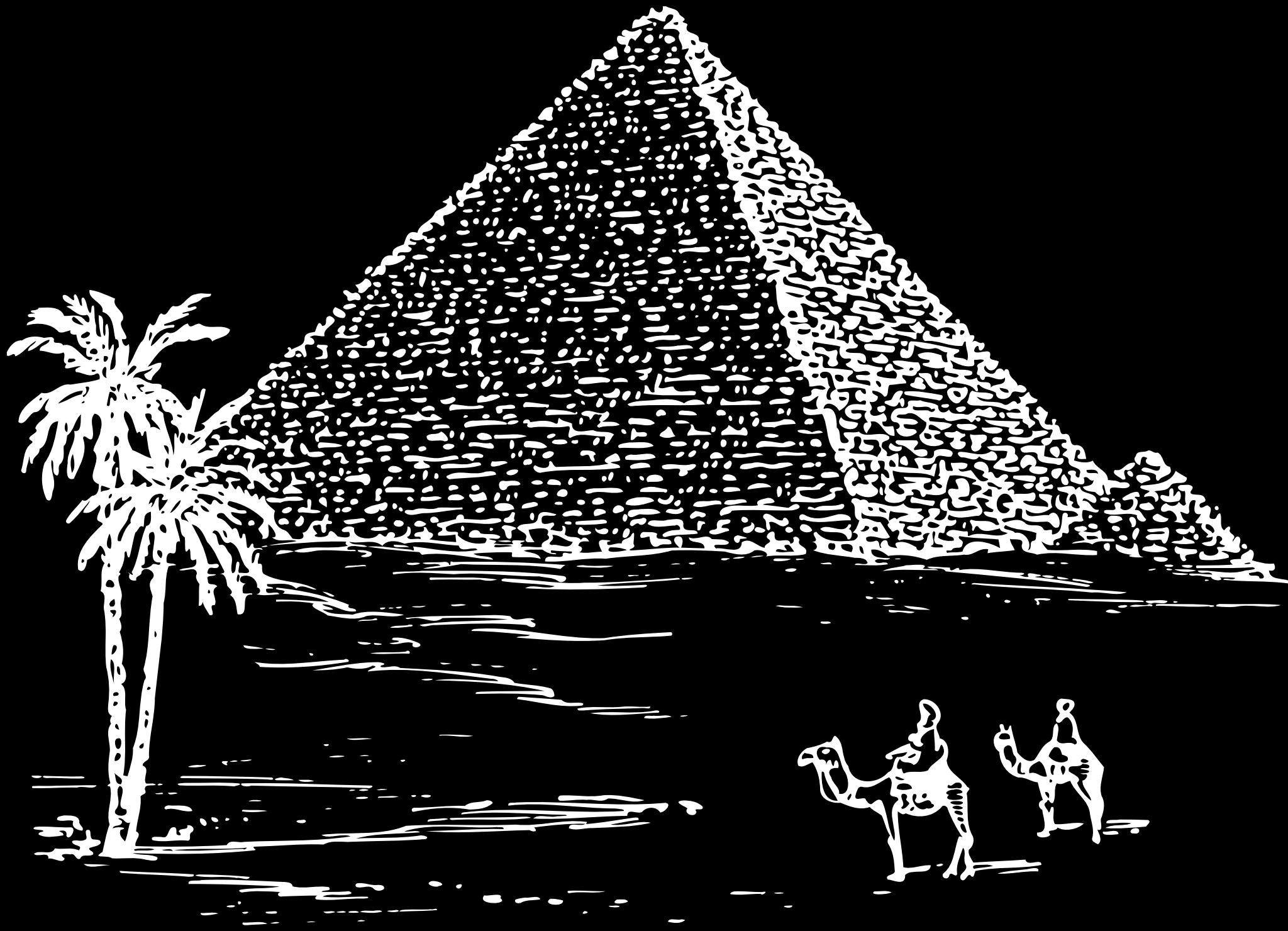
HADESS



**IN A RED TEAM OPERATION WE TRYING TO GET IN
WHILE BEING AS QUIET AS POSSIBLE TO AVOID
DETECTION, EMULATING A TRUE ATTACK.**



HADESS

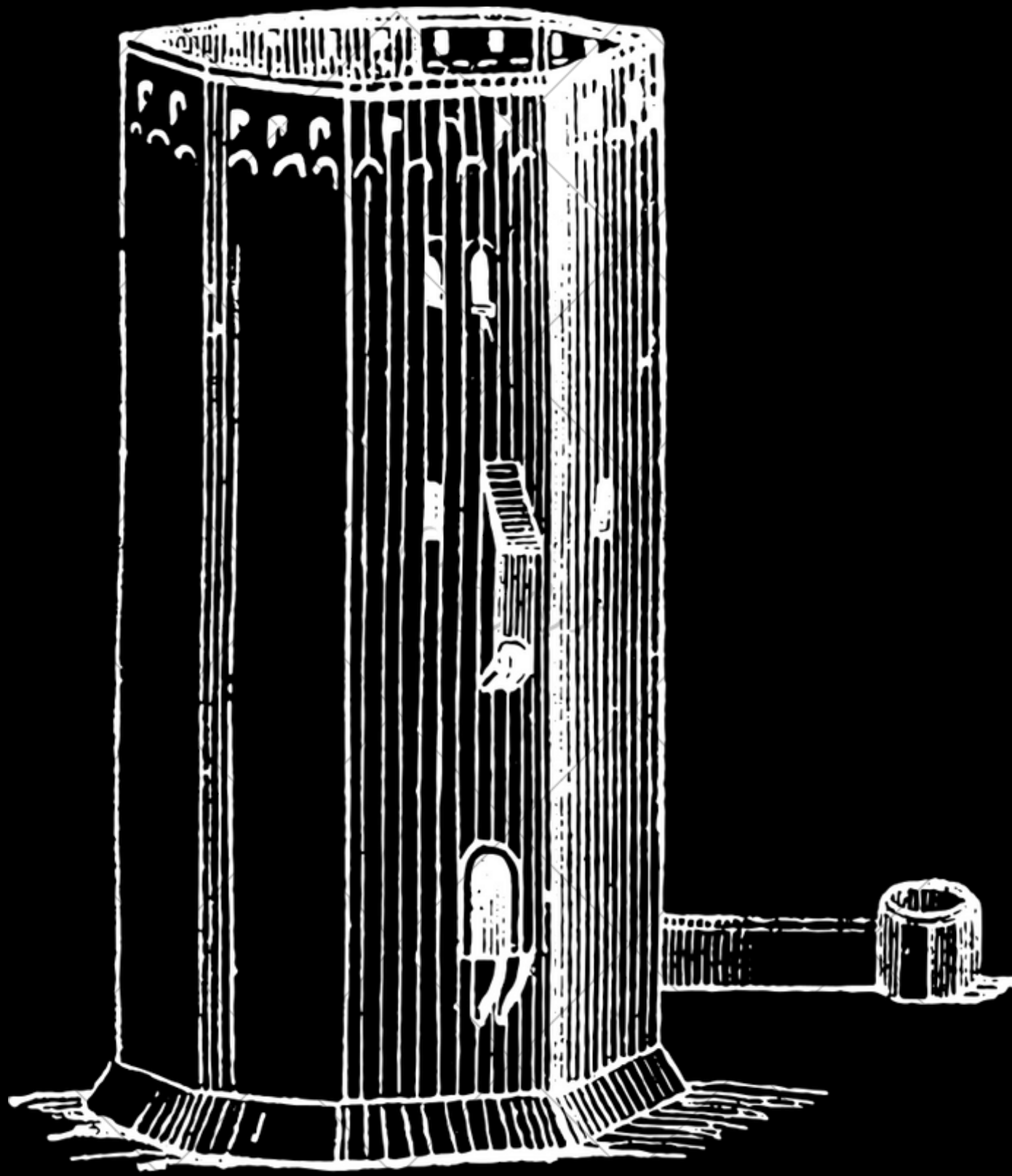


IN A **TRADITIONAL PENETRATION TEST** WE ARE
BOUND BY THE SCOPE.

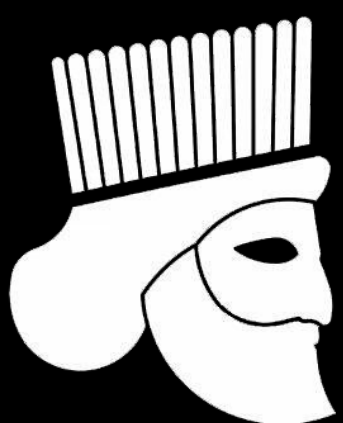
WE WILL NOT BE TRYING TO BREAK IN
PHYSICALLY, USING SOCIAL ENGINEERING, OR
ATTACKING THE WIRELESS NETWORK IF THOSE
THINGS AREN'T EXPLICITLY INCLUDED IN THE
SCOPE OF THE ASSESSMENT.



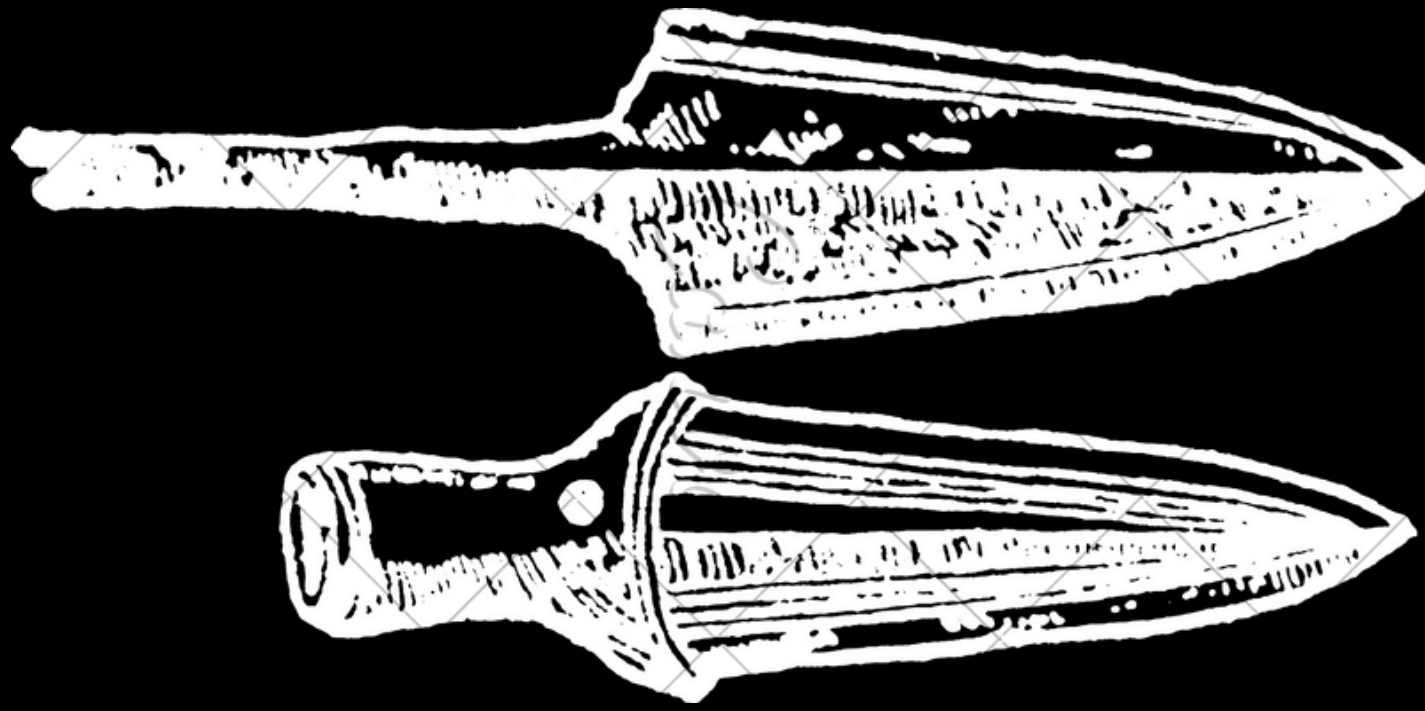
HADESS



FINALLY A **TRADITIONAL PENETRATION TEST**
USES A GRAY-BOX APPROACH.
BUT IN A **RED TEAM OPERATION**, WE TRY TO
AVOID TO COLLECT AS LITTLE INFORMATION
AS POSSIBLE TO TRY AND EMULATE AN
ATTACKER TO THE MAXIMUM EXTENT
POSSIBLE.

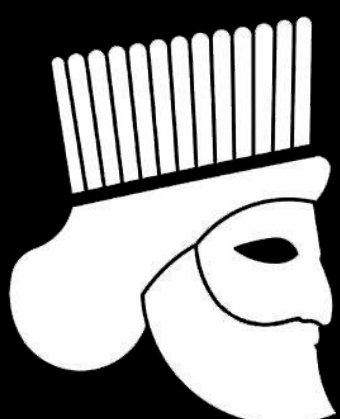


HADESS

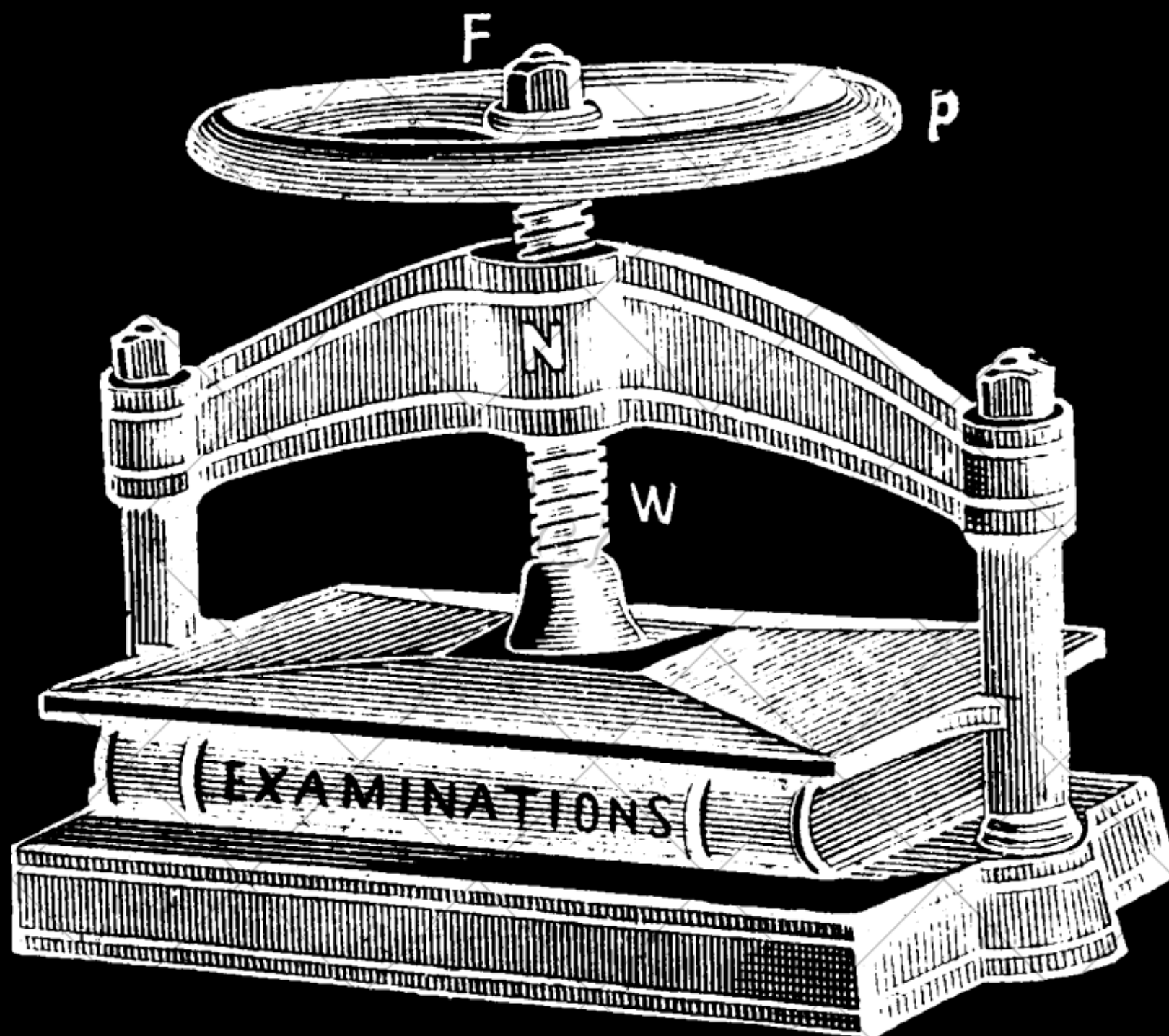


IN SUMMARY, THE MAIN ADVANTAGES OF A RED TEAM ENGAGEMENT IS:

- CLOSEST THING TO A REAL WORLD ATTACKER**
- IT ALLOWS YOU TO BETTER UNDERSTAND THE RISK**
- IT ALLOWS YOU TO BETTEALLOWING YOUR IR TEAM TO CONDUCT FORENSIC ANALYSIS TO DETERMINE WHAT WE GAINED ACCESS TO (WHICH WE CAN CONFIRM OR DENY)R UNDERSTAND THE RISK**
- PROVIDING THE MOST REALISTIC TEST OF YOUR OVERALL SECURITY POSTURE.**



HADESS

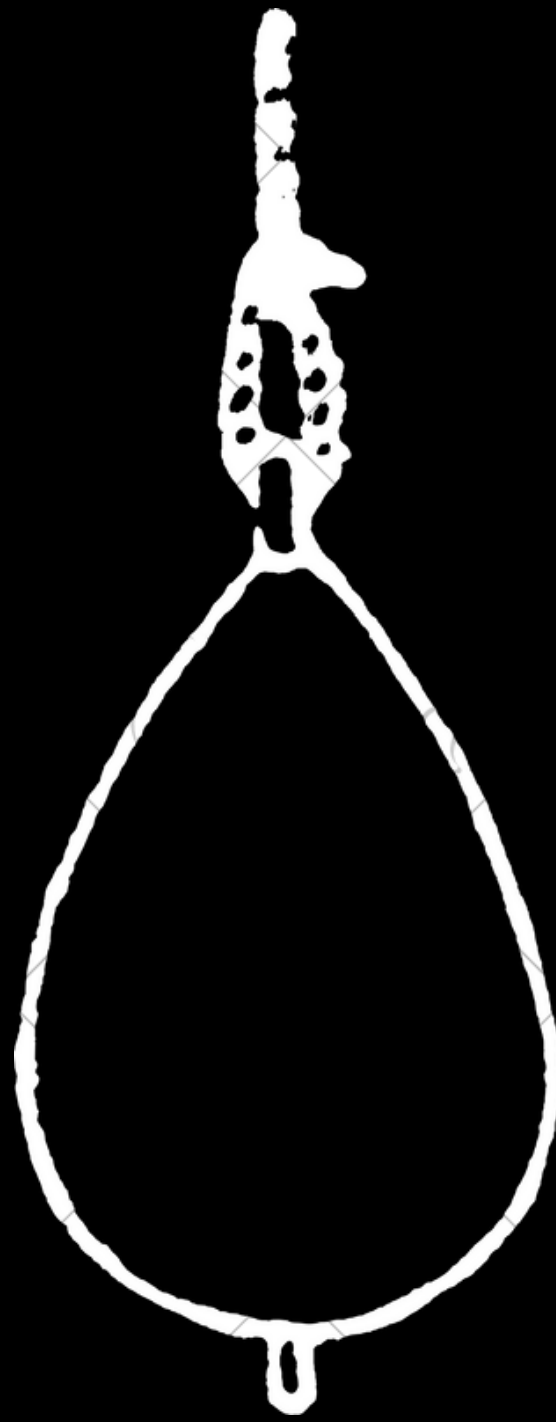


DISADVANTAGES OF RED TEAM OPERATION

THE BIGGEST DISADVANTAGE OF A **RED TEAM** IS
COVERAGE. IN A **RED TEAM** OPERATION,
THE ATTACK TEAM HAS ONE GOAL:
**GAIN ACCESS TO YOUR SENSITIVE INFORMATION
VIA ANY MEANS AVAILABLE.**



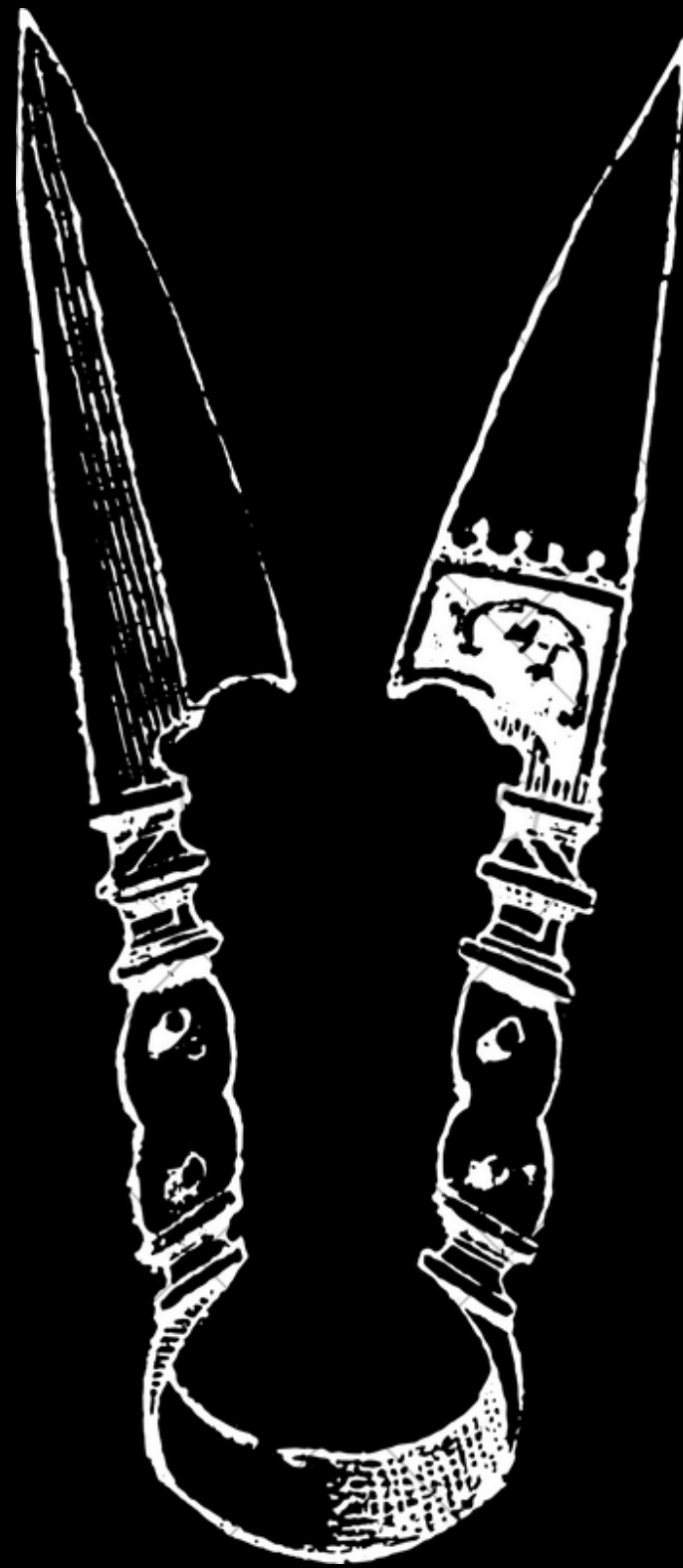
HADESS



IT IS ENTIRELY POSSIBLE THAT THEY WOULD
START WITH **SOCIAL ENGINEERING**, HAVE
SUCCESS, AND THEN MOVE RIGHT INTO AN
INTERNAL **PENETRATION TEST** TO TARGET AND
OBTAIN ACCESS TO SENSITIVE INFORMATION
WITHOUT EVER TESTING ANY OF THE OTHER
ASPECTS OF YOUR PERIMETER SECURITY
(EXTERNAL, WIRELESS, PHYSICAL, ETC.).



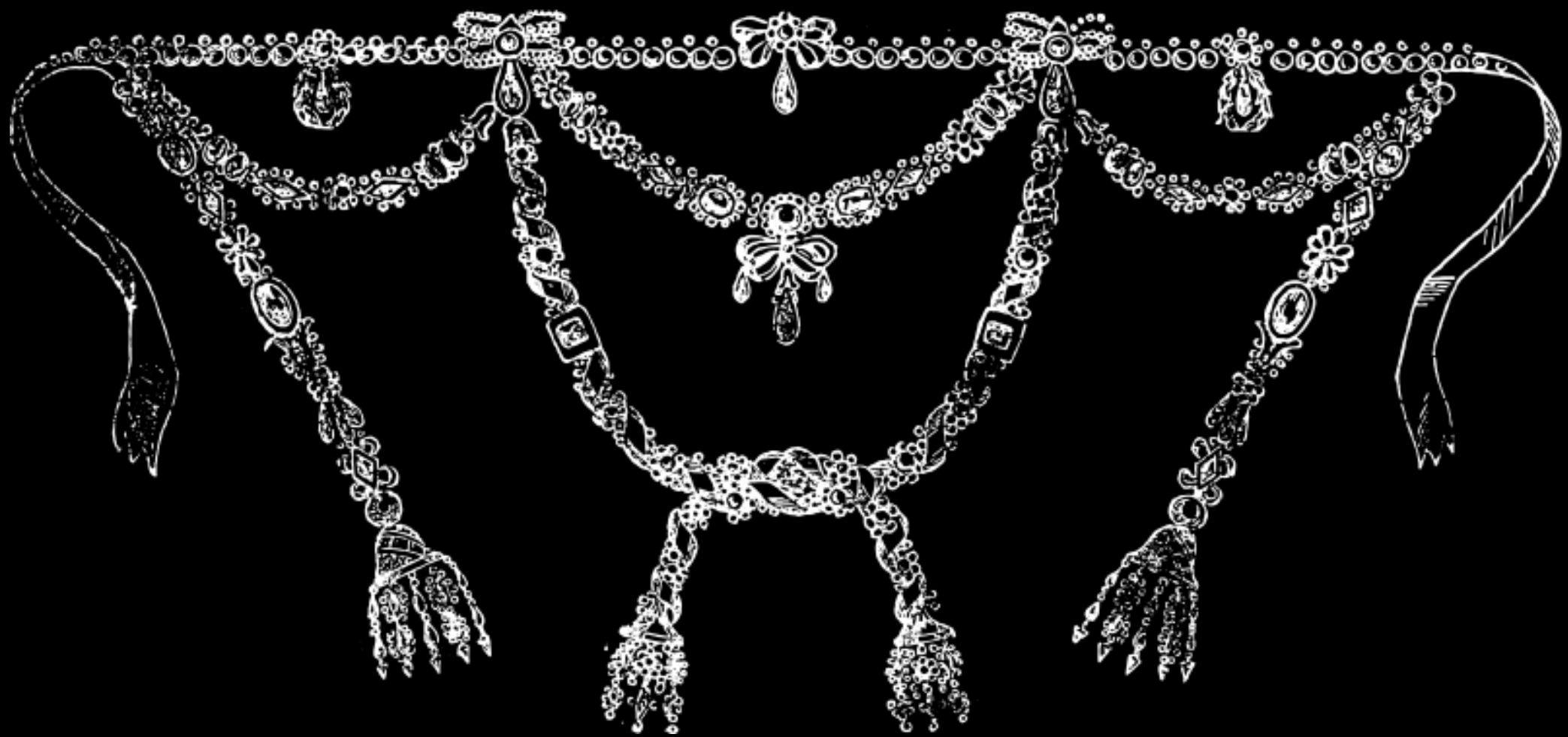
HADESS



**WE WOULD NEVER RECOMMEND DOING A
RED TEAM ENGAGEMENT WITHOUT
TRADITIONAL PENETRATION TESTING
ALREADY IN PLACE.**



HADESS

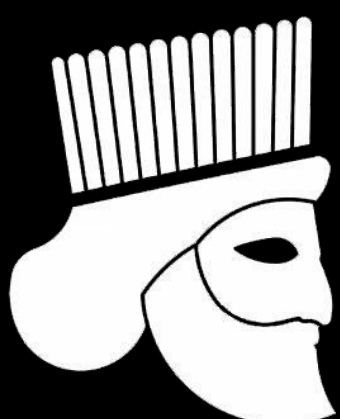


RED TEAM ANSWER THIS QUESTIONS

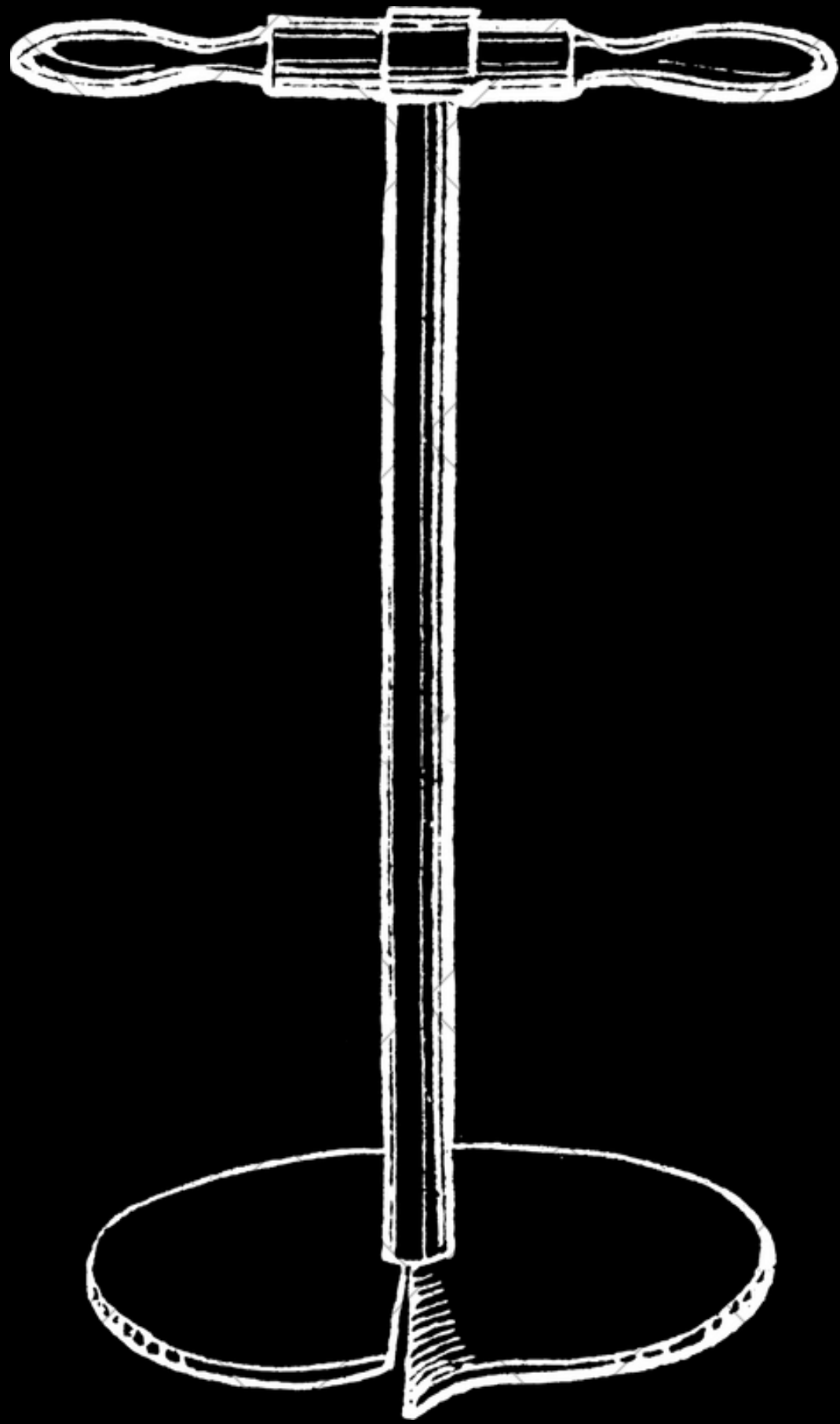
**WHAT IS MY OVERALL RISK? CAN THIS
REALLY HAPPEN?**

PENTEST ANSWER THIS QUESTIONS

**HOW MIGHT MY WIRELESS NETWORK BE
COMPROMISED BY AN ATTACKER?
WHAT ARE ALL THE WAYS AN ATTACKER
MAY GAIN ACCESS?**



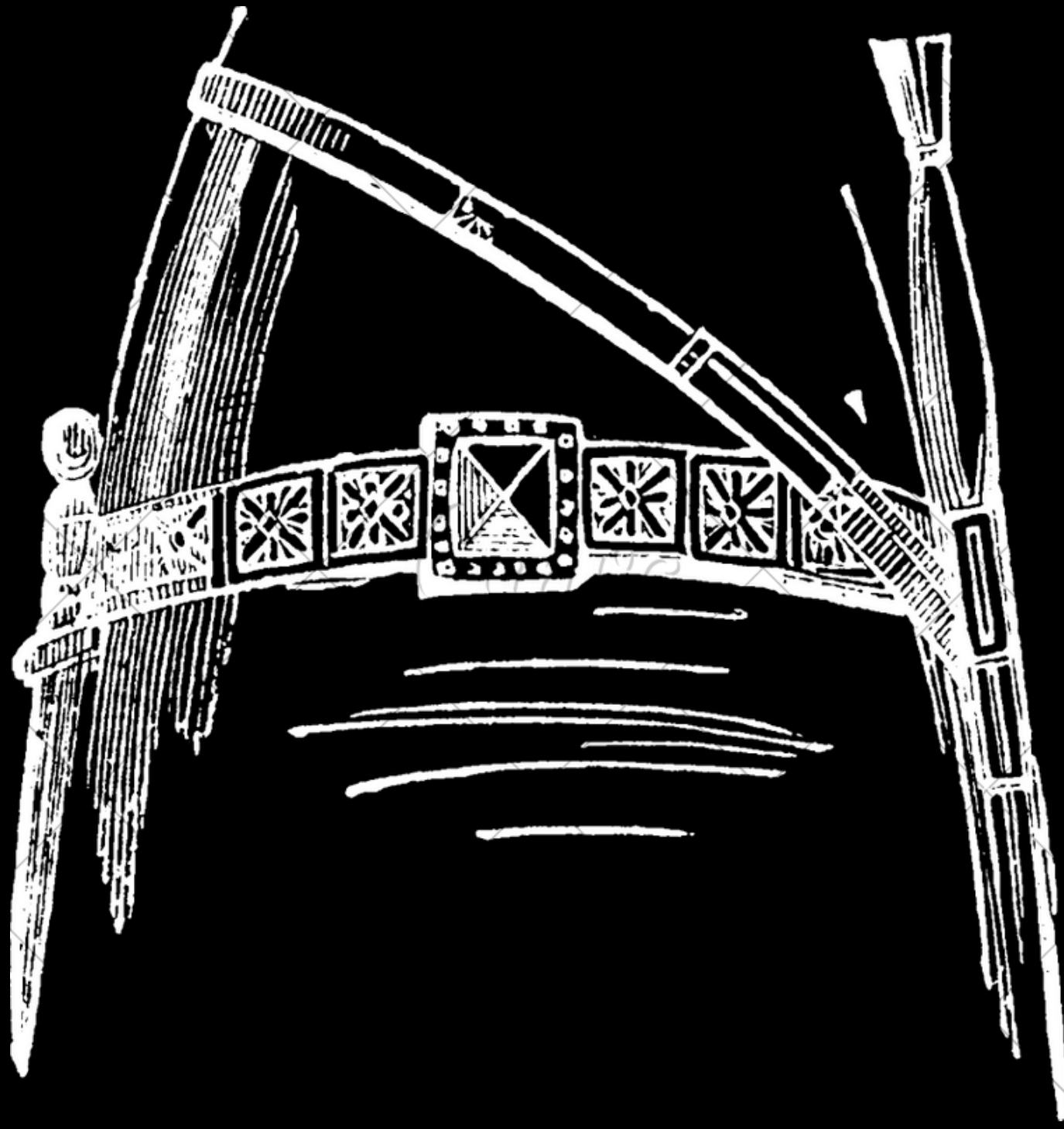
HADESS



RED-TEAM MAY NOT IDENTIFY AND
ENUMERATE ALL IN-SCOPE TARGETS, AND
THEREFORE MAY NOT TEST ALL THE
DEVICES ON YOUR EXTERNAL PERIMETER.



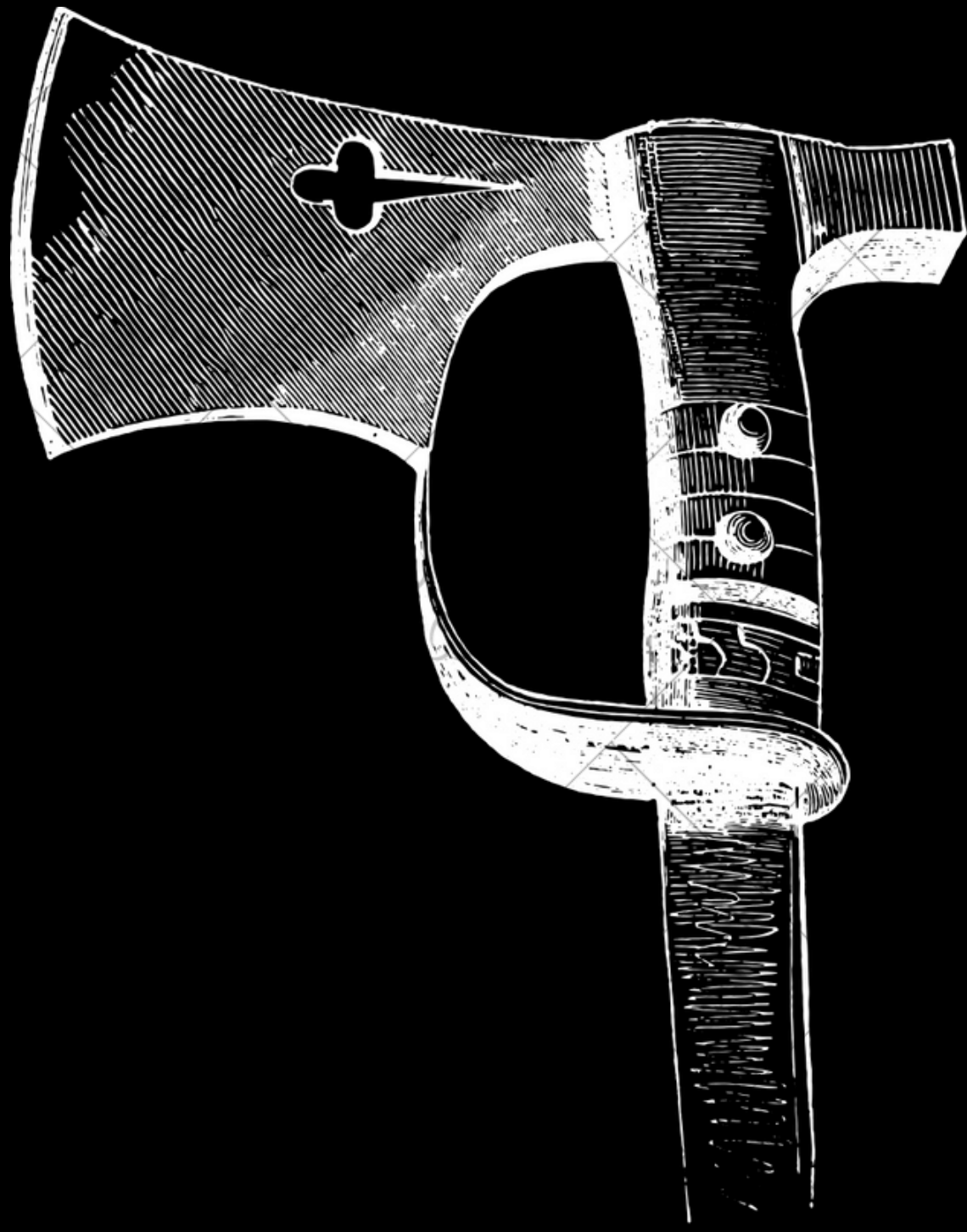
HADESS



RED-TEAM MAY NOT MEET COMPLIANCE
REQUIREMENTS BECAUSE YOU WILL BE
ACTIVELY DEFENDING OUR EFFORTS.
CERTAIN COMPLIANCE REQUIREMENTS,
LIKE PCI, REQUIRE THAT OUR IP
ADDRESSES BE WHITELISTED IN IPS/WAF
TO ALLOW US TO GIVE A THOROUGH TEST.



HADESS

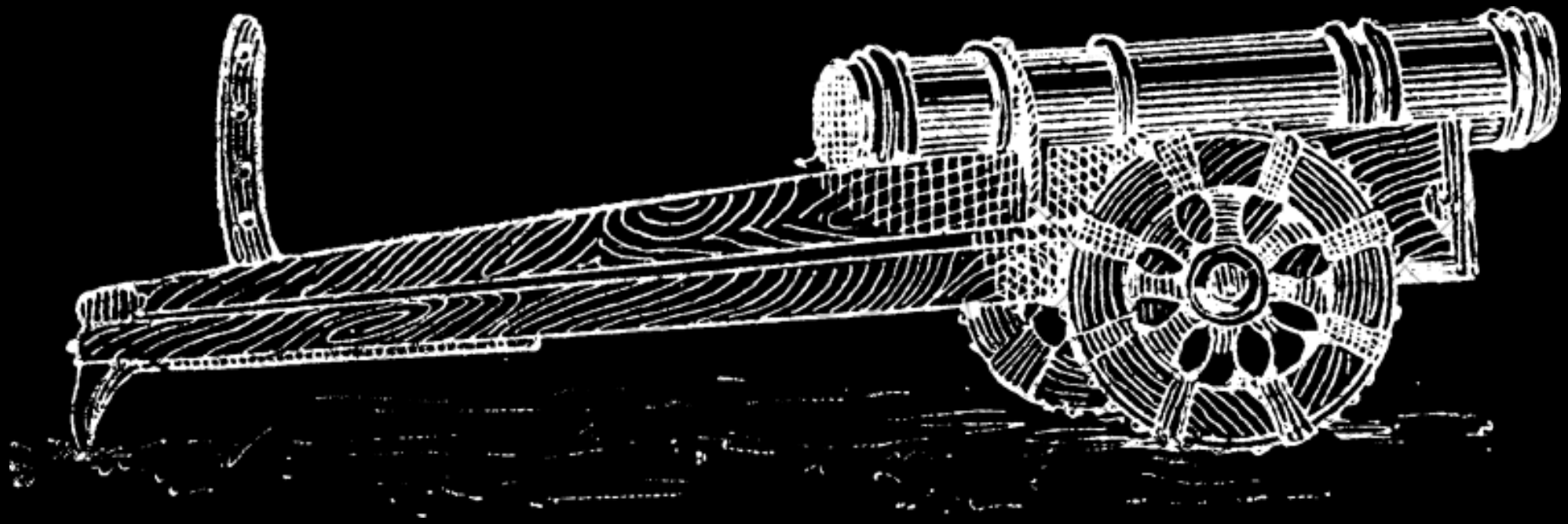


**FINALLY, A RED TEAM OPERATION ALONE
IS LIKELY NOT GOING TO MEET ANY
COMPLIANCE REQUIREMENTS YOU HAVE.
ABSOLUTELY YOU CAN SEE HOW YOUR
TEAM WILL RESPOND TO AN ACTUAL
ATTACK**

BUT...



HADESS



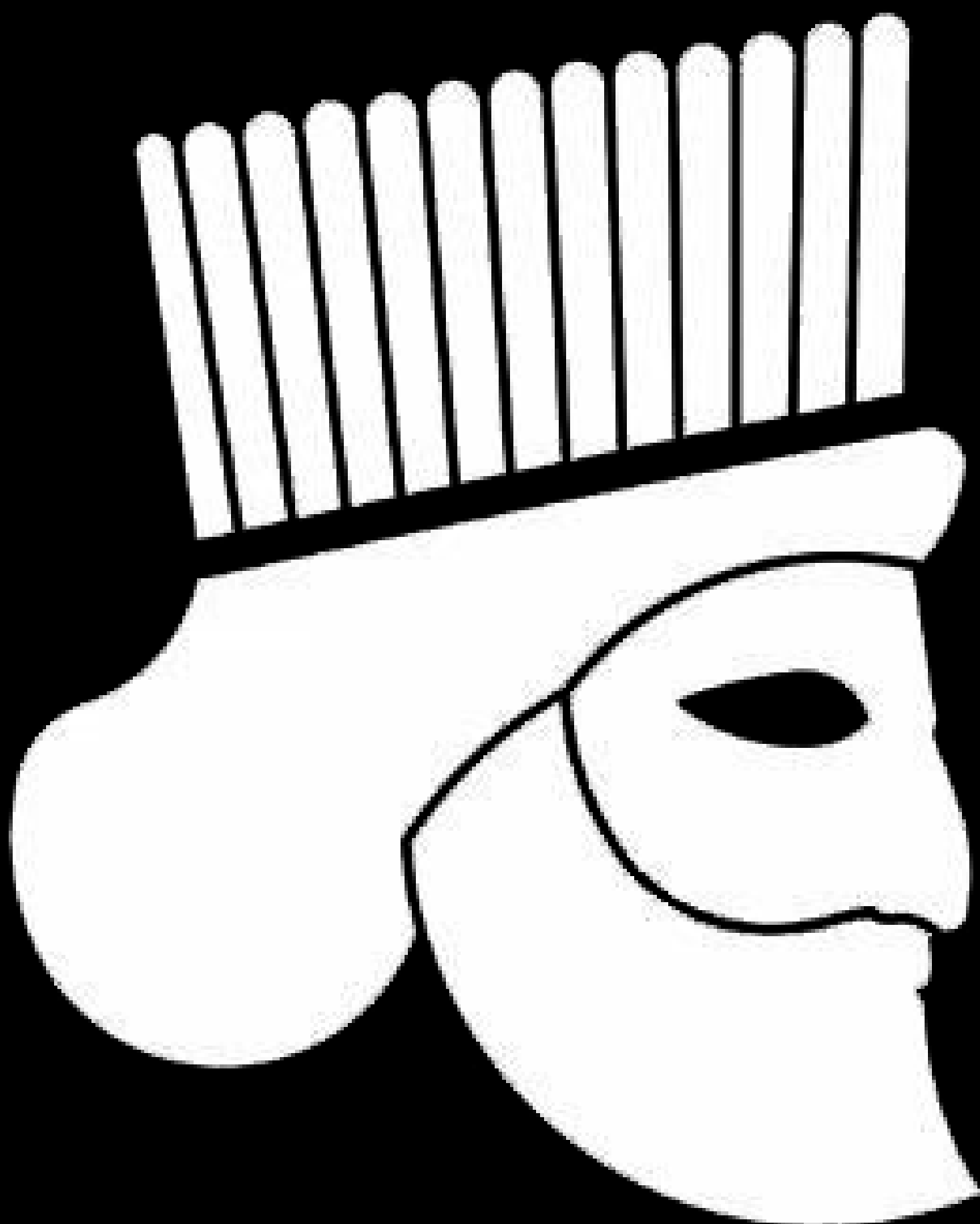
HADESS CAN GIVE YOU A COMPLETE OFFER INCLUDING A SECURITY PACKAGE

- PENETRATION TESTING
- RED-TEAM OPERATION
- SECURE CODING PRACTICE
- STATIC APPLICATION SECURITY TESTING

**BE IN TOUCH WITH US AND GIVE US YOUR
FEED BACK**



HADESS



HADESS

