US010911476B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,911,476 B2**
(45) **Date of Patent: *Feb. 2, 2021**

(54) **SELECTIVELY CHOOSING BETWEEN ACTUAL-ATTACK AND SIMULATION/EVALUATION FOR VALIDATING A VULNERABILITY OF A NETWORK NODE DURING EXECUTION OF A PENETRATION TESTING CAMPAIGN**

(71) Applicant: **XM CYBER LTD.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM CYBER LTD.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/831,982**

(22) Filed: **Mar. 27, 2020**

(65) **Prior Publication Data**

US 2020/0236130 A1 Jul. 23, 2020

Related U.S. Application Data

(63) Continuation of application No. 16/566,969, filed on Sep. 11, 2019, now Pat. No. 10,645,113, which is a (Continued)

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 12/26	(2006.01)
G06F 21/55	(2013.01)

(52) **U.S. Cl.**

CPC ..... ***H04L 63/1433*** (2013.01); ***G06F 21/55*** (2013.01); ***H04L 43/06*** (2013.01); (Continued)

(58) **Field of Classification Search**

CPC H04L 63/1433; H04L 63/1466; H04L 63/1475

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,458,798	B2 *	6/2013	Williams	G06F 21/577 726/25
9,015,847	B1 *	4/2015	Kaplan	H04L 63/1441 726/25

(Continued)

OTHER PUBLICATIONS

Geer et al., "Penetration testing: a duet", doi: 10.1109/CSAC.2002.1176290, 2002, pp. 185-195. (Year: 2002).*

(Continued)

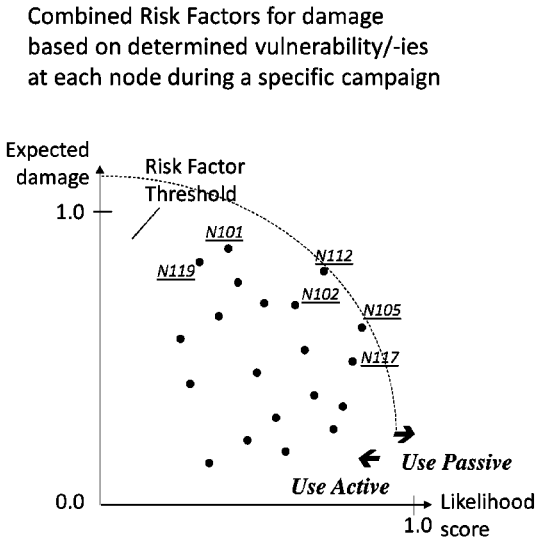
Primary Examiner — Peter C Shaw

(74) *Attorney, Agent, or Firm* — Momentum IP Group; Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system by a penetration testing system. In some embodiments, both active and passive validation methods are used during a single penetration testing campaign in a single networked system. In other embodiments, a first penetration testing campaign uses only active validation and a second penetration campaign uses only passive validation, where both campaigns are performed by a single penetration testing system in a single networked system. Node-by-node determination of whether to use active or passive validation can be based on expected extent and/or likelihood of damage from actually compromising a network node using active validation.

14 Claims, 32 Drawing Sheets



US010880326B1

(12) **United States Patent**
Gofman

(10) **Patent No.: US 10,880,326 B1**
(45) **Date of Patent: Dec. 29, 2020**

(54) **SYSTEMS AND METHODS FOR DETERMINING AN OPPORTUNITY FOR NODE POISONING IN A PENETRATION TESTING CAMPAIGN, BASED ON ACTUAL NETWORK TRAFFIC**

(71) Applicant: **XM Cyber Ltd.**, Herzelyia (IL)

(72) Inventor: **Igal Gofman**, Rosh-Haayin (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/936,446**

(22) Filed: **Jul. 23, 2020**

Related U.S. Application Data

(63) Continuation of application No. PCT/IB2020/056929, filed on Jul. 22, 2020.

(60) Provisional application No. 62/881,768, filed on Aug. 1, 2019.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
G06Q 10/10	(2012.01)
H04L 12/58	(2006.01)
G06Q 10/06	(2012.01)
H04L 29/12	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06Q 10/0635*** (2013.01); ***G06Q 10/107*** (2013.01); ***H04L 51/08*** (2013.01); ***H04L 63/1425*** (2013.01); *H04L 61/307* (2013.01)

(58) **Field of Classification Search**
CPC G06F 21/50; G06F 21/55; G06F 21/554; H04L 63/14; H04L 63/1416; H04L 63/1433; H04L 63/1441; H04L 63/145; H04L 63/20
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,574,737	B1	6/2003	Kingsford et al.
6,711,127	B1	3/2004	Gorman et al.
6,918,038	B1	7/2005	Smith et al.
6,952,779	B1	10/2005	Cohen et al.
7,013,395	B1	3/2006	Swiler et al.
7,296,092	B2	11/2007	Nguyen
7,693,810	B2	4/2010	Donoho et al.
7,757,293	B2	7/2010	Caceres et al.

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230	A	7/2013
CN	103916384	A	7/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.

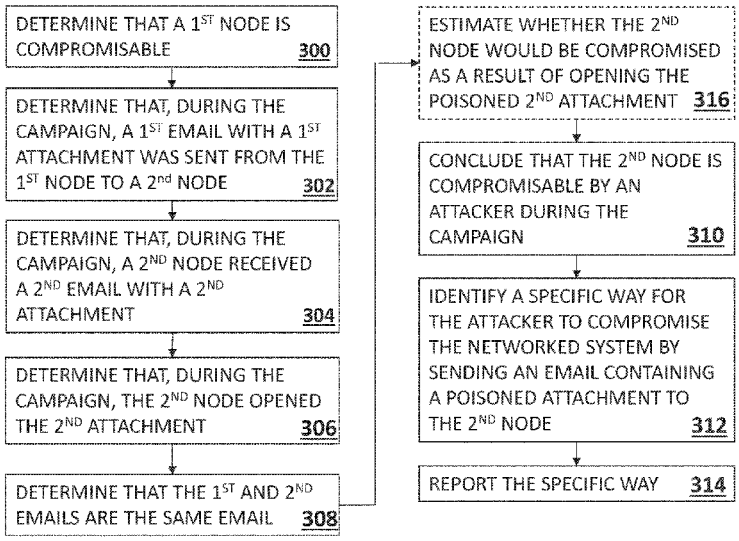
(Continued)

Primary Examiner — Edward Zee
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems for carrying out a simulated penetration testing campaign of a networked system for identifying a specific way for an attacker to compromise a networked system, where the specific way includes a step of poisoning the specific network node by the specific network node receiving a poisoned email body, or a poisoned email attachment, which includes malicious code.

20 Claims, 9 Drawing Sheets



US010686823B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,686,823 B2**
(45) **Date of Patent: Jun. 16, 2020**

(54) **SYSTEMS AND METHODS FOR DETECTING COMPUTER VULNERABILITIES THAT ARE TRIGGERED BY EVENTS**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 295 days.

(21) Appl. No.: **15/940,376**

(22) Filed: **Mar. 29, 2018**

(65) **Prior Publication Data**

US 2018/0219909 A1 Aug. 2, 2018

Related U.S. Application Data

(63) Continuation-in-part of application No. 15/911,168, filed on Mar. 4, 2018, now Pat. No. 10,038,711, which is a continuation of application No. 15/874,429, filed on Jan. 18, 2018, application No. 15/940,376, filed on Mar. 29, 2018, which is a continuation-in-part of application No. 15/874,429, filed on Jan. 18, 2018.

(60) Provisional application No. 62/482,535, filed on Apr. 6, 2017, provisional application No. 62/451,850, filed on Jan. 30, 2017.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 12/26	(2006.01)
H04L 12/24	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 41/048*** (2013.01); ***H04L 43/50*** (2013.01); ***H04L 63/30*** (2013.01); *H04L 63/1416* (2013.01); *H04L 63/1466* (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,182,040	B2 *	1/2019	Hu	G06F 21/602
2003/0140223	A1 *	7/2003	Desideri	H04L 63/20 713/153
2004/0095907	A1 *	5/2004	Agee	H04B 7/0417 370/334

(Continued)

OTHER PUBLICATIONS

Goel, Jai Narayan et al. Ensemble Based Approach to Increase Vulnerability Assessment and Penetration Testing Accuracy. 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7542303 (Year: 2016).*

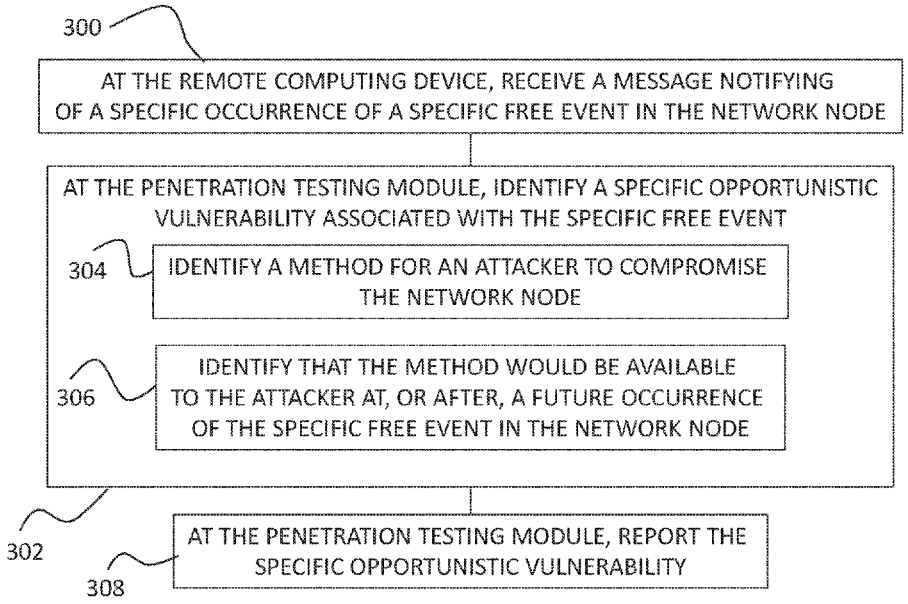
(Continued)

Primary Examiner — Jeremiah L Avery
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems for carrying out campaigns of penetration testing for discovering and reporting security vulnerabilities of a networked system, the networked system comprising a plurality of network nodes interconnected by one or more networks.

21 Claims, 5 Drawing Sheets



US010686822B2

(12) **United States Patent**
Segal

(10) **Patent No.: US 10,686,822 B2**
(45) **Date of Patent: *Jun. 16, 2020**

(54) **SYSTEMS AND METHODS FOR SELECTING A LATERAL MOVEMENT STRATEGY FOR A PENETRATION TESTING CAMPAIGN**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventor: **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 373 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/869,128**

(22) Filed: **Jan. 12, 2018**

(65) **Prior Publication Data**

US 2018/0219903 A1 Aug. 2, 2018

Related U.S. Application Data

(63) Continuation-in-part of application No. 15/681,782, filed on Aug. 21, 2017, and a continuation-in-part of application No. 15/681,692, filed on Aug. 21, 2017, now Pat. No. 10,122,750.

(60) Provisional application No. 62/546,569, filed on Aug. 17, 2017, provisional application No. 62/453,056, filed on Feb. 1, 2017, provisional application No. 62/451,850, filed on Jan. 30, 2017.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
G06F 21/57	(2013.01)
G06F 9/451	(2018.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1433*** (2013.01); ***G06F 9/451*** (2018.02); ***G06F 21/577*** (2013.01); ***H04L 63/20*** (2013.01); *G06F 2221/034* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,952,779	B1	10/2005	Cohen et al.
7,013,395	B1	3/2006	Swiler et al.
7,757,293	B2	7/2010	Caceres et al.
8,001,589	B2	8/2011	Ormazabal et al.
8,112,016	B2	2/2012	Matsumoto et al.
8,127,359	B2	2/2012	Kelekar

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230	A	7/2013
CN	104009881	A	8/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google) published Jul. 10, 2013 Li Qianmu.

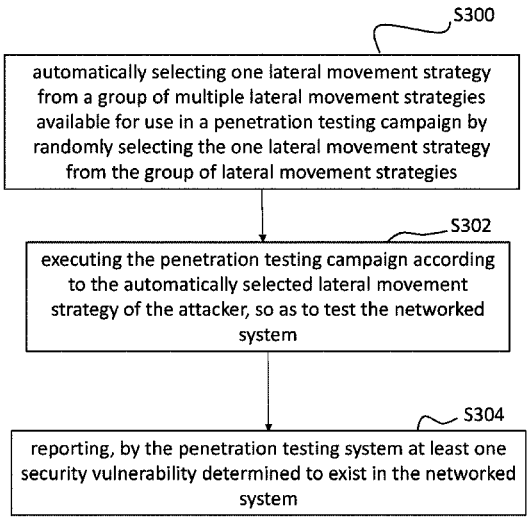
(Continued)

Primary Examiner — Joseph P Hirl
Assistant Examiner — Hassan Saadoun
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems for carrying out campaigns of penetration testing for discovering and reporting security vulnerabilities of a networked system, the networked system comprising a plurality of network nodes interconnected by one or more networks.

12 Claims, 8 Drawing Sheets



US010652269B1

(12) **United States Patent**
Segal et al.

(10) **Patent No.: US 10,652,269 B1**
(45) **Date of Patent: *May 12, 2020**

(54) **USING INFORMATION ABOUT EXPORTABLE DATA IN PENETRATION TESTING**

(71) Applicant: **XM Cyber Ltd.**, Hertsliya (IL)

(72) Inventors: **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/578,419**

(22) Filed: **Sep. 23, 2019**

Related U.S. Application Data

(63) Continuation of application No. 16/379,820, filed on Apr. 10, 2019, now Pat. No. 10,469,521, and a continuation of application No. PCT/IB2019/052951, filed on Apr. 10, 2019.

(60) Provisional application No. 62/755,480, filed on Nov. 4, 2018.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 63/20*** (2013.01)

(58) **Field of Classification Search**
CPC . H04L 63/1433; H04L 63/20; H04L 63/1416; H04L 63/145
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,693,810	B2 *	4/2010	Donoho	G06Q 40/00 706/48
7,934,254	B2 *	4/2011	Graham	G06F 21/55 709/224
7,966,659	B1 *	6/2011	Wilkinson	H04L 63/0209 726/11
8,392,997	B2 *	3/2013	Chen	G06F 21/577 726/25
9,015,301	B2 *	4/2015	Redlich	G06Q 10/10 709/223
9,412,073	B2 *	8/2016	Brandt	H04L 63/1408

* cited by examiner

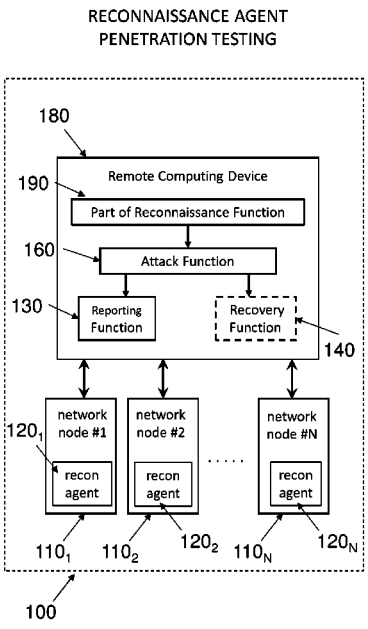
Primary Examiner — Hosuk Song

(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Penetration testing campaigns generate remediation recommendations based at least in part on information about files stored in network nodes of the tested networked system. Information is obtained about files stored in a plurality of network nodes of the networked system, and based on the obtained information, a corresponding data-value score for each network node of the plurality of network nodes is determined according to a common data-value metric. The penetration testing campaign is executed, following which one or more remediation recommendations are selected based on the data-value scores corresponding to at least some of the plurality of network nodes.

20 Claims, 15 Drawing Sheets



US010645113B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,645,113 B2**
(45) **Date of Patent: May 5, 2020**

(54) **SELECTIVELY CHOOSING BETWEEN ACTUAL-ATTACK AND SIMULATION/EVALUATION FOR VALIDATING A VULNERABILITY OF A NETWORK NODE DURING EXECUTION OF A PENETRATION TESTING CAMPAIGN**

(71) Applicant: **XM CYBER LTD.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/566,969**

(22) Filed: **Sep. 11, 2019**

(65) **Prior Publication Data**

US 2020/0106800 A1 Apr. 2, 2020

Related U.S. Application Data

(63) Continuation of application No. 16/400,938, filed on May 1, 2019, now Pat. No. 10,454,966, and a continuation of application No. PCT/IB2018/058849, filed on Nov. 11, 2018, said application No. 16/400,938 is a continuation of application No. 16/186,557, filed on Nov. 11, 2018, now Pat. No. 10,367,846.

(60) Provisional application No. 62/586,600, filed on Nov. 15, 2017.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 12/26	(2006.01)
G06F 21/55	(2013.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06F 21/55*** (2013.01); ***H04L 43/06*** (2013.01); ***H04L 63/1408*** (2013.01); ***H04L 63/1466*** (2013.01); ***H04L 63/1475*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433
USPC 726/25
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

9,781,160	B1 *	10/2017	Irimie	H04L 63/1416
9,824,222	B1 *	11/2017	Kaplan	G06F 21/577
10,291,643	B2 *	5/2019	Marquez	H04L 63/1433
2003/0208616	A1 *	11/2003	Laing	H04L 43/50 709/236

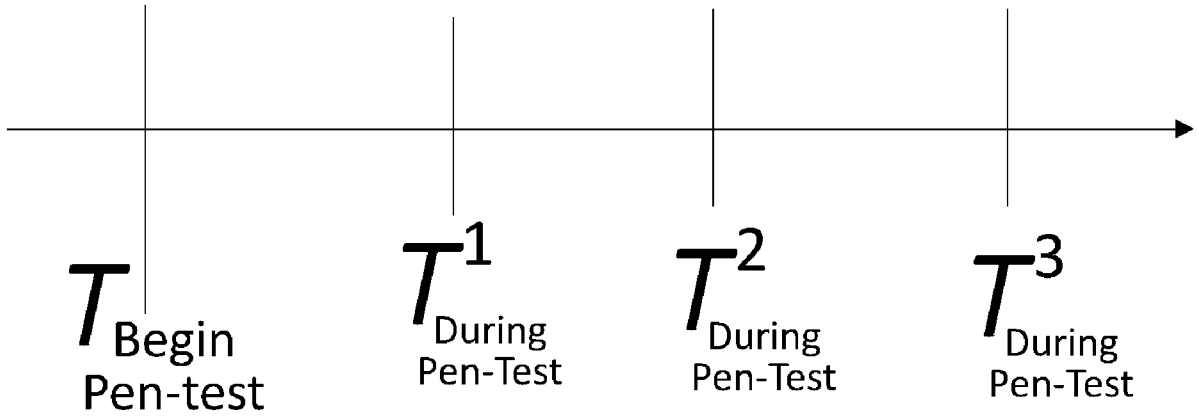
* cited by examiner

Primary Examiner — Peter C Shaw
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system by a penetration testing system. In some embodiments, both active and passive validation methods are used during a single penetration testing campaign in a single networked system. In other embodiments, a first penetration testing campaign uses only active validation and a second penetration campaign uses only passive validation, where both campaigns are performed by a single penetration testing system in a single networked system. Node-by-node determination of whether to use active or passive validation can be based on expected extent and/or likelihood of damage from actually compromising a network node using active validation.

10 Claims, 32 Drawing Sheets



US010637883B1

(12) **United States Patent**
Segal et al.

(10) **Patent No.: US 10,637,883 B1**
(45) **Date of Patent: Apr. 28, 2020**

(54) **SYSTEMS AND METHODS FOR DETERMINING OPTIMAL REMEDIATION RECOMMENDATIONS IN PENETRATION TESTING**

(71) Applicant: **XM Cyber Ltd.**, Hertzelia (IL)

(72) Inventors: **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/716,302**

(22) Filed: **Dec. 16, 2019**

Related U.S. Application Data

(60) Provisional application No. 62/870,742, filed on Jul. 4, 2019.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,574,737	B1	6/2003	Kingsford et al.	
6,711,127	B1 *	3/2004	Gorman	H04L 63/1433 370/230
6,918,038	B1	7/2005	Smith et al.	
6,952,779	B1	10/2005	Cohen et al.	
7,013,395	B1 *	3/2006	Swiler	H04L 63/1433 713/151
7,296,092	B2	11/2007	Nguyen	
7,757,293	B2	7/2010	Caceres et al.	
7,926,113	B1 *	4/2011	Gula	H04L 63/1425 726/25
8,001,589	B2	8/2011	Ormazabal et al.	
8,112,016	B2	2/2012	Matsumoto et al.	
8,127,359	B2	2/2012	Kelekar	
8,321,944	B1	11/2012	Mayer et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230 A	7/2013
CN	103916384 A	7/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.

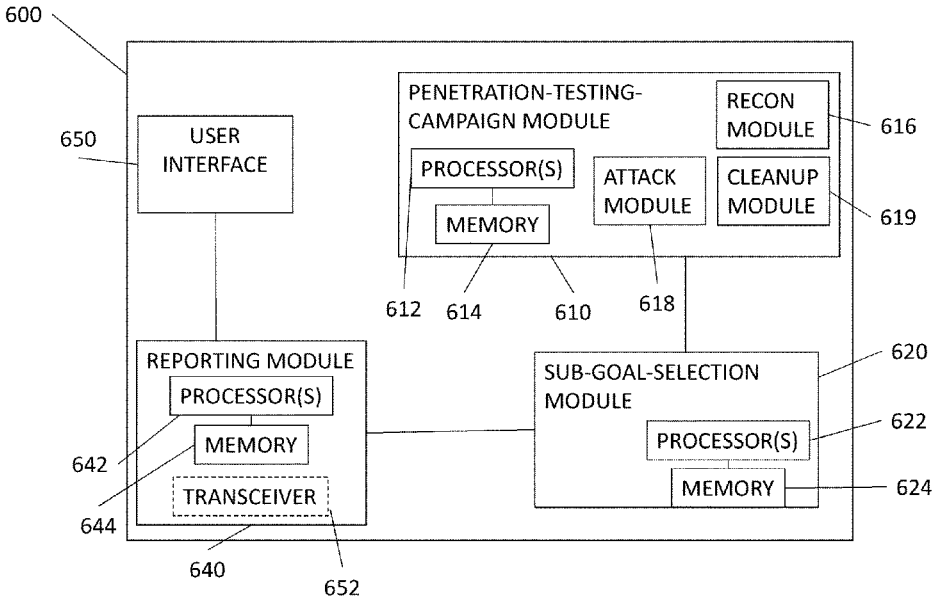
(Continued)

Primary Examiner — Bradley W Holder
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems for providing a recommendation for improving the security of a networked system against attackers. The recommendation may include a recommendation of a single sub-goal to be protected to achieve optimal improvement in security, or of multiple such sub-goals. If the recommendation includes multiple sub-goals, the sub-goals may be ordered such that the first sub-goal is more important to protect, provides a greater benefit by being protected, or is more cost effective to protect than subsequent sub-goals in the ordered list of sub-goals.

20 Claims, 23 Drawing Sheets



US010637882B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,637,882 B2**
(45) **Date of Patent: *Apr. 28, 2020**

(54) **PENETRATION TESTING OF A NETWORKED SYSTEM**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 203 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/874,429**

(22) Filed: **Jan. 18, 2018**

(65) **Prior Publication Data**

US 2018/0219904 A1 Aug. 2, 2018

Related U.S. Application Data

(60) Provisional application No. 62/451,850, filed on Jan. 30, 2017.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)
H04L 12/24 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 43/50*** (2013.01); ***H04L 63/20*** (2013.01); ***H04L 63/30*** (2013.01); *H04L 41/048* (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433; H04L 43/50; H04L 63/30; H04L 63/1466; H04L 63/1408;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,952,779 B1 * 10/2005 Cohen G06F 21/577 726/22
7,013,395 B1 * 3/2006 Swiler H04L 63/1433 713/151
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 104009881 A 8/2014
(Continued)

OTHER PUBLICATIONS

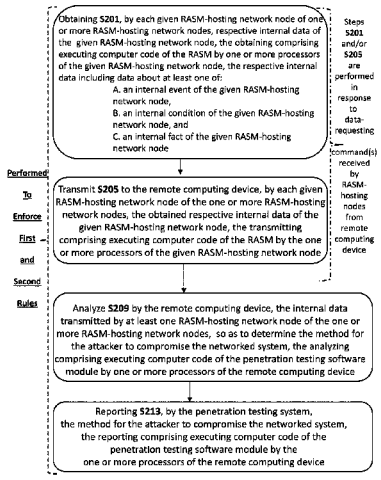
CN103200230 Machine Translation (by EPO and Google) published Jul. 10, 2013 Li Qianmu.
(Continued)

Primary Examiner — Trang T Doan
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system comprising a set of network-nodes by a penetration testing system (e.g. to enforce first and/or second rules) are disclosed herein. The penetration testing system comprises: (i) reconnaissance agent software module (RASM) installed on multiple nodes (each of which is a RASM-hosting node) of the networked system to be penetration-tested and (ii) a penetration testing software module (PTSM) installed on a remote computing device (RCD). Internal data from each of the RASM-hosting nodes is collected and transmitted to the RCD. Analysis of the internal data collected from multiple RASM-hosting network nodes determines a method for an attacker to compromise the networked system. The first and second rules are defined herein. Alternatively or additionally, one or more of the RASM instances are pre-installed on one or more RASM-hosting nodes before the penetration testing commences.

20 Claims, 17 Drawing Sheets



US010581895B2

(12) **United States Patent**
Ashkenazy et al.

(10) **Patent No.: US 10,581,895 B2**
(45) **Date of Patent: *Mar. 3, 2020**

(54) **TIME-TAGGED PRE-DEFINED SCENARIOS FOR PENETRATION TESTING**

(71) Applicant: **XM Cyber Ltd.**, Hertzelia (IL)

(72) Inventors: **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/519,124**

(22) Filed: **Jul. 23, 2019**

(65) **Prior Publication Data**

US 2019/0387015 A1 Dec. 19, 2019

Related U.S. Application Data

(63) Continuation of application No. 15/911,170, filed on Mar. 5, 2018, now Pat. No. 10,412,112.

(60) Provisional application No. 62/522,569, filed on Aug. 31, 2017.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 12/24	(2006.01)
G06F 3/0482	(2013.01)
H04L 12/26	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1433*** (2013.01); ***G06F 3/0482*** (2013.01); ***H04L 41/22*** (2013.01); ***H04L 43/045*** (2013.01); ***H04L 43/50*** (2013.01); *H04L 63/1458* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,068,095	B1 *	9/2018	Segal	G06F 21/577
2014/0237606	A1 *	8/2014	Futoransky	G06F 21/577 726/25

* cited by examiner

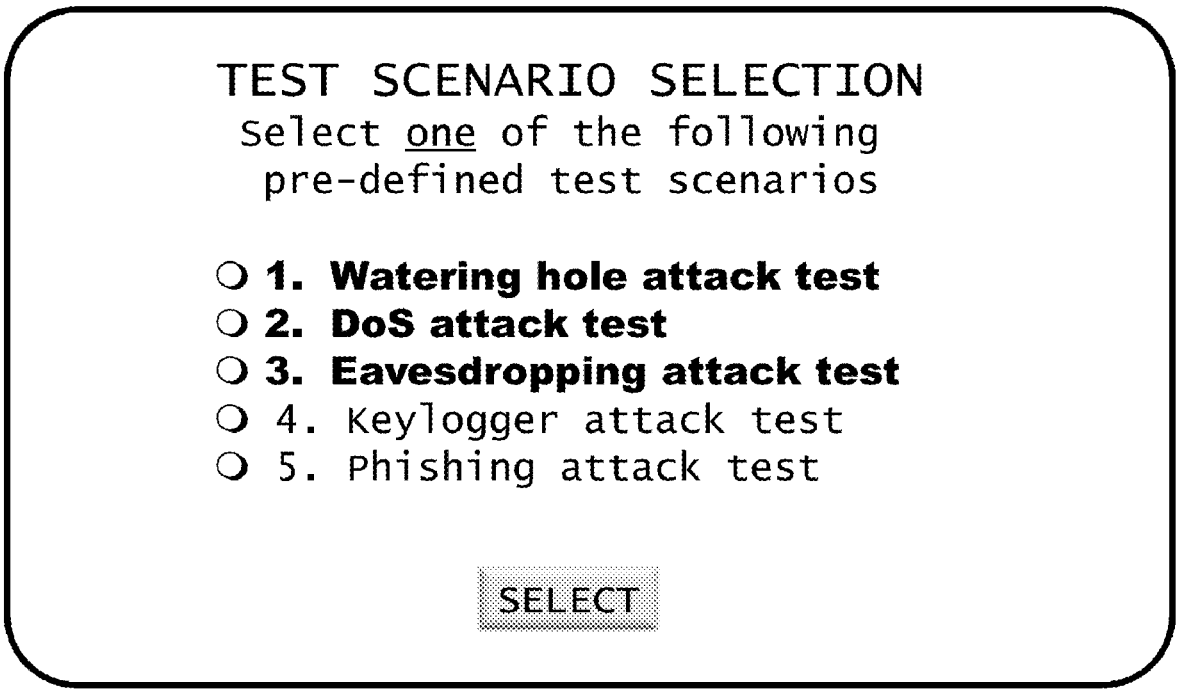
Primary Examiner — David Le

(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems for carrying out campaigns of penetration testing for discovering and reporting security vulnerabilities of a networked system. Penetration testing campaigns are carried out based on pre-defined penetration testing scenarios associated with respective time tags. A penetration testing scenario is selected by a user from a set of pre-defined test scenarios, the set containing only pre-defined test scenarios with time tags matching a scheduled starting time of a penetration testing campaign.

20 Claims, 18 Drawing Sheets



US010574687B1

(12) **United States Patent**
Lasser

(10) **Patent No.: US 10,574,687 B1**
(45) **Date of Patent: Feb. 25, 2020**

(54) **SYSTEMS AND METHODS FOR DYNAMIC REMOVAL OF AGENTS FROM NODES OF PENETRATION TESTING SYSTEMS**

(71) Applicant: **XM Cyber Ltd.**, Hertzelia (IL)

(72) Inventor: **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/662,206**

(22) Filed: **Oct. 24, 2019**

Related U.S. Application Data

(60) Provisional application No. 62/778,941, filed on Dec. 13, 2018.

(51) **Int. Cl.**

G06F 21/57	(2013.01)
H04L 29/06	(2006.01)
G06F 8/61	(2018.01)
G06F 11/36	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06F 8/62*** (2013.01); ***G06F 11/3668*** (2013.01); ***G06F 21/577*** (2013.01); *G06F 2221/033* (2013.01); *G06F 2221/034* (2013.01)

(58) **Field of Classification Search**
CPC ... G06F 11/3668; G06F 2221/033–034; G06F 21/577; H04L 63/1433
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038	B1	7/2005	Smith et al.
6,952,779	B1	10/2005	Cohen et al.
7,013,395	B1	3/2006	Swiler et al.
7,296,092	B2	11/2007	Nguyen
7,757,293	B2	7/2010	Caceres et al.
8,001,589	B2	8/2011	Ormazabal et al.

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230	A	7/2013
CN	103916384	A	7/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.

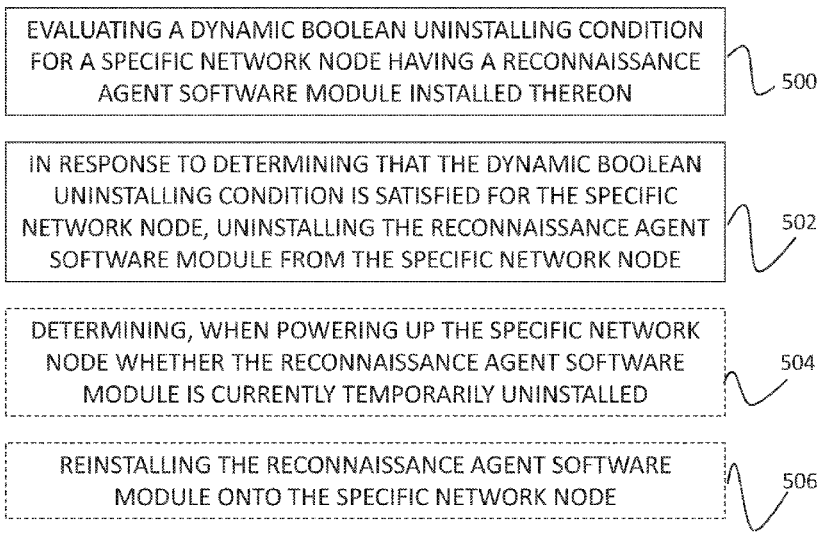
(Continued)

Primary Examiner — Thaddeus J Plecha
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Systems and methods of carrying out a penetration testing campaign of a networked system by a penetration testing system, in which reconnaissance agent software modules are dynamically removed from at least one network node based on changing conditions in the tested networked system. The networked system includes multiple network nodes, and the penetration testing system includes a penetration testing software module and a reconnaissance agent software module installed on at least some network nodes of the multiple network nodes. For one network node, a dynamic Boolean uninstalling condition is evaluated, and in response to determining that the dynamic Boolean uninstalling condition is satisfied for that network node, the reconnaissance agent software module is uninstalled from that network node.

20 Claims, 14 Drawing Sheets



US010574684B2

(12) **United States Patent**
Segal et al.

(10) **Patent No.: US 10,574,684 B2**
(45) **Date of Patent: Feb. 25, 2020**

(54) **LOCALLY DETECTING PHISHING WEAKNESS**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 133 days.

(21) Appl. No.: **15/879,726**

(22) Filed: **Jan. 25, 2018**

(65) **Prior Publication Data**

US 2019/0014141 A1 Jan. 10, 2019

Related U.S. Application Data

(60) Provisional application No. 62/530,222, filed on Jul. 9, 2017.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G06F 21/55 (2013.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06F 21/554*** (2013.01); ***H04L 63/1416*** (2013.01); ***H04L 63/1483*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433; H04L 63/1416; H04L 63/1483; H04L 63/168; G06F 13/00; G06F 15/173; G06F 21/00; G06F 21/554; G01R 31/08
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,952,779	B1	10/2005	Cohen et al.	
7,013,395	B1	3/2006	Swiler et al.	
7,757,293	B2	7/2010	Caceres et al.	
8,001,589	B2	8/2011	Ormazabal et al.	
8,112,016	B2	2/2012	Matsumoto et al.	
8,127,359	B2	2/2012	Kelekar	
8,356,353	B2	1/2013	Futoransky et al.	
8,365,289	B2 *	1/2013	Russ	H04L 63/1433 713/188

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230	A	7/2013
CN	104009881	A	8/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google) published Jul. 10, 2013 Li Qianmu.

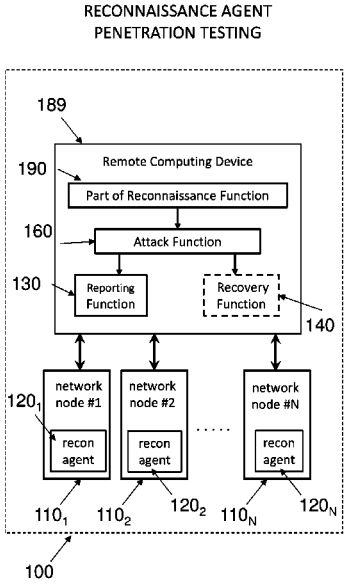
(Continued)

Primary Examiner — Thanhnga B Truong
(74) *Attorney, Agent, or Firm* — Marc Van Dyke; Momentum IP Group

(57) **ABSTRACT**

Methods and systems of testing for phishing security vulnerabilities are disclosed, including methods of penetration testing of a network node by a penetration testing system comprising a reconnaissance agent software module installed in the network node, and a penetration testing software module installed on a remote computing device. Penetration testing systems are provided so as to locally detect weaknesses that would expose network nodes to phishing-based attacks.

14 Claims, 17 Drawing Sheets



US010534917B2

(12) **United States Patent**
Segal

(10) **Patent No.: US 10,534,917 B2**
(45) **Date of Patent: Jan. 14, 2020**

(54) **TESTING FOR RISK OF MACRO VULNERABILITY**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventor: **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 177 days.

(21) Appl. No.: **15/838,733**

(22) Filed: **Dec. 12, 2017**

(65) **Prior Publication Data**

US 2018/0365429 A1 Dec. 20, 2018

Related U.S. Application Data

(60) Provisional application No. 62/522,208, filed on Jun. 20, 2017.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
G06F 21/57	(2013.01)
H04L 29/08	(2006.01)
G06F 21/55	(2013.01)
G06F 9/30	(2018.01)

(52) **U.S. Cl.**

CPC ***G06F 21/577*** (2013.01); ***G06F 9/3017*** (2013.01); ***G06F 21/552*** (2013.01); ***H04L 63/1416*** (2013.01); ***H04L 63/1433*** (2013.01); ***H04L 67/22*** (2013.01); *G06F 2221/033* (2013.01)

(58) **Field of Classification Search**

CPC G06F 21/577; G06F 9/3017; G06F 21/552; G06F 2221/033; H04L 63/1416; H04L 63/1433; H04L 67/22

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,766,458	B1 *	7/2004	Harris	G06F 21/577 709/206
6,952,779	B1	10/2005	Cohen et al.	
7,013,395	B1	3/2006	Swiler et al.	
7,757,293	B2	7/2010	Caceres et al.	
8,001,589	B2	8/2011	Ormazabal et al.	
8,112,016	B2	2/2012	Matsumoto et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230 A	7/2013
CN	104009881 A	8/2014

(Continued)

OTHER PUBLICATIONS

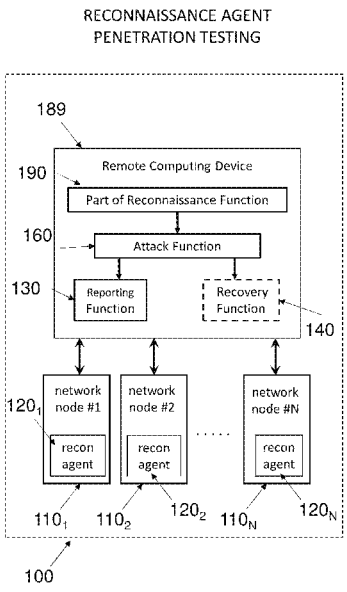
CN103200230 Machine Translation (by EPO and Google) published Jul. 10, 2013 Li Qianmu.

(Continued)

Primary Examiner — Ghodrat Jamshidi
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

Methods and systems are disclosed for penetration testing of a network node by a penetration testing system to determine vulnerability of network nodes to macro-based attacks. A reconnaissance agent runs in a network node to prompt user responses to macro warnings upon detecting file openings by macro-supporting software applications of files not containing auto-executing macros, and the responses are used for determining vulnerability.

26 Claims, 14 Drawing Sheets



US010505969B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,505,969 B2**
(45) **Date of Patent: *Dec. 10, 2019**

(54) **SETTING-UP PENETRATION TESTING CAMPAIGNS**

(71) Applicant: **XM Cyber Ltd.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/135,720**

(22) Filed: **Sep. 19, 2018**

(65) **Prior Publication Data**

US 2019/0036961 A1 Jan. 31, 2019

Related U.S. Application Data

(63) Continuation of application No. 15/681,692, filed on Aug. 21, 2017, now Pat. No. 10,122,750.
(Continued)

(51) **Int. Cl.**
G06F 11/00 (2006.01)
H04L 29/06 (2006.01)
G06F 21/57 (2013.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06F 21/577*** (2013.01); ***H04L 63/20*** (2013.01)

(58) **Field of Classification Search**
CPC ... H04L 63/1433; H04L 63/20; G06F 21/577; F24F 11/58; F24F 11/62; H04W 4/33
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038 B1 7/2005 Smith et al.
6,952,779 B1 * 10/2005 Cohen G06F 21/577 726/22
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014
(Continued)

OTHER PUBLICATIONS

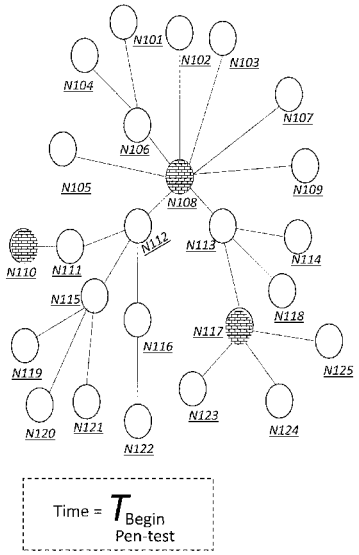
CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.
(Continued)

Primary Examiner — Samson B Lemma
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system by a penetration testing system (e.g. that is controlled by a user interface of a computing device) are disclosed herein. In one example, a penetration testing campaign is executed according to a manual and explicit selecting of one or more network nodes of the networked system. Alternatively or additionally, a penetration testing campaign is executed according to a manually and explicitly selected node-selection condition. Alternatively or additionally, a penetration testing campaign is executed according to an automatic selecting of one or more network nodes of the networked system.

19 Claims, 48 Drawing Sheets



US010498803B1

(12) **United States Patent**
Zini et al.

(10) **Patent No.: US 10,498,803 B1**
(45) **Date of Patent: Dec. 3, 2019**

(54) **IDENTIFYING COMMUNICATING NETWORK NODES IN THE SAME LOCAL NETWORK**

(71) Applicant: **XM Cyber LTD.**, Hertzelia (IL)

(72) Inventors: **Shahar Zini**, Chatswood (AU); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/537,601**

(22) Filed: **Aug. 11, 2019**

Related U.S. Application Data

(62) Division of application No. 16/128,718, filed on Sep. 12, 2018, now Pat. No. 10,440,044.

(60) Provisional application No. 62/654,463, filed on Apr. 8, 2018.

(51) **Int. Cl.**
H04L 29/08 (2006.01)
H04L 29/12 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 67/10*** (2013.01); ***H04L 61/2007*** (2013.01); *H04L 61/6022* (2013.01)

(58) **Field of Classification Search**
CPC H04W 4/06; H04W 76/40; H04W 88/16
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2006/0114903 A1* 6/2006 Duffy, IV H04L 12/1854 370/390
2010/0027551 A1* 2/2010 Arkin H04L 29/12028 370/400
2012/0254922 A1* 10/2012 Rangarajan H04L 12/5692 725/62
2013/0217332 A1* 8/2013 Altman H04H 60/90 455/41.2
2015/0200735 A1* 7/2015 Tjahjono H04H 20/72 370/312
2015/0304116 A1* 10/2015 Chan H04L 12/18 370/230
2015/0381382 A1* 12/2015 Anumala H04L 12/1886 370/390

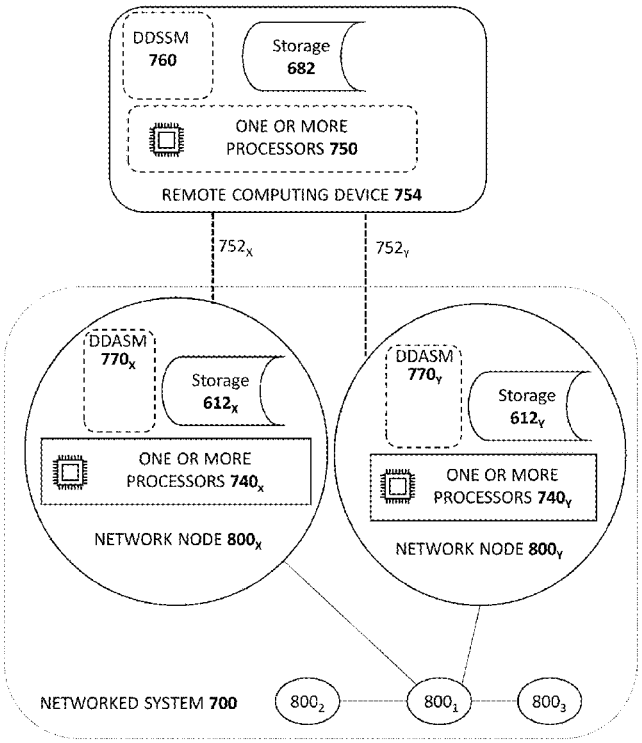
* cited by examiner

Primary Examiner — Christopher C Harris
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for executing a penetration test of a networked system by a penetration testing system so as to determine a method by which an attacker could compromise the networked system, and/or for distributing common sets of data to nodes of a networked system. The methods and systems include identifying network nodes which have shared broadcast domains.

20 Claims, 15 Drawing Sheets



US010469521B1

(12) **United States Patent**
Segal et al.

(10) **Patent No.: US 10,469,521 B1**
(45) **Date of Patent: Nov. 5, 2019**

(54) **USING INFORMATION ABOUT EXPORTABLE DATA IN PENETRATION TESTING**

(71) Applicant: **XM Cyber Ltd.**, Hertzelia (IL)

(72) Inventors: **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/379,820**

(22) Filed: **Apr. 10, 2019**

Related U.S. Application Data

(60) Provisional application No. 62/755,480, filed on Nov. 4, 2018.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 63/20*** (2013.01)

(58) **Field of Classification Search**
CPC . H04L 63/1433; H04L 63/20; H04L 63/1416; H04L 63/145
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038 B1 7/2005 Smith et al.
6,952,779 B1 10/2005 Cohen et al.
7,013,395 B1 3/2006 Swiler et al.
7,296,092 B2 11/2007 Nguyen
7,693,810 B2 * 4/2010 Donoho G06Q 40/00 705/35
7,757,293 B2 7/2010 Caceres et al.
7,921,459 B2 * 4/2011 Houston H04L 41/0604 709/223

(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.

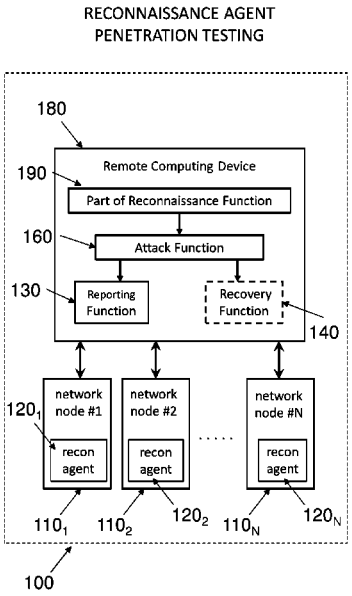
(Continued)

Primary Examiner — Hosuk Song
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Penetration testing campaigns are carried out using a lateral movement strategy based at least in part on information about files stored in network nodes of the networked system. Information is obtained about files stored in a plurality of network nodes of the networked system, and based on the obtained information, a corresponding data-value score for each network node of the plurality of network nodes is determined according to a common data-value metric. The penetration testing campaign is executed, during which a next network node targeted for determining its compromisability is selected based on the data-value scores corresponding to at least some of the plurality of network nodes. Based on results of the penetration testing campaign, a method by which an attacker could compromise the networked system is determined and reported.

21 Claims, 15 Drawing Sheets



US010462177B1

(12) **United States Patent**
Lasser et al.

(10) **Patent No.: US 10,462,177 B1**
(45) **Date of Patent: Oct. 29, 2019**

(54) **TAKING PRIVILEGE ESCALATION INTO ACCOUNT IN PENETRATION TESTING CAMPAIGNS**

(71) Applicant: **XM Cyber Ltd.**, Hertsliya (IL)

(72) Inventors: **Menahem Lasser**, Kohav-Yair (IL); **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/432,982**

(22) Filed: **Jun. 6, 2019**

Related U.S. Application Data

(60) Provisional application No. 62/801,700, filed on Feb. 6, 2019.

(51) **Int. Cl.**

H04L 29/00	(2006.01)
H04L 29/06	(2006.01)
G06F 8/61	(2018.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06F 8/61*** (2013.01); ***H04L 63/20*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433; H04L 63/20; G06F 8/61
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038	B1	7/2005	Smith et al.
6,952,779	B1	10/2005	Cohen et al.
7,013,395	B1	3/2006	Swiler et al.
7,296,092	B2	11/2007	Nguyen
7,757,293	B2	7/2010	Caceres et al.
8,001,589	B2	8/2011	Ormazabal et al.
8,112,016	B2	2/2012	Matsumoto et al.
8,127,359	B2	2/2012	Kelekar

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230	A	7/2013
CN	103916384	A	7/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.

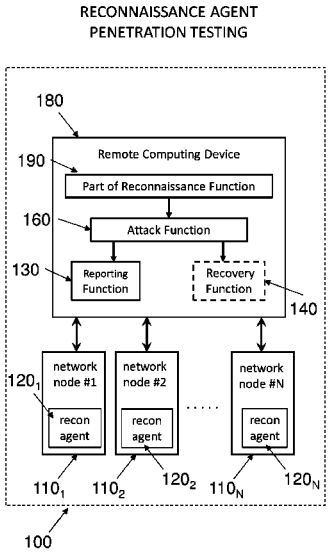
(Continued)

Primary Examiner — Don G Zhao
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

A simulated penetration testing system that assigns network nodes of the tested networked system to classes based on current information about the compromisability of the nodes at a current state of a penetration testing campaign, the classes consisting of (i) a red class for nodes known to be compromisable by the attacker in a way that gives the attacker full control of the nodes, (ii) a blue class for nodes that are not known to be compromisable by the attacker, and (iii) a purple class for nodes known to be compromisable by the attacker in a way that does not give the attacker full control of the purple-class-member network node. The campaign tests whether an attacker would be able to achieve full control of a target node by using privilege escalation techniques and one or more access rights achieved by compromising the target node.

20 Claims, 15 Drawing Sheets



US010454966B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,454,966 B2**
(45) **Date of Patent: *Oct. 22, 2019**

(54) **SELECTIVELY CHOOSING BETWEEN ACTUAL-ATTACK AND SIMULATION/EVALUATION FOR VALIDATING A VULNERABILITY OF A NETWORK NODE DURING EXECUTION OF A PENETRATION TESTING CAMPAIGN**

(71) Applicant: **XM CYBER LTD.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/400,938**

(22) Filed: **May 1, 2019**

(65) **Prior Publication Data**

US 2019/0268369 A1 Aug. 29, 2019

Related U.S. Application Data

(63) Continuation of application No. 16/186,557, filed on Nov. 11, 2018, now Pat. No. 10,367,846, and a (Continued)

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 43/06*** (2013.01); ***H04L 63/1466*** (2013.01); ***H04L 63/1475*** (2013.01)

(58) **Field of Classification Search**
CPC combination set(s) only.
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038 B1 7/2005 Smith et al.
6,952,779 B1 10/2005 Cohen et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014
(Continued)

OTHER PUBLICATIONS

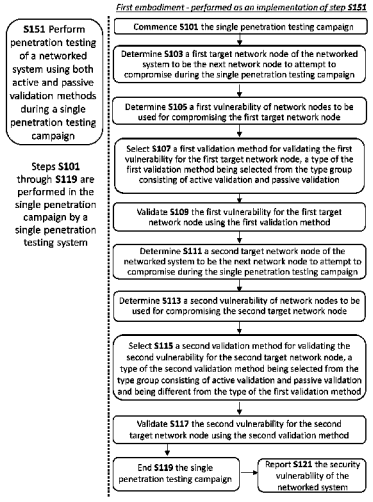
CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.
(Continued)

Primary Examiner — Khang Do
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system by a penetration testing system. In some embodiments, both active and passive validation methods are used during a single penetration testing campaign in a single networked system. In other embodiments, a first penetration testing campaign uses only active validation and a second penetration campaign uses only passive validation, where both campaigns are performed by a single penetration testing system in a single networked system. Node-by-node determination of whether to use active or passive validation can be based on expected extent and/or likelihood of damage from actually compromising a network node using active validation.

16 Claims, 32 Drawing Sheets



US010447721B2

(12) **United States Patent**
Lasser

(10) **Patent No.: US 10,447,721 B2**
(45) **Date of Patent: Oct. 15, 2019**

(54) **SYSTEMS AND METHODS FOR USING MULTIPLE LATERAL MOVEMENT STRATEGIES IN PENETRATION TESTING**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventor: **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/993,453**

(22) Filed: **May 30, 2018**

(65) **Prior Publication Data**

US 2019/0081974 A1 Mar. 14, 2019

Related U.S. Application Data

(60) Provisional application No. 62/558,062, filed on Sep. 13, 2017.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 43/50*** (2013.01); ***H04L 63/20*** (2013.01); *H04L 63/1416* (2013.01); *H04L 63/1425* (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433; H04L 63/20; H04L 63/30; H04L 63/1416; H04L 63/1425; H04L 63/1441; H04L 43/50
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038	B1	7/2005	Smith et al.
6,952,779	B1	10/2005	Cohen et al.
7,013,395	B1	3/2006	Swiler et al.
7,296,092	B2	11/2007	Nguyen
7,757,293	B2	7/2010	Caceres et al.
8,001,589	B2	8/2011	Ormazabal et al.
8,112,016	B2	2/2012	Matsumoto et al.
8,127,359	B2	2/2012	Kelekar
8,356,353	B2	1/2013	Futoransky et al.
8,365,289	B2	1/2013	Russ et al.
8,490,193	B2	7/2013	Sarraute Yamada et al.
8,650,651	B2	2/2014	Podjarny et al.
8,813,235	B2	8/2014	Sidagni

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230	A	7/2013
CN	103916384	A	7/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.

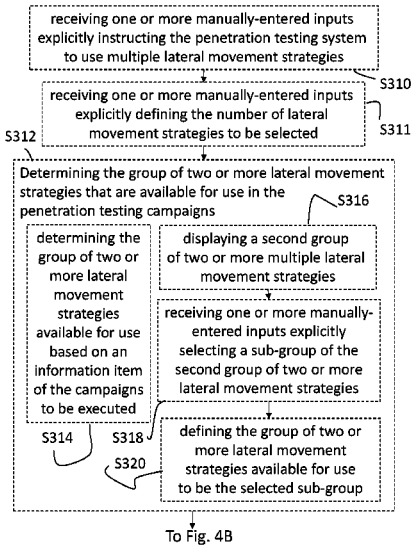
(Continued)

Primary Examiner — Tae K Kim
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for carrying out multiple campaigns of penetration testing using different lateral movement strategies for discovering and reporting security vulnerabilities of a networked system, the networked system comprising a plurality of network nodes interconnected by one or more networks.

20 Claims, 11 Drawing Sheets



US010440044B1

(12) **United States Patent**
Zini et al.

(10) **Patent No.: US 10,440,044 B1**
(45) **Date of Patent: Oct. 8, 2019**

(54) **IDENTIFYING COMMUNICATING NETWORK NODES IN THE SAME LOCAL NETWORK**

(71) Applicant: **XM Cyber LTD.**, Hertzelia (IL)

(72) Inventors: **Shahar Zini**, Chatswood (AU); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Herzliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/128,718**

(22) Filed: **Sep. 12, 2018**

Related U.S. Application Data

(60) Provisional application No. 62/654,463, filed on Apr. 8, 2018.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 29/12 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 61/2007*** (2013.01); ***H04L 63/1425*** (2013.01); ***H04L 67/10*** (2013.01); *H04L 61/6022* (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433; H04L 63/1425; H04L 61/2007; H04L 67/10; H04L 61/6022
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038 B1 7/2005 Smith et al.
6,952,779 B1 10/2005 Cohen et al.
7,013,395 B1 3/2006 Swiler et al.
7,296,092 B2 11/2007 Nguyen
7,620,989 B1 * 11/2009 Couturier H04L 63/1433 726/22
7,757,293 B2 7/2010 Caceres et al.
8,001,589 B2 8/2011 Ormazabal et al.
8,112,016 B2 2/2012 Matsumoto et al.
8,127,359 B2 2/2012 Kelekar
8,356,353 B2 1/2013 Futoransky et al.
8,365,289 B2 1/2013 Russ et al.
8,490,193 B2 7/2013 Sarraute Yamada et al.
8,566,928 B2 * 10/2013 Dagon H04L 29/12066 726/22

(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014

(Continued)

OTHER PUBLICATIONS

Bavithra, MITM Attacks through ARP poisoning, 2017, 8 Pages (Year: 2017).*

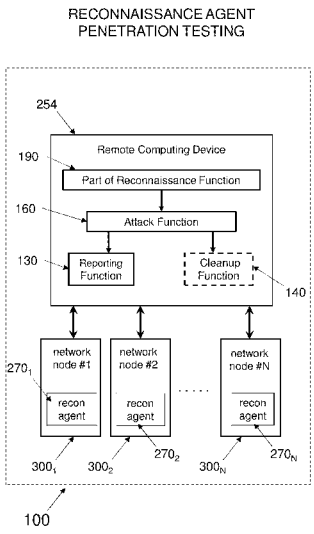
(Continued)

Primary Examiner — Christopher C Harris
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for executing a penetration test of a networked system by a penetration testing system so as to determine a method by which an attacker could compromise the networked system, and/or for distributing common sets of data to nodes of a networked system. The methods and systems include identifying network nodes which have shared broadcast domains.

19 Claims, 15 Drawing Sheets



US010412112B2

(12) **United States Patent**
Ashkenazy et al.

(10) **Patent No.: US 10,412,112 B2**
(45) **Date of Patent: Sep. 10, 2019**

(54) **TIME-TAGGED PRE-DEFINED SCENARIOS FOR PENETRATION TESTING**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertzelia (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 59 days.

(21) Appl. No.: **15/911,170**

(22) Filed: **Mar. 5, 2018**

(65) **Prior Publication Data**

US 2019/0068631 A1 Feb. 28, 2019

Related U.S. Application Data

(60) Provisional application No. 62/552,569, filed on Aug. 31, 2017.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 12/24	(2006.01)
G06F 3/0482	(2013.01)
H04L 12/26	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1433*** (2013.01); ***G06F 3/0482*** (2013.01); ***H04L 41/22*** (2013.01); ***H04L 43/045*** (2013.01); ***H04L 43/50*** (2013.01)

(58) **Field of Classification Search**

CPC ... G06F 3/0482; G06F 3/04842; H04L 41/22; H04L 43/045; H04L 43/50; H04L 63/1433

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,952,779 B1	10/2005	Cohen et al.
7,013,395 B1	3/2006	Swiler et al.
7,757,293 B2	7/2010	Caceres et al.
8,001,589 B2	8/2011	Ormazabal et al.
8,112,016 B2	2/2012	Matsumoto et al.
8,127,359 B2	2/2012	Kelekar

(Continued)

FOREIGN PATENT DOCUMENTS

CN	103200230 A	7/2013
CN	104009881 A	8/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google) published Jul. 10, 2013 Li Qianmu.

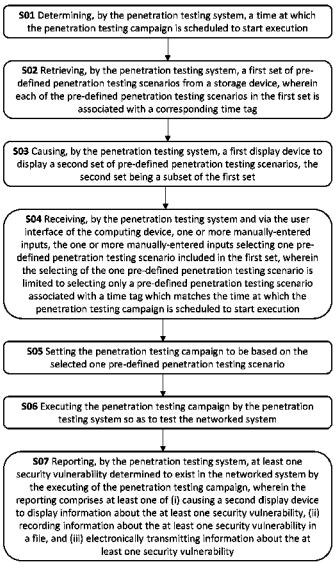
(Continued)

Primary Examiner — Kevin Bechtel
(74) *Attorney, Agent, or Firm* — Mark Van Dyke

(57) **ABSTRACT**

Methods and systems for carrying out campaigns of penetration testing for discovering and reporting security vulnerabilities of a networked system. Penetration testing campaigns are carried out based on pre-defined penetration testing scenarios associated with respective time tags. A penetration testing scenario is selected by a user from a set of pre-defined test scenarios, the set containing only pre-defined test scenarios with time tags matching a scheduled starting time of a penetration testing campaign.

18 Claims, 18 Drawing Sheets



US010382473B1

(12) **United States Patent**
Ashkenazy et al.

(10) **Patent No.: US 10,382,473 B1**
(45) **Date of Patent: Aug. 13, 2019**

(54) **SYSTEMS AND METHODS FOR DETERMINING OPTIMAL REMEDIATION RECOMMENDATIONS IN PENETRATION TESTING**

(71) Applicant: **XM Cyber Ltd.**, Hertzelia (IL)

(72) Inventors: **Adi Ashkenazy**, Tel Aviv (IL); **Shahar Zini**, Chatswood (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/360,063**

(22) Filed: **Mar. 21, 2019**

Related U.S. Application Data

(60) Provisional application No. 62/730,083, filed on Sep. 12, 2018.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 63/1466*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/1433
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,711,127 B1 * 3/2004 Gorman H04L 63/1433 370/230
6,918,038 B1 7/2005 Smith et al.
6,952,779 B1 10/2005 Cohen et al.
7,013,395 B1 * 3/2006 Swiler H04L 63/1433 713/151
7,296,092 B2 11/2007 Nguyen
7,757,293 B2 7/2010 Caceres et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014
(Continued)

OTHER PUBLICATIONS

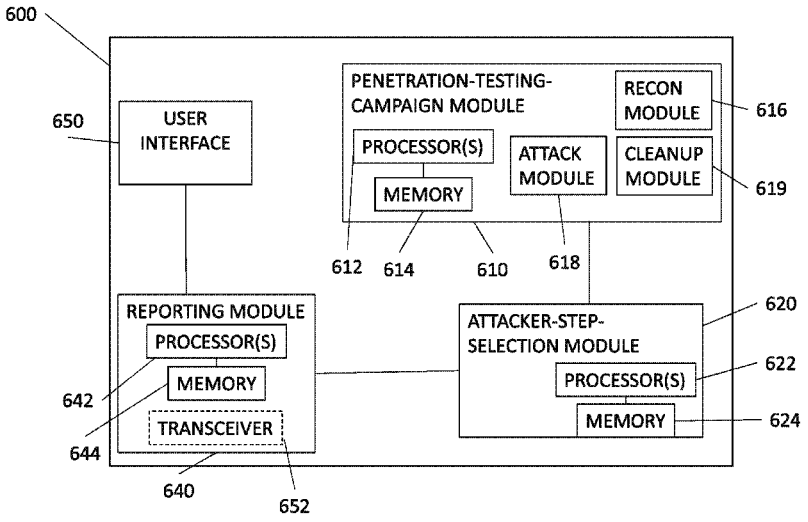
Wang et al.; Shield: vulnerability-driven network filters for preventing known vulnerability exploits; Proceeding SIGCOMM '04 Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications; 2004; pp. 193-204; ACM Digital Library (Year: 2004).*
(Continued)

Primary Examiner — Bradley W Holder
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for providing a recommendation for improving the security of a networked system against attackers. The recommendation may include a recommendation of a single attacker step to be blocked to achieve optimal improvement in security, or of multiple such attacker steps. If the recommendation includes multiple attacker steps, the steps may be ordered such that the first attacker step is more important to block, provides a greater benefit by blocking, or is more cost effective to block than subsequent attacker steps in the ordered list of attacker steps.

20 Claims, 19 Drawing Sheets



US010367846B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,367,846 B2**
(45) **Date of Patent: Jul. 30, 2019**

(54) **SELECTIVELY CHOOSING BETWEEN ACTUAL-ATTACK AND SIMULATION/EVALUATION FOR VALIDATING A VULNERABILITY OF A NETWORK NODE DURING EXECUTION OF A PENETRATION TESTING CAMPAIGN**

(71) Applicant: **XM CYBER LTD.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertzliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/186,557**

(22) Filed: **Nov. 11, 2018**

(65) **Prior Publication Data**

US 2019/0149572 A1 May 16, 2019

Related U.S. Application Data

(60) Provisional application No. 62/586,600, filed on Nov. 15, 2017.

(51) **Int. Cl.**

G06F 7/04	(2006.01)
H04L 29/06	(2006.01)
H04L 12/26	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1433*** (2013.01); ***H04L 43/06*** (2013.01); ***H04L 63/1466*** (2013.01); ***H04L 63/1475*** (2013.01)

(58) **Field of Classification Search**

CPC H04L 63/1433; H04L 63/1475; H04L 63/1466

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038 B1 7/2005 Smith et al.
6,952,779 B1 10/2005 Cohen et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014
(Continued)

OTHER PUBLICATIONS

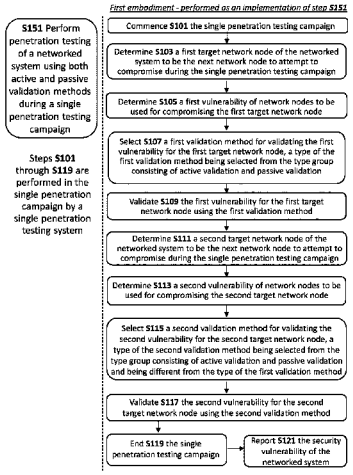
CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.
(Continued)

Primary Examiner — Samson B Lemma
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system by a penetration testing system. In some embodiments, both active and passive validation methods are used during a single penetration testing campaign in a single networked system. In other embodiments, a first penetration testing campaign uses only active validation and a second penetration campaign uses only passive validation, where both campaigns are performed by a single penetration testing system in a single networked system. Node-by-node determination of whether to use active or passive validation can be based on expected extent and/or likelihood of damage from actually compromising a network node using active validation.

5 Claims, 32 Drawing Sheets



US010257220B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,257,220 B2**
(45) **Date of Patent: *Apr. 9, 2019**

(54) **VERIFYING SUCCESS OF COMPROMISING A NETWORK NODE DURING PENETRATION TESTING OF A NETWORKED SYSTEM**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd.**, Hertsliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/983,309**

(22) Filed: **May 18, 2018**

(65) **Prior Publication Data**

US 2018/0270268 A1 Sep. 20, 2018

Related U.S. Application Data

(63) Continuation of application No. PCT/IB2018/053298, filed on May 11, 2018, which is (Continued)

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 12/26	(2006.01)
H04L 12/24	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1433*** (2013.01); ***H04L 41/048*** (2013.01); ***H04L 43/50*** (2013.01); ***H04L 63/30*** (2013.01)

(58) **Field of Classification Search**

CPC H04L 63/1433; H04L 63/30; H04L 63/20; H04L 41/048; H04L 43/50; G06F 21/577;

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,918,038 B1 7/2005 Smith et al.
6,952,779 B1 10/2005 Cohen et al.

(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014

(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google)—published Jul. 10, 2013; Li Qianmu.

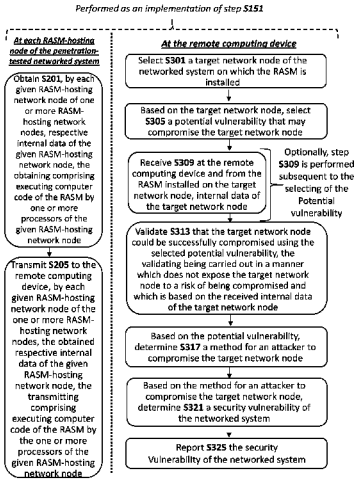
(Continued)

Primary Examiner — Brian F Shaw
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

A method of carrying out a penetration testing campaign of a networked system by a penetration testing system comprising (A) a penetration testing software module installed on a remote computing device and (B) a reconnaissance agent software module (RASM) installed on at least some network nodes of the networked system. In embodiments, at least the following is performed at the remote computing device: a target network node of the networked system on which the RASM is installed is selected; based on the target network node, a potential vulnerability that may compromise the target network node is selected; internal data of the target network node is received; and a validation step is performed. The validation is (i) carried out in a manner which does not expose the target network node to a risk of being compromised and (ii) is based on the received internal data of the target network node.

18 Claims, 12 Drawing Sheets



US010122750B2

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,122,750 B2**
(45) **Date of Patent: *Nov. 6, 2018**

(54) **SETTING-UP PENETRATION TESTING CAMPAIGNS**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM Cyber Ltd**, Herzliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/681,692**

(22) Filed: **Aug. 21, 2017**

(65) **Prior Publication Data**

US 2018/0219900 A1 Aug. 2, 2018

Related U.S. Application Data

(60) Provisional application No. 62/453,056, filed on Feb. 1, 2017, provisional application No. 62/451,850, filed on Jan. 30, 2017.

(51) **Int. Cl.**

G06F 11/00	(2006.01)
H04L 29/06	(2006.01)
G06F 21/57	(2013.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1433*** (2013.01); ***G06F 21/577*** (2013.01); ***H04L 63/20*** (2013.01)

(58) **Field of Classification Search**

CPC H04L 63/1433; H04L 63/20; G06F 2221/034; G06F 21/577

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,952,779 B1 * 10/2005 Cohen G06F 21/577 726/22

7,013,395 B1 3/2006 Swiler et al.

(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 103916384 A 7/2014

(Continued)

OTHER PUBLICATIONS

Co-pending U.S. Appl. No. 15/681,782.

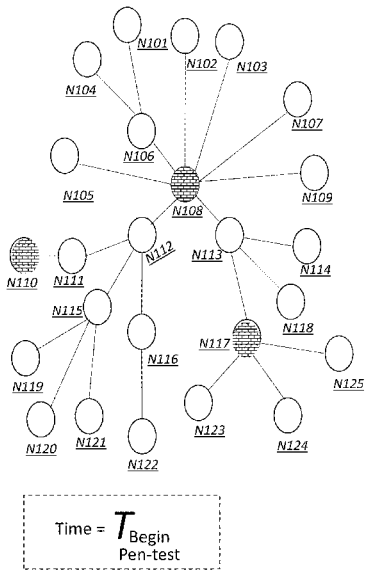
(Continued)

Primary Examiner — Samson B Lemma
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system by a penetration testing system (e.g. that is controlled by a user interface of a computing device) are disclosed herein. In one example, a penetration testing campaign is executed according to a manual and explicit selecting of one or more network nodes of the networked system. Alternatively or additionally, a penetration testing campaign is executed according to a manually and explicitly selected node-selection condition. Alternatively or additionally, a penetration testing campaign is executed according to an automatic selecting of one or more network nodes of the networked system.

14 Claims, 48 Drawing Sheets



US010068095B1

(12) **United States Patent**
Segal et al.

(10) **Patent No.: US 10,068,095 B1**
(45) **Date of Patent: *Sep. 4, 2018**

(54) **SYSTEMS AND METHODS FOR SELECTING A TERMINATION RULE FOR A PENETRATION TESTING CAMPAIGN**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Ronen Segal**, Hertzelia (IL); **Menahem Lasser**, Kohav-Yair (IL)

(73) Assignee: **XM Cyber Ltd**, Herzliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/837,975**

(22) Filed: **Dec. 11, 2017**

Related U.S. Application Data

(60) Provisional application No. 62/506,161, filed on May 15, 2017.

(51) **Int. Cl.**
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***G06F 21/577*** (2013.01); ***H04L 63/1433*** (2013.01); ***H04L 63/20*** (2013.01); *G06F 2221/034* (2013.01)

(58) **Field of Classification Search**
CPC G06F 21/577; G06F 2221/034; H04L 63/1433; H04L 63/20
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,952,779 B1 10/2005 Cohen et al.
7,013,395 B1 3/2006 Swiler et al.
7,757,293 B2 7/2010 Caceres et al.
8,001,589 B2 8/2011 Cormazabal et al.
8,112,016 B2 2/2012 Matsumoto et al.
8,127,359 B2 2/2012 Kelekar
8,356,353 B2 1/2013 Futoransky et al.
8,365,289 B2 1/2013 Russ et al.
8,490,193 B2 7/2013 Sarraute Yamada et al.
8,650,651 B2 2/2014 Podjamy et al.
8,813,235 B2 8/2014 Sidagni
9,076,013 B1 7/2015 Bailey, Jr. et al.
9,183,397 B2 11/2015 Futoransky et al.
9,224,117 B2 12/2015 Chapman
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 104009881 A 8/2014
(Continued)

OTHER PUBLICATIONS

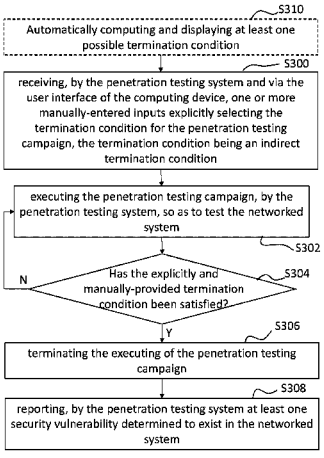
CN103200230 Machine Translation (by EPO and Google) published Jul. 10, 2013 Li Qianmu.
(Continued)

Primary Examiner — Amir Mehrmanesh
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Systems and methods of penetration testing of a networked system by a penetration testing system that is controlled by a user interface of a computing device so that a penetration testing campaign is executed until a termination condition is satisfied, the termination condition being manually and explicitly selected and being an indirect termination condition.

30 Claims, 11 Drawing Sheets



US010038711B1

(12) **United States Patent**
Gorodissky et al.

(10) **Patent No.: US 10,038,711 B1**
(45) **Date of Patent: *Jul. 31, 2018**

(54) **PENETRATION TESTING OF A NETWORKED SYSTEM**

(71) Applicant: **XM Ltd.**, Hertzelia (IL)

(72) Inventors: **Boaz Gorodissky**, Hod-Hasharon (IL); **Adi Ashkenazy**, Tel Aviv (IL); **Ronen Segal**, Hertzelia (IL)

(73) Assignee: **XM LTD.**, Herzliya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/911,168**

(22) Filed: **Mar. 4, 2018**

Related U.S. Application Data

(63) Continuation of application No. 15/874,429, filed on Jan. 18, 2018.
(Continued)

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 12/26 (2006.01)
H04L 12/24 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***H04L 41/048*** (2013.01); ***H04L 43/50*** (2013.01); ***H04L 63/30*** (2013.01)

(58) **Field of Classification Search**
CPC G06F 21/577; G06F 2221/034; H04L 41/046–41/048; H04L 41/145–41/147;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,952,779 B1 10/2005 Cohen et al.
7,013,395 B1 3/2006 Swiler et al.
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103200230 A 7/2013
CN 104009881 A 8/2014
(Continued)

OTHER PUBLICATIONS

CN103200230 Machine Translation (by EPO and Google) published Jul. 10, 2013 Li Qianmu.
(Continued)

Primary Examiner — Kevin Bechtel
(74) *Attorney, Agent, or Firm* — Marc Van Dyke

(57) **ABSTRACT**

Methods and systems for penetration testing of a networked system comprising a set of network-nodes by a penetration testing system (e.g. to enforce first and/or second rules) are disclosed herein. The penetration testing system comprises: (i) reconnaissance agent software module (RASM) installed on multiple nodes (each of which is a RASM-hosting node) of the networked system to be penetration-tested and (ii) a penetration testing software module (PTSM) installed on a remote computing device (RCD). Internal data from each of the RASM-hosting nodes is collected and transmitted to the RCD. Analysis of the internal data collected from multiple RASM-hosting network nodes determines a method for an attacker to compromise the networked system. The first and second rules are defined herein. Alternatively or additionally, one or more of the RASM instances are pre-installed on one or more RASM-hosting nodes before the penetration testing commences.

16 Claims, 17 Drawing Sheets