PEN TEST HACKFEST
EUROPE SUMMIT 2024

SANS

AGENDA | Sunday 21 July

Time (CEST)	Description
8:45 am - 9:30 am	In-Person in Amsterdam **Registration & Networking**
9:30 am - 9:45 am	**Welcome and Opening Remarks** Jean-François Maes, Certified Instructor
9:45 am - 10:25 am	**Keynote - A Current Look at the Threat Landscape, and How AI Plays a Role** Stephen Sims, SANS Fellow In this talk, we'll take a look at the most recent attack techniques and targets. This includes understanding what kind of malware and illicit access items are available on the dark web for sale. Artificial Intelligence (AI) is certainly a growing area where we have the attack surface that comes with the new technology. Attacking this attack surface is what we call adversarial AI. We also have the ability to use this amazing technology as an attack aid, to help us to be more effective in our attacks. We'll also look at current information such as the fact that software supply chain attacks make up ~20% of all breaches.
10:25 am - 10:35 am	**Offensive Operations Capture the Flag Kick Off** Jean-François Maes, Certified Instructor This exciting event highlights the large variety of offensive skills taught across multiple courses in the Offensive Operations curriculum. Test your skills against challenges based on network penetration testing, web, and binary exploitation as well as programming and forensics challenges. Once the CTF has begun, attendees have the opportunity to work through the challenges at their own pace during the summit, with prizes given out at the end of the day to our winners.
10:35 am - 11:00 am	**Automated Vulnerability Hunting - Where Are We Now?** Salim Largo, Security Engineer, Nexova This talk will explore the different types of automated vulnerability hunting tools, including reverse engineering framework, symbolic execution framework, SAST/DAST tools and fuzzers.We'll also address the limitations of automation and the importance of combining it with human expertise for a holistic security approach. The audience will gain knowledge of what are the state-of-the-art tools and techniques they can leverage to perform automated vulnerability research.

PEN TEST HACKFEST
EUROPE SUMMIT 2024

SANS

Time (BST)	Description
11:00 am - 11:20 am	**Networking Break**
11:20 am - 11:50 am	**Let's Talk About The RAX: How CFG Impacts Modern Exploits** Niels Pfau, Red Teamer, Mantodea Security Several years have passed since Microsoft first introduced the Windows Control Flow Guard (CFG), an exploit mitigation trying to secure the control flow integrity of an application. In this talk, we revisit CFG through a demonstration of CVE-2019-0567, utilizing two different attack concepts to evaluate its effectiveness and shortcomings. Additionally, we will explore changes and improvements Microsoft has integrated into CFG throughout the Windows versions. This will include looking at some of the internals used for user-land processes. Finally, we will discuss how combining CFG with other mitigations can solve limitations of a single defense technique.
11:55 am - 12:25 pm	**The Turing Deception: Exploiting Machine Trust** Iulian Timischi, CTI Expert, Bitdefender LLMs are transforming landscapes, but pen testers must be aware of the security risks they introduce in production environments. This talk dives deep into vulnerabilities associated with popular LLM use cases like Retrieval-Augmented Generation (RAG) and SQL database access. We'll equip you with the knowledge to exploit these vulnerabilities through practical demonstrations, allowing you to better assess LLM security during penetration tests. This talk isn't just about exploits. We'll discuss best practices for mitigating these risks and ensuring secure LLM deployments. This includes secure data management practices, proper access control mechanisms, and implementing robust validation techniques for user prompts. By understanding these vulnerabilities and mitigation strategies, you'll be well-equipped to assess LLM security during penetration tests.
12:30 pm - 1:00 pm	**Weaponising AI for Cyber Attacks & Offensive Operations** Manit Sahib, Offensive Security Lead, Global Fund [UN] Weaponising AI for Cyber Attacks & Offensive Operations Overview & Threat Landscape: How AI is being leveraged for malicious activities. Weaponising AI for Offensive Operations [BYO-GPT]: • How to create your own Generative AI to use in Offensive Operations • Demonstration: Using GPT for Threat Intelligence and Adversary Simulation. Weaponising AI for Cyber Attacks [The Deep Fake Central Banking Heist]: • Exploring how APAC was compromised for $25M with AI and Deep fakes • Demonstration: How easy is it to create a Deep Fake to steal Gold, print Money and disrupt the global economy? Outro: Thanks from a Celebrity; generated with AI.

PEN TEST HACKFEST EUROPE SUMMIT 2024

SANS

Time (BST)	Description
1:00 pm - 2:00 pm	**Networking Lunch**
2:00 pm - 2:25 pm	**Pandora: A Red Teaming Tool to Expose Password Management Leaked Credentials** Efstratios Chatzoglou, Penetration Tester, Memorandum Passwords remain a foundational element of cybersecurity, but the increasing sophistication of attacks targeting password management software (PM) necessitates new defensive strategies. This presentation introduces Pandora, a novel red teaming tool designed to exploit vulnerabilities in 18 widely-used PM systems, from desktop applications in MS Windows 10 to browser plugins. Pandora operates by dumping the processes of active PM systems to extract user credentials, demonstrating the feasibility of this attack vector in real-world scenarios.
2:30 pm - 2:55 pm	**Infrastructure Attack as Code: Using Terraform To Attack Cloud** Bleon Proko, Cloud Security Researcher, Permiso Terraform is an IaC tool that allows provision, management and deletion of infrastructure resources automatically. It is used mostly by DevOps Engineers, as well as Administrators on both on-prem and cloud infrastructures. One feature that Terrafom is mostly known about is its ability to be extended to allow for different deployments on different providers, using its plugins, which they call Providers. There are providers for GCP, Azure, and even one for ActiveDirectory based infrastructures. This blog will use one of these providers, the AWS Terraform Provider, to look at what features can an attacker use to enumerate, compromise and persist in an AWS Based infrastructure and how those attacks can be detected.
3:00 pm - 3:30 pm	**Hiding Payloads in Plain .text** Moritz Thomas, Security Consultant, NVISO Confronting advanced EDR systems that employ entropy detection to identify malicious payloads, our team has developed a novel approach to deliver C2 payloads undetected. This session will outline our method for reducing payload entropy, detail the use of the PECOFF format for shellcode concealment, and introduce a custom tool that disguises payloads to evade EDR scrutiny. We will briefly discuss the basics of Shannon entropy, its application in EDR systems, and the practical steps taken to counteract this detection mechanism. The talk will conclude with a demonstration of our tool, which will be made available as open-source.
3:30 pm - 4:00 pm	**Networking Break**

PEN TEST HACKFEST EUROPE SUMMIT 2024

SANS

Time (BST)	Description
4:00 pm - 4:30 pm	**Island Hoping: Move from LOLBins to Living off Langs** Moses Frost, Senior Instructor What keeps me up at night? Is it that I can't break in anymore, or is it that we haven't figured out all the ways to break in? Over the years, we have seen moves to place our applications into smaller attacker surface spaces. We have seen those microservice environments abstract our attack surface. Did we eliminate all attacks? At the same time, we have an explosion of endpoints of applications that run interpreted languages and how those constraints can be broken. When organisms evolve in the wild, they do so under extreme pressure. Has the pressure to find new ways to get a foothold in environments allowed us to evolve? Attackers are crafty, and defenders have to keep up. This talk demonstrates a methodology and tools for moving from container-constrained environments. They are limited to shells and interpreters. Have you been stuck like this before? Let's get beyond that. How does this tool move beyond containers and constrained environments into Windows and other generic workloads? Let's not worry about LOLBins. Bring your land and get off the air-gapped island.
4:35 pm - 5:00 pm	**5G and Beyond, Exploitation and Beyond** Ali Abdollahi, Enterprise Application Security Lead, Canon The advent of 5G and forthcoming 6G technologies not only revolutionize network capabilities but also amplify cybersecurity risks. This presentation delves into the inherent vulnerabilities of these advanced architectures, emphasizing the exploitation potential and the need for heightened security measures. It begins by elucidating the intricacies of 5G and beyond, particularly focusing on network slicing's dual role in enhancing efficiency and expanding attack vectors. The discussion extends to vulnerabilities within user plane functions, accentuating the susceptibility to interception and manipulation amidst heightened data rates. Additionally, it addresses the security implications of HTTP/2 and QUIC protocols, highlighting the potential for denial-of-service attacks and zero-day exploits. A case study of CVE-2024-20685 in Azure's Private 5G Core underscores the tangible threats and disruptions posed by such vulnerabilities, urging proactive security strategies. Looking forward, the presentation anticipates future challenges posed by emerging technologies like quantum computing, necessitating the development of quantum-resistant encryption methods to safeguard network integrity.
5:00 pm - 5:15 pm	**Capture the Flag Awards and Closing Remarks** Jean-François Maes, Certified Instructor
5:15 pm - 7:00 pm	**Networking and Drinks at Parkzuid** Location: Vondelpark 3, 1071 AA Amsterdam