



PRECISION THREAT TACTICS: ADVERSARY TECHNIQUES ON ENTERPRISE ENVIRONMENTS

AMAL JOY



IDENTIFY ()



AMAL JOY(h0n3yb4dg3r)

- Security Researcher at Altered Security
- Infrastructure Security /Redteaming on Networks and Multi Cloud
- Executive member of DC0471 and Volunteer of Adversary Village
- CARTS/CARTP/MCRTA/CCRTA/CRTA/EJPT



AGENDA



AGENDA

- Identify()
- Jab_Forehand()
- Importance_of_post_exploitation_research()
- Authenticated_enum_for_a_change()
- Lateral_movement_in_ease()
- Feature_abuse_for_data_exfiltration()
- Importance_for_purple_teaming()
- Thank_you()



JAB_FOREHAND ()



JAB_FOREHAND ()

- YOU THINK YOUR COMPANY IS FULLY SECURE AFTER BUYING SO CALLED “TOP” SECURITY PRODUCTS WORTH A LOT OF BUCKS.
- YOUR MANAGEMENT THINKS ASSUME BREACH/INTERNAL PENTEST/POST EXPLOITATION RESEARCH RESULTS ARE “JUST INTERNAL” AND WON’T ADD TO SECURITY



IMPORTANCE OF POST EXPLOITATION RESEARCH ()



IMPORTANCE_OF_POST_EXPLOITATION_RESEARCH()

- ❖ TOOLS DOESN'T CONTROL YOU. YOU CONTROL THEM BY YOUR CONCEPTS.
- ❖ IDENTIFYING NEW ATTACK SURFACES.
- ❖ DIGGING DEEP INTO ALREADY KNOW ATTACK SURFACES FOR IMPACT SCENARIOS ON YOUR COMPANY
- ❖ BETTER COLLAB WITH YOUR BLUE TEAM MEMBERS AND UNIT TESTING



AUTHENTICATED ENUM FOR A CHANGE()



AUTHENTICATED_ENUM_FOR_A_CHANGE ()

- ❖ CASUAL AUTHENTICATED ENUM IN OFFENSIVE SECURITY JUST NEEDED A CHANGE
- ❖ INTEGRATE IDENTIFICATION OF POSSIBLE PERSISTENCE VECTORS TO THE ENUMERATION CHECKLIST
- ❖ PERSISTENCE / BACKDOORS WHICH ARE BLENDING IN TOWARDS YOUR TARGET'S DAY TO DAY ACTIVITIES MAKES THE DIFFERENCE.
- ❖ UNDERSTANDING THE TARGET IS A KEY FACTOR TO DECIDE AND PLAN YOUR ENUM



LAB TIME-1 ()



LATERAL MOVEMENT IN EASE ()




LATERAL_MOVEMENT_IN_EASE ()

- ❖ MORE SMOOTHER THE LATERAL MOVEMENT MORE EASIER IS THE LIFE
- ❖ MINDSET TO UNDERSTAND THE POSSIBILITY OF LATERAL MOVEMENT AND CATCHING HOLD OF THE PIVOT
- ❖ EXTENDING THE IDEA TO PICK THE RIGHT CROSS-PLATFORM TOOLS
- ❖ IDENTIFYING BOTH NETWORK BASED AND NETWORK TO CLOUD LATERAL MOVEMENT



LAB-2 ()




FEATURE_ABUSE_FOR_DATA _EXFILTRATION ()



FEATURE_ABUSE_FOR_DATA_EXFILTRATION

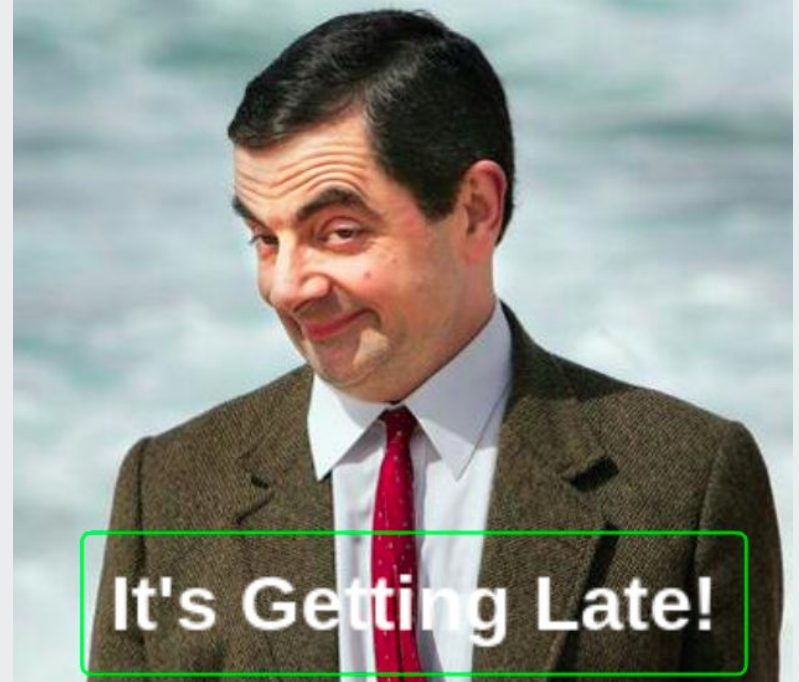
- ❖ USING THE BLENDING IN TECHNIQUE TO IDENTIFY VECTORS FOR DATA EXFILTRATION IS CRITICAL WHILE DOING OFFENSIVE SECURITY OPERATIONS
- ❖ ABUSING VSCODE FEATURE FOR DATA EXFILTRATION.
- ❖ CHANGING ENVIRONMENT NEEDS NEW VECTORS



LAB-3 ()

VSCODE ABUSE FOR DATA EXFILTRATION

LAB-4 () DETECTIONS ON ELASTIC





IMPORTANCE_FOR_PURPLE_ TEAMING ()



IMPORTANCE_FOR PURPLE_TEAMING()

- ❖ RED AND BLUE TEAM COLLABORATION FOR EACH RESEARCH SCENARIOS ARE CRITICAL FOR ENHANCING SECURITY CONTROLS
- ❖ PURPLE TEAMING ALSO HELPS A LOT IN DETECTING THE FALSE POSITIVES BY THE HELP OF UNIT TESTING
- ❖ VARIATION IN PURPLE TEAM ACTIVITIES CAN BE MADE BASED ON ORGANISATIONAL NEED



THANK_YOU ()