الآلية الثلاثية للربط بين أمن المعلومات والتحليل الجنائي الرقمي

مريانا شحود العساف* د. ميساء دياب**

(الإيداع: 19 نيسان 2024 ، القبول: 19 آب 2024)

الملخص:

في ضوء النمو السريع الذي يشهده عالم التكنولوجيا الذي بات مرتبطاً بكافة مجالات الحياة أصبح موضوع حماية المعلومات من السرقة من أكثر المواضيع أهمية بالنسبة للمؤسسات والشركات الكبرى وذلك بسبب المبالغ الهائلة التي يمكن خسارتها في حال تم اختراق أنظمتهم، كما أن المحلل الجنائي الرقمي يعتمد بصورة كبيرة على المعلومات التي يستطيع جمعها من هذه الأنظمة لكشف المخترق.

ولهذا السبب قمنا في هذا البحث بابتكار آلية لحماية المعلومات وتسهيل وتسريع عمل المحلل الجنائي الرقمي في كشف من يحاول اختراق النظام وسرقة المعلومات.

تظهر النتائج التي حصلنا عليها كفاءة الآلية حيث تتميز بالمتانة لمقاومة الهجمات وكشف المهاجم وحماية المعلومات.

الكلمات المفتاحية: التحليل الجنائي الرقمي، الأدلة الرقمية، الجدار الناري، نظام كشف التسلل، نظام منع التسلل، المصيدة.

* طالبة في قسم تقانة المعلومات – كلية الهندسة المعلوماتية –الجامعة العربية الخاصة للعلوم والتكنولوجيا

** محاضر في الجامعة العربية للعلوم والتكنولوجيا اختصاص هندسة برمجيات

The Tripartite Mechanism for Linking Information Security and Digital Forensics

Mariana Alassaf* Dr. Maisa Diab**

(Received: 19 April 2024, Accepted: 19 Augast 2024)

Abstract:

In the light of the rapid growth in the world of technology, which has become linked to all spheres of life, the protection of information from theft has become one of the most important topics for large enterprises and companies because of the enormous amounts that can be lost if their systems are hacked. The digital forensic analyst also relies heavily on the information he can collect from these systems to detect the hacker.

For this reason, in this research, we devised a mechanism to protect information and facilitate the work of the digital forensic analyst in detecting those trying to penetrate the system and steal information.

The results obtained show the efficiency of the mechanism, as it is robust to resist attacks, attacker detection, and information protection.

Keywords: Digital forensics, digital evidence, firewall, intrusion detection system, intrusion prevention system, trap.

* Student in the Department of Information Technology – Faculty of Informatics Engineering – Arab Private University of Science and Technology

** Lecturer at the Arab University of Science and Technology specializing in software engineering

1- المقدمة:

التطور المستمر في عصرنا الحالي والانتشار الواسع للتكنولوجيا، والاعتماد عليها في كافة المجالات ما هو إلا سيف ذو حدَّين حيث رافق هذا التطور انفتاح العقل الإجرامي لطرق استغلال الثغرات التكنولوجية والاجتماعية مما أدى إلى بزوغ فجر الجريمة الإلكترونية. بمعنى آخر، انتشار الجرائم الإلكترونية بكثرة، سواء عن طريق الاستغلال التقني باستخدام الأدوات والأجهزة أو عن طريق الهندسة الاجتماعية لاستغلال الأشخاص والاحتيال عليهم وسرقة معلوماتهم.

من هنا جاءت الحاجة الملحَّة لإيجاد طرق وضوابط قانونية ضد مرتكبي هذه الجرائم، وهذا ما نسميه التحليل الجنائي الرقمي حيث يعتبر التحليل الجنائي الرقمي من العلوم الحديثة التي بدأ الاهتمام بها يتزايد في الآونة الأخيرة خصوصاً مع زيادة الاعتماد على الأجهزة الرقمية بمختلف أنواعها من الحاسبات وأجهزة الموبايل إلى غيرها من الأجهزة الرقمية الأخرى.

كما كانت الحاجة أيضاً لوجود أنظمة حماية قوية تحمي البيانات والمعلومات من المتسللين سواء من خلال شبكة الإنترنت أو من خلال الشبكة الداخلية للأنظمة باستخدام طرق الهندسة الاجتماعية وغيرها من الطرق الحديثة الأخرى.

يقترح البحث آلية جديدة تقاطع الحاجتين السابقتين لحماية مختلف الأنظمة من الاختراق وطريقة مختلفة عن الاعتيادية لجمع الأدلة الجنائيَّة الرقميَّة لضمان قبولها كدليل له صفة الاعتماد أمام المحاكم.

ونخلص في النهاية إلى نتائج توضح أهمية الآلية في الحماية وجمع الأدلة وأفضل التوصيات لضمان استخلاص المعلومات وإجراء تحقيقات سليمة ومعتمدة، وفي الوقت ذاته ضمان الحفاظ على أمن المعلومات.

2- هدف البحث وأهميته:

أولاً: تأمين الأنظمة ضد المتسللين وحماية بياناتها من التعرض للسرقة أو التخريب أو أي نوع من أنواع الهجمات.

ثانياً: التصدي للجرائم المعلوماتية، التي ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكية.

ثالثاً: العثور على الحقائق وإعادة خلق حقيقة الحدث ومعرفة الدافع الرئيسي وراء الجريمة وهوية مرتكب الجريمة، حيث يكشف الفاحص حقيقة حدث ما من خلال كشف بقايا الحدث التي تُركت على النظام وتُعرف هذه البقايا باسم القطع الأثرية artifacts ويشار إلى هذه البقايا أحياناً على أنها أدلة.

3- دراسة مرجعية:

- في هذه الورقة البحثية [1]، تمت مناقشة كيفية الحفاظ على الأدلة الرقمية، بحيث لا يتم المساومة عليها في أي وقت ويمكن تقديمها كدليل غير متغير أمام المحكمة. حيث يهتم الطب الشرعي الرقمي بتحديد الانتهاكات الأمنية والإبلاغ عنها والاستجابة لها كما يتعلق الأمر بكيفية الحصول على الأدلة الرقمية وتحليلها والإبلاغ عنها واستخدام المهارات التقنية واكتشاف آثار الجريمة الإلكترونية. كما أوضحت الطلب الكبير على مجال الطب الشرعي الرقمي بسبب التهديدات المستمرة بانتهاكات البيانات واختراق المعلومات. يتم استخدام الطب الشرعي الرقمي في تحديد الجرائم والقضاء عليها في أي جدل حيث يتم الاحتفاظ بالأدلة في الفضاء الإلكتروني. هذا هو استخدام تقنيات متخصصة للاسترجاع والتوثيق والتحليل الإلكتروني للبيانات. وتتناول الأدلة الجنائية الحاسوبية تحديد الأدلة الرقمية وحفظها، وتحليلها، وتوثيقها، وعرضها. حللت الورقة الاتجاهات الحالية التي تشمل الطب الشرعي لإنترنت الأشياء، والطب الشرعي السحابي، والطب الشرعي للشبكة، والطب الشرعي لوسائل التواصل الاجتماعي. أظهرت الأبحاث الحديثة مجموعة واسعة من التهديدات والهجمات الإلكترونية، والتي تتطلب من محققي الطب الشرعي وعلماء الطب الشرعي تبسيط العالم الرقمي. تقدم الأبحاث في الورقة رؤية واضحة للتحليل الجنائي الرقمي والتي يمكن أن تساعد بشكل كبير في تحقيقه.

- تستعرض هذه الورقة [2]، نُهج وتقنيات التحقق الأمني للنظم الحاسوبية على مختلف المستويات: من مستوى البرمجيات إلى مستوى الأجهزة المادية وتجري مقارنة بين مختلف المشاريع القائمة، استناداً إلى الأدوات المستخدمة والجوانب الأمنية التي يجري بحثها. نظراً لأن العديد من الأنظمة تتطلب مكونات الأجهزة والبرامج للعمل معاً لتوفير الحماية الأمنية الموعودة للنظام، فلا يكفي التحقق فقط من مستويات البرامج أو مستويات الأجهزة فقط بطريقة متعارضة. يسلط هذا البحث الضوء بشكل خاص على مستويات النظام التي تم التحقق منها من خلال المشاريع المختلفة الحالية ويقدم للقُرّاء أحدث التطورات في التحقق من أمان الأجهزة وأنظمة البرامج، ويقترب عدد قليل من النُهج من توفير نظام كامل للتحقق، ولا يزال هناك مجال كبير للتحسين.
- تهدف هذه المقالة البحثية [3]، إلى التحقيق في مفاهيم أمن الشبكة والمخاطر المحتملة واستراتيجيات الدفاع العملية. حيث تبدأ باستكشاف الأنواع المختلفة للهجمات الإلكترونية ومصادرها، وتسليط الضوء على الطرق المختلفة التي يستغل بها المهاجمون نقاط ضعف الشبكة. كما تدرس أسباب إغفال المنظمات في كثير من الأحيان لأمن الشبكة وعواقب عدم إعطائها الأولوية. وفهم تعقيد أمن الشبكة بشكل أفضل، وتصنف المخاوف الأمنية المختلفة باستخدام مثلث وكالة المخابرات المركزية (السرية والنزاهة والتوافر). هذا النهج يتيح تحديد مختلف مجالات الضعف وتأثيرها المحتمل على أمن الشبكة. بعد ذلك، ركزت الدراسة على أهم المفاهيم والخطوات الأساسية التي تنطوي عليها مختلف عمليات أمن الشبكات. والممارسات والنهج العملية التي يمكن للمنظمات اتباعها لتحسين أمن شبكاتها، بما في ذلك تنفيذ السياسات والإجراءات الأمنية، باستخدام طرق التشفير والمصادقة، وإجراء تقييمات أمنية منتظمة. من خلال التركيز على أهمية أمن الشبكة وتقديم إرشادات عملية حول كيفية دفاع المنظمات ضد الهجمات الإلكترونية.
- هدفت الدراسة [4]، إلى تسليط الضوء على التحديات المختلفة التي واجهها التحليل الجنائي الرقمي على مدى السنوات العشر الماضية وتم استخدام تقنيات أخذ العينات والعشوائية واقتراح تصنيف للتحديات حيث يندرج العدد الكبير منها إلى أربع فئات محددة جيداً وسهلة الفهم.

يصور التصنيف الأول التحديات التقنية التي يواجهها الطب الشرعي الرقمي مثل كميات هائلة من البيانات والعمر الافتراضي المحدود للوسائط الرقمية والتقنيات والأجهزة الناشئة وتعقيد الجرائم الرقمية وغيرها الكثير، ويلي ذلك التحديات المتعلقة بالأنظمة القانونية و/أو إنفاذ القانون مثل مقبولية أدوات وتقنيات الطب الشرعي الرقمي والخصوصية وعدم كفاية الأدلة للمحاكمة الجنائية أو المدنية القانونية، وفي التصنيف الثالث التحديات المتعلقة بالموظفين كنقص وجود موظفي الطب الشرعي الرقمي المؤهلين (التدريب والتعليم)، وأخيراً التحديات التشغيلية مثل عدم وجود عمليات وإجراءات موحدة والتدخل اليدوي الكبير والتحليل. مع ذلك، فإن الفئات الفرعية المختلفة للتحديات المقدمة في كل صنف تركز بشكل أكبر على المجالات التي يمكن، على سبيل المثال، أخذها في الاعتبار عند تطوير مناهج ومواد تعليمية جديدة لبرامج البكالوريوس المختلفة، أيضاً كمشاريع بحثية للدراسات العليا. يمكن أن تكون الفئات الفرعية مفيدة أيضاً عند تطوير أدوات الطب الشرعي الرقمي الديناميكية التي تركز على معالجة تحديات الطب الشرعي الرقمي المحددة.

مع التطورات والبحوث المستمرة في الطب الشرعي الرقمي، يمكن أن يكون التصنيف ذا قيمة لمطوري الأدوات في تقييم مدى قدرة أدوات الطب الشرعي الرقمية الحالية والجديدة على مواجهة التحديات المحددة.

- ركزت الدراسة [5]، على جدران الحماية التقليدية، وتطورها، وقضايا الأمن والسياسات المختلفة ومفهوم جدار الحماية الموزع. جدار الحماية هو جهاز أو نظام برمجي أو مجموعة من الأنظمة (جهاز توجيه أو وكيل أو بوابة) مصمم للسماح أو رفض نقل الشبكة بناءً على مجموعة من القواعد واللوائح الأمنية لفرض التحكم بين شبكتين لحماية الشبكة "الداخلية" من "الخارج"، ويمكن أن يكون جدار الحماية أيضاً جهازاً أو برنامجاً يمكن تشغليه على كمبيوتر مضيف

آمن، وفي كلتا الحالتين يجب أن يكون لديه واجهتين للشبكة، واحدة للشبكة التي يهدف حمايتها، وواحدة للشبكة التي يتعرض لها.

كان من السهل دعم وصيانة جدران الحماية المبكرة لأنها كانت مقيدة بعدد أقل من خدمات الإنترنت المتاحة في ذلك الوقت. لقد تغير السيناريو اليوم رأساً على عقب، حيث أن المتطلبات اليوم ليست فقط الوصول الآمن إلى Telnet وFTP وSMTP وUSENET؛ بدلاً من ذلك، يرغب الأشخاص اليوم في الاتصال ب WWW ومشاركة الملفات والأخبار والموسيقى وعقد مؤتمرات الفيديو الصوتية والوصول إلى قاعدة البيانات وما إلى ذلك.

جدار الحماية الموزع (Distributed Firewall) هو آلية لإنفاذ سياسة أمن مجال الشبكة من خلال استخدام لغة السياسة، وخطة توزيع السياسات التي تمكن من مراقبة السياسات من نقطة مركزية، مما يتيح تحديد أي عضو في مجال سياسة الشبكة حيث يؤمن الشبكة من خلال حماية نقاط نهاية الشبكة المهمة، بالضبط حيث يريد المتسللون الاختراق. يقوم بتصفية حركة المرور في كل من الإنترنت والشبكة الداخلية. فهي توفر قابلية غير محدودة للتطوير وتتغلب أيضاً على مشكلة نقطة الفشل التي يمثلها جدار الحماية المحيطي.

يلعب جدار الحماية دور الحاجز أمام أنواع مختلفة من الهجمات، وإبطاء انتشارها، وتعزيز أجهزة الكمبيوتر المتصلة بالشبكة من التدخلات العدائية المتعمدة التي قد تشمل السرية أو تؤدي إلى تلف البيانات أو رفض الخدمة أو غيرها من هجمات الشبكة.

لكن لا يزال هناك العديد من المشكلات الأمنية التي لا يستطيع جدار الحماية التحكم فيها، حيث يعمل جدار الحماية كجسر بين شبكتين LAN، ولكنه غير قادر على التعامل مع التهديدات مثل الموظفون الضارون حيث تعتبر جدران الحماية سيئة للغاية في فحص وتحليل إدراك الأشخاص، كما أن العديد من هجمات الإنترنت يمكنها أن تخدع جدران الحماية التقليدية.

- درسَتْ الورقة البحثية [6]، الفرق بين نظام كشف التسلل IDS ونظام منع التسلل IPS حيث يقوم IDS بإنشاء تنبيهات فقط إذا مرت حركة مرور غير طبيعية في حركة مرور الشبكة، فسيكون ذلك إيجابياً كاذباً أو سلبياً كاذباً، مما يعني أن IDS يكتشف الأنشطة الضارة فقط، ولكن لا يتم أخذ أي اجراء بشأن تلك الأنشطة، في حين أن IPS لديه ميزة الكشف والوقاية من خلال الإجراء التلقائي أو اليدوي المتخذ بشأن تلك الأنشطة مثل إسقاط الاتصالات أو حظرها أو إنهائها.

تم تطوير IDS وIPS في الأصل لمعالجة المتطلبات غير المتوفرة في معظم جدران الحماية ففي أمان الشبكة يخدم جدار الحماية الغرض الرئيسي من الأمان، ولكنه يسمح بحركة مرور الشبكة على منافذ محددة إما داخل الشبكة أو خارجها. لا تستطيع جدران الحماية اكتشاف حركة مرور الشبكة المرسلة على منفذ معين أو منفذ شرعي أو جزء من محاولات التطفل والهجمات.

إن IDS وIPS عبارة عن قائمة من الوظائف المشابهة مثل فحص الحزم، وتحليل الحالة، وإعادة تجميع مقطع TCP، والفحص العميق للحزم، والتحقق من صحة البروتوكول، ومطابقة التوقيع.

4- مفاهيم عامة:

التحليل الجنائي الرقمي: هو العلم الذي يجمع بين العلوم الشُرطية الجنائية وعلوم الحاسب والشبكات بهدف استخراج الأدلة الرقمية من أجهزة الحاسب وأجهزة الشبكة والوسائط الرقمية [7] [16].

الأدلة الرقمية: هي الأدلَّة المستخلصة من خلال تحليل المعلومات الموجودة على الأنظمة الحاسوبيَّة بالطرق العلميَّة والتي يمكن استخدامها والاستفادة منها كدليل قضائي في إثبات أو نفي جريمة معلوماتية أمام المُحاكم [15].

الجدار الناري: عبارة عن جهاز أو برنامج يتم وضعه بين أجهزة الشبكة والوسط الخارجي ويتم إعداده بمجموعة من القواعد للسماح لاتصالات معينة ومنع اتصالات أخرى [12].

نظام كشف التسلل IDS: هي أجهزة أو برامج تقوم بكشف السلوك الخبيث ومحاولات المهاجمين للوصول غير المصرح به إلى الشبكة أو الجهاز للقيام بأعمال مؤذية أو سرقة المعلومات [6] [17].

نظام منع التسلل IPS: هي أجهزة أو برامج قادرة على كشف التهديدات ومنع حزم البيانات الخبيثة وهي تُعد بنمط المراقبة عند نشرها ضمن الشبكة [6] [17].

5- مفهوم التحليل الجنائي الرقمي:

التحليل الجنائي الرقمي هو استخدام لتقنيات العلم والتكنلوجيا في عمليات التحقيق الجنائي للقضايا المخالفة للقانون، وتتضمن فحص الجهاز أو المنظومة المعلوماتية وتحليل العمليات واسترجاع البيانات والملفات من أجل الحصول على دليل رقمي يستخدم في التحقيقات القانونية [7].

في اكتشاف الطب الشرعي، قدم Wietse Venema وDan Farmer الحجة القائلة بأن الفاحص يعمل في بعض الأحيان كعالم آثار رقمي، وفي أوقات أخرى، جيولوجي رقمي حيث أن طريقة التحليل الجنائي الرقمي تعتمد على افتراضات ومن ثم فحص كل فرضية وتسجيل النتيجة، الفرضية عبارة عن سؤال ويجب الإجابة عليه [14].

مثال في الجرائم المعلوماتية فإن المحقق يفترض بأن المتهم قام بحذف الملفات ويتم التحقق من هذه الفرضية من خلال استعادة الملفات المحذوفة باستخدام أدوات معينة فأساس عملية الاستجواب يعتمد على الأدلة المكتشفة [13].

عملية التحليل الجنائي الرقمي يجب أن تتم وفق معايير واجراءات قانونية معتمدة من قبل المحكمة وأهم هذه الإجراءات هو المحافظة على الأدلة الرقمية التي تم اكتشافها بدون أي تعديل أو تخريب وتوثيق كامل العمليات من لحظة الوصول لمكان الجريمة والعمليات التي تمت في مخبر التحليل الجنائي الرقمي لحين وصول الدليل الرقمي إلى المحكمة [16] [7].

التحليل الجنائي الرقمي يمكن تطبيقه على أي جهاز يقوم بإرسال أو استقبال أو تخزين البيانات مثل أجهزة الموبايل وأجهزة الربط الشبكي كالموجهات والمبدلات (switch–router) وأجهزة الحاسب والأجهزة اللوحية tablets [15].

التحليل الجنائي الرقمي وبشكل مماثل للتحليل الجنائي العادي (تحليل DNA وفحص الطلقات النارية) الهدف منه هو الحصول على دليل يمكن أن يستخدم في المحكمة [7].

يجب على المحقق الرقمي أن يقوم بتوثيق وبشكل صريح وواضح كل دليل رقمي محتمل وكيفية الوصول لهذا الدليل [16].

6- منهجية التحليل الجنائي الرقمي:

أحد المبادئ الذي غالباً ما يتم مناقشته في علم الطب الشرعي هو مبدأ تبادل لوكارد Locard's principle، حيث يفترض هذا المبدأ أن "مرتكب الجريمة سيترك شيئاً في مسرح الجريمة أو سيأخذ شيئاً معه، وكلاهما يمكن استخدامه كدليل جنائي". على سبيل المثال، إذا قام أحد الأفراد بالتصفح من حاسوبه الشخصي إلى موقع ويب، فإن خادم الويب أو جدار حماية تطبيق الويب قد يسجل عنوان IP الخاص بالفرد ضمن سجل التجميع. قد يقوم موقع الويب أيضاً بإيداع ملف تعريف ارتباط على الكمبيوتر المحمول الخاص بالفرد [7] [16].

7- مقارنة:

طريقة الآلية الثلاثية	طرق الحماية	طرق التحليل الجنائي الرقمي
تجمع بين مزايا طرق الحماية وطرق التحليل الجنائي الرقمي واستخدام مصيدة تحوي بيانات وهمية.	استخدام الجدار الناري وأجهزة كشف التسلل وأجهزة منع التسلل بالإضافة لبرامج فحص الفيروسات.	استخدام أدوات مخصصة للتحليل والفحص.
يمكنها منع المتسلل بالإضافة لكشف هويته.	يمكن للمتسلل تجاوز هذه الطرق باستخدام أدوات جاهزة في نظام الكالي أو بتطوير أكواد خبيثة يصعب كشفها.	لا تمنع المتسلل إنما تحاول كشف هويته.

8- بيئة العمل والتقنيات المستخدمة:

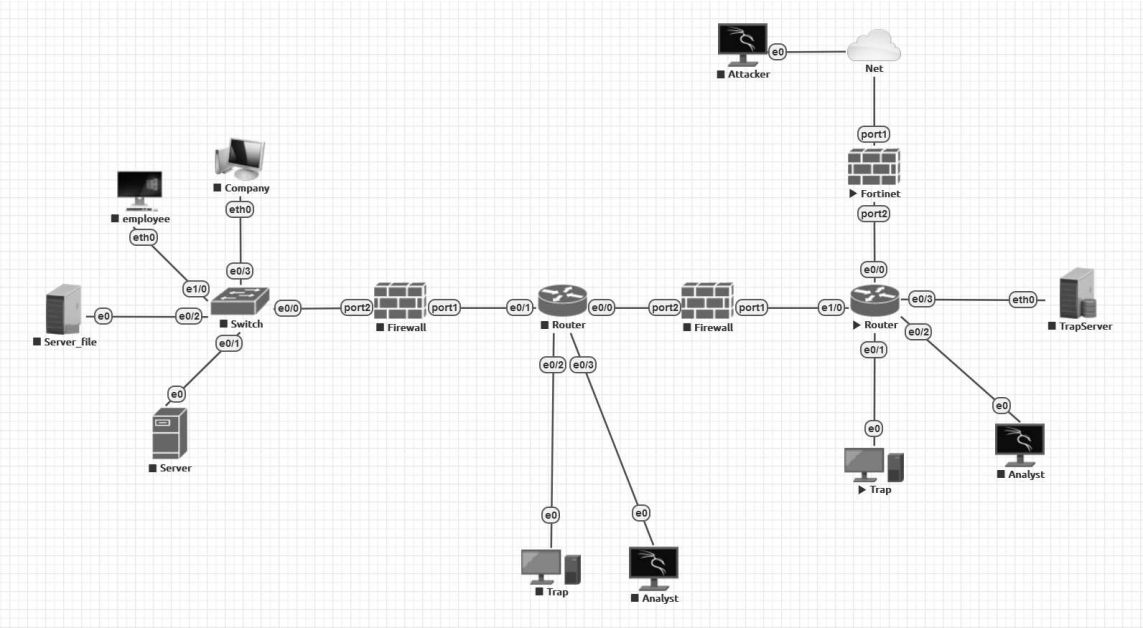
قبل البدء بالعمل مع الأدوات والتقنيات من المهم أن نقوم بإعداد بيئة آمنة لعمليات الاختبار حيث سنقوم بتطبيق عملي للاختراق وهناك العديد من الأسباب التي يجب أن تؤخذ بعين الاعتبار.

1. EVE-NG: هو بيئة محاكاة لمحترفي الشبكات والحماية، يعتبر من أقوى المنصات التي يحتاجها خبراء الشبكات والحماية لتجربة واختبار وإعداد أجهزة الشبكة وأجهزة الحماية بأنظمة تشغيل حقيقية.
2. Bitvise SSH Client: يوفر خادم Bitvise Secure Shell (SSH) إمكانية تسجيل الدخول عن بُعد الآمنة لمحطات العمل والخوادم. يستخدم النَّسخ الآمن (SCP) وبروتوكول نقل الملفات الآمن (SFTP) لنقل الملفات الآمن.
3. UltraVNC Viewer: برنامج قوي وسهل الاستخدام ومجاني يمكنه عرض شاشة جهاز كمبيوتر آخر (عبر الإنترنت أو الشبكة) على شاشتك الخاصة. يسمح لك البرنامج باستخدام الماوس ولوحة المفاتيح للتحكم في الكمبيوتر الآخر عن بُعد.
4. VMware Workstation 16 Player: هو تطبيق افتراضي مبسط لسطح المكتب يقوم بتشغيل نظام تشغيل آخر على نفس الكمبيوتر دون إعادة التشغيل. يوفر واجهة مستخدم بسيطة ودعم نظام تشغيل لا مثيل له وإمكانية النقل عبر نظام VMware البيئي وسنستخدمه لتشغيل eve-ng [20] [21].
5. النظام الهدف (المصيدة): Window 7 ultimate x64
6. النظام المهاجم: kali-linux وهو عبارة عن توزيعة من نظام التشغيل Linux مخصصة لاختبار الاختراق والتدقيق في السلامة المعلوماتية ويحوي على أفضل الأدوات المستخدمة في عملية اختبار الاختراق أو الهاكر الأخلاقي وهو الوريث لنظام BackTrack. الكالي مبني على توزيعة ديبان Debian GNU/Linux [18] [19].
7. الأداة nmap: هي الأداة الأكثر شهرة للقيام بعملية فحص المنافذ port scanning وهي موجودة بشكل تلقائي ضمن الكالي [8].

8. الأداة Metasploit framework: أداة استغلال مفتوحة المصدر تؤمن هيكلية منظمة لعملية الاستغلال ويسمح للعامة باستخدام وتطوير ومشاركة الاستغلال مع بعضهم البعض [9].
9. الأداة msfvenom: أداة خاصة بال Metasploit تسمح لنا بخلق shellcode (كود خبيث يسمح لنا بالحصول على سطر الأوامر في الجهاز الهدف) والتي يمكن أن تستخدم من أجل اختبار الحماية في النظام الهدف [9].
10. الأداة Meterpreter: أداة رائعة للتلاعب أو التحكم بالنظام الهدف عن بعد وتحوي على مجموعة من التعليمات مثل سحب الهاش الخاص بكلمات السر وجمع البيانات الحساسة من النظام الهدف [22].
11. أجهزة مرتبطة بالنظام والشبكة الداخلية (أجهزة توجيه وتبديل وحواسيب وسيرفرات وجدران نارية).

9- السيناريو العملي للآلية الثلاثية المقترحة:

سنحاكي في هذه الآلية نظام أمني كما في الشكل التالي وهذه الآلية تتكون من ثلاث مراحل حيث ستكون المرحلة الأولى لجذب انتباه المخترق إليها وبذلك نُشتِتُه عن المرحلة الثانية وهذا الأسلوب يستخدمه علماء النفس في جذب انتباهك لشيء معين لكي لا تنتبه للشيء الآخر، أما المرحلة الثالثة فهي مرحلة وقوع المتسلل في المصيدة وهي المرحلة الخاصة بالمحلل الجنائي الرقمي لكشف المتسلل وإدانته.

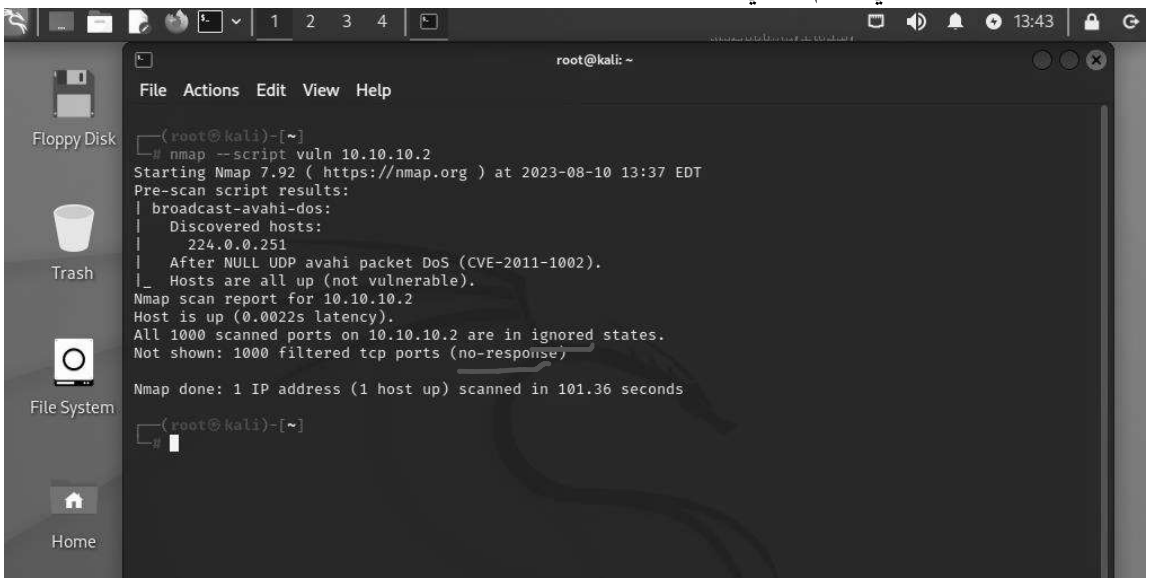


الشكل رقم (1): محاكاة لنظام أمني باستخدام الآلية الثلاثية

يجدر بنا التنويه أن هذه المحاكاة سوف تتم ضمن سيناريو معين لتوضيح الفكرة والهدف منها، ولكن يمكننا بالتأكيد محاكاة سيناريوهات أخرى مع تفاصيل أكثر والوصول لذات النتيجة أي أنَّ المبدأ المتبع هنا "مهما تعددت الطرق فإن الهدف واحد".

المرحلة الأولى: محاولة أحد المتسللين من خارج شبكة النظام (الإنترنت) اختراق الجدار الناري

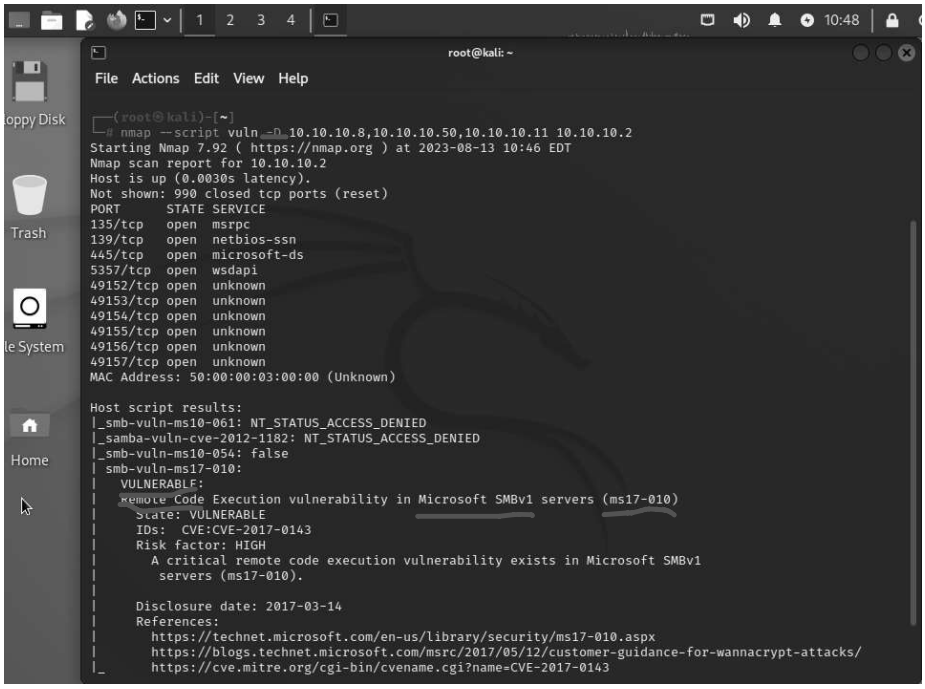
يتم في هذه المرحلة فحص المنافذ من قبل المتسلل باستخدام الأداة nmap عن طريق استخدام سكريبت جاهزة (أكواد برمجية مخصصة للقيام بمهمة معينة والحصول على معلومات عن الهدف حيث يوجد عدد كبير منها في نظام الكالي في المسار usr/share/nmap/scripts وسوف نستخدم في مثالنا السكريبت vuln لاكتشاف الثغرات المصاب بها النظام الهدف) من خلال كتابة التعليمة التالية في سطر الأوامر في نظام الكالي الخاص بالمهاجم وذلك بعد حصوله على عنوان IP لجهاز داخل الشركة عن طريق عملية الاستطلاع وجمع المعلومات أو الهندسة الاجتماعية أو عن طريق استخدام تقنيات المراقبة لحركة البيانات على الشبكة أو باستخدام الأدوات المخصصة لهذه العملية في نظام الكالي مثل خدمة whois أو ping أو Host وغيرها:



الشكل رقم (2): فحص ثغرات النظام

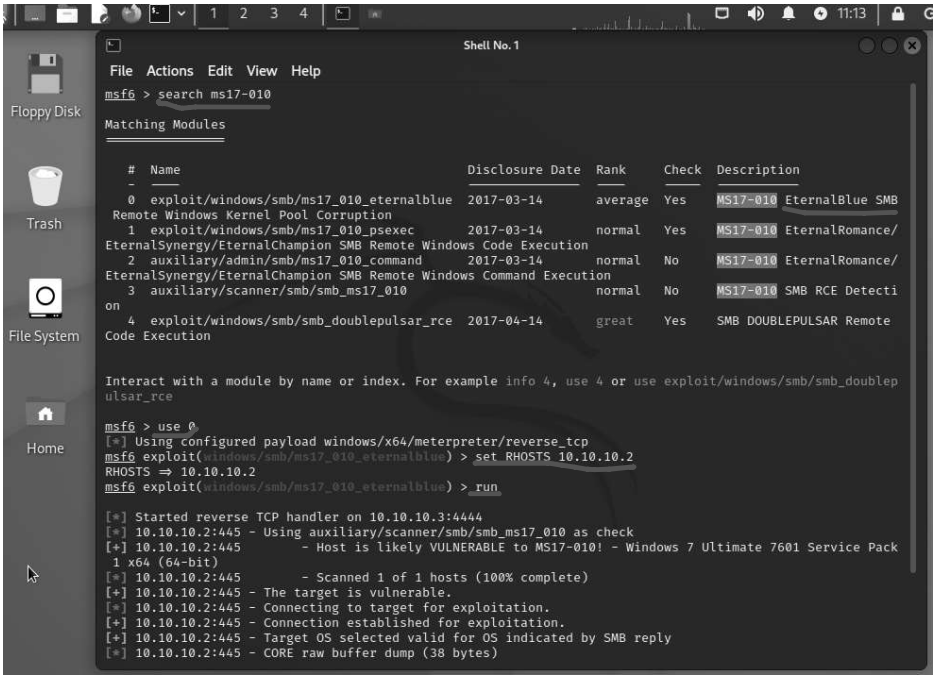
يمكننا من خلال التعليمة السابقة على IP الجهاز الهدف ملاحظة أنَّه تمَّ تجاهل عمليه الفحص وفلترة الحزم المرسلة مما يدل على وجود نظام حماية وهو الجدار الناري، ولكن هذا لا يمنع المهاجم من اتباع طريقة أخرى تمكّنه من التغلب على وجود الجدار الناري وهي بتعديل التعليمة السابقة لتصبح على النحو التالي (الشكل 3) وذلك من خلال عملية تبديل بين عدة عناوين IP الأمر الذي يسمح بتجاوز آلية عمل الجدار الناري (القائمة على وجود مرور لنفس عنوان الIP على عدة منافذ).

من خلال عملية فحص المنافذ في الشكل التالي نلاحظ وجود ثغرة في النظام الهدف وهي ثغرة أمنية موجودة في أنظمة التشغيل ويندوز وتحديداً في بروتوكول SMB وتم استغلالها من قبل العديد من البرامج الخبيثة أشهرها برنامج الفدية WannaCry. وهذه الثغرة تسمح للمهاجم بتنفيذ أوامر على الجهاز الهدف.

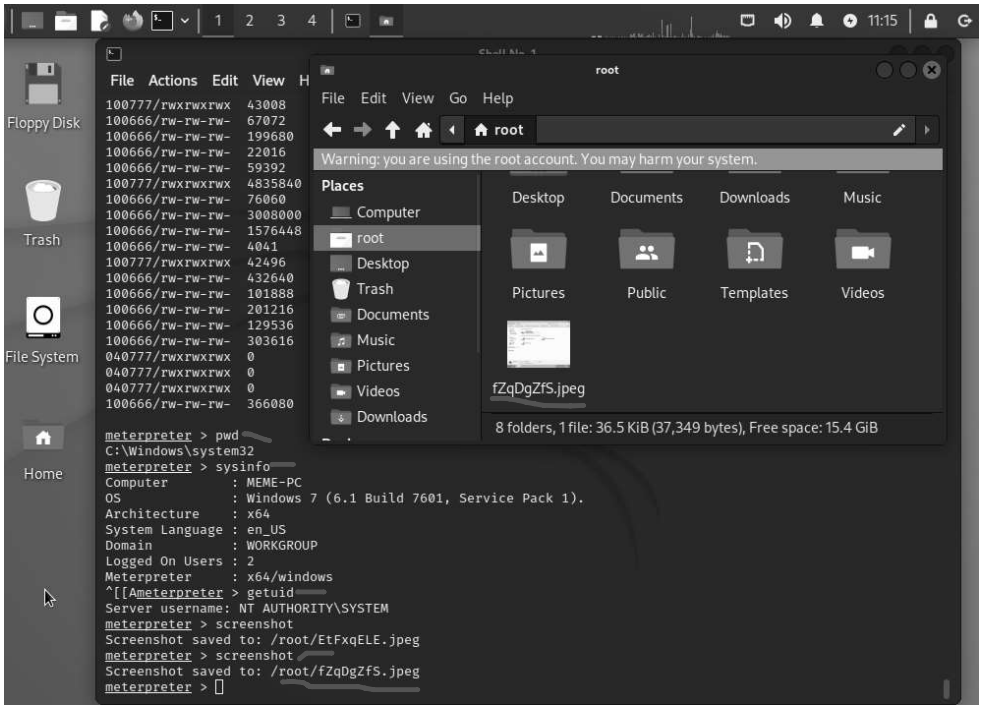


الشكل رقم (2): تجاوز نظام الحماية والكشف عن ثغرات النظام

يقوم المهاجم بعد ذلك باستخدام الأداة Metasploit للبحث عن الثغرة ms17–010 التي حصلنا عليها من عملية فحص المنافذ في الشكل السابق واستغلال هذه الثغرة وتحديد IP الجهاز الهدف RHOST وبدء عملية الاستغلال run كما الشكل (4)، والحصول على سطر الأوامر في الجهاز الهدف كما في الشكل (5).



الشكل رقم (4):البحث عن الثغرة ms17–010 واستغلالها لاختراق الجهاز الهدف



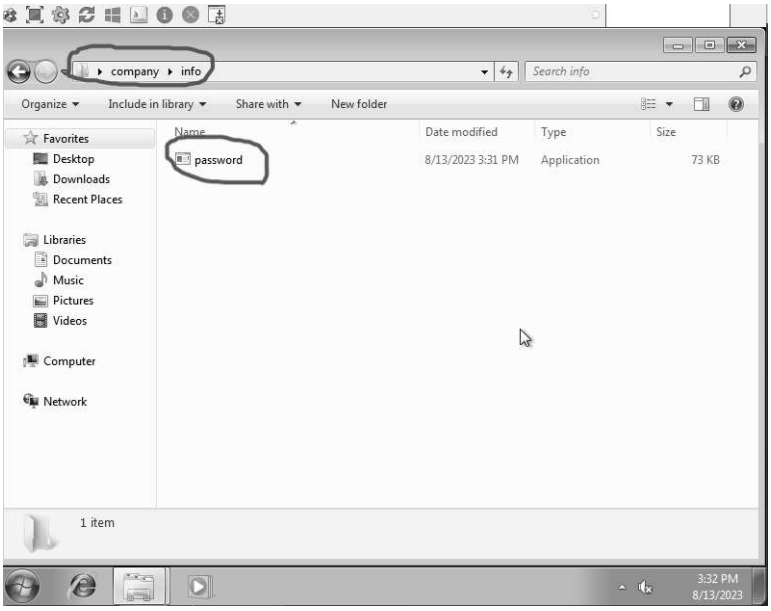
الشكل (5): الحصول على سطر الأوامر في الجهاز الهدف

نلاحظ في الشكل (5) أنَّ المهاجم استطاع اختراق الجهاز الهدف وإنشاء جلسة meterpreter للحصول على سطر الأوامر في الجهاز الهدف، واستخدم التعليمة pwd لعرض المسار الحالي في الجهاز الهدف، أيضاً التعليمة sysinfo لعرض معلومات عن الجهاز ولدينا التعليمة getuid التي يمكن من خلالها الحصول على صلاحيات النظام وهي أعلى من صلاحيات المستخدم العادي، كما قام بأخذ لقطة شاشة وغيرهم الكثير مما يمكنه تنفيذهم.

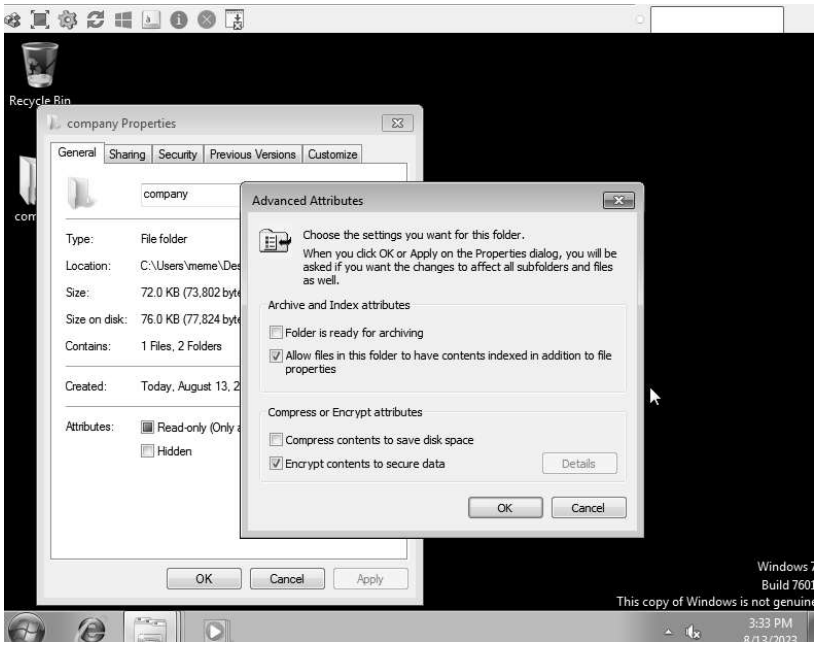
ملاحظة: في هذه المرحلة من الآلية يمكننا استخدام عدة طرق للوصول إلى النظام الهدف و تجاوز أنظمة الحماية المستخدمة مثل عملية تجزئة البيانات المرسلة باستخدام f– مع الأداة nmap أو باستخدام Shellcode، كما يمكننا الحصول على IP الجهاز الهدف بأساليب مختلفة وباستخدام أدوات مختلفة.

المرحلة الثانية: سرقة المعلومات المشفرة من الجهاز الهدف (المصيدة)

بعد تجاوز المهاجم نظام الحماية والوصول للجهاز الهدف ظناً منه أنه سيحصل على ما يريده فإننا في هذه الحالة سنجعله يحصل على ما يريده حتى نحصل نحن على ما نريد، لذلك سنقوم بتزييف كمية كبيرة من البيانات وكذلك سنستخدم سيرفر يحوي أيضاً على بيانات مزيفة وعلينا الحرص في هذه المرحلة على تزييف البيانات بحيث تبدو كأنها بيانات حقيقية تماماً بدءاً من حجمها ونوعها وما تمثله وصولاً إلى أسماء الملفات كاستخدام اسم ملف password لجذب المهاجم له كما في الشكل (6)، وبعد الانتهاء من عملية تزييف البيانات يجب أن يتم تشفيرها (الشكل 7) لزيادة صعوبة الحصول عليها وأيضاً حتى نجبر المهاجم على أخذ هذه البيانات ليتمكن من فك تشفيرها على جهازه حيث أنّه في الواقع سيبدو أنه قد حصل على مبتغاه لكنه لم يحصل سوى على معلومات وهمية لا يمكنه حتى الاستفادة منها، بل على العكس تماماً ستكون هذه المعلومات هي السبب في كشف هويته.



الشكل (6): تزييف الملفات لجذب المهاجم



الشكل (7): تشفير الملفات

يمكننا أيضاً تشفير البيانات باستخدام أحد البرامج المخصصة لهذا الغرض.

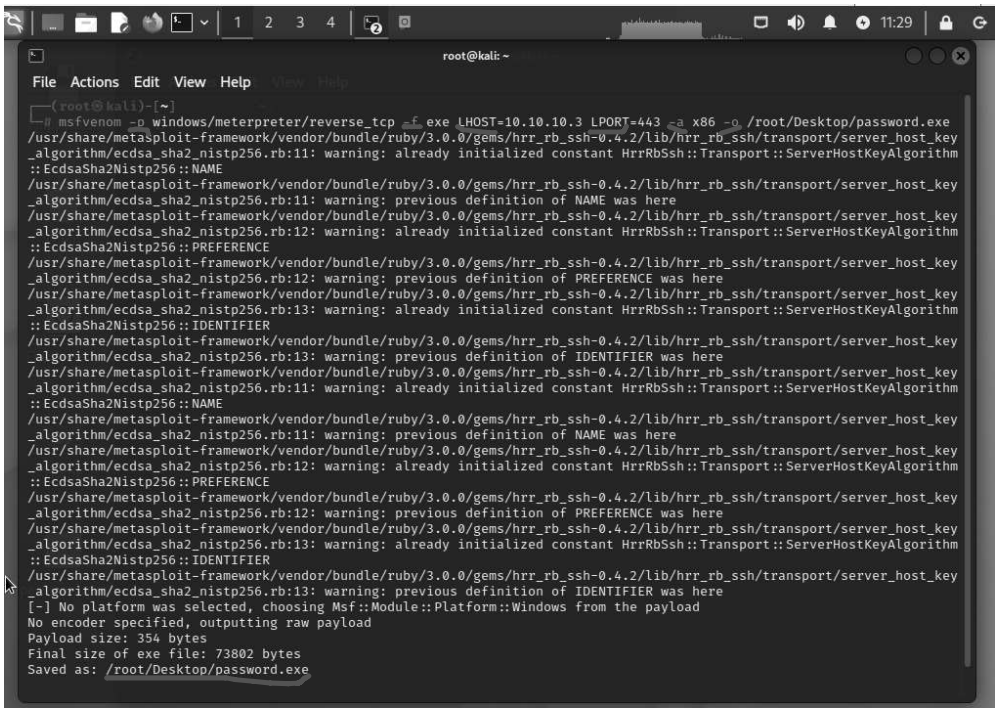
المرحلة الثالثة: فك تشفير المعلومات المسروقة والوقوع في المصيدة

هذه المرحلة هي الأهم في الآلية الثلاثية حيث من خلالها يمكن للمحلل الجنائي الرقمي أن يقوم بالكشف عن هوية المهاجم والحصول على أكبر قدر من المعلومات التي تخصه.

في حين أننا قمنا بتشتيت المهاجم عن طريق نظام الحماية المستخدم في المرحلة الأولى وتجهيز المصيدة في المرحلة الثانية عن طريق تزييف البيانات فإننا في هذه المرحلة وأثناء انشغال المهاجم بفك تشفير الملفات التي حصل عليها سنقوم بتجهيز الطريق الذي يمكننا من الوصول لجهازه وذلك من خلال خلق ملف خبيث shellcode وحقنه في ملف ال

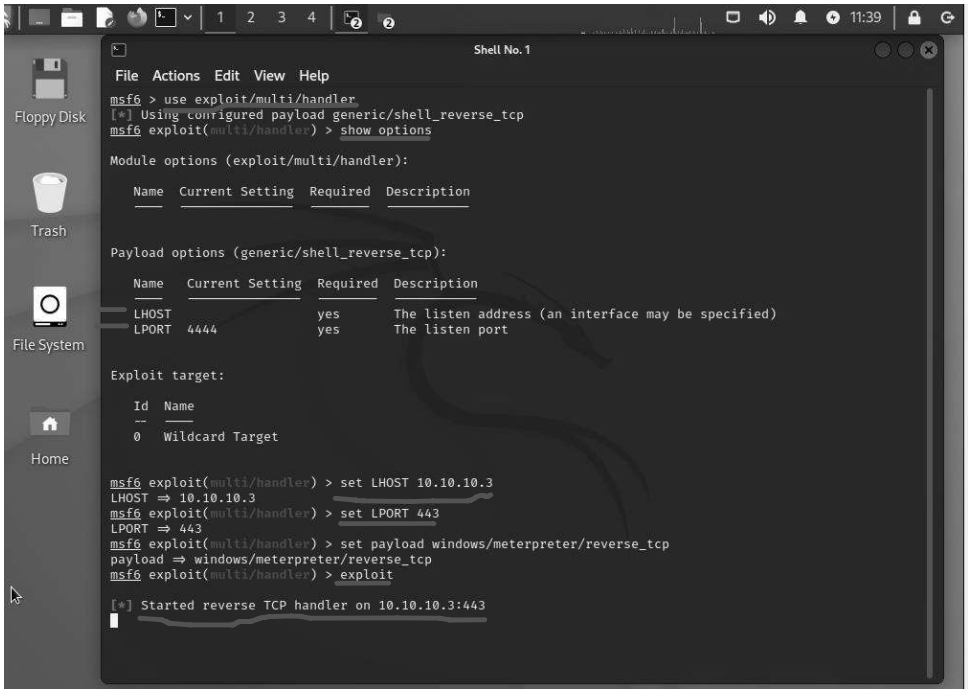
password الذي رأيناه في الشكل (6) حيث أنَّه عندما يقوم المهاجم بفتحه لرؤية البيانات فإن الملف سيقوم بعملية اتصال عكسي إلى جهاز المحلل وذلك وفق الخطوات التالية:

1. استخدام الأداة msfvenom لخلق الملف الخبيث (الشكل 8) مع تحديد ال payload المستخدم (الكود البرمجي أو الطريقة التي تقوم بإيصالنا إلى الاستغلال) باستخدام p– وهو يقوم بإنشاء جلسة meterpreter لاستقبال اتصال عكسي reverse_tcp ثم استخدمنا الخيار f– لتحديد نوع الملف والذي يجب أن يتوافق مع النظام الموجود على الجهاز المصيدة حتى لا يشك المهاجم به و الخيار LHOST لتحديد عنوان الIP لجهاز المحلل لاستقبال الاتصال العكسي عليه، ثم الخيار LPORT لتحديد المنفذ وقد اخترنا 443 لأنه المنفذ الخاص ب https مما يعني حركة بيانات كبيرة عليه نتيجة تصفح الإنترنت وبالتالي صعوبة كشف المهاجم لنا ثم الخيار a– لتحديد المعمارية و o– لتحديد مسار حفظ الملف.



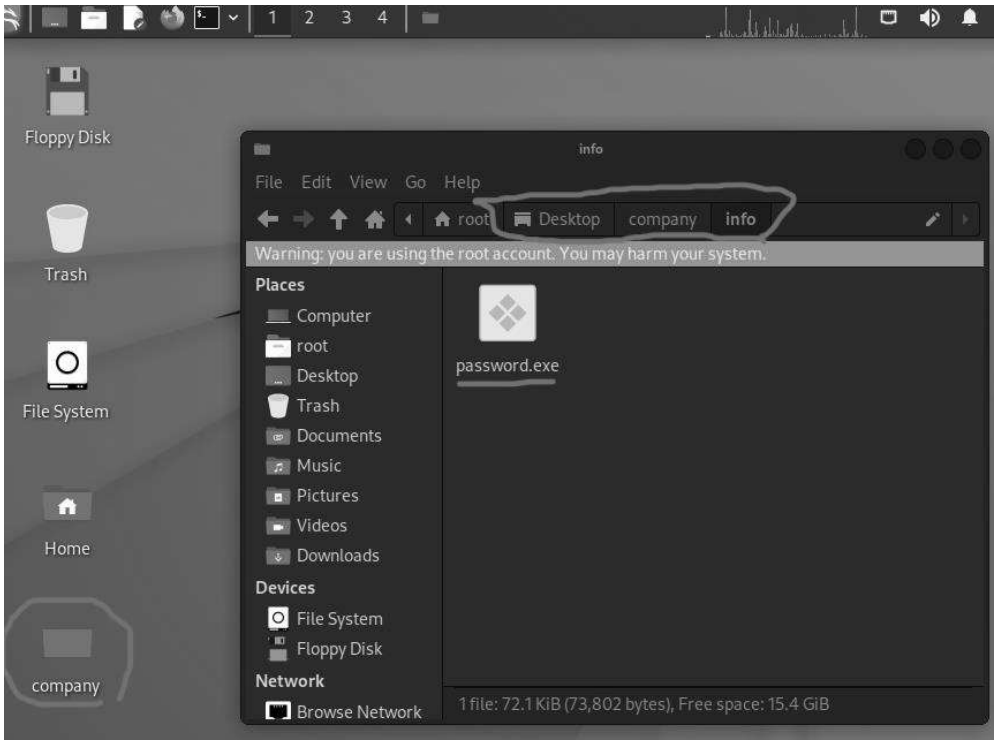
الشكل (8): خلق shellcode

2. استخدام الأداة Metasploit لتجهز عملية الاستغلال والإنصات للاتصال العكسي (الشكل 9) وتحديد عنوان الجهاز المنصت، المنفذ والpayload المستخدمين في خلق الملف الخبيث السابق (الشكل 8).



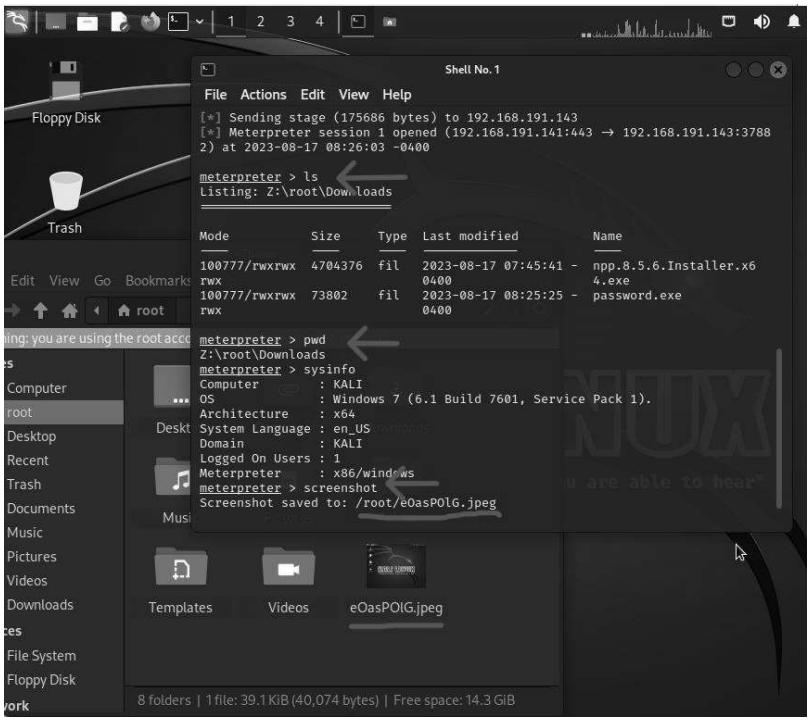
الشكل (9): إعداد الإنصات للاتصال العكسي من جهاز المهاجم

3. يقوم المهاجم بفك تشفير الملفات والوصول إلى الملف password الذي قمنا بحقن الملف الخبيث به (الشكل 10).

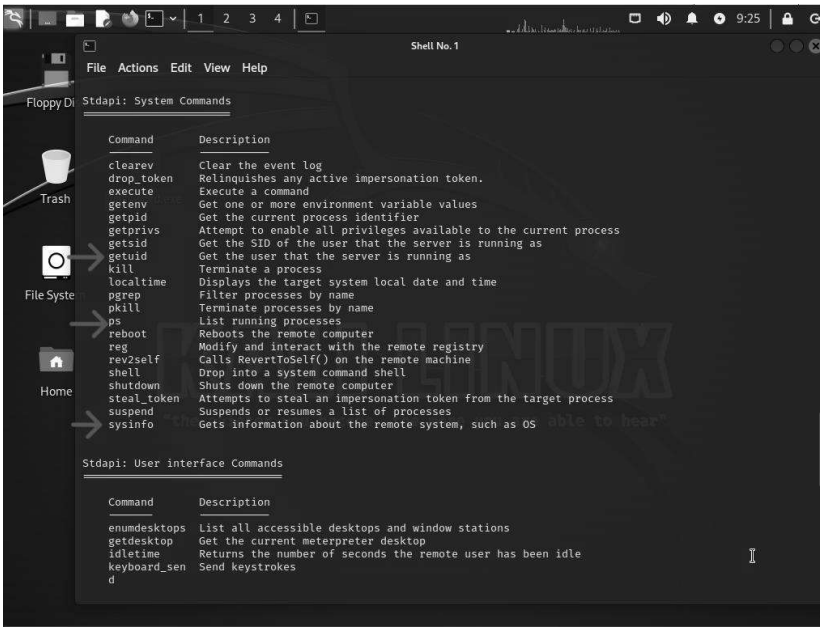


الشكل رقم (10): فك تشفير الملفات وفتح الملف الخبيث

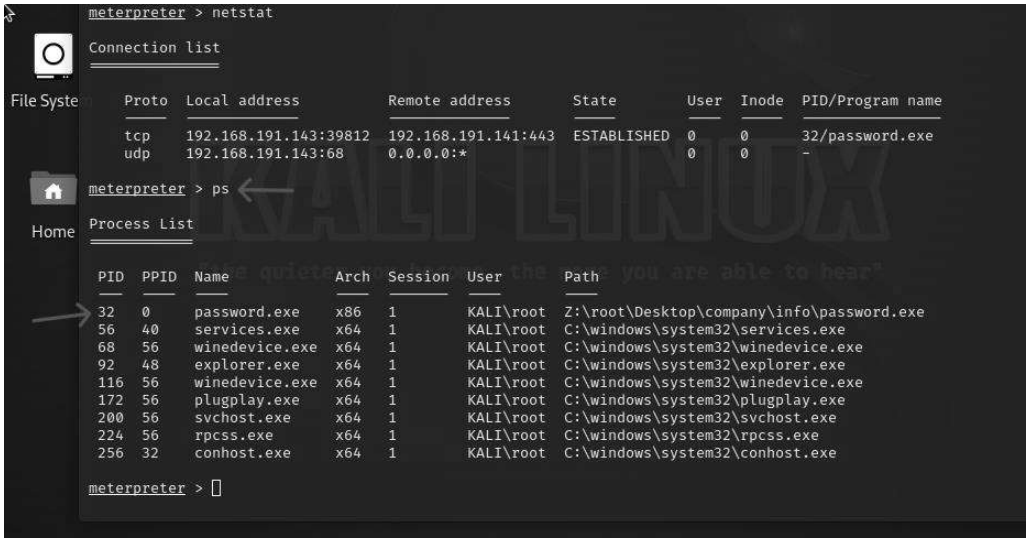
4. عندما يقوم المتسلل بفتح الملف فإن جهاز المحلل يحصل على جلسة الmeterpreter ويتمكن من الحصول على سطر الأوامر والوصول لجهاز المتسلل وتنفيذ العمليات التي يحتاج إليها للحصول على الأدلة الكافية لإثبات إدانة المهاجم (الشكل 11–12–13).



الشكل رقم(11): أوامر للحصول على معلومات عن جهاز المهاجم



الشكل رقم (12): استخدام التعليمة help لعرض كافة الأوامر التي يمكن القيام بها



الشكل رقم (13): استخدام التعليمة ps لعرض العمليات الحالية في جهاز المخترق

5. المقارنة بين نتيجة المحلل لعنوان IP المهاجم والعنوان الفعلي في جهازه حيث نلاحظ أننا حصلنا على النتيجة ذاتها (الشكل 14).

الشكل رقم 3 مقارنة نتيجة التعليمة ifconfig بين جهاز المحلل وجهاز المهاجم

مما سبق يمكننا ملاحظة أن كل مرحلة من المراحل السابقة يمكننا تنفيذها بطرق مختلفة وتقنيات وأدوات مختلفة وهذا ما يجعل لهذه الآلية القدرة على مواكبة تطور التقنيات المستمر ويجدر بنا أيضاً القول إننا في هذا السيناريو استخدمنا لُب الآلية لتوضيح الفكرة الأساسية منها، لكن على وجه الخصوص يمكننا الارتقاء بها لمستويات أعلى من التفاصيل والتعقيد من حيث استخدام أنظمة حماية إضافية مثل الIDS والIPS وجدران الحماية الداخلية لكل جهاز من أجهزة النظام.

10- بعض الأسئلة التي قد تتبادر للذهن

أولاً: ما الذي يضمن وقوع المتسلل في المصيدة وعدم سلوك الطريق الآخر باتجاه أجهزة النظام الحقيقة؟

الإجابة وبكل بساطة هي وجود أكثر من مصيدة ويشترط وجودها خلف كل جدار ناري في النظام حيث لا يمكن للأنظمة الحقيقية الكبيرة أن تحوي مصيدة واحدة فقط (تخيل أنك تسكن في منزل كبير ويوجد لديك فأر في المنزل ماذا ستكون نسبة وقوعه في مصيدة واحدة صغيرة؟!!! وعلى خلاف ذلك ماذا ستكون نسبة وقوعه في المصيدة عند وجود عدد كافٍ منها في أنحاء منزلك؟!).

ثانياً: ماذا لو كان المهاجم ذكياً لدرجة تمكنه من إدراك وجود هذه المصيدة؟

لا مشكلة في هذا، بل وحتى أن هذا أفضل وذلك لأن عامل الخوف في نفس المهاجم من الوقوع بها سيبعده عنها حيث سيدرك قوة هذا النظام ويتراجع عن فكرة اختراقه وبالتالي ملاحظة أصحاب النظام لاختراق جدار الحماية من خلال السجلات الخاصة به واكتشاف وجود ثغرة في إعداد الجدار وإصلاحها بالإضافة لعدم خسارة أي معلومات خاصة بها قد تكلفها مبالغ هائلة.

ثالثاً: هل يمكن أن تكتشف تقنيات الحماية في جهاز المهاجم عن وجود الملف الخبيث؟

أجل بالتأكيد لأن الملف الذي قمنا بخلقه في السيناريو السابق هو ملف غير مشفر، لكن كما سبق وذكرنا أننا نحاكي طريقة معينة لتوضيح آلية العمل إلا أننا وبالتأكد سنستخدم طرق معقدة أكثر في الواقع وتقنيات متطورة لتشفير هذا الملف حتى لا يتم كشفه وأيضاً يمكن استخدام أساليب مختلفة تماماً مثل تحويل السيرفر بأكمله لمصيدة واستخدام أنواع مختلفة من الملفات أو عن طريق استخدام أكواد بايثون أو صفحات ويب وغيرها الكثير.

رابعاً: في حال استخدم المهاجم بيئة افتراضية وعناوين مزيفة لتضليل صحة الأدلة ما هو الإجراء ضد هذا؟

عندما يقوم المحلل بالوصول لجهاز المهاجم يمكنه تثبيت عمليه الاستغلال من خلال نقلها إلى برامج تعمل عند اقلاع النظام ومن ثم العمل في الخلفية لتنصيب أدوات معينة يمكنها ارسال إشارة للكشف عن موقع الجهاز أو الوصول لإعدادات أكثر تعقيداً أو يمكنه مراقبة الميكروفون أو مراقبة شاشة الجهاز أو حتى الوصول لكاميرا الجهاز في حال وجودها وغير ذلك الكثير من عمليات المراقبة لمسجلات النظام وتحديد كل ما يقوم بفعله المهاجم باستخدام جهازه وكل المواقع التي يقوم بزيارتها وإلخ.

11- مصادر محتملة للأدلة الرقمية المعتمدة من قبل المحكمة والتي يمكن الحصول عليها من جهاز المتسلل:

سابقاً في بداية عصر الحاسوب كان المصدر الوحيد الذي يمكن من خلاله جمع الأدلة من جهاز رقمي هو القرص الصلب والأقراص المرنة، حيث كانت الذاكرة المؤقتة محدودة الحجم ولا يمكن استرجاع أي أدلة من خلالها. أما في أجهزة الحاسوب الحديثة فإن الجهاز العادي بالإضافة إلى الأجهزة التي تعمل بمعالجات دقيقة تحتوي على مجموعة من المصادر المحتملة للأدلة والتي يمكن أن يستفيد منها المحقق الجيد.

هنا بعض تلك المصادر:

سجلات النظام system logs، سجلات المُوجه router logs، أجهزة WiFi، رسائل البريد الالكتروني، سجلات المتصفحات، سجلات أجهزة الحماية (الجدار الناري firewall أو أجهزة كشف الاختراق IDS)، سجلات قواعد البيانات... الدليل الرقمي يختلف بحسب الجريمة، مثلا في حالات الابتزاز عبر الانترنت يمكن اعتماد رسائل البريد الالكتروني وسجلات المحادثة على أنها دليل رقمي وفي حالة اختراق منظومة معلوماتية يمكن اعتماد سجلات النظام وسجلات أجهزة الحماية.

12- الاستنتاجات:

- يخلص البحث إلى أنَّ الآلية ذات كفاءة عالية في حماية البيانات ضد المتسللين من خارج النظام وقدرتها على كشف معلومات عن المهاجم وهويته.
- يمكننا أن نستنتج من المرحلة الأولى أن وجود جدران الحماية في الأنظمة غير كافٍ لحمايتها حيث أنَّ آلية عملها باتت مكشوفة لدى المهاجمين مما سمح لهم بتطوير أدوات قادرة على اختراق هذه الأنظمة بسهولة.
- ضرورة تزييف البيانات بصورة احترافية لتبدو على أنها حقيقية ومراعاة كافة التفاصيل الصغيرة فيها لإبعاد الشكوك عن ماهيتها الحقيقة.

- ضرورة وجود أكثر من مصيدة ضمن النظام الواحد وبشكل خاص في الأنظمة الكبيرة لزيادة نسبة وقوع المهاجم فيها.
- يمكننا استخدام طرق ووسائل وتقنيات متعددة بما يتناسب مع مهارة المخترق وكذلك المحلل في كل مرحلة من مراحل الآلية الثلاثية مما يعطي أكبر قدر من إمكانية التطوير والوصول لإضافة كافة التفاصيل والتعقيدات.
- فحص الجهاز أو المنظومة المعلوماتية وتحليل العمليات واسترجاع البيانات والملفات وفحص السجلات من أجل الحصول على دليل رقمي digital evidence هو علم قائم بذاته.
- التحقيقات الجنائيَّة الرقميَّة تتمتَّع بصفة خاصَّة من حيث طبيعتها وطرق العمل على جمع الأدلَّة والتعامل مع البيانات الخاصَّة بالقضيَّة، ويتعاظم دورها مع ضُلوع الاتصالات والبيانات الرقميَّة في كافة مناحي الحياة اليوميَّة ممَّا يجعلها ضروريَّة لكل قضيَّة.
- فيما يتعلَّق بالأدلَّة الجنائيَّة الرقميَّة، هناك طرق علميَّة يوصى بها لجمع هذا النوع من الأدلَّة وهي طرق لا تفرض خطوات معنية، وإنما تفرض نموذجاً معيناً لضمان الحصول على معلومات رقميَّة ترقى إلى مستوى الدليل؛ لأنَّ عدم مراعاة الطرق العلميَّة في جمع الأدلَّة وتوثيق عملية الجمع يمكن أن يؤدِّي إلى رفض الأدلَّة كدليل في القضايا أمام المحاكم.
- إنَّ عملية جمع الأدلَّة الرقميَّة لا تخلو من كونها قد تُشكِّل في بعض الأحيان تعارضاً مع قوانين حماية البيانات التي تحظر معالجة البيانات وخصوصاً الشخصية منها دون شروط معينة. تضمنت قوانين حماية البيانات، وخاصة الحديثة منها، استثناءات تم تخصيصها للحالات التي يتم فيها جمع البيانات الشخصية لأغراض البحث الجنائي في حالات التحقيق في القضايا الجنائية والجرائم.
- إن الدلائل الرقمية والتحقيق الجنائي هما المستقبل القادم لعمليات البحث الجنائي في ضوء التغير الكبير في سلوكيات الأفراد تجاه استعمال الرقميات في كافة شؤون العمل والحياة.

13- نصائح وتوصيات:

- استخدام أنظمة كشف الاختراق ومنع الاختراق ضمن النظام الداخلي بالإضافة للجدران النارية وإعداداها باحترافيه لزيادة صعوبة اختراقها.
- التحديثات الدورية للنظام بما فيه من برامج وتطبيقات وأنظمة حماية للتقليل من خطر استغلال الثغرات في الأنظمة القديمة.
- تدريب الموظفين على طرق الحماية وعدم استخدام أجهزة العمل لتصفح الإنترنت لأنها قد تعرض أمان النظام للخطر حيث أن المواقع الشرعية ممكن اختراقها أو ممكن أن تحوي على إعلانات خبيثة والعديد من الهجمات ممكن أن تتم بدون أي اجراء من المستخدم (كالنقر على رابط أو تحميل ملف).
- يجب توافر نسخة احتياطية للبيانات في أي نظام.
- عدم استخدام كلمات سر بسيطة قابلة للتخمين مثل 123456 أو كلمات سر تحوي على معلومات شخصية كرقم الموبايل أو تاريخ الميلاد، بل استخدام كلمات سر تتجاوز ال8 محارف بما فيهم أحرف كبيرة وصغيرة وأرقام ورموز خاصة والتأكد من عدم مشاركتها مع أي شخص آخر.
- اختيار مضاد فيروسات قوي وتحديثه بشكل دوري، مضاد الفيروسات ضروري للحماية، ولكنه غير كافي لتأمين الحماية الكاملة.

- حذف التطبيقات التي لا نقوم باستخدامها، هذه التطبيقات من الممكن أن تحوي على ثغرات وبهذه العملية أنت تقلل من هذه الثغرات وبالتالي تقلل من احتمالية اختراق جهازك.
- استخدم المواقع الرسمية للحصول على التطبيقات والبرامج ولا تقم بتثبيت أي تطبيق من المصادر غير الموثوقة وخاصة النسخ المجانية للتطبيقات المدفوعة لأن المهاجم يعرف عمّا يبحث المستخدم ويستغل هذا الأمر بشكل احترافي.
- تثبيت إضافة للمتصفح HTTPS Everywhere وهذا سيضمن أن كل عمليات الاتصال مع المواقع الرئيسية ستكون بشكل مشفر وبذلك تمنع أي شخص يحاول التنصت على قناة الاتصال من رؤية أو سرقة معلوماتك المتبادلة.
- تحوي المتصفحات على ثغرات ونقاط ضعف أمنية وإذا لم تقم بعملية التحديث لتطبيق الإصلاحات الخاصة بهذه الثغرات فمن الممكن أن يتم استغلالها من قبل المهاجمين والوصول لجهازك أو إصابة جهازك ببرمجيات خبيثة، لذا حافظ على المتصفحات والإضافات الخاصة بها بأحدث إصدار.

المراجع:

[1]– Tiwari, A., Mehrotra, V., Goel, S., Naman, K., Maurya, S. and Agarwal, R., 2021, October– **Developing trends and challenges of digital forensics.** In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1–5). IEEE.

[2]– Erata, F., Deng, S., Zaghloul, F., Xiong, W., Demir, O. and Szefer, J., 2023– **Survey of approaches and techniques for security verification of computer systems.** ACM Journal on Emerging Technologies in Computing Systems, 19(1), pp.1–34.

[3]– Arogundade, O.R., 2023– **Network security concepts, dangers, and defense best practical.** Computer Engineering and Intelligent Systems, 14(2).

[4]– KARIE, N.M. & VENTER, H.S., 2015– **Taxonomy of challenges for digital forensics**. Journal of forensic sciences, 60(4), pp.885–893.

[5]– CHOPRA, A., 2016– **Security issues of firewall**. Int. J. P2P Netw. Trends Technol, 22(1), pp.4–9.

[6]– ASHOOR, A.S. & GORE, S., 2011– **Difference between intrusion detection system (IDS) and intrusion prevention system (IPS)**. In Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15–17, 2011, 4 (pp. 497–501). Springer Berlin Heidelberg.

[7]– Lopez, A. 2019– **Digital Forensics Tools and Techniques.** Germany: GRIN Verlag.

[8]– Akins, M. 2023– **Mastering Nmap: A Comprehensive Guide to Network Discovery and Security.** (n.p.): Amazon Digital Services LLC – Kdp.

[9]– RAHALKAR, S. & NIPUN, J., 2019– **The Complete Metasploit Guide**. Packt Publishing.

[10]– KATIC, T. and PALE, P., 2007– June. **Optimization of firewall rules**. In 2007 29th International Conference on Information Technology Interfaces (pp. 685–690). IEEE.

[11]– Al–Shaer, E. 2014– **Automated Firewall Analytics: Design, Configuration and Optimization.** Germany: Springer International Publishing.

[12]– LIU, A., 2010– **Firewall Design and Analysis**. World Scientific Publishing Company.

[13]– CARVEY, H. & ALTHEIDE, C., 2011– **Digital forensics with open source tools.** Elsevier.

[14]– EC– COUNCIL, P., 2009– **Computer Forensics: Hard Disk and Operating Systems**. Cengage Learning.

[15]– EC–COUNCIL, P., 2009– **Computer Forensics: Investigating Network Intrusions and Cyber Crime.** Cengage Learning.

[16]– Kävrestad, J., Birath, M., Clarke, N. 2024– **Fundamentals of Digital Forensics: A Guide to Theory, Research and Applications.** Germany: Springer International Publishing, Imprint: Springer.

[17]– Brotherston, L., Berlin, A. 2017– **Defensive Security Handbook: Best Practices for Securing Infrastructure.** United States: O'Reilly Media.

[18]– Deepayan Chanda, P. J. 2021– **Penetration Testing with Kali Linux: Learn Hands–On Penetration Testing Using a Process–Driven Framework.** India: Bpb Publications.

[19]– Singh, G. D. 2022– **The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrack–ng, and Empire.** Germany: Packt Publishing.

[20]– Bernstein, J. 2022– **VMware Workstation Made Easy: Virtualization for Everyone.** (n.p.): Amazon Digital Services LLC – Kdp.

[21]– von Oven, P. 2023– **Learning VMware Workstation for Windows: Implementing and Managing VMware's Desktop Hypervisor Solution.** United States: Apress.

[22]– Cybellium, L. 2023– **Mastering Metasploit.** (n.p.): Cybellium Ltd.