HAKIN9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.16, NO. 03

HACKING CAREER JUMPSTART

Introduction to Password Cracking

Basic OSINT with SpiderFoot

Bypass Kaspersky Endpoint Security for Windows

Automate with Metasploit

AND MORE...

Dear Readers,

This time we wanted to create something that will give an initial boost for those who are just starting their hacking careers, and that's why we prepared an issue full of tutorials and case studies - everything on beginner and intermediate level. Let's dive into it!

We start off with *Hacking Techniques for Beginners* - a lengthy and very helpful article covering techniques every hacker must know! Then we drift off to Nmap with *A Detailed and Friendly Introduction to Network Scanning with Nmap* - the title speaks for itself!

If you're in need of a reliable source of information about Metasploit, we present to you two articles that will get you covered: *Manual Pentesting? Automate it with Metasploit Framework!* and *Explo!t: A View on MS17-10 and its Application*.

To help you expand your hacking skills even more, we prepared great introductions to OSINT - *Basic OSINT with SpiderFoot* - and password cracking - *John the Ripper and Hashcat: A Brief Introduction to Password Cracking*.

Later on you'll learn how to *Bypass Kaspersky Endpoint Security for Windows with TrevorC2 + Pyfuscation*, and then we'll switch to *Reverse Image Search 101*, which will help you understand what is reverse image searching and how to use it.

Last but not least, our authors will help you test your security solution, explain what are insider threats, and present the OWASP top 10 mobile vulnerabilities.

We hope this issue will help you jumpstart your hacking career, as we believe everybody needs a helpful hand and a reliable source of information. We would also like to send gratitude to our contributors, reviewers and proofreaders, who helped us create this unique issue!

Stay safe and enjoy!

Hakin9 Editorial Team

Contents

168 Test Your Security Solution

by Filipi Pires

185 Insider Threats - Employees/Consultants

by Syed Peer

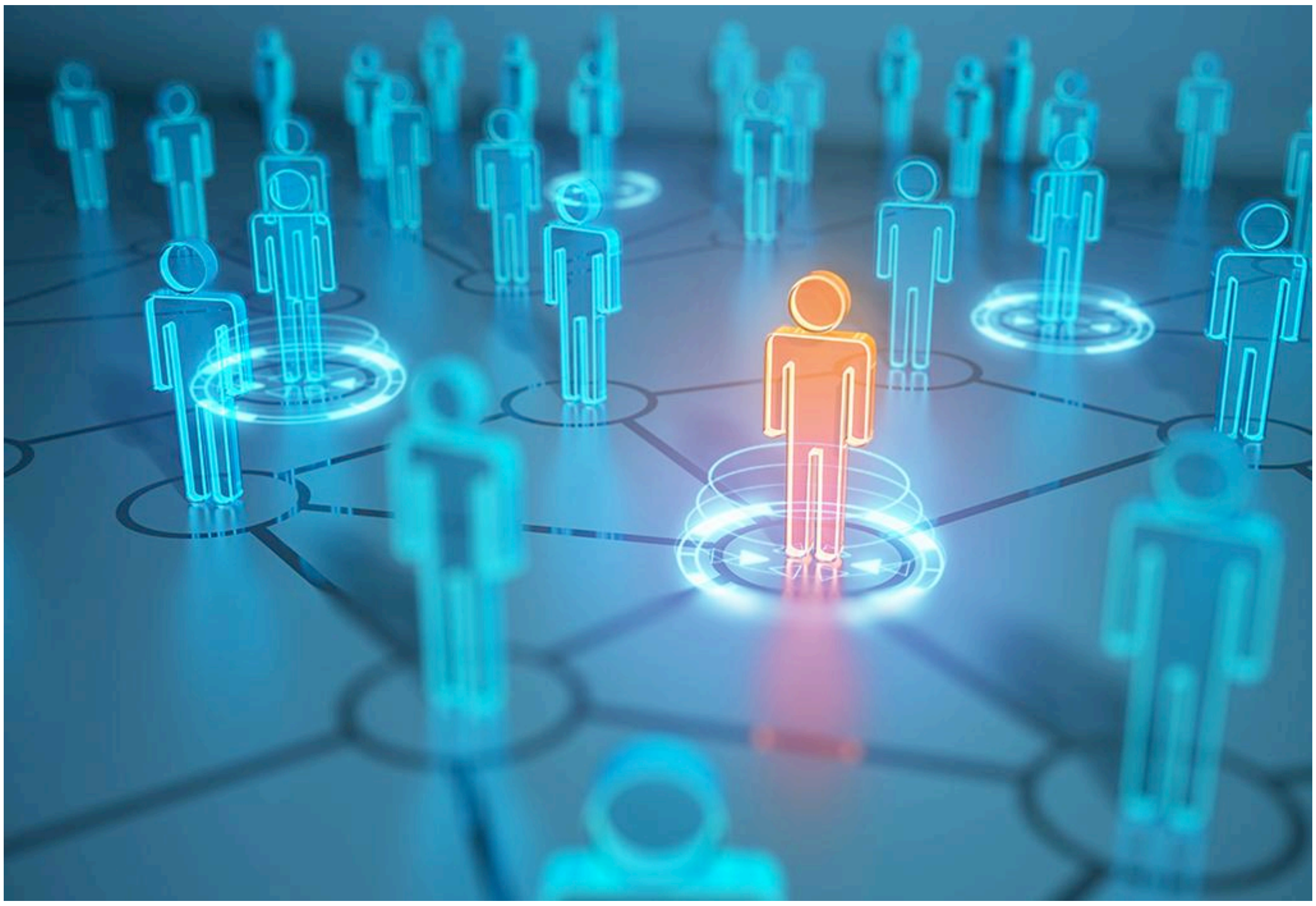
194 OWASP Mobile Top 10

by Dr Akashdeep Bhardwaj, Arohi Magal

INSIDER THREATS – EMPLOYEES/ CONSULTANTS

SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering and Cyber Security teams.



"It is easier to forgive an enemy than to forgive a friend"

— William Blake

Introduction

As information technology teams and businesses grow rapidly, their dependence on critical systems, applications and human capital continues to put a strain on effective project planning, rollout of new initiatives and the organization's future directional road map and technology/process adoption.

Now more than ever, project teams are rarely composed of tried and tested, locally sourced, English speaking *"neighbor next door"* type staffers. Modern teams are most often composed of a small core team (possibly) situated in a native (founder/HQ) location, with additional team members distributed across other satellite offices or other states or globally connected across multiple geographical nations and time zones. Even the necessity for the natively located team and its office has been upended by the pandemic due to the need to keep staffers at a safe working distance remotely.

Considering spiraling project budgeting costs and existing organic skills shortages, it is now standard practice for modern businesses to engage with external providers of services and skilled staff to fill the gap. The modern-day consulting industry is built upon the premise of ever-increasing skills shortages faced by industry. Projects will now routinely onboard "consultants" as part of the larger team expansion necessary to achieve the desired business plan roll out in a timely and cost-effective manner.

Whether on site or working remotely, once onboarded, these external/consultant teams often will have assigned to them the necessary system/applications rights and privileges necessary to complete their work effectively. Externally connected company employees setup in the work-from-home regime, or remote consultants, now add an additional layer of complexity to the security teams' model of how to address the nature and response to the ever-increasing insider threat presented. Recent security surveys of businesses have shown that many now consider the insider threat as a rising concern internally that needs to be urgently addressed.

Insider Threat Definition

As defined by Wikipedia:

> "*An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems*".

Although the initial intent may or may not be malicious at the outset, based upon the nature of the threat actor and the business use case, the final result may ultimately render the action malicious for the vigilant IT SecOps team. Enterprise IT SecOps teams continue to have a hard time clearly identifying insider threats and it has also been reported that up to 90% of insider threats may actually go unreported. As a consequence, threat hunting has now become an essential part of enterprise security programs.

Insider Threat Types

The term *"Insider Threat"* appears at first to denote a hardened, criminally-minded individual hell bent on doing damage to the organization by any and all nefarious means. That is too broad a generalization and, in reality, they could just as easily be a former employee or consultant familiar with the organizational structure, a business partner or even a board member. Data breaches are expensive; according to a new report from IBM and the Ponemon Institute, the average cost of a single data breach in 2020 is $3.86 million. Upwards of 61% of organizations surveyed in 2020 reported having an insider attack within the last 12 months.

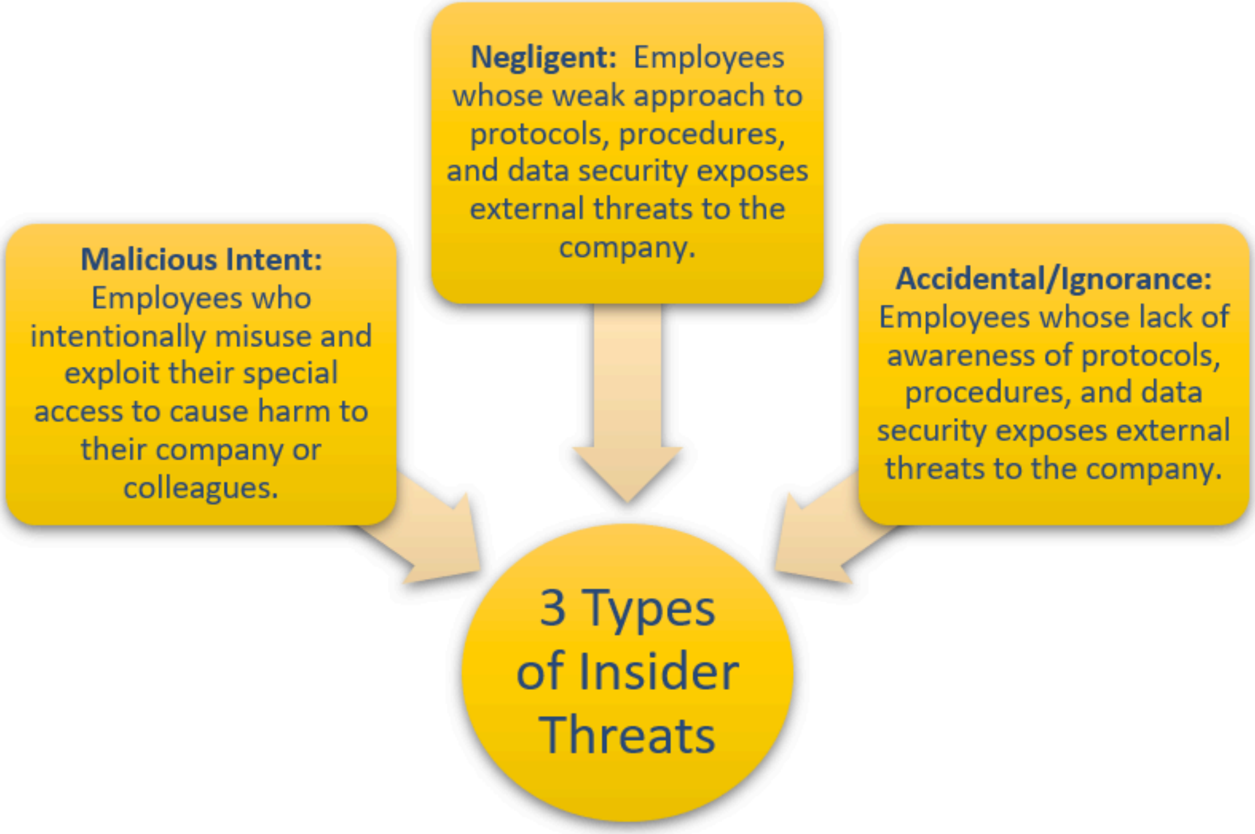
The industry has taken pains to categorize the insider threat actors into three major types, as follows:

Malicious: This is where the employee user/consultant *willfully* engages in harmful actions against the organization, whether it be for material gain or theft by exfiltration of critical data or intellectual property. The bad actor may be working independently for emotional or personal reasons or be part of a larger paid operation directed by outsiders.

A classic example of this in recent history would be the Edward Snowden case where top secret files and recordings were taken from the National Security Agency (NSA) databases during his tenure working there as a contractor consultant. From a security perspective, he had been granted necessary rights and privileges to do his regular work and obliquely his other desired exfiltration plan with ease and without necessary oversight.

Negligent: This is the case of an employee or contractor *willfully* deciding to bypass existing policies in order to shorten his work load or process duration and move forwards quickly. The classic *"haste makes waste"* scenario.

A typical example of this may be an IT Admin that decides to create or use an existing Application *Service Account* to perform a quick and dirty action instead of using his own *named account* that is required by standing policy and procedures for traceability. In the long term, the consequences of this action may be dire and untraceable as the Service Account provides no identifiable information through the logs on who may have executed the action.


Negligent: Employees whose weak approach to protocols, procedures, and data security exposes external threats to the company.
Malicious Intent: Employees who intentionally misuse and exploit their special access to cause harm to their company or colleagues.
Accidental/Ignorance: Employees whose lack of awareness of protocols, procedures, and data security exposes external threats to the company.
3 Types of Insider Threats

Courtesy Xorlogics

Accidental: This is a case of a careless employee who unknowingly initiates an action that can have a detrimental impact on his/her end point initially (compromised desktop/laptop) and later across the organization.

A typical use case would be a low-level employee who falls victim to a targeted spear phishing attack by opening an email attachment maliciously crafted by outsiders to infect the machine and then move laterally across the organization looking for more elevated privilege holders such as Admin accounts. One of the most famous recent cases with a major Social Media platform was the Twitter Crypto currency scam of July 15, 2020. Twitter confirmed that hackers had gained access to administrative tools that enabled them to alter user accounts themselves and post tweets directly. The hackers had used social engineering means to gain access to the tools via Twitter employees.

Another all too common high-risk occurrence is employees using their office emails and/or passwords with external websites and Social Media – all the while working on their company supplied laptops. Almost a quarter of work-from-home employees were identified using this bad behavior.

In summary, we can say that the greatest threat to an organization may already be working within it currently as a regular employee or part of a consultant team. When internal users with the necessary privileged access stray into one of the categories mentioned above, critical enterprise data may be exposed to damage or exfiltration.

Best Practices and Mitigations

Every organization should take the insider threat landscape as seriously as a foreign APT attack on its systems and invest in tools and programs to elevate reconnaissance best practices and equip SecOps teams with necessary tools to do their job efficiently.

The following best practices and mitigation technologies may be considered:

1. **Policies & Procedures**: Documented Policies and Procedures need to be updated and regularly reviewed for new insider threat use cases that have arisen and published as control documents to the workforce.

Regular communication is of the essence here, keeping management updated on the latest trends and the need for compliance. An existing enterprise security framework, such as ISO27001, will help as an effective baseline so you may only need to update or add a section or policy/procedure. Policies must enforce necessary separation of duties to prevent further unauthorized access.

2. **Data Classification**: The first step is always to identify the "critical" data that may be the target of the insider threat. This is no small endeavor and will possibly require the formation of a dedicated team with cooperation between IT, Human Resources, Finance and Audit to identify vulnerable data and how best to secure and limit its exposure.

Senior Management needs to drive this initiative from the highest level across the organization with business areas nominating "captains" to shepherd their business super users towards the intended goal. An automated tool will need to be implemented in the future to allow business owners necessary access to flag data elements and Personal Identifiable Information (PII) items as potential candidates for securing. The selection of the right tool will be instrumental in preventing unauthorized user access across different use cases and ensure that only the right person has visibility to the right data. Thousands of individual user rules by *"business role"* may be generated during this exercise so an automated tool that has oversight across the rules database is the correct direction to take the process forward.

3. **Data Loss Prevention (DLP):** The next logical step after the Data Classification stage completes is the implementation of a best of breed DLP tool. This is an essential accessory in the struggle to prevent unlawful exfiltration of data from any organization. DLP encompasses a broad set of rules and processes enforced to keep data safe.

The DLP tool needs to be accessible to business owners to flag critical data and then set the necessary violation procedures to mitigate the risk quickly. After roll out, the tool should allow for data monitoring, customizable alerts, possible encryption and other product specific features. As technology advances, DLP tools are becoming more widespread across industries and indispensable in targeting sensitive data and watching for a data breach.

4. **Machine Learning**: Investigate the marketplace newly trending product enhancements that leverage Machine Learning (ML) and Artificial Intelligence (AI).

Monitoring and preventive measures implemented will potentially generate a huge number of logs. Endless reams of transactional time stamped data can be the bane of the IT Security team and quickly bring it to its knees. Although thorough and voluminous in themselves, logs cannot provide a full 360° view of what is actually happening and this is where Machine learning enabled systems can filter out much of the noise and help to identify unusual behavior earlier rather than later. Ultimately, this can help to reduce the number of serious data access breaches by insiders.

Allowing for all the benefits that ML brings to threat hunting, as a disclaimer, we must also recognize that professional bad actors will work hard to leave no trace during their kill chain activity and spend time covering up their preceding tracks (i.e. timestomping, indicator removal and log wiping). Currently, many XDR (cross-layered detection and response) tools together with the Threat Hunting teams that utilize them don't detect these bad actor anti-forensics and counter-IR actions. This can lead to a false sense of security and *survivorship bias* on SecOps teams ignoring errant behaviors and ultimately leading to *long tail events*. Such an outcome can also delay meaningful DFIR reporting and frustrate and exhaust SecOps teams with overworked schedules and limited inconclusive results to show at the end of the day for all of their efforts.

5. **User Behavior Analysis Dashboard**: Once a proof of concept has been completed successfully on site, enterprises should invest in a leading User Behavior Analytics Dashboard (UBA) tool.

The 30,000-foot view provided by such dashboards will help the SecOps team members to quickly investigate new incidents to resolution and follow up on unusual user behavior across the enterprise. The User Behavior Analysis (UBA) features will firstly rely on data science to initially collect and aggregate user data for their "normal" regular activities into a database. This data collection stage forms the baseline for that user going forward. Thereafter, the UBA module can report on any anomalous user behavior that deviates from their established baseline, thereby signaling the SecOps teams to further review the suspect actions. For example, an international business development manager on the marketing and sales team that is regularly accustomed to using the VPN to access system resources from the US, UK or Germany would immediately throw a red flag were her next VPN connection from China or the Ukraine, which are not targeted sales markets currently.

6. **Monitor User Access**: Built upon the baseline user databases created by the DLP earlier, insider threats can be managed better thereafter by monitoring all user accesses across the enterprise and not simply those staff that have privileged access.

Monitoring user access to databases, file servers/shares and cloud-based applications (SAAS) is imperative, as these are considered the top three locations for data at risk. The better the monitoring tool, the easier the task will become in the future to identify anomalous behavior going forward. The monitoring exercise can be seen as a training opportunity as well, allowing visibility over negligent or poor employee behaviors (such as opening malicious emails, etc.), which can then be remediated through proper training materials in the Cyber Security Employee Awareness program.

7. **Privileged Access Management (PAM):** The number one cause of data breaches and consequential exfiltration is the appropriation of Admin credentials with elevated authority by bad actors who are then free to move across the network at will.

A typical scenario would be an initial spear phishing attack targeting low level employees via social engineering to gain the first entry point to the network. Thereafter, hackers use lateral movement across the network and a discovery process to procure higher privileged Admin level accounts. Once Admin privileges are acquired, the real intent is executed, be that encryption (ransomware), deliberate damage (scrubbing) or exfiltration (data and IP theft).

8. **User Quarantine**: Risky users (those with recorded unusual behaviors from the UBA) should be monitored closely and, if necessary, quarantined and denied access to critical data. Better to catch the disgruntled user or imposter early than suffer the consequences of a later breach. If necessary, prohibitions may be introduced gradually so as not to alert the user immediately or raise unwarranted suspicions within the business area team members.

9. **Regular Reporting**: Regular vulnerability reporting should be in place and reports created both for audit purposes and to accurately record all insider threat related information – with the introduction of GDPR, senior management should accept nothing less.

Conclusion

With the advent of the COVID-19 pandemic and the following stay at home orders from governments, enterprises both big and small have scrambled to affect the work from home regime across offices, states and international geographies. Therein alone, the insider threat landscape has changed considerably with new policies and due diligence practices being developed and adopted to address the myriad possibilities and exposure use cases. Implementing some or all of the mitigation recommendations presented here may help enterprises stay ahead of the curve and avoid the next data breach.

References:

1. Wikipedia Definition: https://en.wikipedia.org/wiki/Insider_threat

2. Cost IBM: https://www.ibm.com/security/data-breach

3. Bitglass: https://pages.bitglass.com/CD-FY20Q3-Bitglass2020InsiderThreatReport_LP.html