IOprotect Schulung

Exploits verstehen & analysieren - Teil I + II

Datum:
April 2018

IOprotect GmbH
Dürstelenstrasse 136
8335 Hittnau
+41 (0)44 533 00 05
info@ioprotect.ch
www.ioprotect.ch

Exploits verstehen & analysieren - Teil I

Ziel / Beschreibung	Zu den Aufgaben eines Incident Handlers gehört auch die Analyse von bösartigen Dateien, welche Schwachstellen in Applikationen ausnutzen (so genannte Exploits). Das Problem dabei: Die Analyse mit Hilfe automatisierter Sandbox-Lösungen schlägt in solchen Fällen häufig fehl. Dafür gibt es unterschiedliche Gründe: Falsche Zeitzone, fehlende oder falsche Zielapplikation, Detektion der Analyse-Umgebung durch den Exploit etc. Als Konsequenz muss die Analyse von Hand im Lab erfolgen, was mitunter sehr frustrierend sein kann. Doch wie untersucht man Exploits eigentlich? Nach welchen Mustern hält man Ausschau? Welche Tools sind dabei hilfreich? Diese Fragen lassen sich wesentlich einfacher beantworten, wenn auch ein detailliertes Verständnis für den Exploit-Prozess vorhanden ist. Wie besser dieses Know-How aufbauen, als selber einen Exploit Schritt für Schritt entwickeln? Im ersten Teil von IOprotects Practical Hands-On Workshop " Exploits verstehen & analysieren " geht es genau darum: Für eine reale Schwachstelle werden für jede identifizierte Exploit-Phase Ideen zusammengetragen, konkretisiert und anschliessend umgesetzt. Dabei sehen die Teilnehmer, wie kreativ Angreifer heutige Schwachstellen ausnutzen und lernen, welche Massnahmen der Softwarehersteller wie umgangen werden. Der Hands-On Workshop ist eine Kombination aus gemeinsamen Brainstorming-Sessions und anschliessender Möglichkeit der direkten Umsetzung der erarbeiteten Ideen. Nach jeder Übung erhalten alle Teilnehmer die Lösung. Die diskutierte Schwachstelle wurde bei APT-Angriffen eingesetzt. Die Arbeiten erfolgen unter Windows.
Inhalte	Agenda Tag 1 • Einführung in grundlegende Begriffe und Tools • Erklärung der Schwachstelle (Use-After Free) • Einführung in die Labumgebung • Hands-On: Debuggen der Schwachstelle • Erarbeiten der Exploit-Phasen • Brainstorming 1: Erste Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen

	• Brainstorming 2: Zweite Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 3: Dritte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 4: Vierte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 5: Fünfte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 6: Sechste Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen Agenda Tag 2 • Zusammenfassung des ersten Tages • Brainstorming 7: Siebte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 8: Achte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 9: Neunte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 10: Zehnte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Brainstorming 11: Elfte Exploit-Phase • Hands-On: Umsetzen & Lösung besprechen • Zusammenfassung und Ausblick auf Teil II
Zielpublikum	Personen, welche den Exploit-Prozess und die Massnahmen auf OS-Ebene verstehen und selber ihren ersten Exploit entwickeln wollen. Für Personen, welche für die Analyse von Exploits gerüstet sein möchten (Teil II), stellt dieser erste Teil die Voraussetzung dafür dar.
Schlüsselwörter	DEP, ASLR, Shellcode, Use After Free, WinDbg, OllyDbg, Virtual Table, Import Address Table, Export Address Table, Array, Vector, Page Permissions, Register, Stack, Heap, Base Address, Memory Allocation, VirtualProtect, VirtualAlloc, VirtualFree, CreateProcessA, RW Primitive, Debugger, Windows

Voraussetzungen	IOprotect stellt eine Labumgebung zur Verfügung, welche via VNC oder RDP zugreifbar ist. Die Teilnehmer benötigen entsprechend ein System, mit welchem sie auf die Testumgebung zugreifen können (Linux, Windows oder macOS mit RDP- oder VNC-Client). Die Teilnehmer sollten ein Grundverständnis für Debugging-Abläufe, Assembler und Programmierung aufweisen (Schlaufen, Variablendefinition, Funktionsaufrufe, Verzweigungen etc.) oder gewillt sein, dies on-the-fly zu lernen.
Dauer	2 Tage

Kosten pro Person für den Workshop "Exploits verstehen & analysieren - Teil I"	• SCS-Mitglieder:
	  ○ 1 Person kostenlos
	  ○ jede weitere Person CHF 500 exkl. MwSt.
	• IOprotect-Kunden: CHF 1250 exkl. MwSt.
	• Weitere Interessenten: CHF 2000 exkl. MwSt.

Exploits verstehen & analysieren - Teil II

Ziel / Beschreibung	Im zweiten Teil von IOprotects Practical Hands-On Workshop "Exploits verstehen & analysieren" werden unterschiedliche Exploits analysiert und besprochen. Der Grossteil der besprochenen Samples wurde bei sehr gezielten Angriffen (APT) eingesetzt. Die Teilnehmer lernen dabei hilfreiche Tools und Methoden kennen und können diese in der geschützten Labumgebung anhand realer Exploits anwenden. Der Hands-on Workshop zeigt zudem auf, was beim Aufbau einer Labumgebung zu beachten ist. Die Arbeiten erfolgen unter Windows 7 und Windows 10.
Inhalte	• Einführung in grundlegende Begriffe und Tools • Diskussion zu Analyse-Umgebungen • Vor- und Nachteile von automatisierten Analysen • Kennenlernen von Tools für unterschiedliche Tasks • Erläuterung zum Exploit-Analyse-Prozess • Hands-On: Exploit 1 • Hands-On: Exploit 2 • Hands-On: Exploit 3 • Hands-on: Exploit 4
Zielpublikum	Personen, welche ein Verständnis für den Exploit-Analyse-Prozess erhalten wollen und diesen auch selbst anwenden möchten.
Schlüsselwörter	Debugger, WinDbg, OllyDbg, Shellcode, ROP, Heap Spray, OLE, Python, Verschlüsselung, Obfuszierung, RW Primitive, Stack Overflow, Use After Free, Virtuelle Umgebung, Windows 7, Windows 10, DEP, ASLR, CFG, Process Explorer, Advanced Persistent Threats (APT), Windows
Voraussetzungen	IOprotect stellt eine Labumgebung zur Verfügung, welche via VNC oder RDP zugreifbar ist. Die Teilnehmer benötigen entsprechend ein System, mit welchem sie auf die Testumgebung zugreifen können (Linux, Windows oder macOS mit RDP- oder VNC-Client). Das erworbene Wissen von "Exploits verstehen & analysieren – Teil I" ist Voraussetzung für diesen zweiten Teil.

Dauer	2 Tage

Kosten pro Person für den Workshop "Exploits verstehen & analysieren - Teil II"	• SCS-Mitglieder:
	  ○ 1 Person kostenlos
	  ○ jede weitere Person CHF 500 exkl. MwSt.
	• IOprotect-Kunden: CHF 1250 exkl. MwSt.
	• Weitere Interessenten: CHF 2000 exkl. MwSt.