REDOPS
INFORMATION SECURITY

Live Training

Endpoint Security Insights: Shellcode Loaders and Evasion

Inhaltsubersicht

1 Einleitung

In den letzten Jahren ist die Umgehung von Endpoint Protection (EPP) und Endpoint Detection and Response (EDR) Produkten zu einer immer größeren Herausforderung geworden und stellt heute einen wichtigen Aspekt bei jedem Red Team Einsatz dar. Jedes EPP/EDR-System hat seine eigenen Stärken und Schwächen, und es gibt keine Patentlösung für die Umgehung von EPP/EDR. Ein solides Verständnis der Grundlagen der EPP/EDR-Umgehung und der Entwicklung von Shellcode-Loadern ist jedoch von entscheidender Bedeutung, selbst auf Junior-Ebene.

In den letzten sechs Jahren habe ich mir mit Hilfe verschiedener Endpoint Security Produkte ein umfangreiches Wissen über die Umgehung von Endpoint Security angeeignet. In meinem neuen **4-tägigen** online Kurs "**Endpoint Security Insights: Shellcode Loaders and Evasion**" möchte ich dieses Wissen im Zusammenhang mit Shellcode-Loadern und Endpoint Security Evasion weitergeben.

Ein großer Teil der Kurszeit (ca. 50%-60%) ist der schrittweisen Entwicklung und dem Debugging verschiedener Arten von Shellcode-Loadern in C (und teilweise in Assembler) gewidmet, wobei der Schwerpunkt auf direkten Syscalls, indirekten Syscalls, Encryption, Metadaten, Entropie, etc. liegt. Im Allgemeinen besteht der größte Teil der Kurszeit (ca. 70-80%) aus praktischen Übungen für die Kursteilnehmer. Da der Schwerpunkt dieses Kurses nicht ausschließlich auf der Entwicklung von Malware liegt, müssen die Studierenden jedoch keinen Code von Grund auf neu schreiben, sondern in jedem Modul verschiedene Aufgaben lösen, um verschiedene Arten von Shellcode-Loader-POCs zu erstellen. Für mich als Dozent ist es am wichtigsten, dass jeder Studierende die Funktionalität jedes jedes Shellcode-Loaders vollständig versteht.

Für die Windows-Plattform werden die Shellcode-Loader in Visual Studio 2022 erstellt und das Debugging wird mit WinDbg und x64dbg durchgeführt.

Das Hauptziel dieses Workshops ist es, einen attraktiven Workshop anzubieten, der sich darauf konzentriert, den Teilnehmern Folgendes zu vermitteln:

- Verständnis der notwendigen Grundlagen von Windows, wie z.B. Windows NT Architektur, Win32 APIs, native APIs, Systemaufrufe, etc.

- Verstehen der Architektur von Endpunkt-Sicherheitsprodukten und der Mechanismen, die sie zur Prävention oder Erkennung verwenden, wie z.B. AMSI, ETW, Hooking, Callbacks, etc.

- Verstehen der verschiedenen Arten von Evasion Techniken, wie direkte Syscalls, indirekte Syscall, Unhooking über Software-Breakpoints, Unhooking über Hardware-Breakpoints, usw., die in Shellcode-Loadern implementiert werden können, um Endpunkt-Sicherheitsprodukte zu umgehen.

- Schritt-für-Schritt-Erstellung von Shellcode-Loader unter Verwendung der verschiedenen oben genannten Umgehungstechniken.

- Debuggen der Shellcode-Loader, um ihr Verhalten und die potenziellen Kompromittierungsindikatoren (Indicators of Compromise, IOCs) zu identifizieren, die EDRs zur Erkennung verwenden.

- Evaluierung der erstellten Shellcode-Loader mit einem Endpunktsicherheitsprodukt. Aus verschiedenen Gründen werden nur Offline-Tests (keine Endpoint Security Cloud) in Kombination mit Offline-Loadern (interne IP) angeboten.

2 Disclaimer

Die grundlegenden Inhalte für dieses Training sind in verschiedenen Formen frei im Internet verfügbar. Ich möchte klarstellen, dass ich in meinem Training keine neuen Taktiken, Techniken etc. vorstelle. Wenn Sie meine Begeisterung für das autodidaktische Lernen teilen, möchte ich Sie ermutigen, diese Ressourcen selbst zu erkunden und die enorme Fülle an Informationen, die online verfügbar sind, zu nutzen.

Wenn Sie jedoch auf der Suche nach einem qualitativ hochwertigen Live-Training und einem strukturierten Ansatz sind, um einige grundlegende Konzepte zur Umgehung von Endpunktsicherheit und Shellcode Loadern zu erlernen, dann ist mein Kurs "Endpoint Security Insights: Shellcode Loaders and Evasion" eine gute Wahl für Sie.

3 Zentrale Lernziele

- Ihr Verständnis der Grundlagen von Windows zu vertiefen, um Endpoint-Sicherheitsprodukte besser zu verstehen und Shellcode-Loader mit mehr Geschick zu entwickeln.
- Entwickeln Sie ein umfassendes Verständnis der Abwehrmechanismen für die Endpunktsicherheit, einschließlich User Mode Hooking, Windows Event Tracking, Callbacks und mehr.
- Vertiefen Sie Ihr Verständnis von Win32-APIs, nativen APIs, Systemaufrufen, direkten Systemaufrufen, indirekten Systemaufrufen usw.
- Verbessern Sie Ihr Verständnis von Shellcode-Speicherung und Verschlüsselungstechniken.
- Besseres Verständnis dafür, wie die Entropie eines Shellcode- Loader die EDR-Umgehung beeinflusst und wie der Entropie-Aspekt eines Shellcode-Loader verbessert werden kann.
- Erwerben Sie die Fähigkeit, systematisch Ihren eigenen indirekten Syscall-Shellcode-Loader zu schreiben oder fortgeschrittene Bypass-Shellcode-Loader mit Visual Studio zu erstellen.
- Erwerben Sie die Fähigkeit, Ihre Shellcode-Loader systematisch zu analysieren, zu debuggen und zu verstehen, indem Sie Schritt für Schritt angeleitet werden.

4 Was dieser Kurs nicht ist!

- Ein Patentrezept für die Umgehung der Endpunktsicherheit. Der Schwerpunkt liegt auf dem Erlernen der Funktionsweise von Umgehungstechniken wie indirekten Syscalls und deren Implementierung und Fehlersuche in einem Shellcode-Loader.
- Ein kompletter Entwicklerkurs (die Studenten schreiben keinen Code von Grund auf, sondern müssen auf der Grundlage des entsprechenden Playbooks den entsprechenden POC für jedes Kapitel fertigstellen und debuggen)
- Ein vollständiger Reverse-Engineering-Kurs
- Ein vollständiger Kurs über Windows-Internals

5 Wer sollte teilnehmen?

Der Kurs ist vor allem für Penetrationstester, Junior Red Teamers, Blue Teamers usw. interessant, die ihr Wissen über EDRs unter Windows vertiefen wollen, wie sie im Detail funktionieren und wie sie umgangen werden können. Der Kurs richtet sich auch an diejenigen, die mehr über Windows-Internals erfahren möchten, um die Funktionsweise von Endpunkt-Sicherheitsprodukten unter Windows besser zu verstehen, und die Erstellung, das Debugging und das Verständnis ihrer eigenen ausweichenden Shellcode-Loader erlernen möchten.

- Junior Penetration Tester und Junior Red Teamer
- Blue Teamer, Threat Hunter usw.
- Allgemeine Infosec-Profis oder Infosec-Anfänger, die mehr über die Grundlagen von Windows-Internals, EPPs/EDRs unter Windows, Malware-Entwicklung und Debugging usw. lernen möchten.

6 Kursplan und Zeitzonen

Die Schulung ist so konzipiert, dass sie sowohl als Online-Live-Schulung als auch als Live-Schulung vor Ort durchgeführt werden kann. Wenn die Schulung als Online-Live-Schulung durchgeführt wird, findet sie in mitteleuropäischer Zeit (MEZ) statt.

Der erste Durchlauf dieses Kurses als Online-Live-Schulung in English ist geplant für den **11. bis 14. November 2024 geplant**. Künftige Termine werden auf https://redops.at/en veröffentlicht. Der Kurs wird auch in deutscher Sprache angeboten, Termine werden noch bekannt gegeben.

7 Anforderungen an die Teilnehmer

Die folgenden Anforderungen können hilfreich sein, sind aber nicht zwingend:

- Grundlagen in C und x64 Assembly Language
- Grundlagen mit Visual Studio
- Grundlagen mit WinDbg und x64dbg

8 Hardware-Anforderungen

Um effektiv an diesem Kurs teilnehmen zu können, bringen Sie bitte Ihre eigene Hardware mit, die den folgenden Anforderungen entspricht:

- Notebook oder PC mit virtualisierungsfähiger(n) CPU(s)
- Mindestens 16 GB RAM (zur Ausführung von zwei Gast-VM)
- Mindestens 120 GB freier Festplattenspeicher

9 Software-Anforderungen

Vergewissern Sie sich, dass die folgende Software lokal auf dem Notebook installiert und konfiguriert ist, dass Sie für die Teilnahme am Workshop verwenden werden.

- Host-Betriebssystem Windows 10 Professional 64-bit
- Microsoft Remote Desktop Client (für den Zugriff auf den Host)
- Zoom-Client (um am Workshop teilzunehmen)
- Discord-Konto (für schriftliche Fragen während des Workshops)

10 LAB

Jeder Student hat Zugang zu seiner eigenen Laborumgebung, die aus den folgenden virtuellen Maschinen besteht.

- Windows 10 Entwicklung
- Kali Linux
- Windows 10 mit aktivierter Endpunktsicherheit (Offline-Modus)

10.1 Wichtige Informationen

Bitte beachten Sie, dass wir aus ethischen und rechtlichen Gründen keine kommerziellen C2-Frameworks, Endpunktsicherheitsprodukte mit Internet- oder Cloud-Konnektivität in der bereitgestellten Laborumgebung anbieten können.

Auch wenn es unter dem Gesichtspunkt der Umgehung nicht ideal ist, wird **während des gesamten Kurses** nur die **kostenlose Version des Metasploit-Frameworks** verwendet. Außerdem wird der Zugang zu einer Windows-VM mit installiertem Endpoint Security nur im Offline-Modus zur Verfügung gestellt.

Natürlich steht es jedem Kursteilnehmer frei, die selbst erstellten Shellcode-Loader in seinem eigenen Firmenlabor mit kommerziellen C2-Frameworks und Online-EPP/EDR zu testen. Sie können jedoch auch gerne Ihr bevorzugtes C2-Framework außerhalb der offiziellen LAB-Umgebung verwenden. Bitte beachten Sie jedoch, dass ich mit dem von Ihnen gewählten C2-Framework möglicherweise nicht vertraut bin und Sie während der Übungen nicht vollständig unterstützen kann.

11 Kursübersicht und Stundenplan

Endpoint Security Insights: Shellcode Loaders and Evasion ist ein **4-tägiger interaktiver** (Online-) Kurs, der sich an Sicherheitsexperten richtet. Meine Rolle als Kursleiter besteht darin, die wesentlichen Theorien und Konzepte für jedes Modul oder Kapitel vorzustellen, was etwa 20%-30% des Inhalts ausmacht. Die restlichen 70%-80% sind praktischen Übungen und der Beantwortung Ihrer Fragen gewidmet. In Bezug auf den Shellcode-Loader-Teil liegt der Schwerpunkt nicht nur auf der Erstellung des Loaders, sondern wir wollen auch jeden Loader debuggen und verstehen, um einen ausweichenden Shellcode-Loader zu erstellen.

11.1 Tag 1

Modul	Modul-Details	Zeitplan
Einführung in den Kurs	• Überblick über die zu behandelnden Themen. • Kursziele und Erwartungen	8:00 - 8:30
Windows Internals Grundlagen	• Verstehen der Windows NT-Architektur • Einführung in Win32-APIs	8:30 - 9:00
Einführung in die Endpunktsicherheit	• Einführung in die Endpunktsicherheit • Unterschiede zwischen Anti-Virus (AV) und EDR • Einführung in relevante Endpunkt-Sicherheitsmechanismen	9:00 - 9:30
Praktische Übung: EDR-Bewertung oder -Analyse	• Identifizierung der wichtigsten Komponenten und Erkennungsmechanismen von Endpunktsicherheitsprodukten	9:30 - 10:00
	Pause	10:00 - 10:15
Introduction to Shellcode-Loader	• Einführung in Shellcode-Loader • Verstehen des Konzepts der Shellcode-Loader • Verschiedene Arten der Ausführung von Shellcode / Prozessinjektionstechniken • Verschiedene Arten von Shellcode- Loader • Hauptkomponenten und Merkmale eines ausweichenden Shellcode- Loader	10:15 - 11:00
Praktische Übung: Erstellen eines	• Lernen Sie die Grundlagen von Shellcode-Loadern im Kontext von Win32-APIs	

Win32-API-Shellcode- Loader	• Umfassende Anleitung: Erstellen, Debuggen und Verstehen der inneren Funktionsweise Ihres Win32-API- Loader	11:00 - 11:45
Platzierung von Shellcode und Staging	• Erfahren Sie, wo und wie Sie Ihre Nutzdaten/Shellcode an verschiedenen Regionen speichern können. • Erfahren Sie, wie Sie Shellcode außerhalb Ihres Loader speichern können und welche Unterschiede, Vor- und Nachteile es im Vergleich zur lokalen Speicherung gibt.	11:45 - 12:15
	Mittagspause	12:15 - 13:00
Praktische Übung: Platzierung und Staging von Shellcode	• Spielen Sie mit der Platzierung Ihrer Nutzlast in Ihrem Win32-API-Loader an verschiedenen Regionen wie .text, .data usw. • Analysieren Sie die Unterschiede	13:00 - 13:30
Shellcode Obfuskierung	• Lernen Sie, wie Sie Shellcode via UUID, MAC usw. verschleiern können.	13:30 - 14:00
Praktische Übung: Shellcode Obfuskierung	• Spielen Sie mit verschiedenen Arten der Obfuskierung. • Obfuskieren Sie beispielsweise Ihren Shellcode via UUID und implementieren Sie ihn in Ihren Win32-API-Shellcode-Loader.	14:00 - 14:30
Verschlüsselung der Nutzdaten	• Erfahren Sie, wie Sie Ihre Nutzdaten verschlüsseln können, z. B. XOR, RC4 usw.	14:30- 15:00

	Pause	15:00 - 15:30
Zusammenfassung und Fragen und Antworten für Tag 1	• Lassen Sie uns Tag 1 zusammenfassen und alle Ihre Fragen zum Inhalt und zu den Unwägbarkeiten von Tag 1 stellen.	15:30 - 16:30

11.2 Tag 2

Modul	Details zum Modul	Zeitplan
Windows Internals Grundlagen	• Einführung in NTDLL, Native APIs und Systemaufrufe in Windows OS	8:00 - 8:30
Praktische Übung: Einheimische Funktionen	• Debugging nativer Funktionen oder nativer APIs	8:30 - 9:00
Praktische Übung: Erstellen eines nativen API-Loader	• Es ist an der Zeit, eine Stufe tiefer zu gehen und von Win32-APIs zu NTAPIs zu wechseln. • Umfassendes Walkthrough: Erstellen, Debuggen und Verstehen der inneren Funktionsweise Ihres NTAPI-Loader	9:00 - 10:00
	Pause	10:00 - 10:15
Einführung in EDR-User mode Hooking und direkte Syscalls	• Ein Einblick in die Endpunktsicherheit und die Bedeutung des User Mode Hooking • Was direkte Syscalls sind und warum sie EDRs umgehen können.	10:15 - 10:45
Praktische Übung: Erstellen eines direkten Syscall-Loaders und hartkodierter SSNs	• Auch hier ist es an der Zeit, eine Stufe tiefer zu gehen und von NTAPIs zu direkten Syscalls zu wechseln. • Umfassende Anleitung: Erstellen, Debuggen und Verstehen der inneren Funktionsweise Ihres Direct Syscall Shellcode Loaders	10:45 - 12:00

	Mittagspause	**12:00 Uhr - 13:00 Uhr**

Einführung in die Eventracing for Windows (ETW) und indirekte Syscalls	• Einführung in EDRs und ihre Beziehung zu Event Tracing for Windows (ETW). • Theoretische Grundlagen: Das Verständnis indirekter Systemaufrufe.	13:00 - 13:30
Praktische Übung: Erstellen eines indirekten Syscall-Loader mit fest kodierten SSNs	• Übergang: Übergang von direkten Syscalls zu indirekten Syscalls. • Umfassendes Walkthrough: Erstellen, debuggen und verstehen Sie das Innenleben Ihres indirekten Syscall-Loaders.	13:30 - 14:30
Praktische Übung: Erstellen eines indirekten Syscall-Loader mit dynamischem SSN-Abruf über APIs	• Verbessern Sie Ihre Möglichkeiten zur EDR-Umgehung durch Ihren Indirect Syscall Shellcode Loader. • Übergang von fest kodierten SSN-Methoden zum dynamischen SSN-Abruf über APIs • Umfassende Anleitung: Bauen, debuggen und verstehen Sie Ihren erweiterten Indirect Syscall Loader.	14:30 - 15:30
	Pause	15:00 - 15:30
Zusammenfassung und Fragen und Antworten für Tag 2	• Lassen Sie uns Tag 2 zusammenfassen und alle Ihre Fragen zum Inhalt und den Unwägbarkeiten von Tag 2 stellen.	15:30 - 16:30

11.3 Tag 3

Modul	Details zum Modul	Zeitplan
Windows Internals Grundlagen	• Einführung in den Process Environment Block (PEB)	8:00 - 8:30
Praktische Übung: Erstellen eines indirekten Syscall-Loader mit dynamischem SSN-Abruf über PEB walk	• Übergang vom dynamischen Abruf der SSN über APIs zum dynamischen Abruf der SSN über PEB/EAT. • Umfassendes Walkthrough: Erstellen, debuggen und verstehen Sie das Innenleben Ihres erweiterten indirekten Syscall- Loader.	8:30 - 9:30
	Pause	9:30 - 9:45
Praktische Übung: Indirekter Syscall-Loader und EDR-Hooks Teil 1	• Das Huhn-Ei-Dilemma: Indirekte Syscalls und EDRs User Mode Hooking Teil 1 → Halos Gate-Ansatz • Verbessern Sie Ihren indirekten Syscall-Shellcode-Loader weiter und implementieren Sie den Halos-Gate-Ansatz.	9:45 - 10:45
Praktische Anwendung: Indirekter Syscall-Loader und EDR-Hooks Teil 2	• Das Huhn-Ei-Dilemma: Indirekte Syscalls und EDRs User Mode Hooking Teil 2 → Tartarus Gate Approach • Verbessern Sie weiterhin Ihren Indirect Syscall Shellcode Loader und implementieren Sie den Tartarus Gate Ansatz.	10:45 - 11:45
Indirekte Syscalls vs. Unhooking im User mode	• Was sind die Unterschiede, Vorteile oder Nachteile zwischen (in)direkten Syscalls und Unhooking im Zusammenhang mit einem Shellcode-Loader?	11:45 - 12:15

	Mittagspause	12:15 - 13:00
Einführung in User mode Unhooking	• Verschiedene Arten des Unhooking via Software-Breakpoints • Was sind Software-Breakpoints und was sind Hardware-Breakpoints? • Was sind die Unterschiede, Vor- und Nachteile zwischen ihnen?	13:00 - 13:30
Praktische Übung: User mode Unhooking and ETW Patching	• Verbessern Sie weiterhin Ihren indirekten Syscall-Shellcode-Loader und implementieren Sie User-Mode Unhooking und ETW-Patching über Software-Breakpoints.	13:30 - 15:00
	Pause	15:00 - 15:30
Zusammenfassung und Fragen und Antworten für Tag 3	• Lassen Sie uns Tag 3 zusammenfassen und alle Ihre Fragen zum Inhalt und zu den Unwägbarkeiten von Tag 3 stellen.	15:30 - 16:30

11.4 Tag 4

Modul	Details zum Modul	Zeitplan
Einführung in das DLL-Sideloading	• Was ist DLL-Sideloading und wie kann es dazu verwendet werden, Endpunkt-Sicherheitsprodukte zu umgehen? • Was sind die Unterschiede, Vor- und Nachteile zwischen dem direkten Laden von Shellcode über PE und dem indirekten Laden von Shellcode über DLL-Sideloading?	8:30 - 9:00
Praktische Übung: Shellcode Loader DLL Sideloading	• Erfahren Sie, wie Sie mögliche DLL-Sideloads finden können. • Übergang von Ihrem portablen ausführbaren Shellcode-Loader zur Shellcode-Ausführung per DLL-Sideloading	9:00 - 10:00
	Pause	10:00 - 10:15
Praktische Übung: Shellcode Loader DLL Sideloading und Proxying	• Einführung in das DLL-Proxying. • Verbesserung der DLL-Sideloading-Funktionen durch den Übergang vom DLL-Sideloading zum DLL-Sideloading/Proxying	10:15 - 11: 00
Einführung in Entropie und Metadaten	• Was ist Entropie im Zusammenhang mit Shellcode-Loader und wie wirkt sie sich auf die EDR-Umgehung aus? • Welchen nützlichen Effekt könnte die Anwendung geeigneter Metadaten auf Ihren Shellcode im Zusammenhang mit der EDR-Umgehung haben?	11:00 - 11:30

Praktische Übung: Shellcode- Loader Entropie und Metadaten	• Lernen Sie die Prinzipien der Entropie kennen und erfahren Sie, wie Sie diese nutzen können, um die Unauffälligkeit und Effektivität Ihres Ladegeräts zu erhöhen. • Lernen Sie die Grundsätze der Verwendung nützlicher Metadaten kennen, um die Unauffälligkeit und Effektivität Ihres Loader zu erhöhen.	11:30 - 12:15
	Mittagspause	12:15 - 13:00
Praktische Übung: Shellcode- Loader und Zertifikate	• Erfahren Sie mehr über die Grundsätze der Verwendung nützlicher Zertifikate, um die Unauffälligkeit und Effektivität Ihres Loader zu erhöhen.	13:00 – 14:00
Praktische Übung: Malware/Kompilierungs-optimierung	• Erfahren Sie, wie Sie den Malware-Kompilierungsprozess in Visual Studio im Hinblick auf die Umgehung der Endpunktsicherheit verbessern oder optimieren können. • Verbessern Sie Ihren Shellcode-Loader mit der optimierten Kompilierung in Visual Studio	14:00 -15:00
	Pause	15:00 - 15:30
Zusammenfassung und Fragen und Antworten für Tag 4	• Lassen Sie uns Tag 4 zusammenfassen und alle Ihre Fragen zum Inhalt und zu den Unwägbarkeiten von Tag 4 stellen.	15:30 - 16:00
Fragen und Antworten	• Ihre Zeit, um Zweifel zu klären, Erkenntnisse auszutauschen und Antworten auf Fragen zu erhalten	16:00 - 17:00

11.5 Haftungsausschluss für Kursinhalte

Bitte beachten Sie, dass der Inhalt dieses Kurses möglicherweise aktualisiert und überarbeitet wird. Mit dem Fortschreiten des Kurses und neuen Erkenntnissen kann es zu Ergänzungen, Änderungen oder Verbesserungen des Materials kommen. Bitte seien Sie versichert, dass alle Änderungen vorgenommen werden, um Ihre Lernerfahrung zu verbessern und um sicherzustellen, dass der Kurs auf dem neuesten Stand bleibt. Wir bitten Sie um Ihr Verständnis für eventuelle inhaltliche Änderungen.

Um die Exklusivität und Interaktivität des Kurses zu gewährleisten, werden **keine Aufzeichnungen** gemacht. Wir bitten auch alle Kursteilnehmer, keine Aufnahmen mittels Screen-Recording oder ähnlichem zu machen. Ihr Engagement und Ihre Anwesenheit sind daher unerlässlich, um den Nutzen dieses außergewöhnlichen Kurses zu maximieren.

12 Benefits

Durch die Teilnahme am Kurs **Endpoint Security Insights** erhält jeder Teilnehmer folgende Informationen:

- Ein dynamischer **4-tägiger** Online-Kurs mit interaktivem Lernen (70-80% Praxisanteil)
- Zugang zu einem dedizierten LAB für jeden Teilnehmer mit installierter Endpoint Security (Offline-Modus)
- Umfassende Folien und detaillierte Playbooks für alle Module
- Zugang zu allen Workshop-POCs
- Ein 60-Tage-Fenster für den speziellen Workshop-Discord-Kanal
- Ein Abschlusszertifikat zur Anerkennung Ihrer Leistungen.

13 Training Preis

Entdecken Sie die Preisoptionen für den Workshop **Endpoint Security Insights**:

- Preis: 2499 € (exklusive Mehrwertsteuer)
- Begrenzt auf 8 Plätze

14 NDA

Bitte beachten Sie, dass jeder Teilnehmer vor Kursbeginn eine **Geheimhaltungsvereinbarung** (**Non-Disclosure Agreement,** NDA) unterzeichnen muss. Damit erklärt sich der Teilnehmer bereit, sein persönliches Kursmaterial nicht an Dritte weiterzugeben, alles Gelernte nur in einem ethischen Kontext zu verwenden und keine Daten/Informationen über das Gelernte oder den Kurs selbst an Anbieter von Sicherheitsprodukten weiterzugeben.

Ausführliche Informationen oder das ausdrückliche NDA-Dokument werden allen Teilnehmern vor dem Kurs zugesandt.

15 Häufig gestellte Fragen (FAQs)

Ist es zwingend erforderlich, das Non-Disclosure Agreement (NDA) vor Kursbeginn unterschrieben an die RedOps GmbH zu senden?

Ja, es ist obligatorisch, die unterzeichnete NDA für jeden Kursteilnehmer separat zu senden. Bitte senden Sie es mindestens 1 Woche vor Kursbeginn an office@redops.at.

Bekomme ich Kursunterlagen wie Folien und Handouts?

Wenn Sie sich für den Kurs anmelden, erhalten Sie eine mit Wasserzeichen versehene PDF-Kopie der Kursunterlagen. Diese PDF-Datei, die Ihren vollständigen Namen und Ihre E-Mail-Adresse enthält, wird Ihnen vor Beginn des Kurses elektronisch zugesandt. Die Weitergabe dieser Datei an Dritte ist strengstens untersagt und führt zum Ausschluss von zukünftigen Kursen.

Kann ich Sie vor Kursbeginn kontaktieren, damit ich mich vorbereiten kann?

Ja, natürlich können Sie das. Wenn Sie Fragen oder Bedenken haben, wenden Sie sich bitte an office@redops.at. Um den Prozess zu beschleunigen, erwähnen Sie bitte "Training Preparation" in der Betreffzeile Ihrer E-Mail. Im Allgemeinen ist es jedoch nicht notwendig, sich im Voraus vorzubereiten, da wir alle notwendigen Grundlagen im Kurs abdecken.

Welche Software benötige ich für die Teilnahme an dem Kurs?

- Host-Betriebssystem Windows 10 Professional 64-bit
- Microsoft Remote Desktop Client (für den Zugriff auf den Host)
- Zoom-Client (um am Workshop teilzunehmen)
- Discord-Konto (für schriftliche Fragen während des Workshops)

Wie erhalte ich Zugang zu den LABs, die mit diesem Kurs verbunden sind?

Der Zugang zu den Laboren erfolgt über RDP (3389), das über den Microsoft Remote Desktop Client von jeder unbeschränkten Internetverbindung aus aufgerufen werden kann.

Werden die Übungen nach dem Kurs online verfügbar sein?

Bitte beachten Sie, dass die Labore nur für die Dauer des Kurses verfügbar sind. Am Ende des Kurses werden die Labore deaktiviert. Sie erhalten jedoch alle Workshop-POCs und können diese in Ihrem eigenen Labor in Ihrem Unternehmen oder zu Hause weiter verwenden.

Kann ich mein bevorzugtes Command and Control (C2) Framework für die Laborübungen verwenden?

In der offiziell bereitgestellten LAB-Umgebung wird nur die kostenlose Version des Metasploit-Frameworks verwendet. Die bereitgestellten Shellcode-Loader-POCs sind grundsätzlich für die Verwendung mit verschiedenen C2-Frameworks konzipiert. Sie können jedoch gerne Ihr bevorzugtes C2-Framework außerhalb der offiziellen LAB-Umgebung verwenden. Bitte beachten Sie jedoch, dass ich mit dem von Ihnen gewählten C2-Framework möglicherweise nicht vertraut bin und Sie während der Übungen nicht vollständig unterstützen kann.

Bekommen die Teilnehmer am Ende des Kurses ein Zertifikat?

Alle Teilnehmer, die den Kurs abschließen, erhalten eine digitale Teilnahmebescheinigung.

Gibt es eine Mindestteilnehmerzahl für die Durchführung eines Kurses?

Ja, wir behalten uns das Recht vor, den Kurs zu stornieren, wenn nicht genügend Teilnehmer vorhanden sind. Wir werden Sie so schnell wie möglich informieren und Ihnen eine volle Rückerstattung oder einen Platz in einem späteren Kurs anbieten.

16 Urheberrecht

Die in diesem Workshop vorgestellten Konzepte, Methoden und Materialien wurden von der RedOps GmbH sorgfältig entwickelt und kuratiert. Alle zugehörigen Inhalte, einschließlich der grundlegenden Ideen und übergreifenden Konzepte, sind das exklusive geistige Eigentum der RedOps GmbH und entsprechend geschützt.

17 Kontakt

Wenn Sie oder Ihr Unternehmen Fragen zum Kurs haben, zögern Sie bitte nicht, mich zu kontaktieren. Ich beantworte Ihnen gerne alle Fragen, die Sie haben.

Website: https://redops.at/en

E-Mail: office@redops.at